ITU-T

Trust in ICT

2017

HIGH
MEDIUM
LOW
TRUST

Foreword

Trust is highly dynamic. Decision-making behaviour is affected by past experience and associated predictions for the future. The degree of trust in ICT is the accumulated value of the degree of trust present in the vast web of relationships that forms the modern ICT ecosystem.

We are connecting everything, our vehicles, homes, offices, factories and the rest of the machinery that makes up our modern lives. A 'sword-and-shield' approach to cyber threats will be incapable of ensuring security and privacy in this hyperconnected environment. It is clear that, beyond conventional protections to security and privacy, the time has come to integrate trust into the ICT ecosystem.

ITU standardization is prioritizing its support for 5G systems, the Internet of Things (IoT) and trust. These three fields are highly interdependent. It is my firm belief that achieving the great potential of 5G and IoT will depend to a large degree on our success in building trust into the ICT ecosystem.

ITU is pioneering international efforts to establish the technical foundations of a trusted ICT environment. Part of the challenge is defining and raising awareness of the concept of trust in ICT. We are both shaping the conversation around the meaning of trust in ICT and developing technical mechanisms to move from theory to implementation.

This publication offers a compendium of the first outputs of ITU's study of trust in ICTs. The publication aims to build greater understanding of the concepts, driving forces and key features of trust in the ICT context. It details technical approaches with potential to improve trust in ICT and proposes future directions in related ITU standardization work.

Chaesub Lee

Director of the ITU Telecommunication
Standardization Bureau

ICT

First new ITU standards on trust

Based on the significant efforts made to build converged Information and Communications Technology (ICT) services and a reliable information infrastructure while taking into account social and economic considerations, ITU members have focused on trust standardization. For this, ITU newly defined that 'trust' is the measureable belief and/or confidence which represents accumulated value from history and the expecting value for future. ITU also recognized that, in ICT environments, trust affects the preference of an entity to consume a particular service offered by another entity and it affects the decision making of an entity to transact with another entity. Furthermore, trust is a broader concept that can cover security and privacy as trust revolves confidence that people, data and devices will function or behave in expected ways as well as it can be used to build new value-chain for future ICT infrastructure and services. Figure 1 shows trust keywords and various trustworthiness attributes that are categorized into three major factors: ability, integrity and benevolence. Many attributes can represent trustworthiness, which can be applied to ICT infrastructures and services.

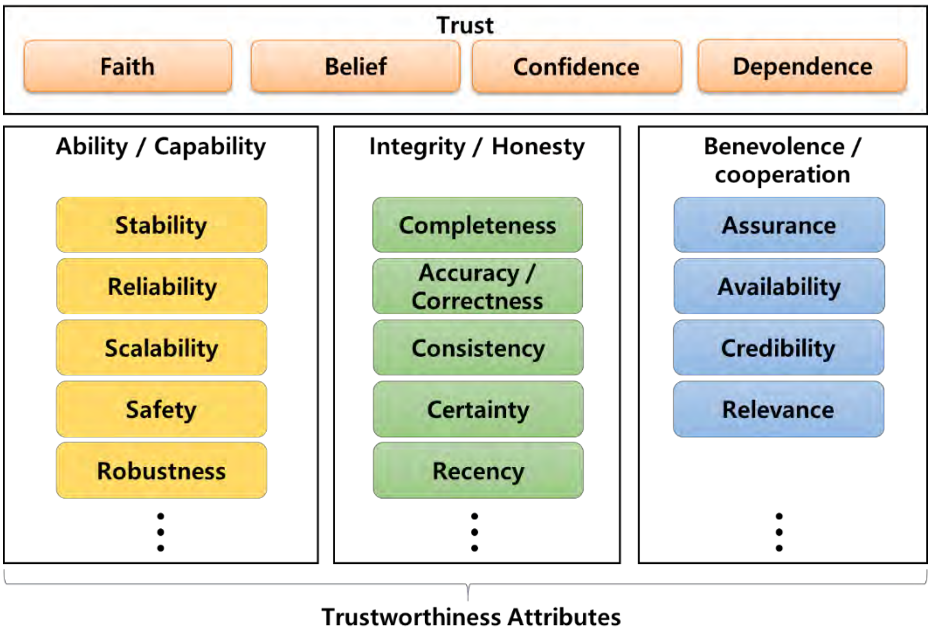


Figure 1 – Trust keywords and trustworthiness attributes

In this regard, ITU members have firstly approved new standards on trust for ICT infrastructures and services, as follows.

– Recommendation ITU-T Y.3051 "The basic principles of trusted environment in ICT infrastructure" is devoted to the issue of creating trusted environment in ICT infrastructure providing information and communication services. It provides the definition, common requirements and the basic principles of creating trusted environment.

– Recommendation ITU-T Y.3052 "Overview of trust provisioning for information and communication technology infrastructures and services" provides an overview of trust provisioning in ICT infrastructures and services. From the general concept of trust, the key characteristics of trust are described. In addition, the trust relationship model and trust evaluation based on the conceptual model of trust provisioning are introduced.

The work on trust was based on the preliminary studies convened by the individual experts and the correspondence group on trust. You will find corresponding technical reports in this flipbook.

With the progress of trust standardization work and successful completion of the above two standards, ITU-T members are continuously contributing to develop companion standards on trust. There are several on-going work on Y.trustworthy-media (Trustworthy smart media services), Y.trustnet-fw (Trustworthy networking), etc. From the perspectives of standardization, trust should be quantitatively and/or qualitatively calculated and measured, which is used to evaluate the values of physical components, value-chains among multiple stakeholders, and human behaviors including decision making. Accordingly, a new work on trust index to evaluate and quantify trustworthiness has been started.

With the help of trust standardization, future ICT infrastructures will require more reliable techniques to cope with the risks of knowledge sharing towards a knowledge society. Building and validating trusted relationships will be contingent on trust-related information and its processing for supporting trustworthy services and applications.

Ideas from members are welcome to stimulate trust standardization activities in the future, taking into account key technical, policy and governance issues through global collaboration with related standardization bodies.

Dr Gyu Myoung Lee,
Co-chairman of the ITU-T Study Group 13
Working Party 3/13 "Network Evolution and Trust"

Table of contents

Page

HTTPS

1.

Standardization of Trust Provisioning Study

ITU-T Technical Report "Standardization of Trust Provisioning Study" (2015)

Foreword

This Technical Paper was developed by Mr. Gyu Myoung Lee.

Summary

Moving towards an interconnected knowledge society from an information society requires a trusted Information and Communication Technology (ICT) infrastructure for sharing information and creating knowledge. To advance the efforts to build converged ICT services and reliable information infrastructures, ITU-T has recently started a work item on future trusted ICT infrastructures. This technical report introduces basic concepts of trust and present various use cases for trust provisioning. And then it provides a strategy for trust provisioning in the ICT infrastructure, services and applications based on trust taxonomy in different domains, and architectural framework for trusted social cyber physical infrastructures and for trust decision making for trustworthy ICT eco-system along with technical details for trust provisioning. Finally this report identifies roadmap and working priority for future standardization in ITU-T based on related standardization activities.

Table of contents

1 Scope

Moving towards an interconnected knowledge society from an information society requires a trusted Information and Communication Technology (ICT) infrastructure for sharing information and creating knowledge. To advance the efforts to build converged ICT services and reliable information infrastructures, ITU-T has recently started a work item on future trusted ICT infrastructures.

- Therefore, this technical report addresses the following key items:
- Definitions, key characteristics and features on trust from different perspectives for a clear understanding of trust;
- Use cases for trust provisioning based on the technical report of ITU-T Correspondence Group on Trust (CG-Trust), materials from other Standards Developing Organizations (SDOs) and related literature;
- A strategy for trust provisioning in the ICT infrastructure, services and applications based on trust taxonomy in different domains;
- Architectural framework for trusted social cyber physical infrastructures and for trust decision making for trustworthy ICT eco-system;
- Technical details for trust provisioning including trust modelling and decision making;
- Roadmap and working priority for future standardization in ITU-T based on related standardization activities.

2 Abbreviations and acronyms

AOSSL	Always On Secure Sockets Layer
API	Application Programming Interface
ARH	Abdul-Rahman and Hailes
ARL	Agent Registration List
B2B	Business-to-Business
B2C	Business to Consumer
BEA	Bid Evaluation Agent
BRS	Beta reputation system
CA	Contractor Agent
CFP	Call for Proposal
CG-Trust	Correspondence Group on Trust
CNP	Contract Net Protocol
CoI	Community of Interest
CPSS	Cyber-Physical-Social Systems
D2D	Device-to-Device
DIKW	Data, Information, Knowledge, Wisdom
DL	Description Logic
DoS	Denial of Service
FOAF	Friend-Of-A-Friend
GPS	Global Positioning System
GSM	Global System for Mobile Communications

HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL
HVAC	Heating, Ventilating, and Air Conditioning
IA	Initiator Agent
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IF-MAP	Interface to a Metadata Access Point
IoT	Internet of Things
IT	Information Technology
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
M2M	Machine-to-Machine
MANET	Mobile Ad Hoc Network
MAPE-K	Monitor, Analyse, Plan, Execute, Knowledge
MAS	Multi Agent System
NAC	Network Access Control
OBU	On Board Unit
OTA	Online Trust Alliance
OWL	Web Ontology Language
P2P	Peer-to-Peer
PDR	Packet Delivery Ratio
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PLC	Power Line Communication
PML	Proof Markup Language
PoA	Point of Attachment
QL	Query Language
QoE	Quality of Experience
QoS	Quality of Service
RDF	Resource Description Framework
RFID	Radio Frequency Identification
RL	Rule Language
SCP	Social-Cyber-Physical
SDK	Software Development Kit
SDO	Standards Developing Organization
SED	Self-Encrypting Drive
SLA	Service Level Agreement
SOA	Software Oriented Architecture
SSL	Secure Socket Layer

SSN	Semantic Sensor Network
TA	Technical Attribute
TaaS	Trust as a Service
TC	Trust Certificate
TCG	Trusted Computing Group
TEP	Trust Establishment Protocol
TLS	Transport Layered Security
TM	Trust Metric
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TSL	Transport Security Layer
TTL	Time to Live
UE	User Equipment
USB	Universal Serial Bus
USDL	Unified Service Description Language
VANET	Vehicular Ad Hoc Network
WPH	Wireless Portable Hard drive
WSN	Wireless Sensor Network
XaaS	Everything as a Service

3 Introduction

Trust is a broad concept with application across many disciplines and subject areas but with no commonly agreed definition. A review of the economic literature on trust found that the existence of uncertainty was one factor present in most definitions of trust. It is a critical factor that highly influences the likelihood of entities to interact and transact in digital environments. Trust is crucial that it affects the appetite of an entity to consume a particular service or product offered by another entity. This example can be seen in our everyday life where trust decisions are made. When purchasing a specific product, we may favour certain brands due to our trust that these brands will provide excellent quality compare to the unknown brands. Trust on these brands may come from our past experience of using these brands' products (termed "belief") or from their reputations that are perceived from other people who bought items and left their opinions about those products (termed "reputation"), or from suggestions of your surrounding such as families and friends (termed "recommendation").

Similarly, trust also affects the decision of an entity to transact with other entity in online environment. Both consumers and providers in an electronic market must trust each other before decisions to consume or to provide the services are made. If trust is not established between them, fraudulent transactions may occur regularly. Such situation would disadvantage the honest consumers and providers, and it further refrain them from taking the advantage of the online transactions. The significance of trust also applies in digital environments where a high number of entities mutually interact with each other to provide and consume the information and/or resources.

Although the significance of trust in our physical world is as important as it is in the digital environments, building trust and confidence in the latter is much more difficult. This is due to our inability to have the physical view on an entity, unlike in our physical world where we can view the building of the bank, observe its safe deposits, meet the bank personnel, etc. Another issue with trust is that it is difficult to quantify the exact trustworthiness value of an entity. This is even harder when each entity have different interpretation and perception of the term "trustworthy". Therefore, they may assign different trustworthiness values for a provider or a service. For example, a service consumer assigns "very trustworthy" to the provider for a transaction that he has performed. However, another consumer assigns "untrustworthy" for the similar transaction from the same provider. These differences further increase the difficulty to determine the exact trustworthiness of a provider.

As the world becomes more dependent on digital environments, particularly on ICT, telecommunication infrastructure is increasingly recognized as a vital prerequisite for participation in today's growing digital economy. Broadband telecommunication infrastructure not just only improves the transmission speed at which users send and receive multimedia data, but also allows service providers and individual users to enhance legacy services and to develop previously inconceivable tools that improve business and society. The benefits of broadband telecommunication infrastructure can expand beyond the ICT area itself, accelerating throughout the economy and serving as an essential input for all other areas such as smart building, smart city, smart farming, and so on. As a transformative technology, its role is similar to the impact of electricity which induced growth and innovation over the last two centuries. Broadband telecommunication infrastructure can also be an important enabler of civic and political advancement.

The introduction of sensors and devices into currently physical spaces poses particular challenges and increases the sensitivity of the data that is being collected. Connected devices are effectively allowing companies to digitally monitor our private activities. Moreover, the sheer volume of granular data generated by a small number of devices allows those with access to the data to perform analyses, providing the ability to make additional sensitive inferences and compile even more detailed profiles of consumer behaviour.

The processing and analysing big data leveraging by cloud computing technologies are becoming an important resource that can lead to new knowledge, drive value creation, and foster new products, processes and markets. However, the large scale collection and analysis of data can poses difficult privacy, security and trust issues ranging from the risks of unanticipated uses of consumer data to the potential discrimination enabled by data analytics and the insights offered into the movements, interests and activities of an individual.

From recent advances toward a hyper-connected society from the increasing digital interconnection of humans and objects for upcoming zettabyte era, ICT has played a significant role in the convenience of daily life. However various problems due to the lack of trust have been anticipated as aforementioned. Therefore, it is important to process and handle data in compliance with user needs and rights in various application domains without human intervention. Based on the significant effort to build the converged ICT services and reliable information infrastructure, ITU-T has recently started a new work on the future trusted ICT infrastructure to cope with the emerging trends considering social and economic issues. Therefore, in order to cope with the development of a large number of complex and intelligent applications and services, it is needed to create a trusted environment for ICT infrastructure in order for sharing information and creating knowledge. Consequently, there is a critical need to develop a trusted infrastructure as one of the most important parts in the future ICT environment.

The ultimate purpose for trust provisioning in ICT infrastructure is to develop a trust infrastructure that cooperates with ICT applications and services to assess and compute all aspects of trust among any entities in the future ICT environments; in order to support these applications and services for better quality of services and experience. The trusted service platform could be considered as a core service to secure computing systems, networking applications and services in ICT environments, as Trust as a Service (TaaS).

This technical report contains the following key items:

- Section 4 describes definitions, key characteristics and features on trust from different perspectives for a clear understanding of trust as standardization activities for trusted information infrastructure in ITU-T CG-Trust.
- Section 5 illustrates various use cases for trust provisioning based on the technical report of ITU-T CG-Trust, materials from other SDOs and related literature. In addition, this section also analyses these uses cases in terms of purpose, method, actors and considerations for measuring trust.

- Section 6 proposes trust taxonomy in different domains in order to identify important issues for trust provisioning in the ICT infrastructure, services and applications, and describe a strategy for solving these issues, particularly considering trust provisioning process.
- Section 7 demonstrates feasible methods to implement architecture for trusted social cyber physical infrastructures and a framework for trust decision making for trustworthy ICT eco-system. Furthermore, it emphasises key functionalities, requirements and standard interfaces for autonomic decision making.
- Section 8 focuses on developing a generalized trust definition for all entities in Internet of Things (IoT) in which trust can be formalized and produced within a service platform in the future. Supporting to our goal, topics on trust provisioning strategies for services, applications and ICT infrastructure and ideas on trust ontology will be discussed here. In addition, this section suggests a framework for autonomic trust management based on Monitor, Analyse, Plan, Execute, and Knowledge feedback loop to evaluate the level of trust in an IoT cloud ecosystem. It also introduces Blockchain technology as a tool for trust provisioning.
- Section 9 provides details for related standardization activities in ITU-T and other SDOs. In addition, this section shows important work items for standardization and discuss next step for future standardization in ITU-T.

4 Understanding of Trust

This section presents different meanings of trust from various perspectives as a key achievement of ITU-T CG-Trust standardization activities. It also describes general aspects of trust like characteristics, key features and relationships with knowledge, security and privacy.

In general, trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives. Trust is not a new research topic in computer science, spanning areas as diverse as security and access control in computer networks, reliability in distributed systems, game theory and agent systems, and policies for decision making under uncertainty. The concept of trust in these different communities varies in how it is represented, computed, and used.

Trust is a complex notion with different keywords (see Figure 1) and a multi-level analysis is important in order to understand it. Therefore, this section aims to provide a clear understanding of trust, from definitions, key characteristics and features on trust from different perspectives.

4.1 Definition of Trust

Trust is a broad concept used in many disciplines and subject areas but until now, there is no commonly agreed definition. It is a critical factor that highly influences the likelihood of entities to interact and transact in both real world and ICT environments. Trust is crucial that it affects the appetite of an entity to use services or products offered by another entity. This example can be seen in our everyday life where trust decisions are made. When purchasing a product, we may favour certain brands or certain models due to our trust that they will provide better quality compare to others. This trust may come from our past experience of using these brands’ products (termed “belief”) or from their reputations that are perceived from people who bought items and left their opinions about those products (termed “reputation”), or from suggestions of your surrounding such as families and friends (termed “recommendation”). Similarly, trust also affects the decision of an entity to transact with other entity in ICT environment. Both consumers and providers should trust each other before decisions to consume or to provide the services are made; otherwise fraudulent transactions may occur.

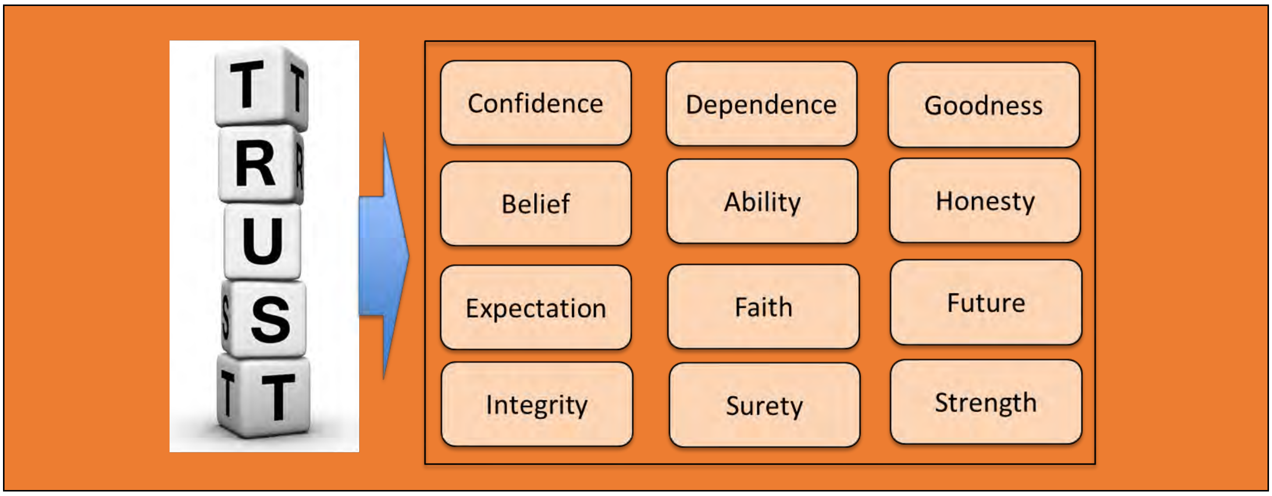


Figure 1 – Keywords for trust

4.1.1 Generic Definition of Trust in ICT

Trust concept itself is a complicated notion with different meanings depending on both participators and situations and influenced by both measurable and non-measurable factors. There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism.

Previous research has shown that trust is the interplay among human, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation [1]. The competence is measurement of abilities of the trustee to perform a given task which is derived from trustee’s diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee.

Trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives.

(Note) Trust may be human to human, machine to machine (e.g. handshake protocols negotiated), human to machine (e.g. when a consumer reviews a digital signature advisory notice) or machine to human (e.g. when a system relies on user input and instructions without extensive verification).

The term trust in the context of ICT world differs from the concept of trust among people. This notion of trust stands in contrast to some more intuitive notions of trust expressing that someone behaves in a particular well-behaved way. Trust in ICT is an important concept in the sense that a trusted resource is one that you are forced by necessity to trust. The failure of this resource would compromise the function, integrity or security of a system which are not in expected ways.

Nevertheless, trust is an important feature in the decision-making process not only used by humans in daily life but also by applications and services in ICT environment.

4.1.2 Trust Definitions under Different Perspectives

E-commerce: A variety of existing notions of trust in the context of ICT world addresses particular aspects (e.g. trust in electronic commerce (e-commerce) systems based on reputation and recommendation, or trust in public key infrastructures.)

Security could be itself a key component of trust. For example, increasing security to increase trust comes from peoples being more willing to engage in e-commerce if they are assured that their credit card numbers and personal data are cryptographically protected.

Currently, some systems are taking advantages of social relationship models to offer secure and reliable services by using the reputation and trust such as eBay, Amazon and Google's Web Page Rankings.

Building security: In security aspects, trust relates much to the degree of confidence one has in the correctness of a function. For example, a company policy controls access at the entrance, so that only eligible persons in possession of a smart card or in knowledge of a PIN code are granted access to a corporate building.

4.1.3 Different stakeholders' viewpoints on trust

According to stakeholders of ICT world, there are different viewpoints of trust. For example, in telecommunications, the user trusts the operator while he believes to get a correct bill. At the same time the operator provides the accounting and billing system to produce correct billing data. The user in this case may trust the operator.

4.2 General Aspects of Trust

4.2.1 Trust Notation

It is challenging to concisely define "trust" of an entity due to its uniqueness to each individual entity. Several authors attempts to define trust from a sociological point of view. They define trust as the trusting behaviour that one person has on another person in a situation where an ambiguous path exists. In such definition, trust is used to mitigate the risks of the dealings with others. Other authors further define trust as the capacity and belief of an entity that the other entity would meet its expectations. However, one of the most prominent works that attempt to derive the notion of trust and was used by many research in online environment is conducted by Gambetta [2]. The authors state that someone is deemed as trustworthy, subject to the probability that he will perform a particular action that is beneficial or non-detrimental for us. This definition is further extended by incorporating the notion of competence along with the predictability. Gambetta et al. definition on trust is also supported by the author in [3] which further defines trust in an electronic forefront as the competency belief that an agent would act reliably, dependably and securely within a given context. This belief can be quantitatively derived from a subjective probabilistic that an agent has over another in a given period of time.

Trust in an electronic network can be divided into two types: direct (personal) trust and third party trust.

- Direct (personal) trust is a situation where a trusting relationship is nurtured by two entities. This type of trust is formed after these entities have performed transactions with each other, e.g. entity. A inherently trusts entity B after a number of successful transactions that involved both entities.
- On the contrary, third-party trust is a trust relationship of an entity that is formed from the third party recommendations. This means no previous transaction ever occurred between the two interacting entities. For example, entity A trusts entity B because B is trusted by entity C. In this example, entity A derives trust of B from C, and A also trusts entity C does not lie to him.

As with any types of trust relationship, there is a link with the risk. Risk is not within the scope of this technical report, however, it is important to note that risk affect the trusting relationship between the entities. Author in [4] stresses that an entity will only proceed with the transaction if the risk is perceived as acceptable.

4.2.2 Trust Characteristics

There are several important characteristics of trust that further enhance our understanding about trust digital environments [5].

Trust is dynamic: as it applies only in a given time period and maybe change as time goes by. For example, for the past one year Alice highly trusts Bob. However, today Alice found that Bob lied to her, consequently, Alice no longer trusts Bob.

Trust is context-dependent: trust applies only in a given context. The degree of trust on different contexts is significantly different. For example, Alice may trust Bob to provide financial advice but not for medical advice.

Trust is not transitive in nature but maybe transitive within a given context: That is, if entity A trusts entity B, and entity B trusts entity C then entity A may not trust entity C. However A may trust any entity that entity B trusts in a given context although this derived trust may be explicit and hard to be quantified.

Trust is an asymmetric relationship: Thus, trust is a non-mutual reciprocal in nature. That means if entity A trust entity B, then the statement "entity B trusts entity A" is not always true.

The nature of trust is fuzzy, dynamic and complex. Besides asymmetry and transitivity, there are additional key characteristics of trust: implicitness, antonymy, asynchrony, and gravity [6] [7].

Implicit: It is hard to explicitly articulate the confidence, belief, capability, context, and time dependency of trust.

Antonymy: The articulation of trust context in two entities may differ based on the opposing perspective. For example, entity A trusts entity B in the context of "buying" book, however from entity B to entity A the context is "selling" book.

Asynchrony: The time period of trusting relationship may be defined differently between the entities. For example, entity A trusts entity B for 3 years, however, entity B may think that the trust relationship only last for the last 1 year.

Gravity: The degree of seriousness in trust relationships may differ between the entities. For example, entity A may think that its trust with entity B is important, however, entity B may think it differently.

4.3 Key features of Trust

4.3.1 Classifications for trust provisioning

At architectural perspective, trust can be classified into three layers: data trust, information trust, and knowledge/intelligence trust.

Depending on services and applications, the trusts domains should be well identified and measured at objectively or subjectively manners.

At technical perspectives, trust could be classified into three dimension: technical trust (like data security), business/trading/community trust (or credits), and human trust (perceived by individual human or group of members). Some mechanisms or solutions of trusts may be accounted by defining trust metric or trust index.

The capability or attributes of trusts can be also classified into application types, costs, technical complexity, and human credibility/reputation. Depending on applications, most of trust solutions may be clarified and mapped.

4.3.2 The Trust Metrics and Technical Attributes

It is challenged to determine the necessary and sufficient information that should be used for deriving measures of trust. Technically, trust is based on several Trust Metrics (TMs) which are generally defined as the information used in trustworthiness evaluation process between trustor and trustee. Each TM is derived from some Technical Attributes (TAs) as illustrated in Figure 2.

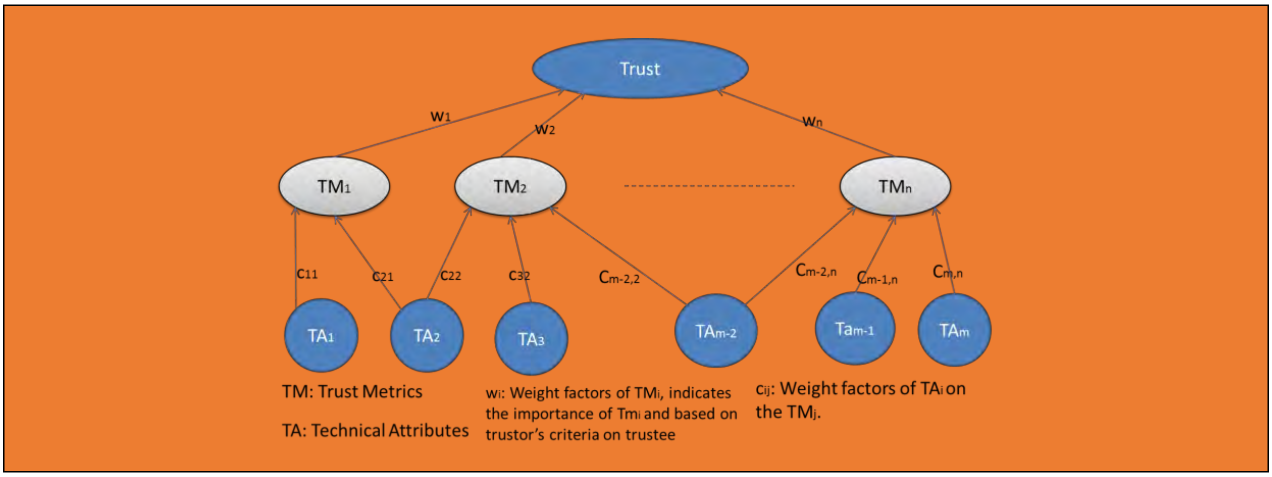


Figure 2 – General Trust Model with Trust Metrics and Technical Attribute

Depending on services and applications, the required attributes of trust may vary. For example, for a particular application, technical attributes may be consisted of security, reliability and availability. Whereas, for other applications, security and reliability may be needed for such trust provisioning.

4.3.3 Level of trust

Due to the diversity of applications and their inherent differences in nature, trust is hard to formalize in a general setting, and up to now no commonly accepted definition is appeared. However, it is important to quantify level of trust in ICT. The level of trust can be measured classified which is similar with Quality of Service (QoS) as objective manner (e.g., measured quantitatively) or Quality of Experience (QoE) as subjective manner (e.g., counted qualitatively). A certain level of trust should be derived from the associated services and applications of trust.

4.3.4 Trust domain

Different trust domains may share the same physical components. Also, a single trust domain may include various levels of trust. Depending on what levels of trust the users need to know including sensitivity of information and associated resources, there may be a lot of service level agreement (SLA) of trust.

4.4 Trust in ICT Environment

As disused in previous sub-sections, the term trust in the context of ICT world differs from the concept of trust among people. This notion of trust stands in contrast to some more intuitive notions of trust expressing that someone behaves in a particular well-behaved way. Trust in ICT is an important concept in the sense that a trusted resource is one that you are forced by necessity to trust. The failure of this resource would compromise the function, integrity or security of a system which are not in expected ways.

As trust can be interpreted in different ways, here there are various meanings from literature for more clear views on trust in terms of telecommunication systems and ICT and show relationships between knowledge and trust.

Traditionally, as a lexical-semantic, trust means reliance on the integrity, strength, ability, surety, etc., of a person or object. Generally trust is used as a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates.

On the other hand, trust in computer science in general can be classified into two broad categories: "user" and "system". The notion of "user" trust is derived from psychology and sociology, with a standard definition as "a subjective expectation an entity has about another's future behaviour". "System" trust is "the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose".

In a specific context, for instance in IoT, trust is reliance on the integrity, ability or character of an entity. Trust can be further explained in terms of confidence in the truth or worth of an entity. For example, EU uTRUSTit project defined that trust is the user's confidence in an entity's reliability, including user's acceptance of vulnerability in a potentially risky situation [8].

4.4.1 Knowledge and Trust

To understand trust, it is required to analyse the collected data from entities, extract the necessary information for trust; understand the information and then create the trust-related knowledge for the trust computation.

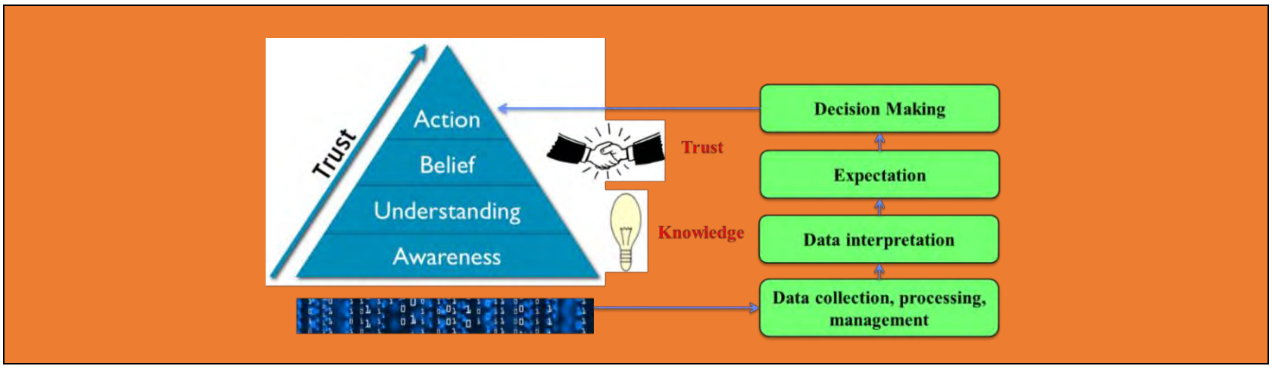


Figure 1 – Knowledge and Trust[1]

The social and economic value of data is mainly reaped during two moments: first when data is transformed into knowledge (gaining insights) and then when it is used for decision making (taking action). The knowledge is accumulated by individuals or systems through data analytics over time. So far data processing, management and interpretation for awareness and understanding have been considered as fundamental processes for obtaining the knowledge. As shown in Figure 1, trust is positioned as belief between knowledge (i.e., awareness and understanding) and action. It means that expectation process for trust should be additionally considered before decision making.

4.4.2 Relationships with security and privacy

Definition of security and privacy:

Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation.

Privacy concerns the expression of or adherence to various legal and non-legal norms. In the certain contexts this is often understood as compliance with data protection regarding the right to private life. Although it would be highly complex to map into personal data protection, the globally accepted privacy principles give a useful frame: consent, purpose restriction, legitimacy, transparency, data security and data subject participation.

As shown in Figure 4, trust can be interpreted as 3 different views:

- Trust has intersections with security and privacy (Left hand side of Figure 4);
- Trust has more broad scope covering security and other aspects such as reliability, dependability and ability (Middle of Figure 4);
- Trust has independent area compared to privacy and security. Trust mainly concerns beliefs, credentials, delegation, recommendation and reputation (Right hand side of Figure 4).

[1] Illustration compiled from trust pyramid - http://www.johnhaydon.com/how-make-people-trust-your-nonprofit/

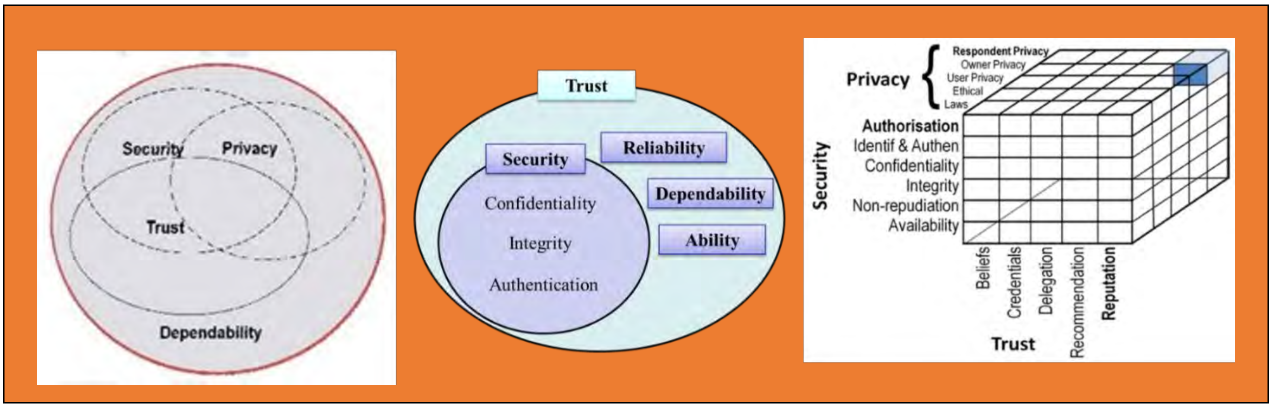


Figure 2 – Different views on trust

5 Use cases and explanation of trust provisioning

This section illustrates various use cases for trust provisioning based on the technical report of ITU-T CG-Trust and materials from other SDOs (e.g., oneM2M) as well as related literature. In addition, this section also analyses these uses cases in terms of purpose, method, actors and considerations for measuring trust.

5.1 Trust Use Cases in Networking Aspects

5.1.1 Trust-based routing protocols

5.1.1.1 Description

Secure routing is especially important in wireless networks. However there are many attacks toward wireless network routing protocols due to their open, distributed and dynamic nature.

In ad-hoc and sensor networks, it is very important to secure each node. An adversary may overtake some critical nodes and inject malicious behaviours, which leads to revelation of secure information and collapse of entire network. There are two common types of misbehaving nodes: selfish nodes and malicious nodes. If a node does not cooperate in packet forwarding due to some resource constraints, such as low memory or battery life, it is said to be selfish node. A selfish node may not have any intention to destruct the system; an adversary may reprogram a compromised node to behave selfishly. On the other hand, a malicious node has an objective to destruct the system badly, even at the cost of its own resources.

The security attacks in ad-hoc and sensor networks may be compared and classified from multiple perspectives. One way of classifying attacks is based on capabilities and resources an adversary has in his possession. In this type of classification, attacks may be classified as outsider (external) attack and Insider attack. In outsider attack, attacker lacks authentication and key information and such type of attack can easily be dealt with classical security mechanism such as cryptography, encryption and authentication. In insider attack, an adversary already has all key and cryptographic information, therefore such type of attack cannot be dealt with traditional security measures.

Another classification is based on adversary's intention to destruct the system. The attacks may be classified as Trust Management related attack and network related attack. The intention of Trust Management related attack is to degrade the performance of trust management system which leads to the inaccurate decisions. For example, in trust aware routing mechanisms, if misbehaving nodes are not properly detected and isolated by trust management system, then these nodes may become part of selected routing path and perform malicious activity. In network related attack, the intention of an adversary is to destruct overall performance of network by intentionally dropping data packets, energy drain and reporting incorrect sensed data. Such attacks can be detected and prevented by trust management system. For example, a black-hole attack intentionally drops all the received packets, which in results degrade the overall network performance in terms of Packet Delivery Ratio (PDR). Yet another way to characterize attacks is based on perspective of the efficacy of countermeasure, such as, traditional security solutions and trust based security solutions, to prevent attacks.

Traditional routing mechanisms cannot deal with several kinds of attacks. To make the wireless network securer, one natural idea is to include trust relationships between individual nodes, i.e., who trusts who and how, into route / path selection decisions. Thus, by making use of a trust-based platform, the routing protocols could avoid the malicious nodes which lead to link broken, low throughput, high delay.

5.1.1.2 Actors

Trust Platform: responsible for trust evaluation between nodes in wireless networks

Node as trustor: based on its knowledge (data with some simple analytical methods) with support from Trust Platform to assess the trustworthiness between the trustor and the trustee.

Node as trustee: responsible for providing information to Trust Platform when required in order to prove itself as being trustful.

5.1.1.3 Pre-condition

Trust Agent (a part of the Trust Platform) periodically collects related-trust data from nodes in the networks.

5.1.1.4 Triggers

When on-demand routing protocols occur (This type of protocol finds a route on demand by flooding the network with Route Request packets)

Periodically maintain the trust-based routing metrics of the networks (for each physical links) in case of Table-driven routing protocols.

5.1.2 Trust-based malicious node detection and prevention

5.1.2.1 Description

The major objective of providing security in wireless networks are to defend the network resources against variety of attacks, such as Denial of Service (DoS) attack, wormhole attack, black-hole attack, routing table overflow and poisoning attack, packet replication attack, gray-hole attack and modification of packets attack. Nodes in wireless networks are placed in large numbers in hostile environment, which makes difficult to protect against tampering or captured by an adversary force that can launch insider attacks to make a node compromised and can have easy access to valid keys and memory contents. Then, an adversary can learn contents of memory and have access to valid secret keys stored in the compromised nodes and use them to launch insider attacks.

Protocols and algorithms based on traditional security mechanisms such as authentication, encryption and cryptography are not completely suitable for Mobile Ad Hoc Network (MANET), Vehicular Ad Hoc Network (VANET) and Wireless Sensor Network (WSN) as these mechanisms assumes that all participating nodes are cooperative and trustworthy and also require extensive computation, communication and storage. In recent years, the concept of trust and reputation has been applied to field of wireless communication networks to monitor varying behaviour of nodes and counter insider attacks. Reputation and trust are two very useful tools that are used to facilitate decision making in diverse fields. Trust based security is a new way of providing security without using cryptography approaches. Trust in the field of wireless communication networks may be defined as degree of reliability of other nodes performing actions.

Trust and reputation management systems can be used to assists wireless networks in decision making process. Trust between the nodes in maintained by recording the transactions of a node with other nodes in the network, either directly or indirectly. A trust value will be calculated from the record that aids sensor nodes to deal with uncertainty about the future actions of other nodes.

Trust based approaches are very useful to deal with node misbehaviour. The problem to address uncertainty in decision making is dealt with trust and reputation management systems by maintaining past behaviour of nodes. If a node holds a good reputation it will be forwarded with packets and considered as trustworthy node; otherwise, it will be considered untrustworthy. The words trust and reputation has been commonly used in our personal and business dealings. The repute of a person in established from the actions performed previously and it goes on increasing with the time if he or she remains consistently sincere in their dealings.

The same idea is applied in trust and reputation based systems; a well reputed node is chosen for communication in neighbourhood. Trust based approaches has been widely used in popular wireless communication networks such as WSN, MANET, VANET and wireless multimedia sensor networks. Therefore, to develop a trust-based mechanism for malicious node detections and prevention, trust and reputation systems should be taken into account. It is important to investigate on trust and reputation models, what key requirements and elements are involved in the design of trust and reputation systems, and how these systems can be effective to provide better security.

5.1.2.2 Actors

Trust Platform: responsible for trust evaluation between nodes in wireless networks and an intelligent engine to detect whether a node with a specific trust level in a particular context is malicious or not.

Nodes: responsible for providing information in order to prove itself as being trustful.

5.1.2.3 Pre-condition

Trust Agent (a part of the Trust Platform) periodically collects related-trust data (both direct trust and indirect trust) from nodes in the networks and analyse the misbehaviour.

A node gathers direct trust by its own personal experiences with other neighbouring nodes through direct interaction. On the other hand, indirect trust is gathered by a node from other node's experiences with the subjective node.

5.1.2.4 Triggers

A decision making component of the trust platform is used for detecting and excluding misbehaving nodes and selecting trustworthy nodes for mutual interaction.

5.1.3 Trust-based access control mechanism

5.1.3.1 Description

Trust provides device with a natural way of judging other device similar to how we have been handling security and access control in human society. Trust relationship between two devices helps in influencing the future behaviours of their interactions. When devices trust each other, they prefer to share services and resources at certain extent. Trust management allows the computation and analysis of trust among devices to make suitable decision in order to establish efficient and reliable communication among devices.

Designing device identities and securing the interaction of the devices are two of the major challenges of any network system like wireless network or IoT. Consider for a moment, how a user can attach device available publicly to his/her personal space of device for a short time? How can he/she trust this device? How will this device access his/her personal information? Note that level of access control from device i to device j is directly proportional to the trust device i is holding for device j. Access control and the trust are closely related as level of access granted by particular device to other device or service depends on the level of trust between these devices.

These issues can be addressed with trust-based access control mechanism in which the trust level for each device is calculated by the trust platform; then mapped to an access control policy.

Once a device wants to access a resource, the trust platform will analyse trust-related information of the device (both direct and indirect trust) and calculate the trust score. The information is both periodically collected and proactively collected depending on the design of the trust platform as well as network architecture. Trust score is then mapped to access permissions for providing access to the resources or devices with the principle of least privilege.

5.1.3.2 Actors

Trust Platform: responsible for trust evaluation between nodes in wireless networks and an intelligent engine to detect whether a node with a specific trust level in a particular context is malicious or not.

Nodes: responsible for providing information in order to prove itself as being trustful.

Access Control Policy and Mapping manager: to map each trust level (of each device) to a specific access control policy.

5.1.3.3 Pre-condition

Trust Platform periodically collects trust-related data from nodes in the networks.

5.1.3.4 Triggers

Once a device want to use/access a resource, it will request for the access control.

5.1.3.5 High Level Illustration

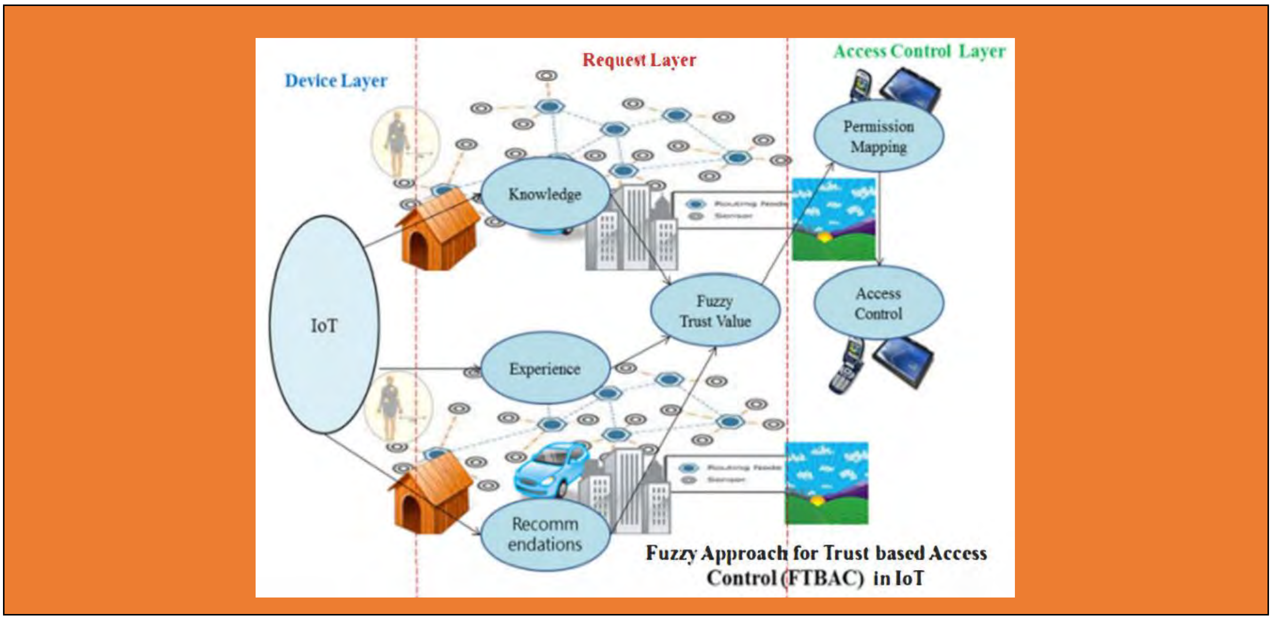


Figure 3 – High level illustration of trust based access control [112]

5.2 Use Case of Services and Applications in IoT

In IoT environment, not only personal data, devices in house, office, and transport means will have much sensitive data to be collected. User interfaces on devices will shrink or disappear, making it more difficult for consumers to know when data is being collected, or to exercise any control. Data from the IoT will feed new kinds of algorithmic decision-making and the burgeoning data analytics industry. And securing many inexpensive connected devices, as well as the data they generate, may present both technological and economic challenges.

The European Commission's July 2014 Communication stated that consumers must "have sufficient trust in the technology, the behaviours of providers, and the rules governing them" in order for the IoT to reach its full potential. Similarly, the Article 29 Working Party noted last September that the IoT "must also respect the many privacy and security challenges."

IoT relies on the principle of the extensive processing of data through sensors that are designed to communicate unobtrusively and exchange data in a seamless way. The exponential volume of data that can be collected, and its further combination, its storage in and the use of predictive analytics tools cannot transform data into something useful but also allow companies - and potentially malware - to have very detailed profiles of individuals; and the sharing and combination of data through cloud services will increase the locations and jurisdictions where personal data resides. In order to reach the full IoT potential, services and applications must make use of big data analytics which depend on collecting data from many different sources and using it for purposes that may be different from those for which it was collected. Therefore, it is needed to ensure that companies are accountable for using all of this data in a way that is consistent with consumers' expectations.

5.2.1 Trusted Data Usage Mechanism in Smart Cities

In big cities, a very large number of people commute between suburbs and the centre on public transport (e.g., buses and trains). Commuters on these vehicles are usually in quite close proximity, most carry handheld de-vices with one or more network interfaces (WiFi, Bluetooth, Global System for Mobile Communications (GSM)), their patterns of mobility are quite "seasonal" (in the sense that they travel usually at the same time, repeating the same path day after day), and tend to stay on the vehicle for quite a prolonged period of time. In addition, devices are often diversely equipped: some have Global Positioning System (GPS) receivers, others have embedded cameras, sensing abilities (e.g., temperature, light), etc. [9].

As a result, a wide variety of services could be occurred or shared among people, through their devices. For example:

- Location information sharing: a device with a GPS receiver could be serving location information to others.
- Exact time information: a GSM device could offer this.
- News headlines, stock market levels: someone able to access the Internet through a GPRS phone could forward fresh information to others.
- Gaming: devices could participate in a shared game for the duration of their trip.
- Software components: new applications/functionalities could be shared and downloaded from a peer.
- Information about traffic and delays: commuters traveling in different directions could inform each other's.

However, at the same time severe trust issues can be observed as more sensitive data is being exchanged between entities and clearly it is mandatory to have trustworthy communication among each devices and services. In general, entities must be capable of building up an opinion about every other device/service they interact with and eventually more authoritative and reliable communication can be built up with the same pair of hosts.

Initially, peers that have not been encountered will have a neutral reputation, neither positive nor negative. This value would be increased after successful interactions, while appropriately decreased following unsatisfactory service deliveries.

This is very essential to resist against malicious attacks like Sybil attacks, where malicious hosts can simply generate more identities to avoid being punished for past misbehaviours. This would obviously be high in sensitive operations, such as monetary transfers, and relaxed for minor tasks, such as location information gathering.

5.2.1.1 Definition

The success of any data sharing platform in smart cities depends on the compliance on data protection regulations and, beyond legal obligations, on the establishment of trust relationships with participants sharing their data. For trusted data exchange, each process from sensing to actionable knowledge requires trust enabled mechanisms such as data perception trust, trustworthy data fusion/mining and reasoning with trust related policies.

The solution is just to share data to a trusted source (in specific trust domain and specific content of data) by leveraging a trusted data usage mechanism in which data usage policies should be personalized set. The data owners can trace back to check how their data is used.

The trust based data usage mechanism allows benefits such as policy enforcement to share data based on the properties of data consumers, allowing IoT shared platform to keep track of data usage history, and more importantly allow data owners to monetize their data sharing by allowing them to dynamically adjusting their policies on the fly.

5.2.1.2 Actors

Trust Platform: responsible for trust evaluation between data owners and data consumers.

Data Usage Manager: responsible for matching trust level to data usage policy

Data Owners: responsible for providing user preferences, trust-related information and personal data usage policy if necessary.

Data Consumers: responsible for providing trust-related information and data usage purposes for trust evaluation.

5.2.1.3 Triggers

Creation of new data from data owners.

Request of data consumption from applications, services or people with any purpose.

Request of data usage policy changes from both data owners and data manager platform.

5.2.2 Secure Remote Patient Care and Monitoring

E-health applications, that provide the capability for remote monitoring and care, eliminate the need for frequent office or home visits by care givers, provide great cost-saving and convenience as well as improvements. “Chronic disease management” and “aging independently” are among the most prominent use cases of remote patient monitoring applications. Remote patient monitoring applications allow measurements from various medical and non-medical devices in the patient’s environment to be read and analysed remotely. Alarming results can automatically trigger notifications for emergency responders, when life-threatening conditions arise. On the other hand, trigger notifications can be created for care givers or family members when less severe anomalies are detected. Dosage changes can also be administered based on remote commands, when needed.

In many cases, the know-how about the details of the underlying communications network and data management may be outsourced by the medical community to e-health application/ solution provider. The e-health solution provider may in turn refer to Machine-to-Machine (M2M) service providers to provide services such as connectivity, device management. The M2M service provider may intend to deploy a service platform that serves a variety of M2M applications (other than e-health solution provider). To that end, the M2M service provider may seek to deploy optimizations on network utilization, device battery or user convenience features such as ability of using web services to reach application data from a generic web browser. The M2M service provider may try to provide uniform Application Programming Interfaces (APIs) for all those solution providers to reach its service platform in a common way. From the standpoint of the M2M application, the application data layer rides on top a service layer provided by this service platform. By providing the service platform and its APIs, the M2M service provider facilitates development and integration of applications with the data management and communication facilities that are common for all applications.

As part of providing connectivity services, the M2M service provider may also provide secure sessions for transfer of data for the solution providers that it serves. In many jurisdictions around the world, privacy of patient healthcare data is tightly regulated and breaches are penalized with hefty fines. This means the e-health application provider may not be able to directly rely on the security provided by the M2M service provider links/sessions and instead implement end to end security at application layer. This puts additional challenges on the M2M service platform for trust, since it needs to provide its optimizations on encrypted data.

5.2.2.1 Description

One particular issue with e-health is that not only the data is encrypted, but it may also contain data at different sensitivity levels, not all of which appropriate to each user. For instance in the US the Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of protected health information. Different actors within a healthcare scenario may have different levels of authorizations for accessing the data within the health records, so the information system must take care to present the health data to each user according to the level of authorization for that user. A process, common to address this issue is redaction. This means that one starts with a document that originally includes data of all sensitivity levels and then removes any piece of information that has a higher sensitivity level than the pre-determined redaction level. The end result is a redacted version of the initial document that can be presented to a person/entity that has the matching authorization level. Persons with lower authorization level are not authorized to view this particular version of document. The redaction engine can produce multiple versions of the initial records, where each version corresponds to one redaction level including material at specific sensitivity level (and lower).

Care must be taken to ensure that only authorized users have access to data. Therefore, the system must match the redaction level of data with the authorization level and present the proper version of the record for each actor.

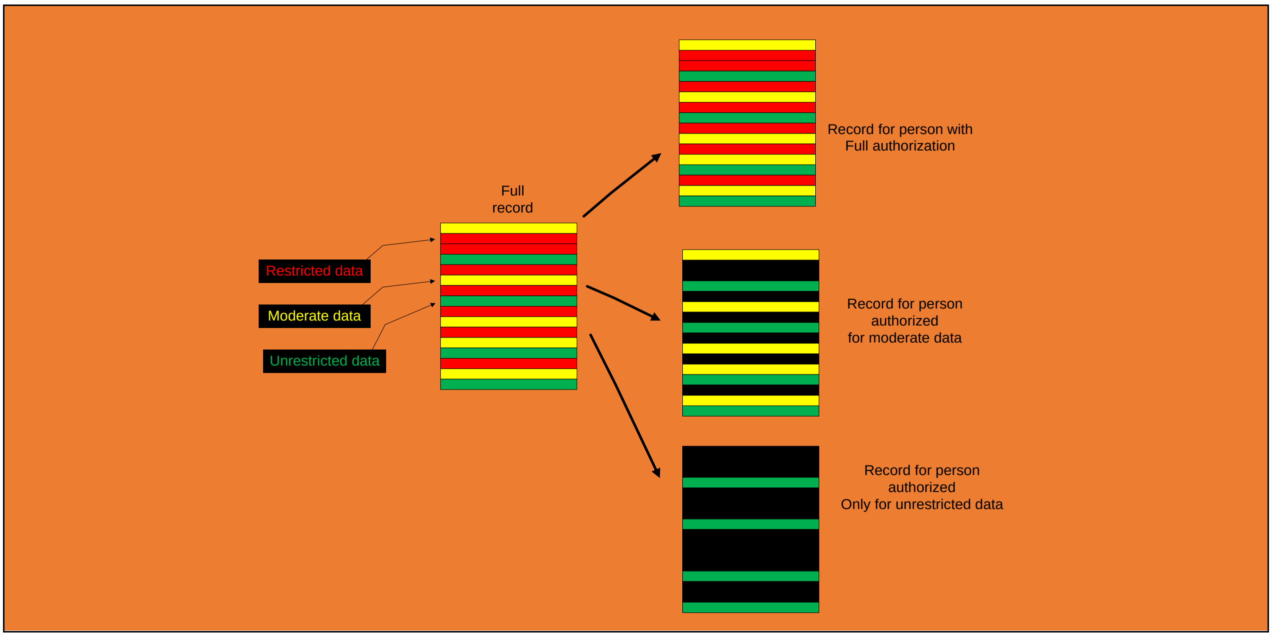


Figure 4 – An illustration of a process with 2 levels of redaction [113]

The rexdaction engine may reside at a policy control server or at the application server operated by the M2M application service provider. The policy server may also hold policies on which users get which authorization level, while an authorization server may be in charge of authenticating each user and assigning her the proper authorization level.

In a system relying on notifications based on prior subscriptions, data must be examined first to determine which subscribers should receive notifications and then only those subscribers should be capable to retrieve the data about which the notification is sent.

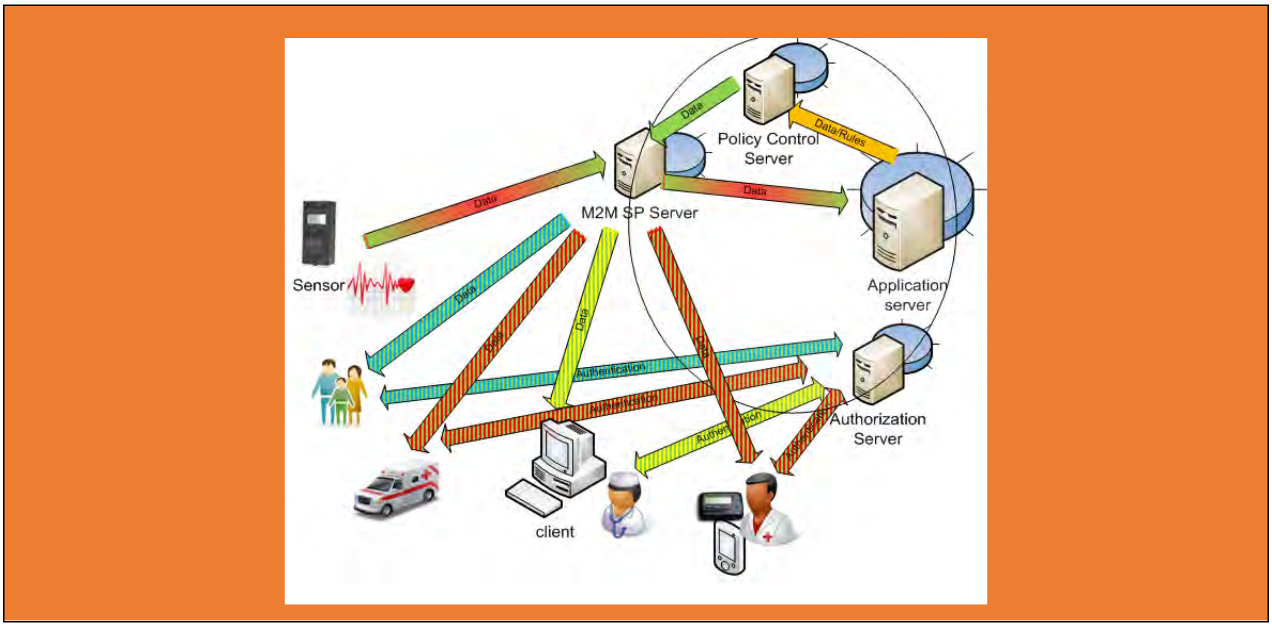


Figure 5 – An e-Health application service model [113]

Again, these challenges can be solved by using trust-based access control mechanism in which the trust level for each person is calculated by the trust platform; then mapped to an authorized access control rules.

5.2.2.2 Actors

A Patients: using sensor (medical status measurement) devices

E-Health application service providers: providing sensor devices and operating remote patient monitoring, care and notification services

Care givers: (e.g. nurses, doctors, homecare assistants, emergency responders) and other administrative users with authorization to access healthcare data (e.g. insurance providers, billing personnel). It also refers to these entities as "participants in the healthcare episode" in some occasions.

M2M service providers, network operators: providing connectivity services for the patients, e-health application providers and care givers.

Trust Platform: responsible for trust evaluation between nodes in wireless networks and an intelligent engine to detect whether a node with a specific trust level in a particular context is malicious or not.

Access Control Policy and Mapping Manager: to map each trust level (of each device) to a specific access control policy.

5.2.2.3 Pre-condition

A categorization rule set, that is able to categorize various entries within a medical record according to the sensitivity levels and label them accordingly, must exist.

A redaction engine that is able to examine the raw medical record and produce different versions of the record at different redaction levels with only data that is at or below a sensitivity level.

A policy engine that is able to examine medical records and determine level of criticality (applicable to one of the flows described).

A set of authorization policies that describe what authorization level is required to be able to access data at each redaction level.

An authorization engine/server that interacts with each user of the e-health application to verify their claimed authorization level, for example the server may perform an authentication function with the user.

The e-health application server that is capable of interacting with the authorization server to check the authorization level of each user to determine the user's redaction level before serving data at the requested (or appropriate) redaction level to that user.

Trust Platform periodically collects trust-related data from nodes in the networks.

5.2.2.4 Triggers

Creation of new measurement data by a remote medical device.

Analysis of received measurement data at application servers, and determination of need for redaction, or creation of alarms and notifications, etc.

Requests from participants in a health care episode (caregivers) for sensitive medical records.

Arrival of new participants (new doctors, etc.) in the health care episode.

5.2.3 Trust for Time critical and Real-time applications

5.2.3.1 Definition

One of the most discussed and vital applications of real time network is smart grid network. Future Smart Grids will be capable of informing consumers of their day-to-day energy use, even at the appliance level. While this is beneficial and supports valuable efforts to curb greenhouse gas emissions and reduce consumers' energy bills, it introduces the possibility of collecting detailed information on individual energy consumption use and patterns within the most private of places like our homes.

The overall vision for the Smart Grid is that it will possess the following qualities [10];

Intelligent — capable of sensing system overloads and rerouting power to prevent or minimize a potential outage; of working autonomously when conditions require resolution faster than humans can respond and cooperatively in aligning the goals of utilities, consumers and regulators.

Efficient — capable of meeting increased consumer demand without adding infrastructure.

Accommodating — accepting energy from virtually any fuel source including solar and wind as easily and transparently as coal and natural gas; capable of integrating any and all better ideas and technologies—energy storage technologies, for example—as they are market-proven and ready to come online.

Motivating — enabling real-time communication between the consumer and utility so consumers can tailor their energy consumption based on individual preferences, like price and/or environmental concerns.

Opportunistic — creating new opportunities and markets by means of its ability to capitalize on plug-and-play innovation wherever and whenever appropriate.

Quality-focused — capable of delivering the power quality necessary —free of sags, spikes, disturbances and interruptions—to power our increasingly digital economy and the data centres, computers and electronics necessary to make it run.

Resilient — increasingly resistant to attack and natural disasters as it becomes more decentralized and reinforced with Smart Grid security protocols.

"Green"— slowing the advance of global climate change and offering a genuine path toward significant environmental improvement.

However, it is a must to take great care not to sacrifice consumer privacy. We recognize the value of the information on the grid, which will give consumers more control over their electricity usage and give utilities the ability to manage demand requirements, but the dissemination of data must be done in a trustworthy and transparent manner. To make Smart Grids transparent and trustworthy, an actor is empowered to monitor (invoke services) and provide information exchange with all relevant stakeholders.

5.2.4 Home energy Management

This use case is to manage energy consumption at home so that consumers can be aware of their daily home energy consumptions and able to control this consumption by remote actions on home appliances.

5.2.4.1 Description

Innovative services can be developed from the data (energy) collection and sent to either the consumers/ equipment or to Business-to-Business market.

The use case focuses on a home gateway that collects energy information from the electrical home network and communicates it to an IoT system for aggregating and processing of the data. Services can then be developed from the collected data.

The home gateway performs an initial treatment of the data received from various sources (sensors, context) as follows:

- Aggregating and processing the obtained information;
- Sending some information to the remote service platform e.g. sending alerts;
- Using some information locally for immediate activation of some actuators/appliances;
- Connected (wirelessly or via wireline) to home devices, including the home electrical meter, for information on global or individual consumption of the appliances;
- Providing displayable consumed energy-related information to the end-user/consumer terminals (PC, mobile phone, tablet, TV screen, etc.).

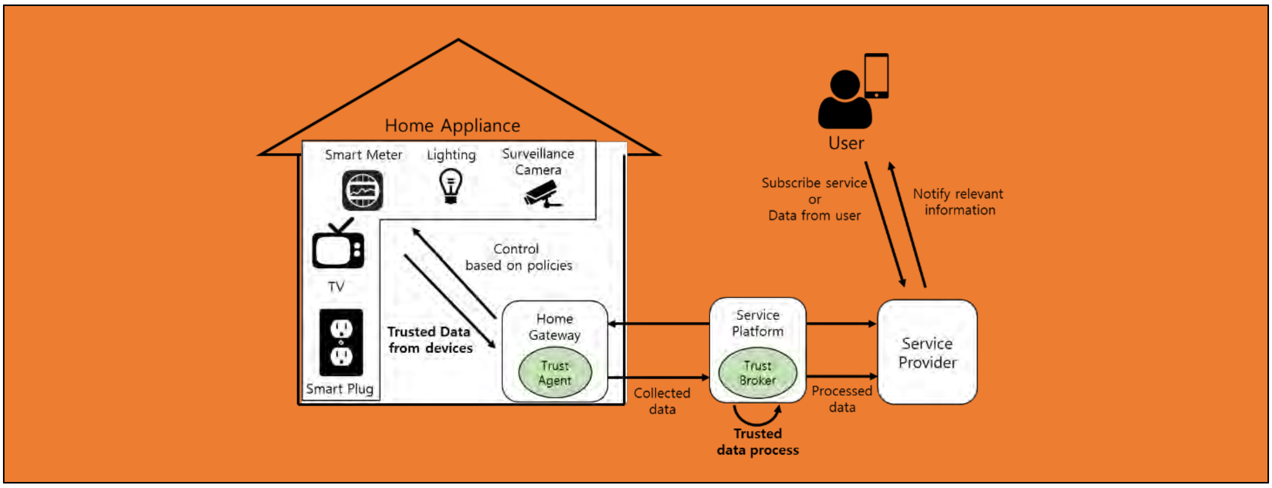


Figure 6 – Home energy management system high level illustration

5.2.4.2 Actor list

User: user of home appliance who are able to control home appliance using terminal device (e.g. laptop, smartphone, etc.)

Home appliance: appliances which may be from multiple vendors

Home Gateway: a device installed in the user's home and receives remote control commands from the management server

Communication operator (LAN/PAN/WAN): in charge of communicating the collected information via any protocol (e.g. ZigBee, Power Line Communication (PLC), Bluetooth 4.0, Wi-Fi, etc.)

Service Server: in charge of providing services/common functionalities for applications

5.2.4.2 Analysis

Trusted data collection and aggregation

Data should be trustworthy from devices (home appliances) to home gateway and gateway to service platform. Devices produce data, and data is collected in a gateway and service platform. When data is produced and transmitted to other entity, trustworthiness of data is required to be maintained.

Trusted data process and analysis

Information which is processed by home gateway and service platform should be trustworthy. Collected data is processed and analysed in a gateway to decide extra actions depending on policies stored in the gateway. Also, the gateway can put additional data (e.g. location, time, etc.) to collected data for sending data to service platform. Service platform also can process and analyse data from the gateway to produce useful information to a user. Since the gateway and service platform manipulate collected data, the trustworthiness of information (i.e. processed and analysed data) is required to be maintained in each process.

Trustworthy application

Application (service provider) notifies processed information to user depending on their subscription profile. The trustworthiness of application is recommended to be maintained in each process.

Privacy

When home energy management system notifies energy consumption information to user, providing displayable consumed energy-related information to the end-user/consumer terminals (PC, mobile phone, tablet, TV screen, etc.) may be unintentionally exposed. Application (or service provider) utilizes user's data for big data process, and this may cause user privacy issue.

5.2.5 Smart Office Service

5.2.5.1 Description

Trust based smart office service provides users with various office facilities based on the trust level of users. This service can allow different type of permission (or access) to facilities according to user's trust information. For example, it is assumed there are three kinds of trust level like high, middle and low trusted user. For the permission of cloud storage service, high trusted user can access with the authority of read, write, and middle trusted user can access with the authority of read only. Low trusted user has no right to access. Figure 9 shows an example of smart office service with different priority of users and different permission to office facilities.

For the trust management, various properties like social/business relationship and membership can be considered to analyse user's trust level.

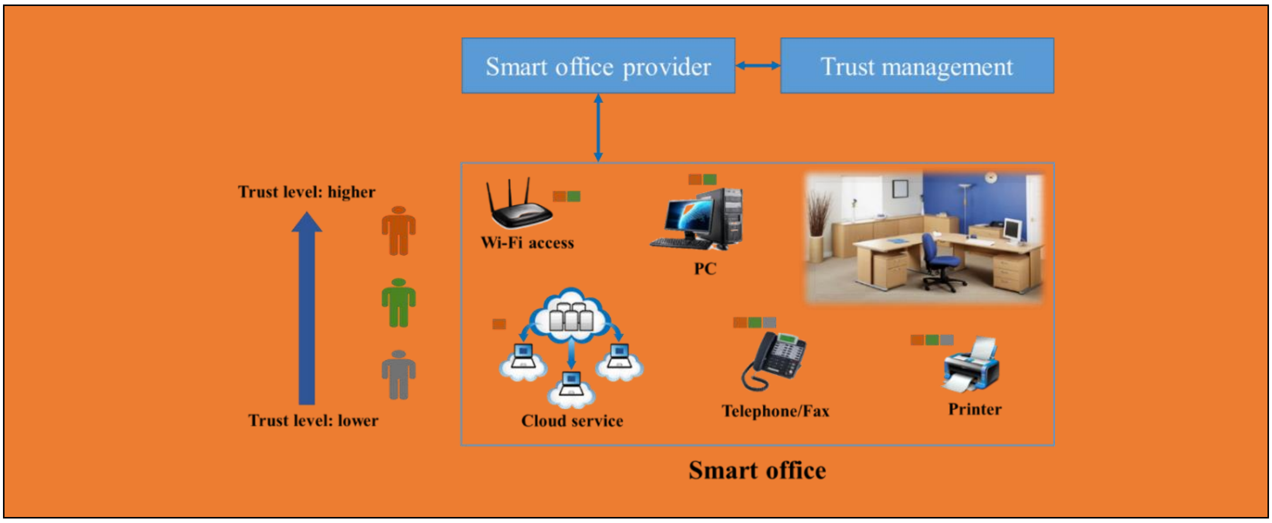


Figure 9 – Example of smart office service using trust information

5.2.5.2 Actor list

User

Smart office

Smart office provider

Trust management

5.2.6 Document sharing

5.2.6.1 Description

This use case considers a social IoT environment [11] with no centralized trusted authority. In the social IoT, each device has the subjective value between other devices based on the owner's social relationship as well as the Community of Interest (CoI) [12] of each device.

Alice and Bob are co-workers and they have a meeting with Charlie who belongs to other company. Bob wants to check a document for the meeting in Alice's Wireless Portable Hard drive (WPH). Without the social IoT trust, Alice takes the document from her storage and sends the document to Bob using Universal Serial Bus (USB) or else notifies a guest account to Bob. However, Alice does not need to do anything with the social IoT trust. When Bob requests the document to Alice's WPH, Bob's smartphone sends the social information of Bob and its CoI value. WPH calculates the subjective trust value (Ta,b) of Bob in the view of Alice by using given information of Alice and Bob. After that, WPH judges Bob has enough authorization to get the document. If Ta,b value exceeds the threshold value, WPH sends the document to Bob's smartphone. If Charlie who is not related to Alice sends the request query to WPH, WPH calculates the subjective trust value (Ta,c) of Charlie in the view of Alice in the same procedure and deny the request from Charlie because Ta,c is lower than the threshold. To prevent the system from Sybil attack, some physical security techniques may be used like fingerprint identification, etc.

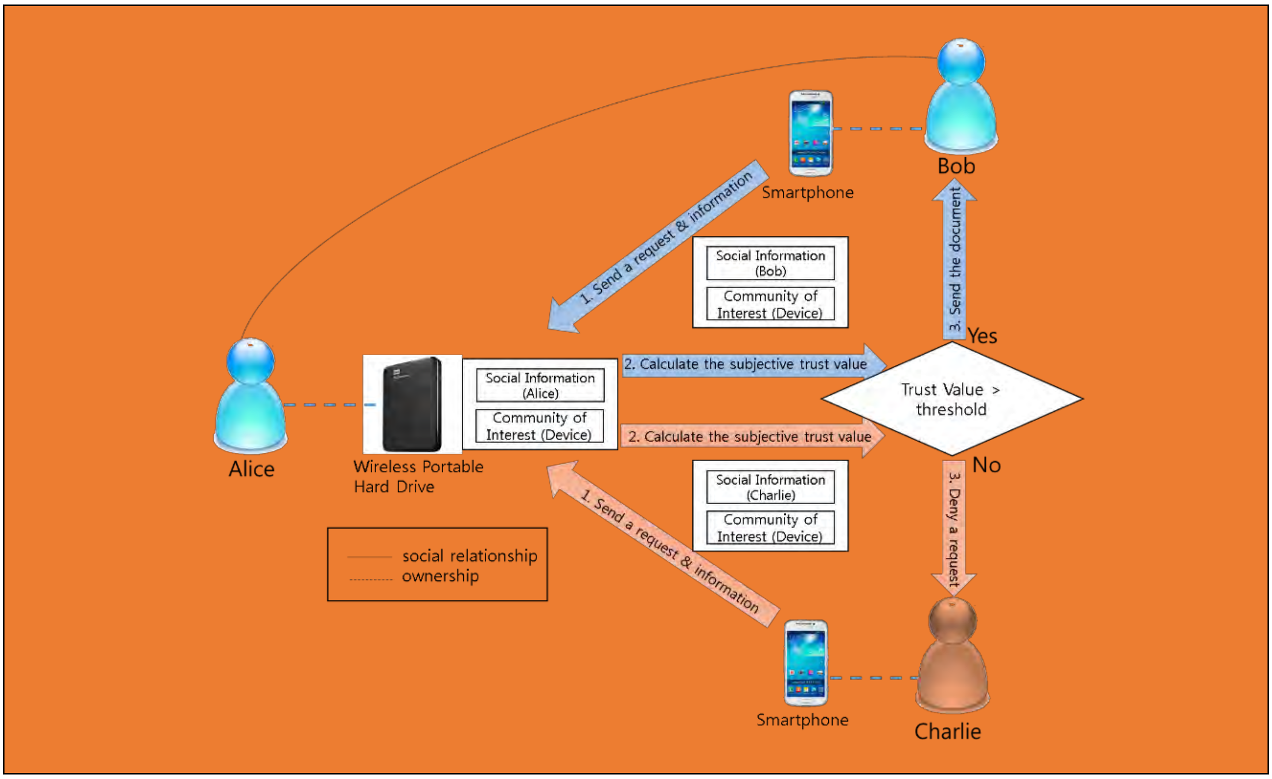

Bob
Smartphone
1. Send a request & information
Social Information (Bob)
Community of Interest (Device)
3. Send the document
Yes
2. Calculate the subjective trust value
Trust Value > threshold
Alice
Social Information (Alice)
Community of Interest (Device)
2. Calculate the subjective trust value
No
Wireless Portable Hard Drive
1. Send a request & information
Social Information (Charlie)
Community of Interest (Device)
3. Deny a request
social relationship
ownership
Smartphone
Charlie

Figure 10 – Document sharing scenario in social IoT environment

5.2.6.2 Actor list

User: A user who takes the ownership of the things (e.g. WPH, smartphone, etc.) and wants to share the documents in the WPH.

Smartphone: A device which is an intermediate entity and is available to send its owner's social relationship information and its CoI information to WPH.

Wireless Portable hard drive: A device is mainly in charge of collecting the social information and calculating the subjective trust value and judging authorization to share the document.

5.2.6.3 Analysis

Trusted data collection and aggregation

Social relationship information: This trust property represents whether or not the trustee is socially cooperative with the trustor. The social friendship relationship among device owners to characterize the cooperativeness is used.

CoI information: This trust property represents whether or not the trustor and trustee are in the same social CoI (e.g. co-location, co-work, or parental object relationship).

Ownership: This trust property represents whether or not the objects (smartphones) used by the device owner.

5.2.7 Multi-hop device-to-device network path selection

5.2.7.1 Description

In the case of Figure 7, Alice wants to exchange information with another peer in multi-hop Device-to-Device D2D environment. Alice's smartphone requests the social information of Node 1~3 and its CoI value. Then, it calculates subjective trust values (Ta,n1, Ta,n2, Ta,n3) of other nodes in the view of Alice by using given information. If Ta,n1 is the highest value, Alice's smartphone judges Node 1 has enough authorization to send information and select the path with Node 1. The social IoT trust also can be used in the path selection process for the reliable exchange of information. To complement the objective trust, the subjective trust is required in addition.

5.2.7.2 Actor list

User: A user who takes the ownership of the things (e.g. smartphone, laptop, etc.) and wants to exchange information with another peer via other users

Device (Smartphone): A device which is an intermediate entity and is available to send its owner’s social relationship information and its CoI information to other devices.

5.2.7.3 Analysis

Trusted data collection and aggregation

Social relationship information: This trust property represents whether or not the trustee is socially cooperative with the trustor. The social friendship relationship among device owners to characterize the cooperativeness is used.

CoI information: This trust property represents whether or not the trustor and trustee are in the same social CoI (e.g. co-location, co-work, or parental object relationship).

Ownership: This trust property represents whether or not the objects (smartphones) used by the device owner.

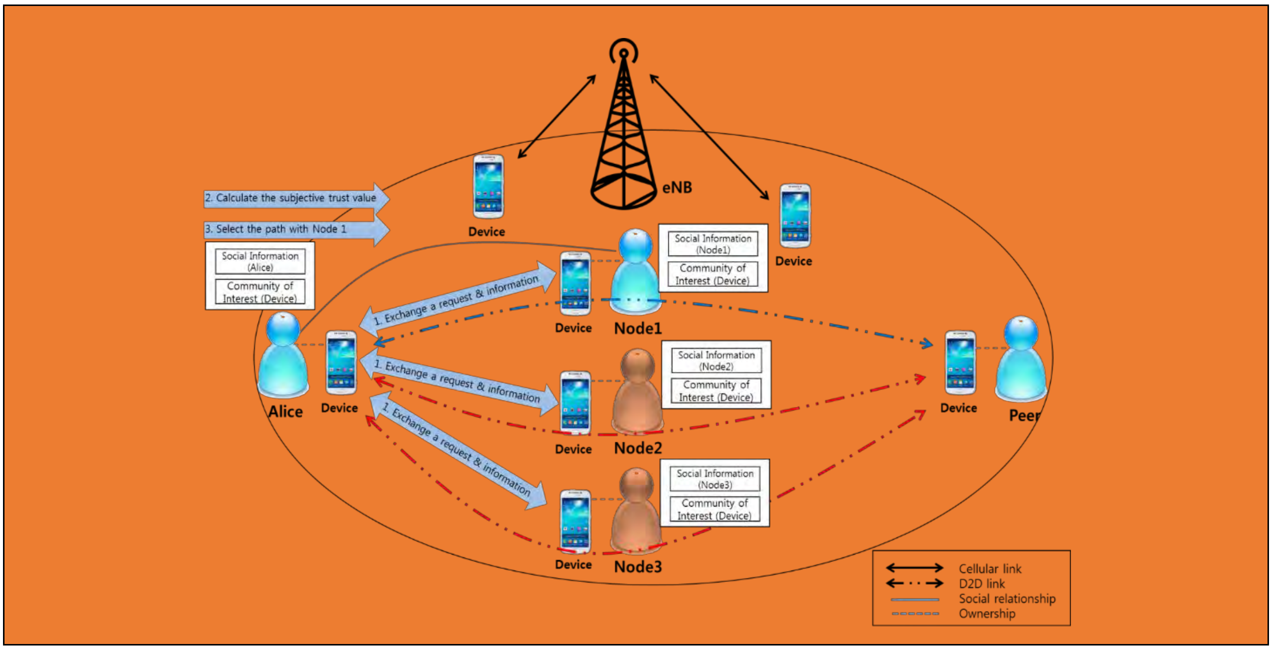

eNB
Device
Device
2. Calculate the subjective trust value
3. Select the path with Node 1
Social Information (Alice)
Community of Interest (Device)
Social Information (Node1)
Community of Interest (Device)
1. Exchange a request & information
1. Exchange a request & information
1. Exchange a request & information
Alice
Device
Device
Node1
Social Information (Node2)
Community of Interest (Device)
Device
Node2
Social Information (Node3)
Community of Interest (Device)
Device
Node3
Device
Peer
Cellular link
D2D link
Social relationship
Ownership

Figure 7 – A path selection scenario in multi-hop D2D environment

5.2.8 Trust provisioning of used car transaction service

5.2.8.1 Description

While the used car market has been growing consistently in worldwide, there exists inevitable distrust in used car transactions. Comparing to purchasing a new car, buying a used car involves high level of uncertainty and risk. The market for used car is called as "the market for the lemons", which is produced by asymmetric information, in which buyers can not accurately assess the exact condition of a car through examination before sale is made while sellers can more accurately assess the condition of a car prior to sale. Specifically, owners of good cars will not sell their cars while only owners of defective cars will sell their cars. When sellers are going to sell their used vehicle, they have a weak motivation of disclosing the problems of their cars. As a result, consumers are hardly satisfied with the used cars because of unexpected car trouble. General transaction model and each entity's information level of a used car are depicted in Figure 8.

Basically current used car transaction involves following inevitable problems; (1) asymmetric information, (2) conflicting motivation of disclosing the condition of used car due to (1), and (3) distrust among entities due to (2). Thus, an appropriate intervention is needed for avoiding dispute among entities and activating the used car market as illustrated in Figure 9.

In order to overcome sequential problems discussed, it is direct remedy to make participants share information. Trust management platform can play an important role in mediating entities who participate in used vehicle market and sharing trustful data and information.

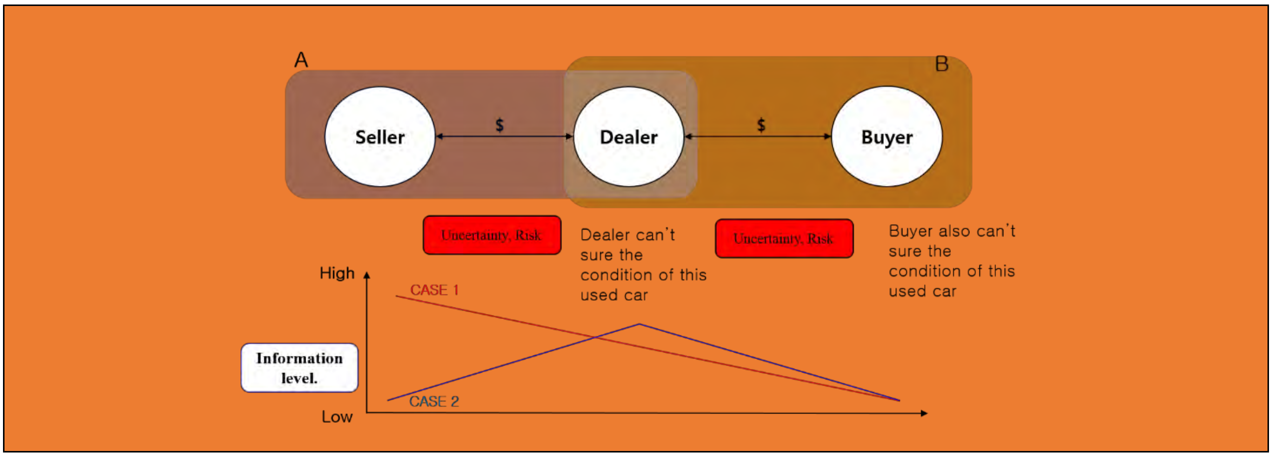

A
B
Seller
$
Dealer
$
Buyer
Uncertainty, Risk
Dealer can't sure the condition of this used car
Uncertainty, Risk
Buyer also can't sure the condition of this used car
High
CASE 1
Information level.
CASE 2
Low

Figure 8 – Used car transaction model and each entities' information level

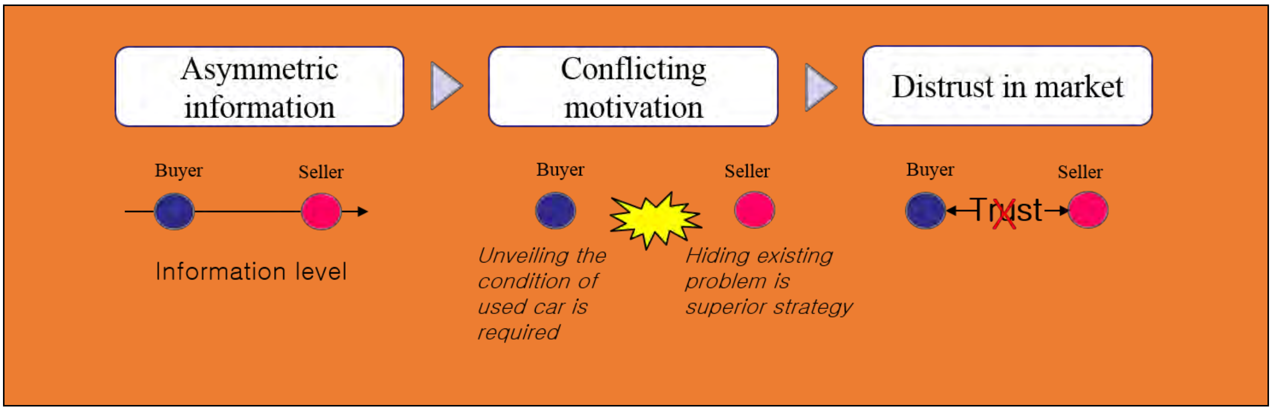


Figure 9 – Asymmetric information, conflicting motivation, and distrust in used car transaction

5.2.8.2 Actor list

Dealer: The major role of a dealer is mediating buyer and seller (owner) to gain economic profit.

Buyer: A buyer is someone who wants to purchase a used car from a dealer or seller.

Owner (Seller): An owner (seller) is someone who wants to sell his or her car to others including a dealer and individual buyer.

(Trust) Service Broker: Trust service broker is a broker mediating an interaction among buyers, sellers, and dealers through the information transferred by trust management platform. Based on the information, trust service broker can inform the identified level of trust of owner, registered vehicle, and seller.

Trust Management Platform: Trust management platform responses various requests from a service broker and others. Trust management platform analyses the level of trust by tracing the accumulated data from various sources including social network, insurance company, vehicle repair shop, public, and the car itself.

5.2.8.3 Analysis

Participants' advantage of adopting used car transaction through trust management platform.

This sub-section describes how trust can be achieved in used car transaction by trust management platform, which plays a role in reducing the information gap among entities, refining data from various data sources, and mediating entities through trust service broker. By adopting this platform, each entity participating in used car ecosystem can take following advantage. Details are explained in Table 1.

Table 1 – Analysis of Trust provisioning of used car transaction service

	Main advantages	Side advantages
Seller	- Providing trustful data which influence on selling price	- Reasonable vehicle maintenance based on trustful data transmitted by vehicle itself - Reducing insurance cost by a vehicle specific data
Dealer	- Reducing investigation effort - Decreasing dispute	- Restoring confidence in used car transaction
Buyer	- Reducing uncertainty and risk from purchasing used goods	- Succession to well-maintained vehicle - Purchasing relatively low retail price in P2P market
Insurance Corp.	- Realizing usage-based insurance by absorbing deadweight loss	
Government	- Reducing dispute - Revitalizing market - Promoting international vehicle transaction	- Improving road infrastructure and traffic flows
Vehicle Manufacturer	- Detecting defective vehicle model in early stage	- Gathering real data for improving vehicle performance
OBD2 Scanner manufacturer	- Creating new revenue stream	- Taking opportunity of analysing vehicles' historical data

5.2.9 Trust provisioning of car sharing system

5.2.9.1 Description

This use case is about car sharing system. Car Sharing is to offer a new service model for automobile transportation. Simply, Car sharing is a self-service, on-demand alternative to car ownership; a service that is offered to urban residents (Business to Consumer, B2C) and businesses (Business-to-Business, B2B).

This service is mainly designed around a particular user profile – first of all, people who live in cities but do not drive a car every day and secondly tourists who live in cities but do not own a car. Thus, people who need a car at short notice but take an alternative to car ownership.

The brief procedure of this service is illustrated in Figure 10: 1) joining the membership, 2) unlocking the car door, 3) driving away, 4) parking to any reserved spot provided by the service provider and/or public, and 5) paying as you drive (including gas, insurance, and etc.).

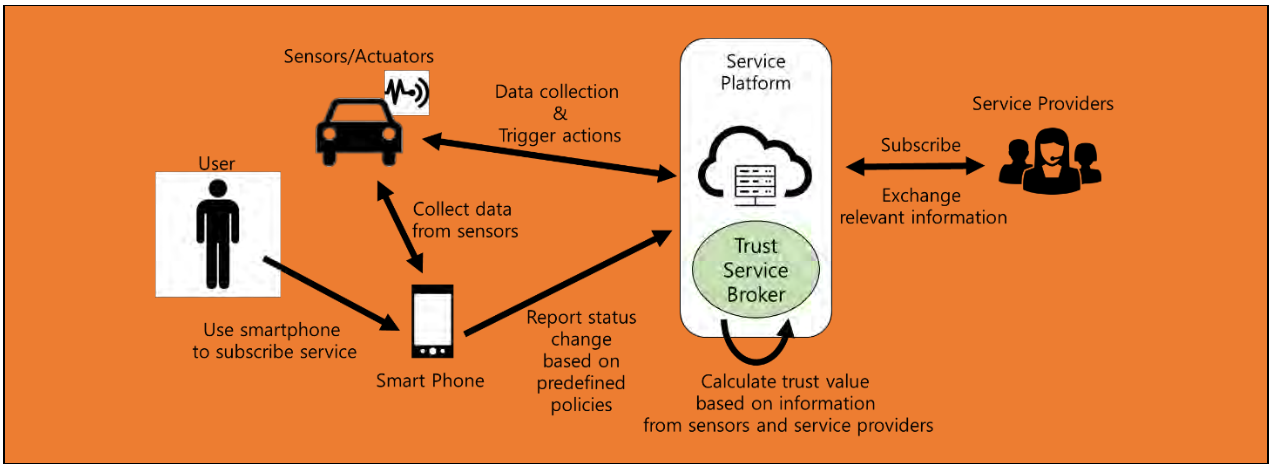


Figure 10 – High level Illustration of car sharing system

5.2.9.2 Actor list

Users: A user who takes the ownership of the shared things which are car.

Sensors (or Sensor Devices): Sensor Devices can be various based on its usage, and do not have any direct communication interfaces to the service platform.

Smartphone: A device which is an intermediate entity and is available to connect from sensors to a service platform. The basic role is similar to the general gateway, but it has some sensors and some applications (navigation) itself used by services.

Service Platform: In charge of providing common functionalities for the services. It is mainly in charge of collecting the status and configuration information of sensors and controlling them via the smartphone and/or gateway.

Service Providers: Companies which provide its own services for the user through the service platform. The service providers can be various according to the types of services.

5.2.9.3 Trigger

A user wants to take an ownership of the car.

5.2.9.4 Pre-conditions

The user preliminary joins a membership of the car sharing service.

Sensors built in the car are required to periodically (normal) and non-periodically (urgent) send sensor data to the service platform based on the trigger defined by the service providers.

The service platform collects and manages data and configurations related to the services. Generally, each service has its own data and configuration set, simply called resources.

The service providers in the service domain have a service agreement each other for unified services.

The Smartphone has a navigation and car sharing application.

5.2.9.5 Analysis

Trusted data collection and aggregation

Data should be trustworthy from devices (sensors) to gateway (smartphone) service platform. Devices produce data, and data is collected in a service platform. And, data is transmitted from service platform to devices. Devices report their status to the service platform via gateway. When data is produced and transmitted to other entity, trustworthiness of data is required to be maintained.

Trusted data process and analysis

Information which is processed by service platform and application should be trustworthy. Applications send registration information with proper access right of the resources and grant that request to service platform. Service platform detects changed status by processing collected data from devices and notifies to applications. Service platform provides payment information to applications. Since the gateway and service platform manipulate collected data, the trustworthiness of information (i.e. processed and analysed data) is required to be maintained in each process.

Trustworthy application

Car sharing system use case has multiple service providers (applications), so trustworthy application and interactions between applications are important. Two applications exchange data and information (e.g. location information, transaction information, etc.) to provide proper services. Since applications handle many data and information, the trustworthiness of application is required to be maintained in each process

Privacy: user profile information is used to find authorized user. User's payment information is propagated to service platform and applications. User profile and payment information contains many user privacy data (e.g. location, amount of payment, credit card information etc.). Privacy preserving is required to consider operating system.

5.2.10 Trust provisioning of mobility management

5.2.10.1 Description

Figure 11 describes handover scenario in mobility management as a user using User Equipment (UE) moves one network to another network. Handover (or handoff) refers to the process of transferring an ongoing session connected to the network to another channel.

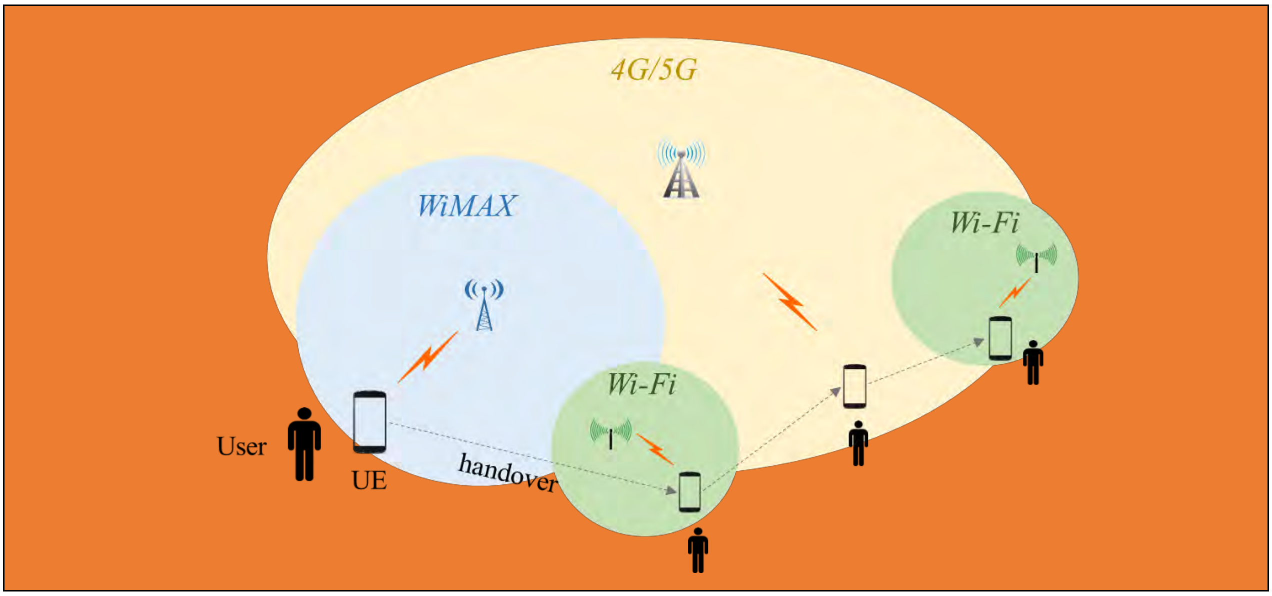


Figure 11 – A handover scenario among heterogeneous mobile networks

To control handover between different mobile networks, it is necessary to identify the candidate list of Point of Attachments (PoAs) currently accessible by an UE. Based on this information, the UE can choose one of the reachable PoA to establish a new communication link. For the network selection, the handover control function defined in [ITU-T Y.2804] may get some information such as signal quality or available resources of the candidate PoAs. Trust may be applicable during network selection.

5.2.10.2 Actors

Network provider: includes resources and trust-related properties such as QoE (previous experience of network usage), and available bandwidth, etc.

User: user profile, previous activity, etc.

Device: device profile, available network interface, etc.

5.2.10.3 Analysis

Need to make a process of trust provisioning in terms of:

- Overall flow diagram starting from development of simple trust metric or index;
- Trust provisioning will be more accurate or acceptable when data is accumulated or new technologies are developed.

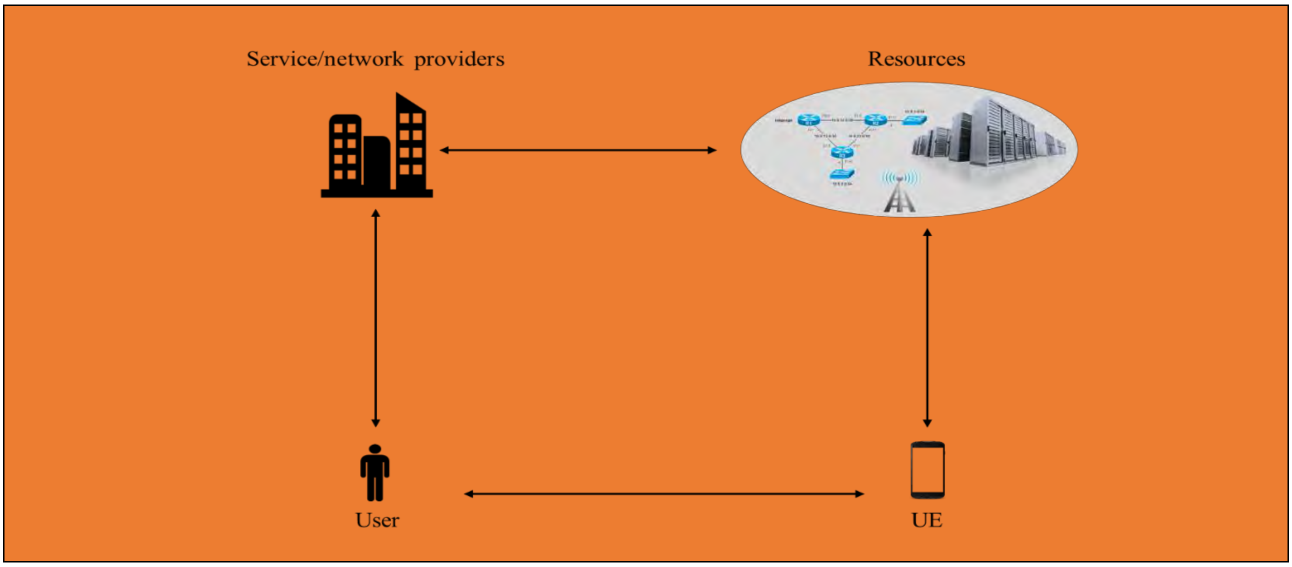


Figure 12 – Trust entities and their relations in mobility scenario

5.2.11 Smart Building use case

5.2.11.1 Description

Smart building might reveal descriptions of a building of the upcoming from imaginations. Nonetheless, the realism is smart buildings available nowadays with increasing in their numbers particularly, the huge growing in the numbers of M2M services provider and users smart devices in term of innovating and using these sensors devices, specifically, among enterprise buildings around the world. In fact, the smart devises are available in different shapes and uses, which connect to each other through gateway platform. The gateway platforms are linked through Internet to edge cloud computing (e.g., fog computing) services, which is offering environment of computing such as applications, processing and storage for smart devices as areas of smart grid. This will help to create smart building systems such as, smart home, smart health care services and smart educational services. Smart building enterprise has amalgamation between smart devices to create autonomous environment [104].

By applying urbane building automation systems to integrate individual building systems, smart device M2M services provider could have an excellent chance to increase their sales and marketing for their smart devices around the world by influencing on enterprises in current time to move toward smart building systems. Seamless incorporation relied on building automation systems carries a numbers of advantages to both the smart device M2M services provider and the larger enterprise [105]. These advantages for enterprises to adopt smart building framework are variety starting from control centre unite such as; reducing overall expenses in term of decreasing energy consumption or workers number, also, building control in case of video monitor and doors control.

Moreover, building detection in term of noticing fire or gas leak. Building performance in case of supporting decision making and improving staff productivity. Consequently, smart building system is a use case as real example for enterprise requirements to enhance trust in case of heterogeneous sensors, gateways and control centres unite. There are various smart devices using different protocols such as USB, ZigBee, 6LoWPAN and Bluetooth, also, many of M2M services provider innovate smart devices and professional users (enterprises) utilize sensor devices, the main aim of this use case is allowing these components to create a high standard of Trust [105]. (See Figure 17)

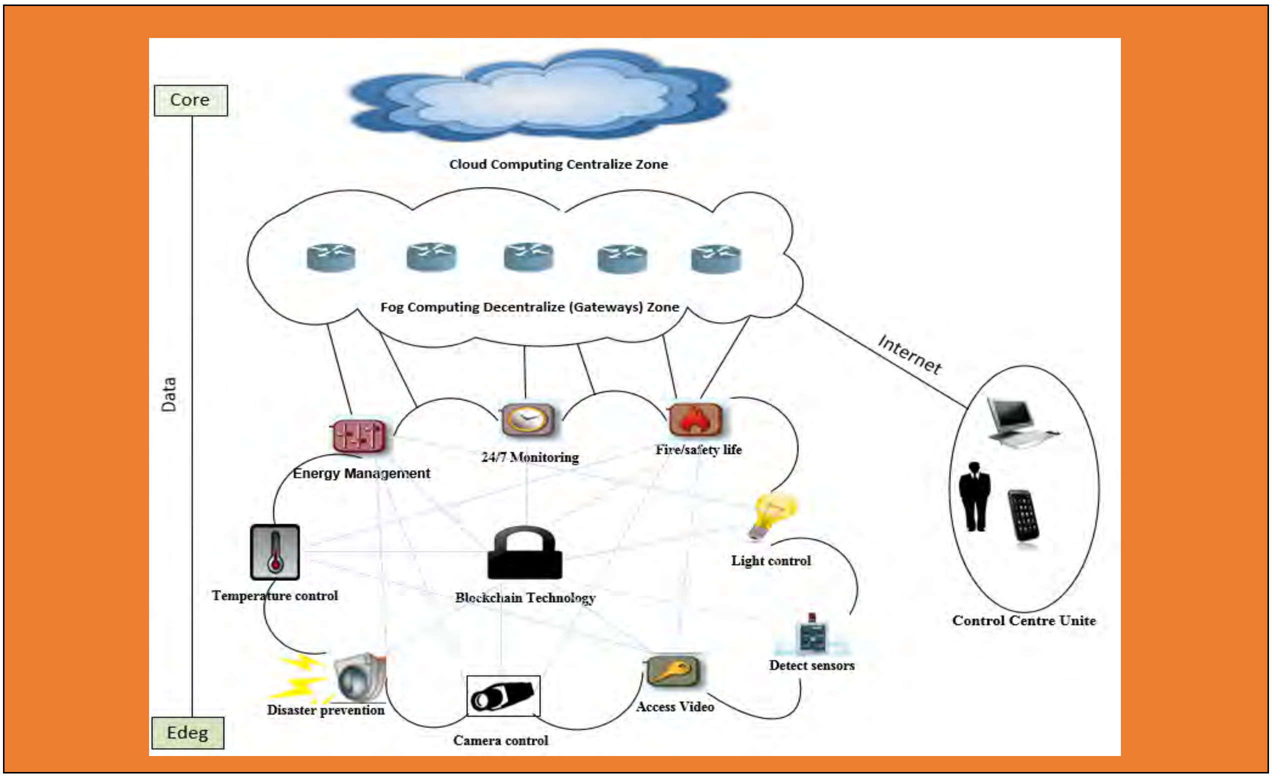


Figure 13 – Smart building with M2M connections

5.2.11.2 Actors

M2M services provider: a company that produces and offering smart deceives (sensors) in different form and use, they also provide sensors in diverse protocols, which will use by final users such as single user or enterprise.

User: an enterprise, which is interested to convert from ordinary enterprise to become smart enterprise in term of smart building systems.

Sensor device: smart devices, which are available in different form and uses to help a company to be a smart building system such as fire detecting sensor, gate-opening sensor and light switcher sensor, and their relation to each other in term of M2M, these sensor devices usually provide by M2M services provider.

Gateway: A sensor connecter, which is linking smart devices in the different floor and location within smart building enterprise, through internet to get computing services, which provides by edge cloud computing services in case of exchange the data.

Control centre: The heart of the smart building, entirely data collected by the sensor device report to the control centre and all instructions send from the control centre. The control centre is responsible of the adjusting of the smart devices installed everywhere in the smart building.

Computing provider: edge cloud computing services, which is offering environment of computing such as applications, processing and storage for smart devices as areas of smart grid.

Trust technology: a technology, which is applying in enterprise smart building to enhance trust in case of M2M service relationship, among environment of heterogeneous sensors, for example Blockchain.

5.2.11.3 Analysis

Table 2 – Analysis of Smart Building Enterprise use case

Stakeholders	Main Advantages	Side advantages
M2M services provider	Providing full facility services of smart building system, such as sensors, gateway and control centre.	Increasing their sales and marketing by enhance trust reputation.
User	Applying smart building system, which will reflect on their cost, productivity and performance.	Controlling entire a company by using smart devices
Sensor device	Executing enterprise orders in the smart way.	Producing useful data could help enterprise
Control centre	Distributing the commands between the gateways in different locations.	Organizing the duties in the smart building
Gateway	Connecting sensors devices with internet	Forwarding the orders from control centre to sensors
Computing provider	Providing computing environment through the gateways platform	Supporting smart sensors in term a huge data
Trust Technology	Creating environment of Trust among M2M	Tracking any malicious in P2P Network

Smart building enterprise has merger between smart devices to create autonomous environment. Smart device M2M services provider could have an excellent chance to increase their sales and marketing for their smart devices, to do that it needs to increase the trust among sensors, devices, control centre with gateway connection, also gateway with other smart devices in different floor connection. Therefore, it requires Blockchain technology to track the transactions between sensors device to block any malicious, which will reflect on M2M services providers and the (users) enterprises.

5.3 Summary of User Cases

Table 3 – Summary of user cases in Section 5

ID	Use case	Purpose	Method	Actors	Considerations for measuring trust
Trust provisioning of ICT infrastructure					
0	Trust-based routing protocols	Selecting trustworthy routing path	Trustworthy level → Trust routing table	Trust Platform Node as trustor Node as trustee:	Routing data Data from trust agents Node data
0	Trust-based malicious node detection and prevention	Resisting and remediation of entities form Sybil attacks	Trust level → Continues trust evaluation	Trust Platform Nodes	Node experience History Trust agents Relationship
0	Trust-based access control mechanism	Managing access control in trustworthy manner	Trust level → Usage behaviors	Trust Platform Nodes	Data from trust platform, nodes Social/business relationship

ID	Use case	Purpose	Method	Actors	Considerations for measuring trust
0	Multi-hop device-to-device network path selection	Selecting appropriate network	Trust level → Right of accessing device	User A A's device User B B's device	**Social** data (relationship) CoI (Community of Interest) Device data
0	Trust provisioning of mobility management	Controlling handover among heterogeneous mobile networks	Level of trust → Network selection	User A A' device N/W service provider	QoE (previous experience of network usage) **Social** data such as user profile, previous activity **Device** profile, available n/w interface
Trust provisioning of Services and Applications in IoT					
0	Home energy management	Managing energy consumption	Trustworthy energy-related data → Providing information	User Service provider Service platform Home gateway Home appliance	**Devices** data Energy-related device data such as smart meter, lighting, TV, smart plug, surveillance camera, and etc.
0	Smart office service	Managing office facilities	Trust level of → Usage rights	User Smart office Smart office provider Trust mgt.	**Social** data Social/business relationship Membership
0	Trusted Data Usage Mechanism in Smart Cities	Service Sharing	Trustworthy data → Transparent UE history	Trust Platform Data Usage Manager Data Owners Data Consumers	**UE** data **Social** data **Operator data**
0	Document sharing	Sharing document appropriately	Trust value → Right of accessing document	User A A's Device User B B' device	**Social** data (relationship) CoI (Community of Interest) **Device** data
0	Secure Remote Patient Care and Monitoring	Provide trustworthy medical service remotely	Trustworthy communication → Usage rights	A Patients E-Health application service providers Care givers M2M service providers, network operators Trust Platform Access Control Policy and Mapping Manager	categorization rules Redaction engine. policy engine authorization policies authorization engine/server application server Trust Platform
0	Trust for Time critical and Real-time applications	Preserve privacy of both the network and users	Trust value → Right of access	User Provider Operators/Service Providers	User data Information from Intermediate nodes Server data

ID	Use case	Purpose	Method	Actors	Considerations for measuring trust
0	Trust provisioning of used car transaction service	Mediating transparent used car transaction	Trustworthy data → Transparent car history	Seller (User A) Seller's car Service broker Trust mgmt. platform Buyer (User B)	**Social** data **Vehicle** data External Data from 3rd parties such as insurance company, public organization, social network services.
0	Trust provisioning of car sharing system	Promoting trustworthy car sharing	Trustworthy data → Usage of shared car	User A A' device Sensor attached in sharing car Service platform Service provider	**Sensor (Device)** data **Social** data **Operator data**
0	Trust in smart Building system	Enhancing the Trust between M2M to support Services providers and users	Applying Blochchain Tool to track any malicious in P2P network	M2M services provider User Sensor device Control centre Gateway Computing provider Trust Technology	Trust value for smart devices data in terms of (QoS) requirements : Reliability Availability Turnaround time Data integrity

Trustor and trustee relationship can be represented by receiver and sender relationship. It is plausible trustee provides trustworthy data to make a trustor trust in a trustee. For example, home appliance devices (trustee) provide energy-related data for users (trustor) to control these devices in use case of home energy management. In this sense, trustee is an information sender and trustor is a receiver.

6 A strategy for trust provisioning of ICT infrastructure, services and applications

This section proposes trust taxonomy in different domains in order to identify important issues for trust provisioning in the ICT infrastructure, services and applications, and describe a strategy for solving these issues, particularly considering trust provisioning process.

Trust and reputation are the pillars of many social phenomena that shape the Internet socio-economic scene. It is important to have a big picture of Trust in the future network in order to successfully develop and deploy trust into applications and services of ICT infrastructure. Figure 1 is the taxonomy providing initial insights into the ways trust benefits can be felt.

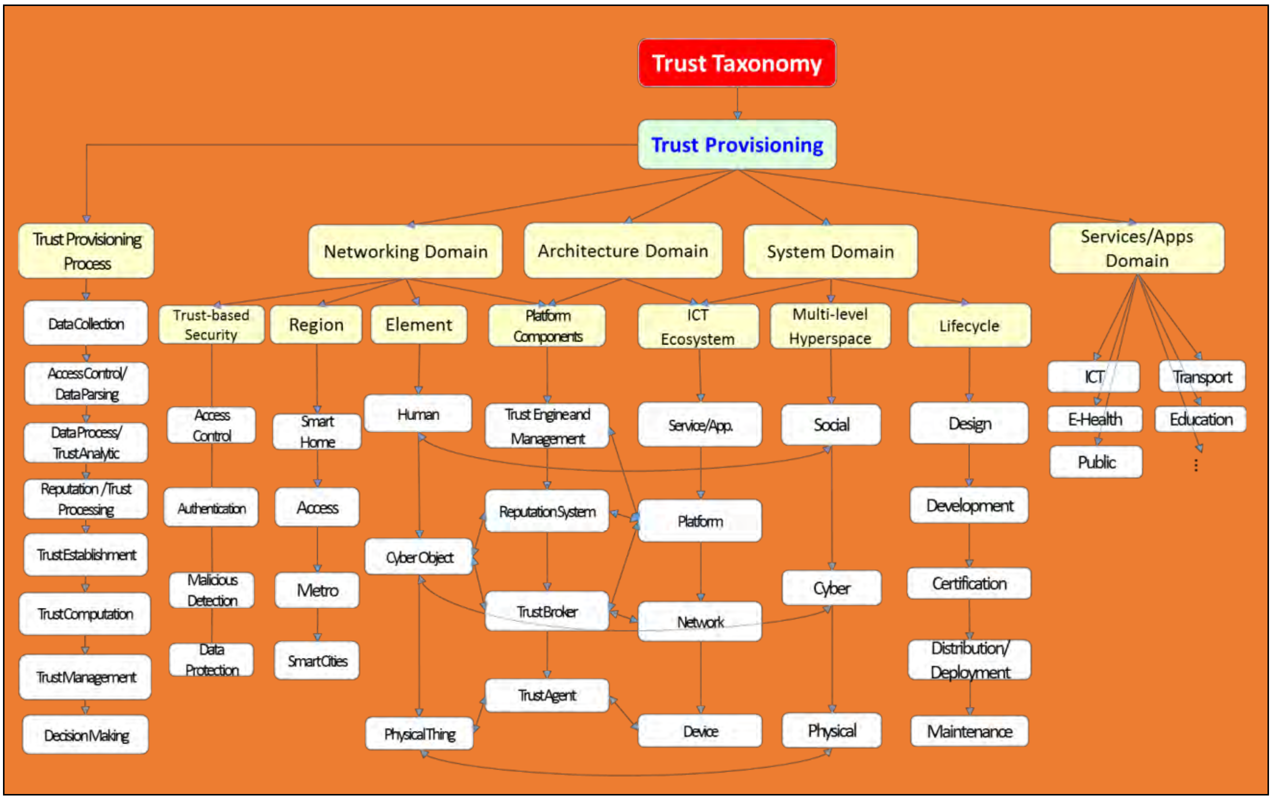


Figure 1 – Overall Trust Taxonomy in different domains

Due to huge domain of trust usages, there are a large number of challenges for designing, developing and deploying a trust platform for ICT systems. This section follows the structure of the overall trust taxonomy as illustrated in Figure 1 for briefly describing trust provisioning strategies of ICT infrastructure.

6.1 Understanding of Trust Taxonomy

Generally, trust involves in all aspects and in all perspectives of any systems. For example, in perspective of Networking Domain, trust can be provisioned into Security, Region, and Element aspects as illustrated in the Figure 18. There are four basic domain perspectives, namely Networking Domain, Architecture Domain, System Domain and Services/Apps Domain. In each domain, there are some aspects in which trust can play a role for better improvements. It is necessary to consider trust design, trust development and trust deployment by breaking down to all necessary processes.

Basically, the required number of processes of trust provisioning is different from each domain and each aspect. And the detailed specification of each provisioning process is also different among these domains aspects. However, the generic trust provisioning is same as in all domains and aspects. A trust infrastructure consists of 8 fundamental processes as illustrated as "Trust Provisioning Process" category in the Trust Taxonomy figure. They are Data Collection, Data Access Control and Data Parsing, Data Process and Trust Analytic, Reputation and Trust Processing, Trust Establishment, Trust Computation, Trust Management and Decision Making.

In the remaining of this section, it describes in details of all the Trust Provisioning Processes. These processes are generic and used for all domains in the trust taxonomy. After that, it briefly mentions several domain-specific trust provisioning strategies in each particular domain.

6.2 Trust Provisioning Processes

6.2.1 Data Collection Strategy

A significant amount of trust related data needed to be collected and handled into an intelligent way. There are many strategies for big data collection and big data storage that can be used in the Trust Agents for reputation information, interaction history, sensor data, user related data, service/app related data, and context related data.

Each service or application will require its own strategy with elements of complete enumeration and sampling. Over time some aspects of a data collection strategy may move from complete enumeration to sampling (or vice versa), particularly as knowledge is developed and requirements or resources change. Sampling strategies are often punctuated by complete enumeration from time to time in order to re-evaluate baseline data.

It is not feasible to construct a perfect strategy for any one fishery or subsector that will meet all requirements for all time. Flexibility and the adoption of alternative approaches must form a key component of any strategy, whether it is designed for assessment of fish stocks, the evaluation of markets or the assessment of community dependence on fisheries.

In general, however, any strategy will require the following steps:

- Evaluate existing data sets in relation to the objectives of the programme, including accessibility of the data.
- Describe the operating characteristics of the sector or subsector.
- Decide on the approach to be taken: complete enumeration or sampling, including cost-benefit and cost effectiveness analysis and an evaluation of operational considerations.
- Design methods according to the approach adopted, including the form of stratification to be used in sampling;
- Implement a test phase to validate the method, including participation by other stakeholders;
- Establish a continuing feedback mechanism between data sources and data users to ensure that data types, quantity, quality and origin are consistent with the requirements for determination of the performance indicator.

It is needed to understand big data strategies and the techniques used with each strategy. For example in the Figure 2 the first dimension is labelled business objective. When developing big data capabilities, companies try to measure or experiment. When measuring, organizations know exactly what they are looking for and look to see what the values of the measures are. When the objective is to experiment, companies treat questions as a hypothesis and use scientific methods to verify them.

The second dimension is labelled data type. In their normal course of functioning, companies collect data on their operations (e.g., sales) and capture it in their database that has a structure or schema. It is called as transactional data. In other instances, companies deal with data that come from sources other than transactions and are typically unstructured (e.g., social media data). This combination results in four quadrants, each representing a different strategy: performance management, data exploration, social analytics, and decision science.

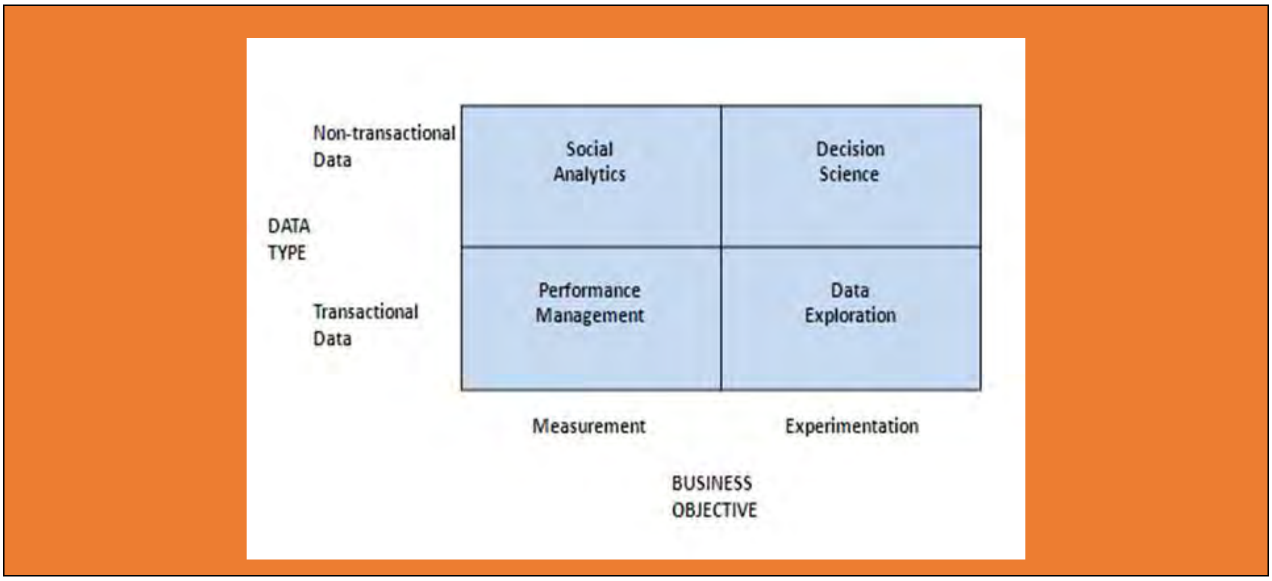


Figure 2 – Data collection dimensions and strategies

6.2.2 Data Parsing and Access Control

The collected data in the data repository should be parsed in an appropriated manner for task-oriented, robust, flexible and efficient data accessing and information extraction. Those offering connected devices "should be clear about what data they collect, for what purposes and how long this data is retained."

For the data access control strategy, data obtained from connected devices is "high in quantity, quality and sensitivity" and, as such, "should be regarded and treated as personal data."

The strategy needs to start with a big data parser and management platform that delivers in core areas:

- Big data integration;
- Big data governance and quality;
- Big data security.

6.2.3 Data Processing and Trust Analytic

6.2.3.1 Trust Model and Trust Metrics

Many have recognized the value of modelling and reasoning about trust computationally. A wide of variety of literature now exists on trust, ranging from specific applications to general models. However, as many authors in the field have noted, the meaning of trust as used by each researcher differs across the span of existing work.

Two common ways of determining trust are through using policies or reputation. Several authors adopt these categories from [13], as they best describe the distinction we observe between the "hard evidence" used in policies, and the estimation of trust used in reputation systems. Policies describe the conditions necessary to obtain trust, and can also prescribe actions and outcomes if certain conditions are met. Policies frequently involve the exchange or verification of credentials, which are information issued (and sometimes endorsed using a digital signature) by one entity, and may describe qualities or features of another entity. For example, having the credential of a university degree means its holder has been recognized by the issuing university as having a certain education level. This associates the holder with the university and to those educated in his field. Credentials can be used when trust in the entity itself is unknown, but there is existing trust in what is associated through the entity's credentials.

Reputation is an assessment based on the history of interactions with or observations of an entity, either directly with the evaluator (personal experience) or as reported by others (recommendations or third party verification). How these histories are combined can vary, and recursive problems of trust can occur when using information from others (i.e., can I trust an entity's recommendation about another entity?). At a basic level, both credentials and reputation involve the transfer of trust from one entity to another, but each approach has its own unique problems which have motivated much of the existing work in trust.

A trust decision can be a transitive process, where trusting one piece of information or information source requires trusting another associated source. For example, one might trust a book and its author because of the publisher, and the publisher may be trusted only because of the recommendation of a friend. Winslett's work [14] in policy-based trust uses (or refers to) "credential chains" (the issuer of one credential is the subject of another), the majority of transitive trust computation has been focused on using reputation. A key recent example of this approach is Golbeck and Hendler [15] [16], which describe how trust is computed for the application TrustMail. Reputation is defined as a measure of trust, and each entity maintains reputation information on other entities, thus creating a "web", that is called a web of trust.

6.2.3.2 Trust Ontology

It is needed to use of a knowledge base for storing trust models and trust related context specific data that does not alter the calculations or use of trust related information, such as reputation (entity opinions). The knowledge base should clarify how information is stored and accessed and ontology is one of the prospective solution. For example, a trust network can be seen as a structure capturing metadata on a web of individuals with annotations about their trustworthiness. Considering social network as our context, a trust network can be seen as an overlay above the social network that carries trust annotations of the metadata based on the social network, such as user profiles and information.

Social networks are gaining increasing popularity on the web while semantic web and its related technologies, are trying to bring social networks to their next level. Social networks are using the semantic web technologies to merge and integrate the social networking user profiles and information. Such efforts are paving the path toward semantic web-driven social ecosystems. Merging and integrating social networking data and information can be of business value and use to web service consumers as well as to web service providers of social systems and networks. Ontologies, at the core of semantic-web driven technologies lead the evolution of social systems on the web. Describing trust relations and their subcomponents using ontologies, creates a methodology and mechanism in order to efficiently design and engineer trust networks.

"Structure of a given system is the way by which their components interconnect with no changes in their organization". Determining the structure of a society of agents on a trust network structure within a semantic social system, can help us determine the organizational structure of a system. Having this capability, an organization's certain factors such as flexibility, change capacity, etc., can be determined.

The work by Golbeck and Hendler uses ontologies to express trust and reputation information, which then allows a quantification of trust for use in algorithms to make a trust decision about any two entities. The quantification of this trust and associated algorithms are called trust metrics. Given an existing quantification of trust, approaches exist to transfer that trust to other entities, which may not have been evaluated for trust. One area of research assumes we are given a web of trust, where a link between two entities mean a trust decision has been made and the value of that trust is known. How trust decisions are made do not matter, as long as the resulting trust values can be quantified. If there is no link between a pair of entities, it means no trust decision has yet been made. This is the case in which trust transitivity can be applied, a simplified example being if A trusts B and B trusts C, then A trusts C. Building on work in reputation management (described earlier as empowering individual agents to make trust decisions instead of a single, central authority making decisions for them), multiple researchers are exploring ways to transfer trust within a web of trust.

6.2.4 Reputation and Trust Analytic

Reputation is third-party information and is considered as both social product and social process. It is a social product because it is produced by opinions of entities; on the other hand, reputation is as an information flow influencing in the social IoT. Reputation should not to be confused with trust but partially affects the trust. There are several well-known reputation systems in the context of e-commerce systems, such as eBay [17] and Internet-based systems such as Keynote [18]. These systems use a centralized trust authority to maintain the reputation and feedbacks. There are also some distributed approaches for reputation mechanisms in which reputation has been built over time based on feedbacks from both customers and entities behaviours. These systems use several heuristics for updating reputation and integration due to the use of deterministic numbers for representing reputation (See Figure 3).

In this sense, Recommendation is considered as the opinion of trustor-related entities to trustee to help the trustor judge the trust to trustee. The reason to separate Reputation and Recommendation is that natural human information processing usually relies on both surrounding suggestions (e.g. from friends, relatives, and colleagues) and global opinions (e.g. ranking/ratings levels in public media).

Therefore, a reputation system is needed to build for managing Reputation and Recommendation TMs. It is one of the most important parts in the trust service platform which consists of four basic modules called Reputation Measurement & Evaluation (which is also called Feedback Mechanism), Propagation and Maintenance. A reputation ontology with a social IoT relationship map is proposed in order to put all the reputation-related knowledge of social IoT services together and presented in a structured form. A machine learning algorithm and a reasoning mechanism are used for the measurement and evaluation process. Then a propagation process is conducted to deal with many aspects of transmission of the reputation; and a propagation maintenance is used for the modifications in both reputation structure and content through the network and over time.

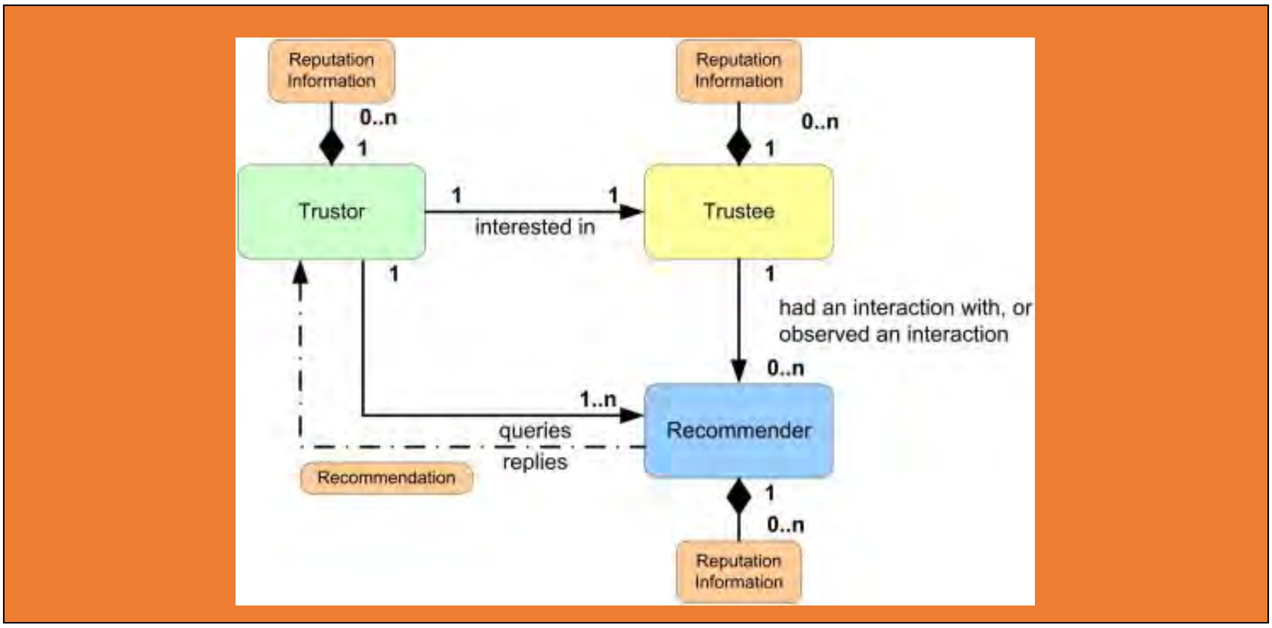


Figure 3 – A reference model for reputation systems

The reputation system should deal with some typical challenges such as bootstrap new services and feedback motivation and customers support. In some scenarios, customers do not need to understand the whole complicated feedback evaluation process, the system can automatically calculate feedbacks on behalf. For example, feedback of a web service could be derived from some QoS technical properties such as reliability, availability, capability, delay and jitter. The system also needs to deal with some post-processing phases such as matching, unfair feedbacks, risk remedies (unexpected events occur), self-adjustment, bias detection, reward and punishment.

6.2.5 Trust Establishment

It is needed to develop a protocol that could establish a level of trust among interacting agents. In order to provide that necessity, there are some of trust establishment protocols available in the literature and with possibility of enhancing it further in future work.

Establishing trust relationships between peers is an essential approach to prevent threats. For example, in Peer-to-Peer (P2P) systems, peers often interact with unknown or unfamiliar peers. P2P systems benefits highly from trust mechanisms for a peer to decide whether another party is trustworthy by using the knowledge of others.

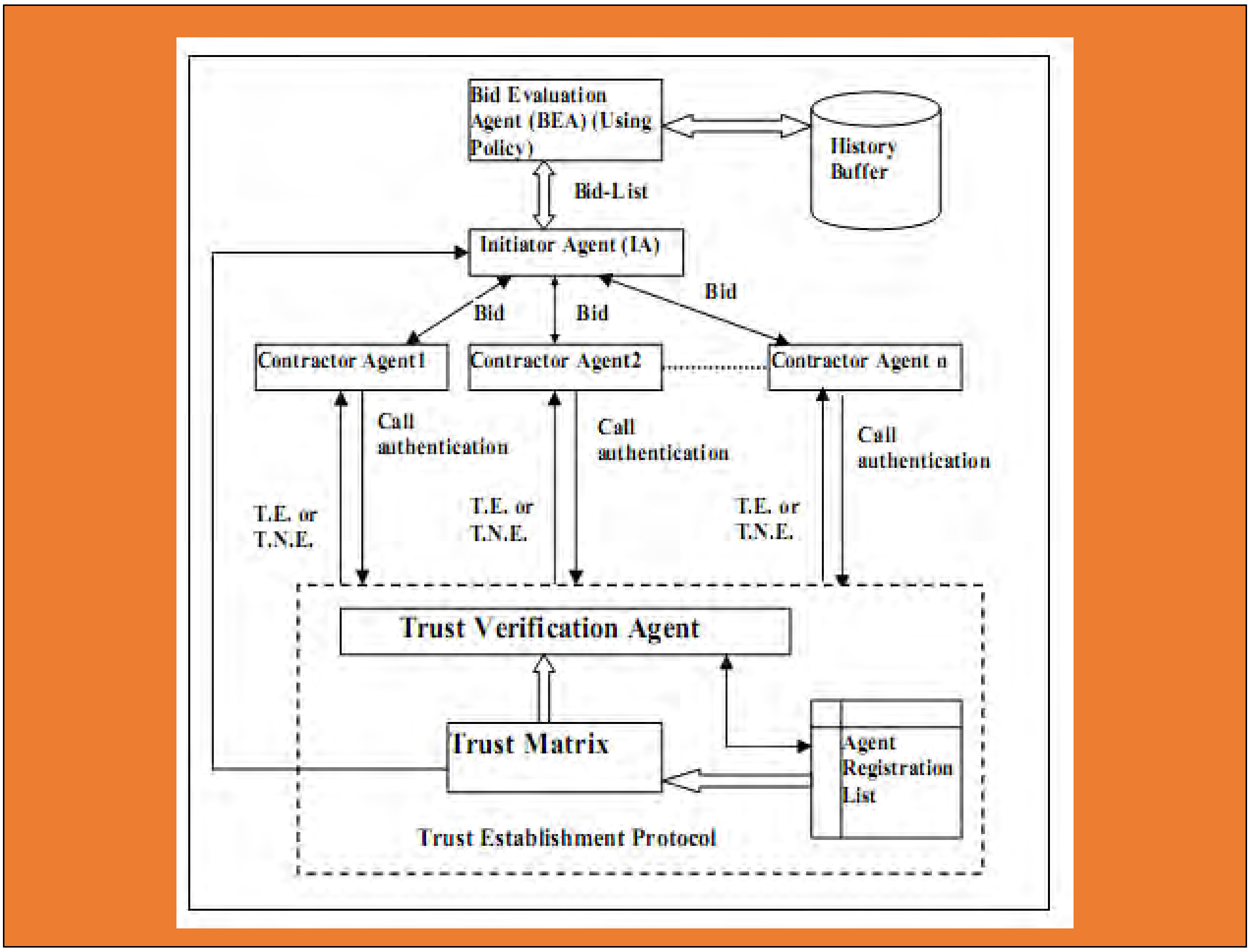


Figure 4 – Trust Establishment Contract Net Protocol Architecture [19]

The high level view of Trust Establishment Protocol (TEP) is shown in the Figure 4. The protocol mainly comprises of an Initiator Agent (IA), Bid Evaluation Agent (BEA), Contractor Agent (CA) and TEP, wherein TEP further comprises of Trust Verification Agent (TVA), Trust Matrix (TM in Figure 21) and Agent Registration List (ARL). The IA sends the list of keywords to be searched in the form of Call for Proposal (CFP) to the perspective CAs. CAs are not allowed to directly revert back to IA unless or until they possess Trust Certificate (TC). Therefore instead of reverting back to the respective IA, the CA executes TEP. Now, when a CA calls for authentication to TEP the TVA gets activated and in first instance it demands for certificate that authenticates the agents as registered agents. In turn CA presents all the certificates, it is possessed with. The TVA verifies the same and consults ARL if the same CA is a registered agent and had delivered the reliable results in past. If an entry for the same exists, the TM is consulted to compute trust percentile.

6.2.5.1 Trust Establishment Policy

To establish trust metrics and calculate trust score, there are a large number of properties that need to take into account. These properties could be trust-related attributes as well as ICT environment-related attributes. These policies for trust establishment vary from domain to domain, aspects to aspects. However, there are several categories for the policy which are in all ICT infrastructure domains.

6.2.5.1.1 Social Patterns

Exchange is a central and traditional object within the social sciences, notably in economics science where market exchange analyses circulation of goods and services between agents (exchange is trust regulated, that is to say mostly unknown individuals are implicated), thus in sociology and in anthropology where the key concept is social exchange, which gathers all kinds of non-economics exchange between individuals. Social patterns may be distinguishing themselves on two strongly differentiating variables.

In one hand, the social distance that separates two individuals: this social distance can be loose in the case of a market or an organization (this is the reason why the contract - commercial or labour - is so important to support exchange between unknowns). Or, at the opposite, this distance can be strong as often in the case of the family (included friends, neighbours, and other kind of strong social bonds and where exchange is gift-regulated) and network (as a community of individuals that share something like a life experience, an interest in something, etc.) where familiarity, real or virtual, allows individuals to exchange without contracts. On the other hand, the degree of structure of the institution defines the degree of liberty of which the actors can dispose in order to exchange (notably the choice of the partner and the nature of exchanged things). This degree can be loose, as in a network or a market where individuals have all latitude to choose themselves and to exchange what they want to or strong as in a family or an organization/institution where exchange is more constrained by formal hierarchies and rules.

- Family: a community with a strong social distance and a strong degree of structure.
- Network: a community with a strong social distance and a loose degree of structure.
- Market: a community with a loose social distance and a loose degree of structure.
- Organization: a community with a strong social distance and a loose degree of structure, as a company.

6.2.5.1.2 The Lifespan of Elements of Reputation and Recommendation

In an environment where exists neither a central regulating entity nor authorizing accreditations or the revocation of objects, a fair assumption is let’s make the time: the data elements are automatically revoked after their lifespans expire. A temporal semantics can easily be added to an element of reputation-related properties if both parties agree on a creation/expiration date. This information is simply concatenated with existent data before the signature. Nevertheless, nothing guarantees that the both entities will choose correct values for this information: the reality may be different (dishonest devices or simply malfunction). However there is no real benefit to cheat on these values. Indeed, each entity may filter a received element of reputation and recommendation according to its local trust policy: an element can be rejected if its creation date is too old, its validity period is considered to be abnormally long although being still valid or if its lifespan is of course expired. No information having an infinite lifespan in the system is guaranteed by this timestamp.

6.2.5.2 Reputation Boot-Strap and Incentive Policies

Basically, bootstrapping techniques is required for the new-coming entities and incentive policies for those who have already established some history of experiences Figure 5.

It is important to initialize trust rates for new services, which have no rating history, the so-called trust bootstrapping process. Trust bootstrapping assists the requestors in their service selection decision. Trust bootstrapping is the initial step in trust building process. Trust bootstrapping is important for reliable interaction with services and service providers that are new to the system.

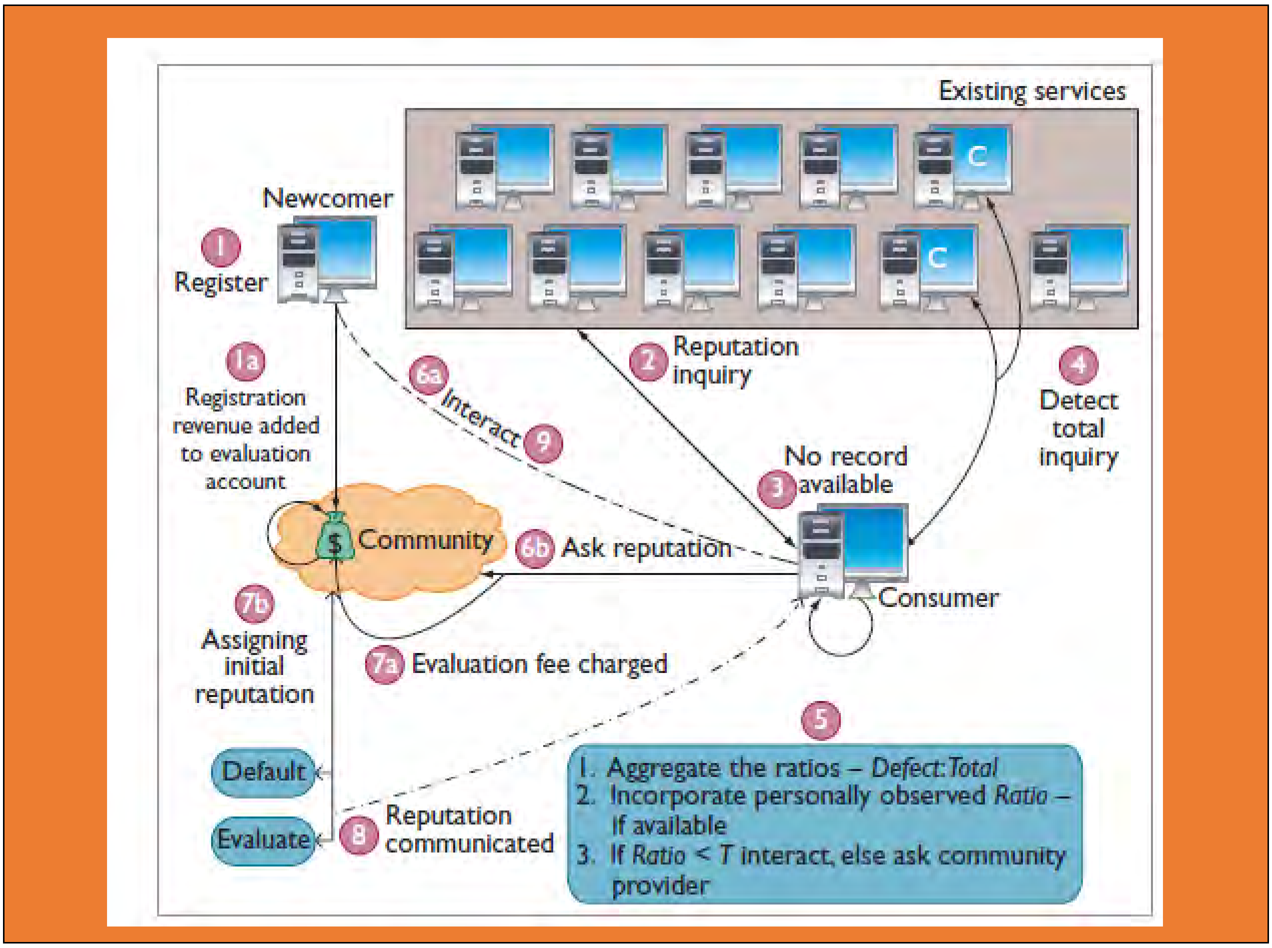

Existing services
C
C
Newcomer
1
Register
1a
Registration revenue added to evaluation account
6a
Interact
9
2
Reputation inquiry
4
Detect total inquiry
No record
3
available
$
Community
6b
Ask reputation
Consumer
7b
Assigning initial reputation
7a
Evaluation fee charged
5
Default
Evaluate
8
Reputation communicated
1. Aggregate the ratios – Defect:Total
2. Incorporate personally observed Ratio – If available
3. If Ratio < T interact, else ask community provider

Figure 5 – Reputation bootstrapping using an adaptive approach

Trust bootstrapping is a mechanism to assign trust rate for a new service that its trustworthiness is unknown and before having any requestor interacting with it. Trust goes through three development phases: trust building, stabilising trust, and dissolution [20]. Most studies assume a system where trust already exists (i.e. stabilising trust phase). However, it is important to initialise trust rates for new services and service providers (i.e. building trust phase). Building trust phase is a crucial stage in any trust relationship. Trust bootstrapping is the first step in the trust building development phase and the important step in the trust establishment process. It is important to establish trust for service providers and select a service based on its provider's trustworthiness in addition to the service's own trustworthiness. The trustworthiness of a service provider can enhance the requestor's trust in its services. A requestor can select a service from providers of the highest level of trust. Considering trustworthiness of service providers supports trust bootstrapping the providers' new services. For example, if a provider is known to be trustworty, the requestors will trust the provider's services and encourage to select its new services.

A low initial reputation is assigned if the rate of maliciousness (ratio of defective to total transactions) is high, and high initial reputation is assigned otherwise.

6.2.6 Trust Computation

The goal of this sub-section is to provide a brief idea about the existing strategies available in the research literature and identify the vital points that needs to be addressed and enhanced.

The paper [21] suggests the combination of trust, mobility and QoS estimations to provide a more reliable and rewarding pervasive service experience in MANET. The decentralized trust management model allows the dynamic calibration of the service selection, based on a history of service provisions; this should in turn promote co-operative behaviours among the various peers. An effective lightweight metric needs to be devised to allow communication of expected future movements, a subject of further work.

With respect to trust provisioning in health care services and applications, the paper [22] presents the importance of inclusion of trust into the development of software systems. Furthermore they have identified that several factors should be considered in the process of software development.

There are a number of recent papers which aim to incorporate security engineering into mainstream software engineering. Yet, capturing trust and security requirements at an organizational level, as opposed to an Information Technology (IT) system level, and mapping these into security and trust management policies is still an open problem. In this regard, [23] discuss a set of concepts founded on the notions of ownership, permission, and trust and intended for requirements modelling. It also extends Tropos, an agent-oriented software engineering methodology, to support security requirements engineering. These concepts are formalized and are shown to support the automatic verification of security and trust requirements using Data log. To make the discussion more concrete, they have illustrate the proposal with a Health Care case study.

Related to smart grid applications, [24] discusses the trust management toolkit, which is a robust and configurable protection system augmentation, which can successfully function in the presence of an untrusted (malfunctioning) smart grid (i.e., communication based, protection system nodes). The trust management toolkit combines reputation based trust with network flow algorithms to identify and mitigate faulty smart grid protection nodes. The toolkit assigns trust values to all protection nodes. Faulty nodes, attributed to component or communication system malfunctions (either intentional or unintentional), are assigned a lower trust value, which indicates a higher risk of failure to mitigate detected faults.

Furthermore, [25] presents an approach for modelling user trustworthiness when traffic information is exchanged between vehicles in transportation environments. Their multi-faceted approach to trust modelling combines priority-based, role-based and experience-based trust, integrated with a majority consensus model influenced by time and location, for effective route planning. The proposed representation for the user model is outlined in detail (integrating ontological and propositional elements) and the algorithm for updating trust values is presented as well.

Establishing trust relationships between peers is an essential approach to prevent threats. In P2P systems, peers often interact with unknown or unfamiliar peers. P2P systems benefits highly from trust mechanisms for a peer to decide whether another party is trustworthy by using the knowledge of others. In this regard, [26] proposes a challenge response protocol to identify malicious or unreliable peers in P2P systems.

Nowadays, WSNs appear to be mature enough to be used by various applications. These applications rely on trustworthy sensor data to control the processes. Related to this, [27] proposed a novel trust model for sensor data during their entire life cycle. Capitalizing on subjective logic, they have implemented new design operators for the combination and aggregation of opinions. Opinion on data is then used by applications for further decision making.

Relevant same area, [28] has proposed a different approach for securing information aggregation in WSNs. By extracting statistical characteristics from gathered information, this framework evaluates sensor nodes' trustworthiness using an information theoretic metric. By employing unsupervised learning algorithm, the framework can detect the compromised nodes. Moreover, with the help of the powerful Josang's belief model, the uncertainty existing in the sensory data and aggregation results is explicitly represented and quantified. Compared with the conventional schemes that are based on cryptography schemes, the proposed framework can effectively block the false data in the presence of multiple compromised nodes that would bypass outlier detection.

6.2.7 Trust Management System

There have been many proposed trust management protocols for different types of networks such as MANETs, WSNs, P2P networks and social IoT. The concept of "Trust" originally derives from social sciences and is defined as the degree of subjective belief about the behaviours of a particular entity. [29] first introduced the term ”Trust Management" and identified it as a separate component of security services in networks and clarified that "Trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships."

A trust management concerns part or all of trust properties in different contexts for different purposes and should achieve the following goals [30]:

(1) Trust relationship and decision: trust management provides an effective way to evaluate trust relationships of any two entities and assist them to make a wise decision to communicate and collaborate with each other.

(2) Data perception trust: data sensing and collection should be reliable in the trust management system.

(3) Privacy preservation: user privacy including user data and personal information should be flexibly preserved according to the policy and expectation of IoT users. This objective relates to the IoT system objective properties in general.

(4) Data fusion and mining trust: the huge amount of data collected in IoT should be processed and analyzed in a trustworthy way with regard to reliability, holographic data process, privacy preservation and accuracy.

(5) Data transmission and communication trust: data should be transmitted and communicated securely in the IoT system. Unauthorized system entities cannot access private data of others in data communications and transmission.

(6) Quality of services: QoS should be ensured.

(7) System security and robustness: trust management should effectively counter system attacks to gain sufficient confidence of system users.

(8) Generality: trust management for various systems and services is preferred to be generic that can be widely applied, which is a system objective property.

(9) Human-Computer Trust Interaction: trust management provides sound usability and supports human–computer interaction in a trustworthy way, thus can be easily accepted by its users.

(10) Identity trust: The identifiers of system entities are well managed for the purpose of trustworthy. Scalable and efficient identity management in is expected.

[31] proposed a mechanism for extracting trust information from the security system of a service based on the needs of an entity. Trust is used as a security metric between an entity and systems. [32] proposed a P2P trust model. An adaptive trusted decision making method based on historical evidences window is used to improve system efficiency. In Ad hoc network, an entropy theory based distributed trust model provided a mechanism to select trusted paths [33]. The trust value of each path is obtained through multi-layer and multi-level calculation, and someone can choose credible routes to implement the interaction. For WSN, a cluster-based layered trust scheme is characterized as a typical model [34]. Based on the trust values, a node assigns a trust state to other nodes. It calculates the trust value of the sensor nodes at each level, and choose a set of nodes to participate in the transaction. From above investigated trust solutions, some elements or attributes of trust management can be extracted:

- Service. It defines the role of the trust management. The basic idea of trust management is that the security decision needs to rely on the additional safety information provided by a trusted third party. Trust, as a “soft” third party, provides a service for the service requester and the service provider in a network system.
- Decision making - the purpose of the trust management. Trust is collected to judge the credibility of the cooperative nodes, based on which make a decision to deliver a service, select a credible routing and transmit a data.
- Self-organizing. It depicts the way of the trust management. Based on trust decision, a series of nodes or even sub-networks can be selected and self-organized to perform a certain task (i.e. forwarding the packages, sensing the data) cooperatively in network scene (i.e. IoT).

In this trust management approach, service, decision making and self-organizing are the three basic essential elements.

Trust management in MANETs is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Examples would be in building initial trust bootstrapping, coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone. In addition, trust management has diverse applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing and other purposes.

As shown in Figure 6, trust management, including trust establishment, trust update and trust revocation in MANETs is also much more challenging than in traditional centralized environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. The dynamic nature and characteristics of MANETs result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time [115].

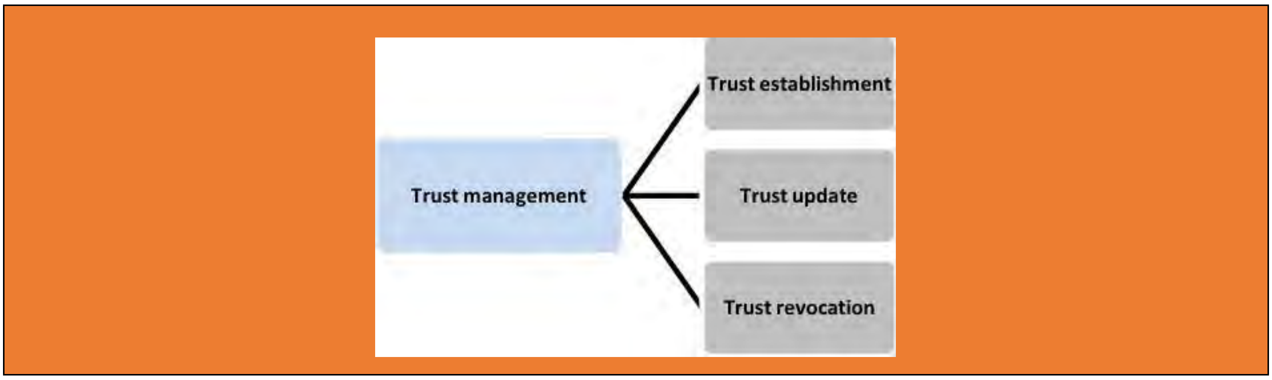


Figure 6 – Trust Management Tasks break down

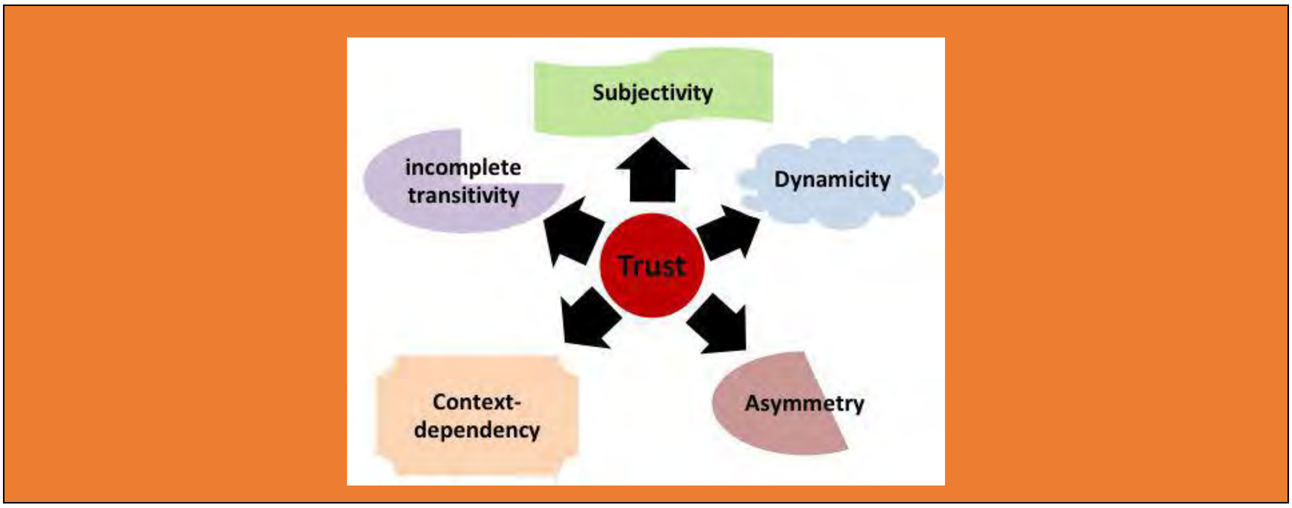


Figure 7 – General Trust Model with Trust Metrics and Technical Attributes

Due to the unique characteristics of MANET environments and the inherent unreliability of the wireless channel, the concept of trust in MANETs should be carefully defined. The main properties of trust in MANET environments can be summarized as follows (See Figure 24).

Although many trust management schemes have been proposed to evaluate trust values, no work clearly addresses what should be measured to evaluate network trust. [35] defined trust in their model as reliability, timeliness, and integrity of message delivery to the intended next-hop. Also most trust based protocols for secure routing calculated trust values based on the characteristics of nodes behaving properly at the network layer. Trust measurement can be application dependent and will be different based on the design goals of proposed schemes.

Various performance metrics that have been used to evaluate trust management schemes for MANETs. Note that a single work may use multiple performance metrics. Standard system performance metrics typically used to evaluate trust management systems; these metrics include overhead (e.g., control packet overheads), throughput, packet dropping rate, and delay. “Route usage” refers to the number of routes selected particularly when the purpose is for secure routing. “Trust level” is a recently used system metric. Example metrics using the trust level include confidence level of the trust value, trustworthiness, opinion values about other nodes, and trust level per session. “Others” indicates metrics that consider system tolerance based on incorrect reputation threshold, availability, convergence time to reach steady state in trustworthiness of all participating nodes, and percentage of malicious nodes.

6.2.8 Decision Making

Trust is collected to judge the credibility of the cooperative entities in the system, based on which make a decision to deliver a service or application. The decision making is personalized, service/app-specific and context-aware that is similar as trust. A machine learning mechanism should be used for decision making trust provisioning in which all trust score, context, and user preferences are taken into account for making good decisions.

6.3 Trust Provisioning in Networking Domain

6.3.1 Security and Privacy

Trust Establishment provisioning for security and privacy:

As mentioned before, Laih [26] proposed a challenge response protocol to identify malicious or unreliable peers in P2P systems. The proposed protocol verifies every contacted peer and records the corresponding trust value making it more effective than the traditional polling algorithms. Only in the worst case, the protocol may use the same number of messages as a polling algorithm when the requesting peer specifies the same Time to Live (TTL) and every peer returns all of its neighbours as referrals. Additionally, since all challenge information is chosen at random, malicious peers have little opportunity to tamper with the P2P systems. This protocol illustrates the details in the processes for rating, gathering, and trust construction. It can be applied in both hybrid and distributed P2P networks.

Opposed to P2P networks, in open Multi Agent Systems (MASs), agents are owned by a variety of stakeholders and they can participate or leave a system dynamically. It may be noted that participating agents are likely to be unreliable, self-interested and possessed with incomplete knowledge. Moreover, since agents are designed to behave intelligently and work in team therefore their intensions don’t remain static and hence might change with time. Hence it is required to implement a protocol that could establish a level of trust among interacting agents. In order to meet the above stated need, a trust establishment protocol has been proposed in [19] by using existing protocol called contract net protocol (CNP) to help monitoring and selecting their interaction partners.

6.3.2 Region

A trust management provisioning strategy for data usage policy in smart cities could be integrated with Smart city Data manager for data analytic and data protection

A general architecture for Smart Cities consists of three layers:

- Infrastructure Layer: The layer contains variety of IoT objects that are deployed to send their data to different applications. Because of IoT scenario, it considers that these IoT objects can belong to different domains, such as, smart sensors from the WSN domain, smart street lights/traffic signal poles from smart city domain or home alarms system/intelligent Heating, Ventilating, and Air Conditioning HVAC system from smart home/building domain. It also considers that some kind of infrastructure access/control mechanism is used by each of these domains independent of each other’s.
- Platform Layer: The layer consists of the several functional entities: Trust Manager, Ontology Manager, Policy Manager, Data Manager, and Application Manager. For the trusted data usage model, the Trust Manager will collaborate with the Ontology Manager and Data Manager to set the

policies for data usage, depending on each data owner. The Data Manager used to work with IoT data or resources from the infrastructure, and the Data Manager works with IoT applications.

- Application Layer: The layer contains end-user applications that receive the shared data from the shared infrastructure.

The trust-based data usage mechanism allows benefits such as policy enforcement to share data based on the properties of data consumers, allowing IoT shared platform to keep track of data usage history, and more importantly allow data owners to monetize their data sharing by allowing them to dynamically adjusting their policies on the fly.

6.4 Trust Provisioning in Architecture Domain

6.4.1 CT Ecosystem

Trust ontology and Trust model provisioning for social networks have been proposed for ICT ecosystem such as [36]:

Friend-Of-A-Friend (FOAF) [37] represents a vocabulary and introduces an ontology for describing a web of connected individuals. This ontology can serve as a tool to model and eventually create a network of society of users by describing personal information about each person (realizing the node itself) and by describing personal information regarding a set of users whom the user knows about (realizing the neighbours on the network). Nodes on such a network are identified by their email address and email serves as their unique identification.

- Jennifer Golbeck [38] introduces an ontology, that creates an important schema which extends FOAF by using foaf:Person, giving the users this possibility to state and represent their trust in individuals they know. Metric used to express trust is a value on the scalar range of 0-9, in which each scale represents a trust level. These levels are set as properties under the domain of foaf:Person. These levels correspond to: Distrusts absolutely, Distrusts highly, Distrusts moderately, Distrusts slightly, Trusts neutrally, Trusts slightly, Trusts Moderately, Trusts highly, Trusts absolutely, according to [38].
- Context was introduced as a property of trust. Trust is context-sensitive, as a result meaning and semantics of trust can change depending on the context. This notion is represented in this ontology under general trust or specific trust or topical trust, according to [38].
- Toivonen and Denker [39] study the trust in the context of communication and messaging. They state that there are many factors which can have immense impact on the honesty and trustworthiness of the messages we send and receive. The context-sensitivity of trust has been realized and taken into account in their work. The work focuses on drastic changes that many issues, namely reputation, credibility, reliability, trustworthiness and honesty could have, and how they affect the progress of establishing and grounding trust, according to [41]. As a result of the work being done, a set of ontologies have been defined to capture context-sensitive messaging and trust. An ontology is developed to capture and denote the role of context-related properties and information. This ontology captures the domain of message communication and exchange and describes how the context information is actually attached to the messages. This ontology is constructed mainly to visualize how trust is related to message and communication.
- Proof Markup Language's trust Ontology Inference web [40] at Stanford University, has built a semantic web-enabled knowledge platform and infrastructure. This platform is designated to help users on the network to exploit the value of semantic web technologies in order to give and get trust ratings to and from resources on the web. This process is referred to as justification of resources. Proof Markup Language (PML) contains a term set for encoding the justifications and is designated to work in a question answering fashion. PML is designated to help software agents to filter the resources on the web of semantics by proof checking them and justifying the credibility of these resources, on behalf of the users.
- With respect to metrics used for presenting the trust computational values and modelling the mathematical notion of trust, there exist two approaches: presenting a trust metric with discrete

values and metrics with continuous values. Brondsema and Schamp [41] model and represent trust and distrust in a similar fashion using continuous values. Having continuous range of values allows easier propagation of trust values, along the edges on the networks, using inference mechanisms. They represent the relationship as the class and main concept of the ontology. Each relation is directed from source (trustor) to sink (trustee). Properties of relations are wrapped under the concept of trust item. The most important feature of this work is, like Jennifer Golbeck's ontology, they have incorporated the notion of "Topical trust" in their ontology. It is used as an attribute and property, which allows to state different features and properties of a relationship. Trust topics and trust values are stated as properties of the trust relationship.

In order to describe trust relationships, an ontology is presented using Resource Description Framework (RDF), which in turn eases extending the FOAF vocabulary and profiles. Using the RDF properties, and taking into account that relationship can be described using FOAF vocabulary and ontology, then trust relationships can be described using trust ontology. Other technology that has been integrated is Web-of-Trust, which is used to describe Web-of-Trust resources such as key fingerprints, signature and signing capabilities and identity assurance. Ontology's RDF schema is made of 2 classes or concepts and 5 attributes or properties. As mentioned, the primary concept is Relationship between two people. Like most trust ontologies, there are two properties that are required for every Relationship, and they form the endpoints of every relationship; trustor and trusted using FOAF vocabulary, both trustor and trusted have foaf:Person objects as their targets.

6.5 Trust Provisioning in System Domain

6.5.1 System Lifecycle

Trust can be used for software development. It is one of the trust provisioning strategies in the perspective of system.

OPTET, an EU-funded project under the 7th Framework Programme, adopts a unique approach designed to cover all relevant trust aspects of a software development and operation life cycle. The project has developed a unified cross-disciplinary model of trust and trustworthiness, which is used to represent and quantify the trust of all stakeholders and the trustworthiness of socio-technical system.

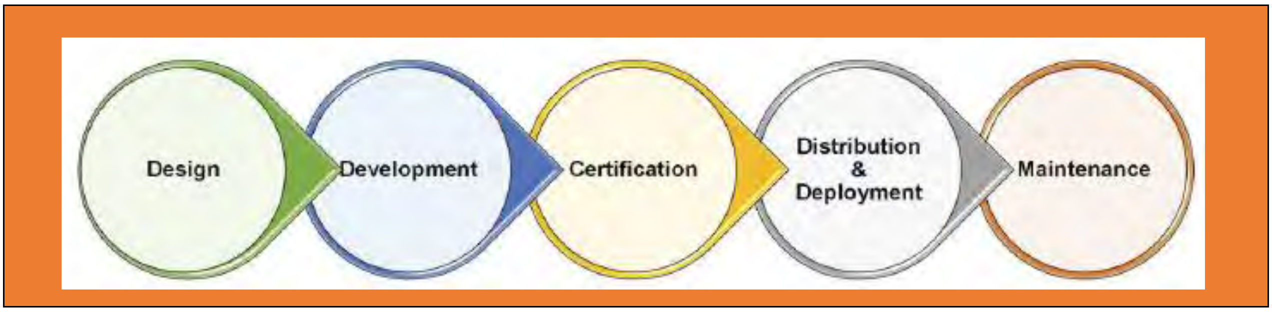


Figure 8 – The OPTET Lifecycle[2]

OPTET plans to cover the whole life cycle of trustworthy ICT systems (from requirements right through to production, via the stages of implementation, validation and integration), with a multidisciplinary approach and by taking into account the drivers of stakeholders' trust. Thus, it defines its own engineering-based development approach which describes different phases for the trust and trustworthiness attributes lifecycle in a custom software development methodology are described in Figure 25. This OPTET lifecycle identifies additional activities to the typical development lifecycle processes and verifies that trust and trustworthiness are adequately addressed, both at design time, deployment time and runtime.

[2] OPTET project website: http://www.optet.eu/about/

6.6 Trust Provisioning for Services and Applications

The entities participating in an ICT service platform need to establish and manage trust relationships in order to assert different trust aspects including identity provisioning, privacy enforcement, and context information provisioning. Current trust management models address these trust aspects individually when in fact they are dependent on each other.

Identity Provisioning

One metric that influences the identity provisioning trust is the authentication method. Identity providers that use very strong biometric authentication should be more trusted than others that use only username/password authentication. It is also possible to associate the identity provisioning trust value with a specific session, according to the type of authentication used for that session, in case the identity provider supports more than one type of authentication method. The user registration policy also influences the identity provisioning trust. Identity providers that allow users to freely register without verifying the identity of the user (e.g. Google and Yahoo) may not be trusted as much as identity providers that do not allow free registration, such as a university or a bank.

Privacy Enforcement

Trust in privacy enforcement depends upon the existence of privacy policies in the context provider and service provider, which state how the context owner's data will be handled. These privacy policies should be compared with the context owner's privacy preferences and, in case they match, it is assumed that the privacy expectations will be followed. The following metrics have also been proposed to calculate trust values regarding privacy enforcement aspects: user interest in sharing, confidentiality level of the information, number of positive previous experiences, number of arbitrary hops, a priori probability of distrusting, and service popularity in search engines. The number of arbitrary hops is related with identities issues and the chain of certificate authorities between the source and the target of the information. Privacy enforcement trust values can be also obtained from trusted third parties specialized in privacy protection issues. Privacy protection organizations take care of privacy policies certification in the same way identities are certified today by certification authorities. It is noted that privacy recommendations will be provided by informal organizations such as virtual users' communities and customer protection organizations.

Context Information Provisioning

The trust in the context providers can be evaluated, for example, through cryptographic mechanisms based on Public Key Infrastructure (PKI, identity coupled) and through the following metrics and mechanisms: reputation of context provider, statistical analysis of context information provided from the source, and context aggregators that compare redundant information from different sources in order to increase trustworthiness. It is also possible to evaluate the trust of the context information based in the trustworthiness of the quality aspects of one particular instance of context, or in the method used to obtain the information. One example is location information, which trustworthiness may vary depending on how the information is obtained: from outlook calendars, user personal GPS position, or position of the GSM/WiFi base station to which the user is connected.

ICT service platform is typically a distributed system without a unique central point of control. In such a system, in some cases implemented in a fully adhoc configuration, multiple administrative domains may exist. To illustrate this, consider a weather service which provides for mobile phone users the local weather forecast based on the latitude/longitude of the GSM cell they are in. In this case, the weather service provider, the mobile phone operator, and the user personal devices are examples of different administrative domains controlled by different administrative entities.

In this multi administrative domain scenario it is not possible to have a centralized trust provider responsible for the management of all trust relationships due to privacy and scalability reasons. In order to support distributed management of trust it is designed a distributed trust management architecture, which is presented in Figure 9 [42].

In case trust evidence is not available in one administrative domain, architecture must support the propagation of recommendations requests to other domains, for example, using existing social network connections such as buddy lists.

As future work it is needed to use context information to improve the recommendation process. For example, context can be used to determine the suitable target entities to request recommendations from. This will allow anonymous and still useful recommendations exchange. Context can also be used to dynamically adapt the user goals. In certain context situations (e.g. health care service) users may not have privacy as first goal when they need the best service adaptation (e.g. to send an ambulance to their current trustworthy location).

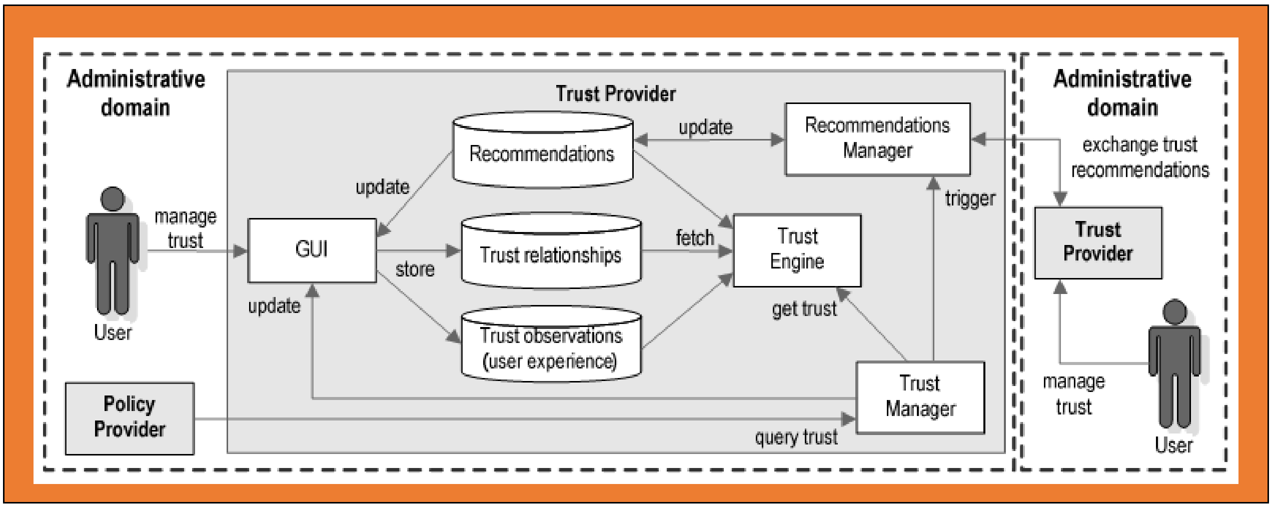


Figure 9 – Distributed trust management architecture [42]

7 Architecture framework for trusted social cyber physical infrastructure

7.1 Social-Cyber-Physical Infrastructure

While traditional ICT infrastructures have focused on computer-centric approaches to data processing as well as network-centric approaches to information collection, the emerging ICT infrastructures will use human-centric approaches. The transformation toward a hyper-connected society will contribute to our everyday lives with ICT problem-solving support, and will (hopefully) change to a more user-friendly, fun and enjoyable experience in terms of ICT provision.

The advent of applications such as content distribution, cloud computing and IoT requires the underlying network to be able to understand the context of various services. An emerging networking paradigm enables in-network knowledge generation and distribution in order to develop the necessary network control intelligence for handling complexity and uncertainty of future networked services and the multitude of users [43]. To support this paradigm, telecommunication infrastructures must be enhanced to make better use of the knowledge of networks, services, end users and their devices.

The evolving trend of telecommunication systems and ICTs has been to move from the living space of home appliances to large-scale communities in buildings, such as workspaces and digital infrastructures like smart cities. The IoT plays a major role in the rapid development of these technologies. The IoT initially focused on network connectivity for supporting heterogeneous communications interfaces but recently it has been developing to provide convergent services that integrate ICT in various industrial areas to offer a common service platform. These convergent services have been required to obtain reliable knowledge from raw data. As an aim of intelligent service provision is to make autonomous decisions without human intervention, trust has been highlighted as a key issue in the processing and handling of data, as well as the provisioning of services which comply with users' needs and rights.

The social IoT [44] transforms smart objects into social entities which are capable of bridging human-to-object interactions. In this way, a social network of objects is created by intelligent reasoning/recommendation mechanisms. These mechanisms extract the social knowledge hidden in the rich profiles of humans and services maintained by various social network services [44].The paradigm of Cyber-Physical-Social Systems (CPSS) [45] [46] has recently gained momentum as an environment that combines knowledge from various smart spaces to form an ecosystem, in which intelligence and reasoning about the social aspects that are embedded in human behaviour in smart spaces act as the glue for integrating physical, cyber and social worlds (See Figure 27).

Based on the CPSS, Figure 11 depicts the concept of a Social-Cyber-Physical (SCP) infrastructure as the future ICT infrastructure. This infrastructure consists of three regions – physical world, cyber world and social world. The main elements of ICT infrastructures rely mostly on 3C (i.e., Computation, Communication, Control) to extract knowledge from the information available in the data obtained from various systems, including sensors and actuators. The social world in relation to a trusted technology with an individual and communities is also important. The three different areas need an infrastructure that is more reliable and closely correlated through cross-tier trust management.

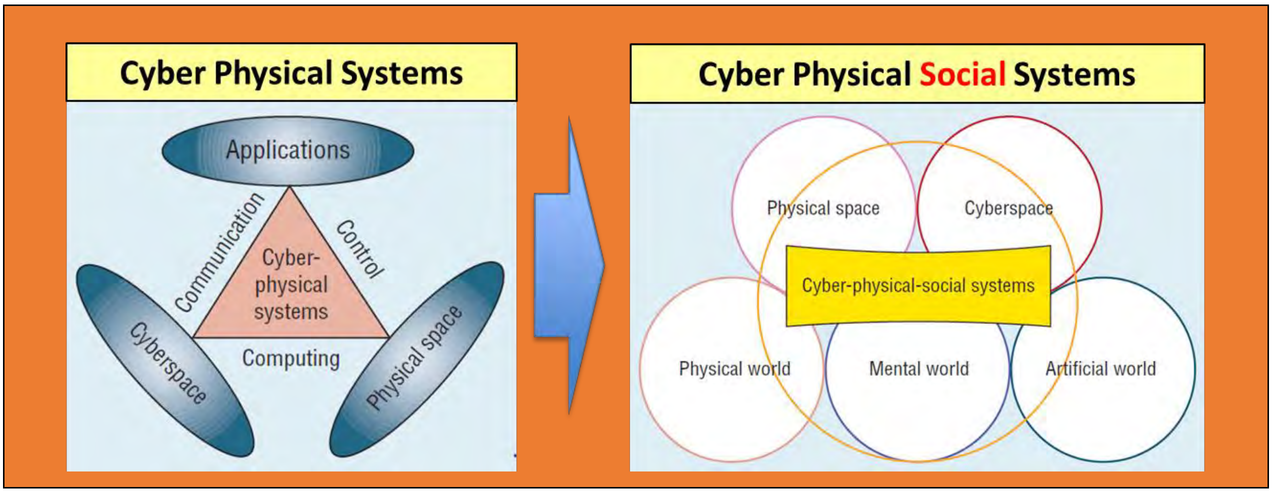


Figure 10 – From cyber physical systems to cyber physical social system

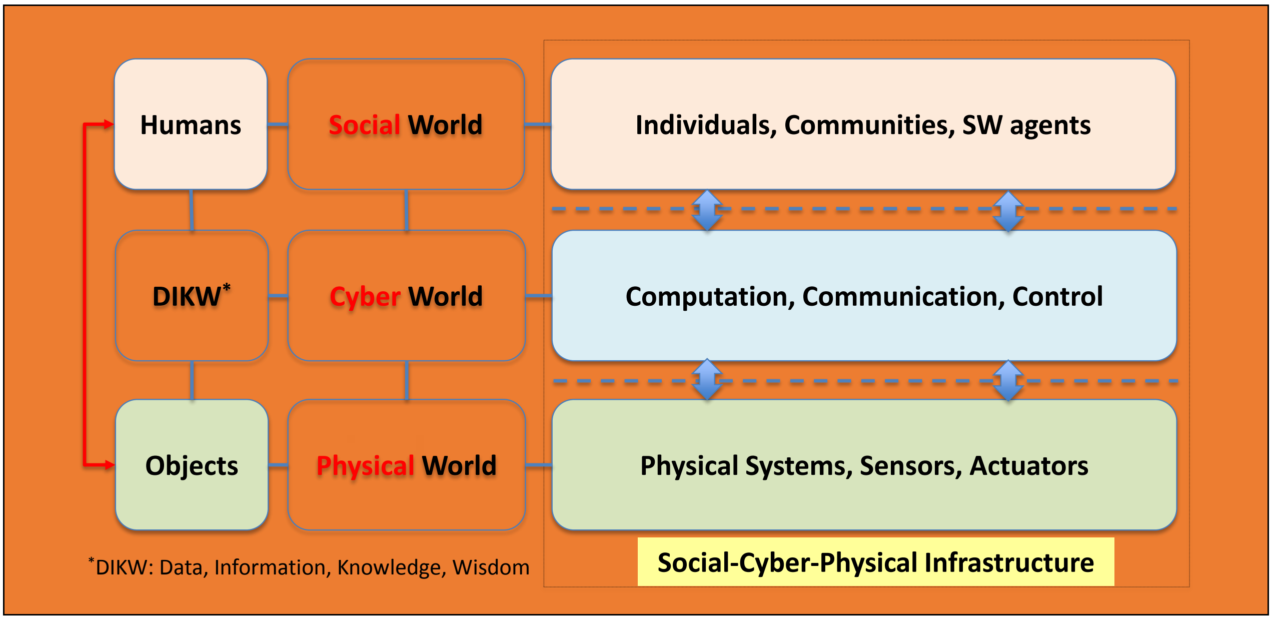

Humans
Social World
Individuals, Communities, SW agents
DIKW*
Cyber World
Computation, Communication, Control
Objects
Physical World
Physical Systems, Sensors, Actuators
*DIKW: Data, Information, Knowledge, Wisdom
Social-Cyber-Physical Infrastructure

Figure 11 – The concept of a social-cyber-physical infrastructure

Most importantly, the transition to the SCP infrastructure depends upon how to acquire useful knowledge from data and information. Trust is essential in this knowledge acquisition process; also, for awareness and understanding of a specific context it is really important to have confidence in decision making. In other words, trust should be additionally considered in systems that behave intelligently and rationally to sense real-world behaviour, perceive the world using information models, adapt to different environments and changes, learn and build knowledge, and act to control their environments [47]. This is mainly related to the Data, Information, Knowledge, Wisdom (DIKW) process in the cyber world (See Figure 11).

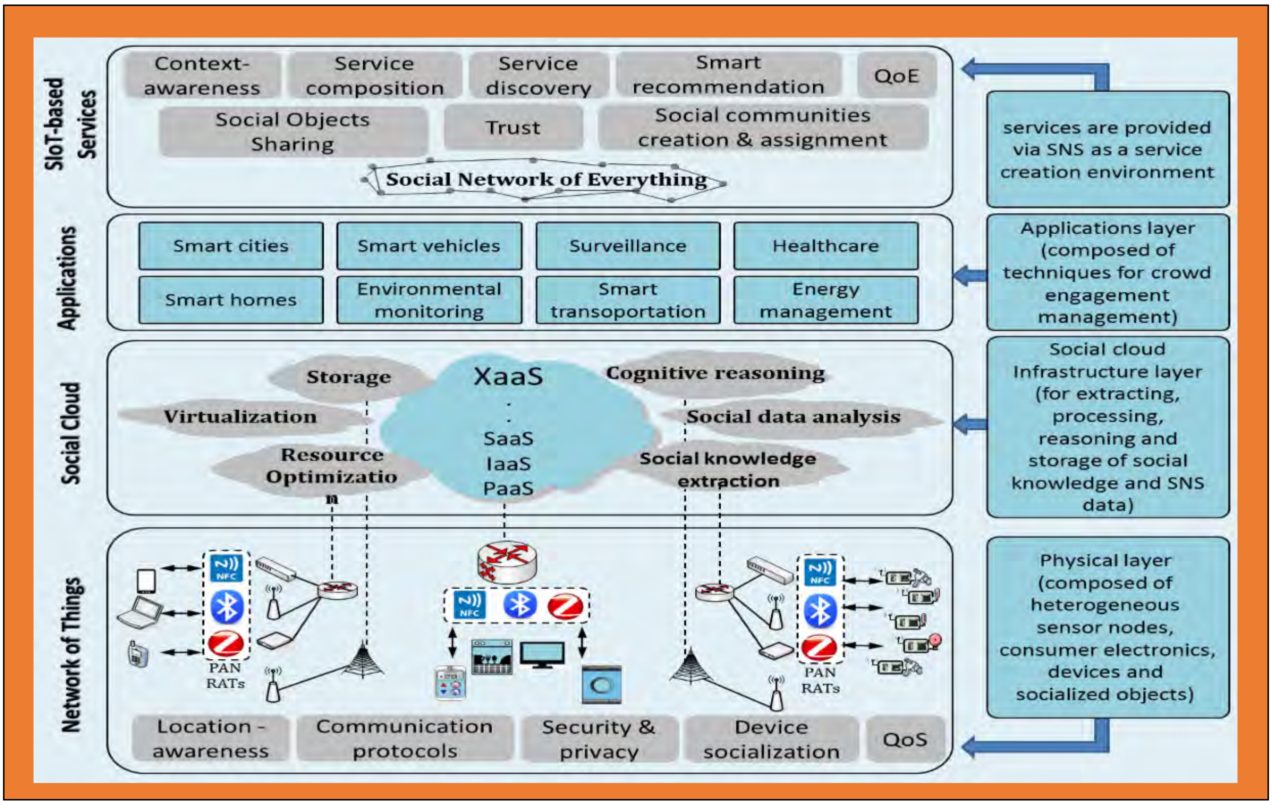


Figure 12 – A conceptual framework for the integration between the SIoT and the SoC

To strengthen trust while building a hyper-connected society, a trustworthy SCP infrastructure will be a key work item for international standardization working on the development of technology and trust, while at the same time expanding the functions of the core technology components.

As an example of SCP infrastructure, as shown in Figure 29, the SCP infrastructure for Everything as a Service (XaaS) integrates all ends of networking and computation by providing scalable storage, tools and methodologies for optimization, intelligence, network virtualization, and social data analytics. These capabilities are offered to a wide variety of applications in many domains giving a great opportunity for building novel social IoT-based services. In here, the Social Cloud provides an infrastructure which is capable of realizing the vision of social IoT by allowing platform-independent sharing of physical resources and services based on the trust existing between nodes on the social network of everything.

7.2 Social-Cyber-Physical Trust Relationships

The SCP infrastructure comprise objects from the physical world (physical objects), the cyber world (virtual objects) and the social world (humans with attached devices), which can be identified and integrated into information and communication networks. All of these objects have their associated information, which can be static and dynamic [48]. Thus, social trust between humans and objects is quite important.

As shown in Figure 13, trust may be human to human, object to object (e.g., handshake protocols negotiated), human to object (e.g., when a consumer reviews a digital signature advisory notice) or object to human (e.g., when a system relies on user input and instructions without extensive verification). In addition to individual trust, community trust also needs to be considered. For SCP relationships, trust as a cross-domain relationship is needed, taking into consideration coexistence, connectivity, interactivity and spatio-temporal situations between vertical layers.

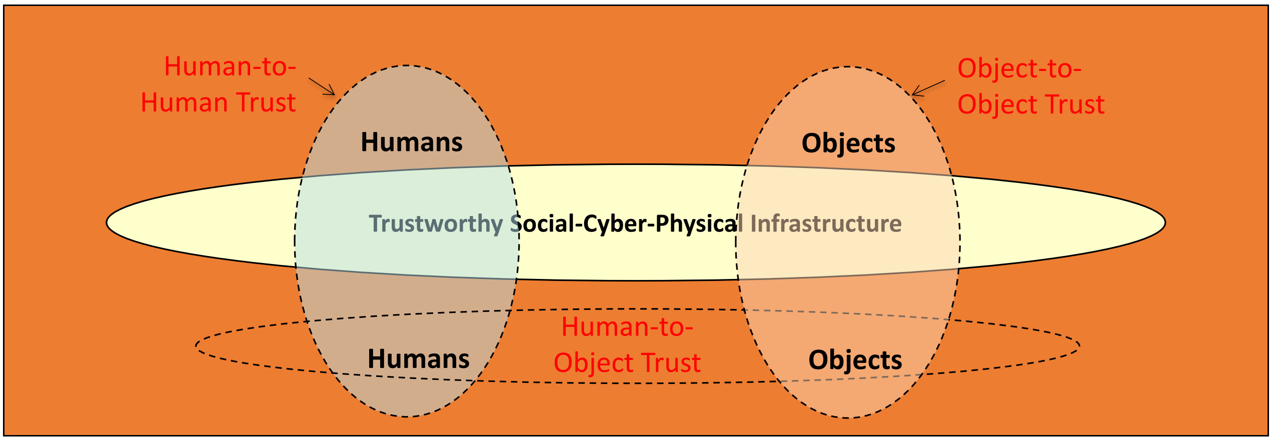


Figure 13 – Trust relationships in a trustworthy social-cyber-physical infrastructure

7.3 Trust Components and Platform Architecture

The choice between centralized and decentralized trust management system must be taken into account, depending on trust model and trust-related information processing. In the centralized approach, the trust information can be computed on demand, whenever an entity needs to rely on its cooperative entities, and delivered to the requesting entity at that moment. On the other hand, the distributed approach computes trust on a regular basis and be propagated throughout the topology. An entity itself in the large scale network like social IoT possibly lacks of knowledge to evaluate trust. It certainly needs help from others such as trusted authorities. Moreover, a real-time trust data flow would result in communication overhead, detrimental to network performance as well as to constrained entities battery life. However, the traditional strategies for centralized system are difficult to suit for solving trust issues of a large scale distributed network like social IoT because of their poor scalability as well as center-dependence leading to single point of failure. Thus, it is considered edge or fog computing architecture [49] which could be considered as semi-distributed system.

In order to deploy the trust service platform, besides the Reputation System, it is necessary to define and incorporate three new basic components to the ICT ecosystem: Trust Agent, Trust Broker and Trust Analysis and Management. The following briefly presents these components by describing their responsibilities and interactions in the system (See Figure 14).

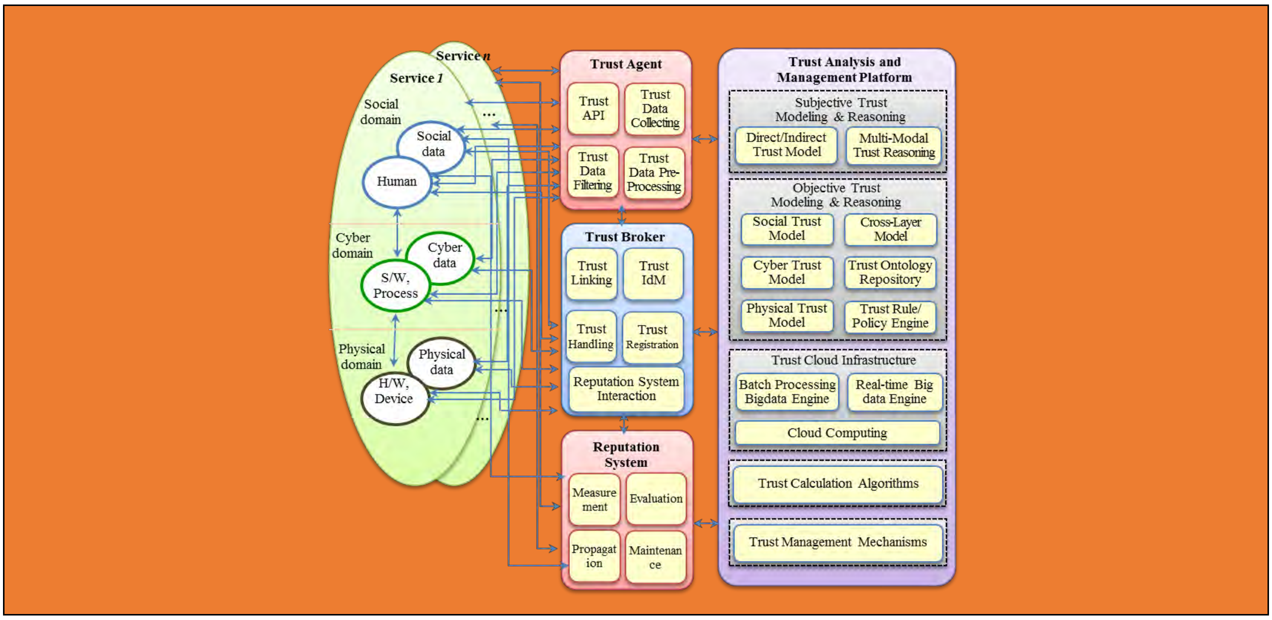

Service n
Service 1
Social domain
Social data
Human
Cyber domain
Cyber data
S/W, Process
Physical domain
Physical data
H/W, Device
...
Trust Agent
Trust API
Trust Data Collecting
Trust Data Filtering
Trust Data Pre-Processing
Trust Broker
Trust Linking
Trust IdM
Trust Handling
Trust Registration
Reputation System Interaction
Reputation System
Measure ment
Evaluation
Propagat ion
Maintenan ce
Trust Analysis and Management Platform
Subjective Trust Modeling & Reasoning
Direct/Indirect Trust Model
Multi-Modal Trust Reasoning
Objective Trust Modeling & Reasoning
Social Trust Model
Cross-Layer Model
Cyber Trust Model
Trust Ontology Repository
Physical Trust Model
Trust Rule/ Policy Engine
Trust Cloud Infrastructure
Batch Processing Bigdata Engine
Real-time Big data Engine
Cloud Computing
Trust Calculation Algorithms
Trust Management Mechanisms

Figure 14 – Trust components interactions in the trust service platform

- Trust Agent: used to collect trust-related data from physical, cyber and social ICT domains. The data could be trust agents or opinions of entities as recommendation or feedbacks to other entities, applications or services.
- Trust Broker: used to provide the trust knowledge to various type of applications and services in the ICT ecosystem. It is required to register information such as knowledge, trust ontology or service requirements prior to use the trust service platform.
- Trust Analysis and Management: Beside a part for collaborating with the Reputation System, all trust-related mechanisms such as ontology-related manager, information model, reasoning mechanisms, trust cloud infrastructure, Knowledge based trust evaluation mechanisms, and trust calculation algorithms are implemented at this module.

7.4 Develop a framework for decision making in the trust analysis system of trustworthy ICT Eco-system

Ongoing research agenda includes designing a fully automating trust decision making process under dynamically changing ICT environment. In this regard different decision mechanisms can be observed in the literature with different techniques.

Utility functions provide a natural and advantageous framework for achieving self-optimization in distributed autonomic computing systems. In this regard, [50] introduced an architecture for incorporating utility functions as part of the decision-making process of an autonomic system. Utility functions were shown to be effective in handling reconfiguration decisions against multiple objectives.

In the context of autonomic trust computing, utility functions map possible states of an entity into scalar values that quantify the desirability of a configuration as determined by user preferences. Given a utility function, the autonomic system determines the most valuable system state and the means for reaching it. In the approach proposed in [50], a utility calculator repeatedly computes the value that would be obtained from each possible configuration. Despite their advantages, utility functions may suffer from complexity issues as multiple dimensions scale depending on the evaluation method used. In contrast, although genetic algorithms use fitness functions, which are akin to utility functions, the process of natural selection efficiently guides the search process through the solution space.

The paper [51] proposes an approach to leverage genetic algorithms in the decision-making process of an autonomic system. This approach enables a system to dynamically evolve reconfiguration plans at run time in response to changing requirements and environmental conditions. A key feature of this approach is incorporating system and environmental monitoring information into the genetic algorithm such that specific changes in the environment automatically drive the evolutionary process towards new viable solutions. They have applied this genetic-algorithm based approach to the dynamic reconfiguration of a collection of remote data mirrors, with the goal of minimizing costs while maximizing data reliability and network performance, even in the presence of link failures.

Furthermore machine learning techniques are often employed as decision mechanisms for a variety of systems as it allows computers to evolve behaviours, based on empirical data, for example from sensor data. Regarding this, a decision making system based on a neural network and a reinforcement learning algorithm is discussed in [52].

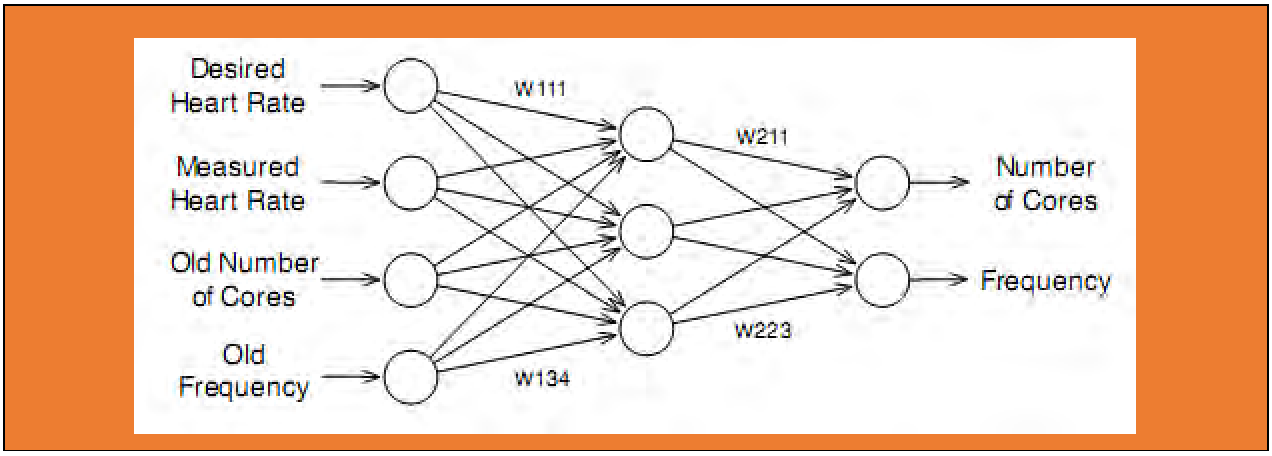


Figure 15 – Neural network topology [52]

Martina et el implemented an artificial neural network, with the purpose of learning the best policy for control. This means the neural network has to produce the next step control outputs from the current situation, with the purpose of reducing the error between the measured heart rate and the desired one. Every time we have a new sample, we feed that into the network and update its weights according to the gradient of the error we are experiencing.

The network topology as shown in Figure 15, is composed by four different input sources, corresponding to the desired heart rate, the actual heart rate and the two control inputs: number of cores and frequency. With three neurons in the (single) hidden layer and two output neurons we learn the relationship between the inputs and the (possibly optimal) control strategy. It is worth stressing that we didn’t train the network before launching the experiments and the network itself is trained online, updating the weights according to the experienced error with a gradient descent method.

Another alternative technique that can be applied to trust decision making process is use of reinforce learning mechanisms as stated in [53]. Reinforcement learning is about learning from interaction how to behave in order to achieve a goal. In here, learner is not told which actions to take, as in most forms of machine learning, but instead must discover which actions yield the most reward by trying them. In the most interesting and challenging cases, actions may affect not only the immediate reward but also the next situation and, through that, all subsequent rewards. These two characteristics (i.e. trial-and-error search and delayed reward) are the two most important distinguishing features of reinforcement learning.

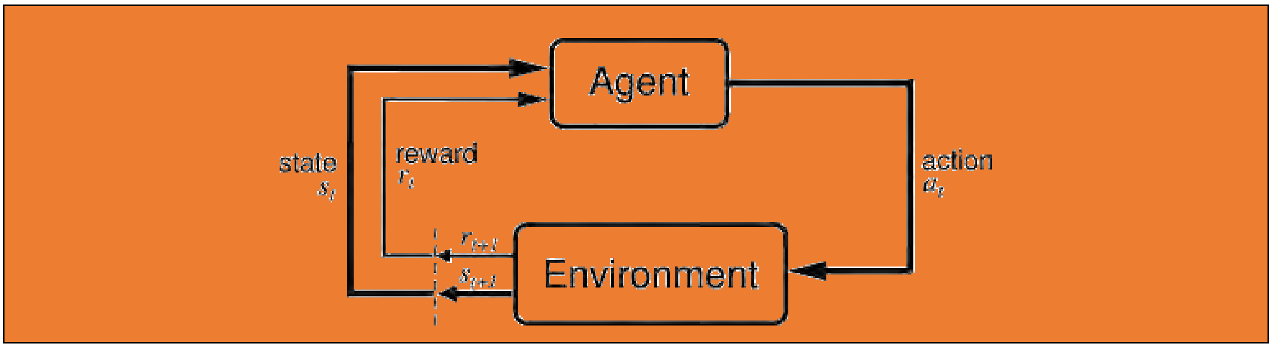


Figure 16 – The agent-environment interaction [53]

The reinforcement learning agent and its environment interact over a sequence of discrete time steps. The specification of their interface defines a particular task: the actions are the choices made by the agent; the states are the basis for making the choices; and the rewards are the basis for evaluating the choices. Everything inside the agent is completely known and controllable by the agent; everything outside is incompletely controllable but may or may not be completely known. A policy is a stochastic rule by which the agent selects actions as a function of states. The agent's objective is to maximize the amount of reward it receives over time.

Another interesting application related to trust decision implementation is proposed in [54] based on well-known Kalman Theory [55]. It has proposed an autonomic and lightweight computational trust model for pervasive systems based on a Kalman filter. When a service delivery occurs, a number of attributes describing the quality of the service are measured and compared against the promised values; these discrepancies are used to train a Kalman filter to assess the trustworthiness of a service provider.

Basic example is presented to explain the techniques involved with Kalman theory to achieve decision making capability. For instance, let’s suppose client device A is willing to assess the trustworthiness of server device B before deciding whether to interact with (e.g. request a service from) B or not. It does so by means of a basic Kalman filter that predicts B’s trustworthiness at time t + 1 based on t previous observations of B’s behaviour (direct experiences).

After each observation, the filter updates its inner state, so to make a more accurate estimate the next time. The Kalman filter is particularly appealing to IoT as it is extremely light-weight, both in terms of memory requirements and computational load (the recursive Kalman equations can be efficiently computed, adding a negligible overhead on the device). Moreover, even in its simplest formulation, the Kalman filter is able to capture many facets of human trust: it makes a prediction based on an arbitrary long history of interactions; it implicitly represents the concept of confidence in the trust prediction, as the more frequently A interacts with B, the more quickly the filter stabilises and reduces the distance between prediction and actual state; finally, it enables simple yet effective modelling of the subjective nature of trust by means of the measurement and system errors. In particular to model cautiousness of behaviours and to model confidence.

7.5 Specify key functionalities and standard interfaces for autonomic decision making

An autonomic system must be able to configure itself according to high-level policies and objectives, thereby improving its effectiveness. One of the most important goals of self-configuration is the ability of a system to reconfigure itself online, seamlessly incorporating new components while existing ones adapt to these new features. On the other hand an autonomic decision making system (self-optimization) must be capable of monitoring and tuning itself according to performance analysis. Performance-based tuning strategies play a key role in the autonomic trust computing systems definition and are strictly related to the decision making process.

Furthermore, the decision make process directly related may properties of the Trustor and Trustee. According to [56], these influencing properties can be categorized in to five items as below:

- Trustee's objective properties, such as a trustee's security and dependability. Particularly, reputation is a public assessment of the trustee regarding its earlier behaviours and performance.

- Trustee's subjective properties, such as trustee honesty, generosity and goodness.
- Trustor's subjective properties, such as trustor disposition and willingness to trust.
- Trustor's objective properties, such as the criteria or policies specified by the trustor for a trust decision.
- Context that the trust relationship resides in, such as the purpose of trust, the environment of trust (e.g., time, location, activity, devices being used, their operational mode, etc.), and the risk of trust.

Autonomic decision making refer to a broad interdisciplinary field interested in all aspects like economics, forecasting, statistical decision theory, and cognitive psychology. In general, decision making is process and it takes some time and effort until the choice is made, involving several activities, such as:

- Identification of the decision problem;
- Collecting and verifying relevant information;
- Identifying decision alternatives;
- Anticipating the consequences of decisions;
- Making the decision;
- Informing concerned people and public of the decision and rationale;
- Implementing the selected alternative;
- Evaluating the consequences of the decision.

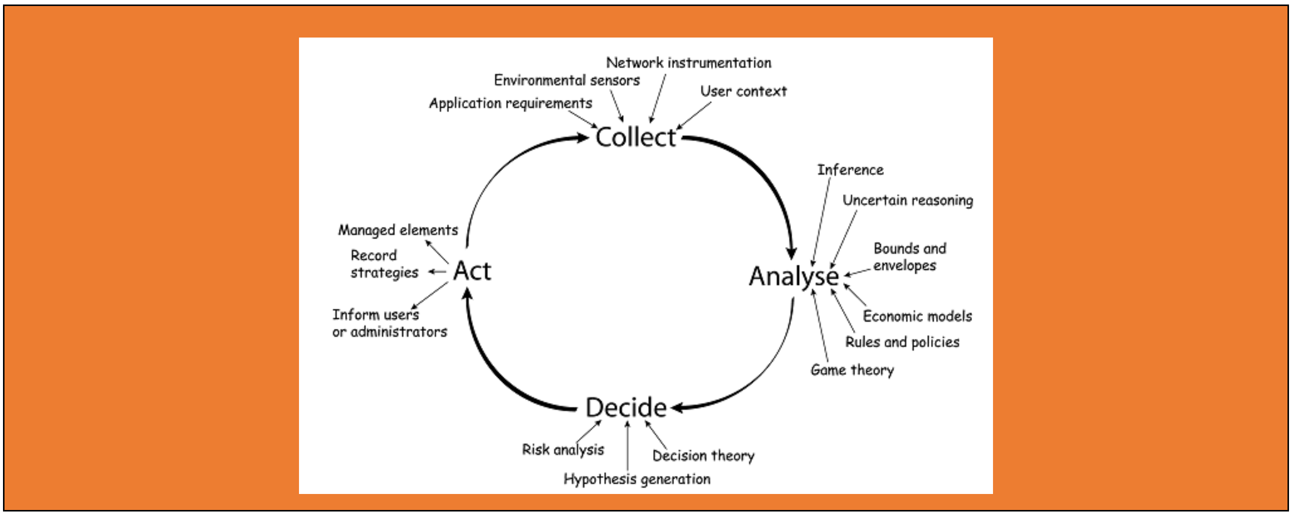


Figure 17 – Autonomic control loop [57]

There are many techniques that can be observed in the literature which address above control loop. Some of them are discussed below [52]:

- Heuristic solutions

  This methods start from a guess about application needs and adjust this guess. Heuristic solutions are designed for computational performance or simplicity at the potential cost of accuracy or precision. Such solutions generally cannot be proven to converge to the optimum or desired value.

- Standard control-based solutions

  Which employ canonical models– two examples being discrete-time linear models and discrete event systems – and apply standard control techniques such as Proportional Integral controllers, Proportional Integral and Derivative controllers, optimal controllers, Petri nets. Assuming the model to be correct, some properties may be enforced, among which stability and convergence time are probably the most important ones, thereby providing formal performance guarantees.

- Advanced control-based solutions

  This technique requires complex models, with some unknown parameters (e.g., the machine workload) that may be estimated online, to provide Adaptive Control. Adaptive Control requires an identification mechanism and the ability to adjust controller parameters on the fly.

- Model-based machine learning solutions

  This requires the definition of a framework in which to learn system behaviour and adjust tuning points online. Neural networks are often useful to build a model of the world for control purposes. Neural network solutions may be used to predict the system reaction to different inputs and, given some training samples, to build a model. The structure of the network and the quality of the training data are critical to performance. The accuracy of the results depend on these crucial choices, and thus no a priori guarantees can be enforced.

  Another model-based family of techniques is Genetic Algorithms. Using a genetic algorithm requires selecting a suitable representation for encoding candidate solutions (in other words, a model). In addition, some standard operators (crossover and mutation) must be defined and a mathematical function must be provided to rate candidate solutions and select among them. The overhead of both neural networks and genetic algorithms may in principle be very significant.

- Model-free machine learning solutions

  This method do not require a model of the system. A notable example is Reinforcement Learning, even if a recent research trend is to complement Reinforcement Learning solution with a model definition. According to [58], Reinforcement Learning agents face three major challenges. The first challenge is how to assign credits to actions, the second is how to balance exploration versus exploitation and the third is generalization. The convergence time of a Reinforcement Learning algorithm is often critical [26] and complementing them with a model of the solution space may decrease it [59].

In summary, decision making is an essential functionality of ICT system. Apart from autonomic approaches, trust based decision making solutions should be developed to provide more reliable and secure networking and services.

8 Trust modeling and policy/rule-based decision making

There is a great diversity of trust models and they can be classified considering different features. However, one of the aspects that takes more relevance, especially when one talks about testbeds, is the type of information from which they compute trust. Some use experiences from previous interactions, some opinions from other agents in the system, some analyse the underlying social network of agents or study the information about the virtual organization to which agents belong, and even more complex examples exist. Many combine several types of information to achieve better estimations.

8.1 Information context of a trust model

Information context denotes the sources of information and the flow of information from which a trust model computes trust [60]. To graphically depict an information context of a general-purpose trust model, a schema from [61] [62] can be build. The schema is shown on Figure 18 is centered on the agent that uses the trust model, called agent a. It shows three information sources from which a`s trust model computes trust. The agent can obtain information by interacting with agents, by asking for opinions, or by using information from the environment.

Because the first two information sources are the most common in current trust models, it is highlighted them and encapsulated other possible sources for trust computation in a special component called environment; examples of such include the analysis of social networks, information about the virtual organizations, etc.

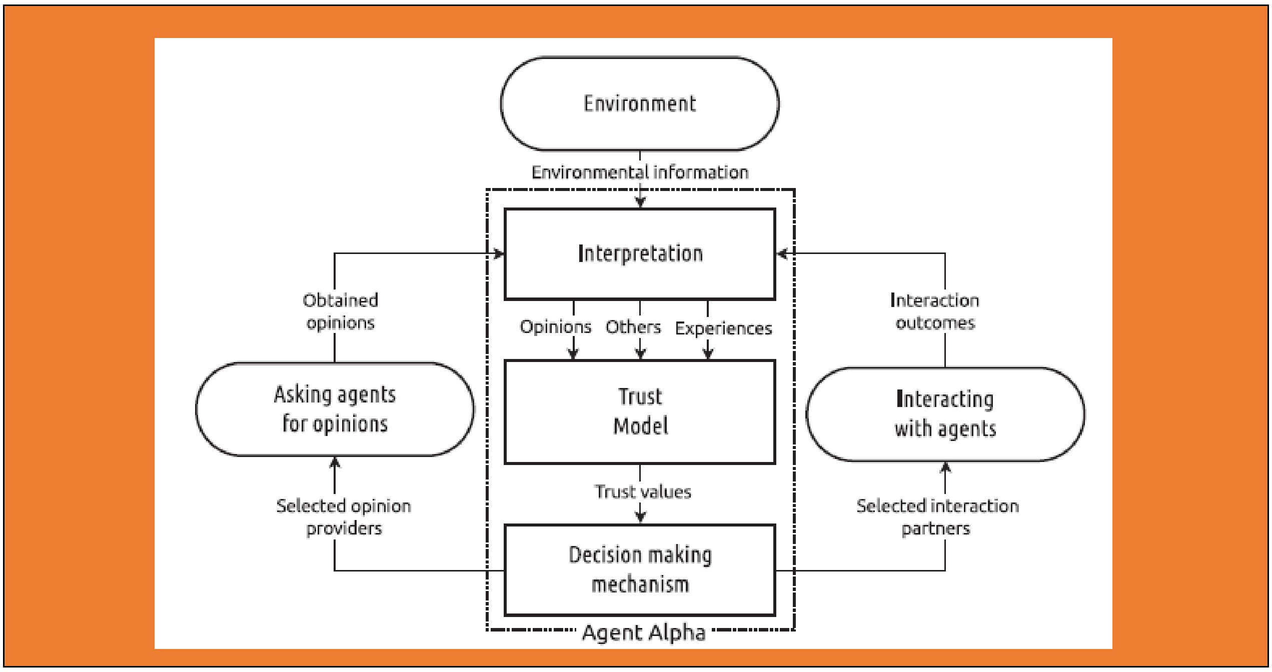


Figure 18 – Information context of a trust model

Agent Alpha uses a trust model that obtains information by (i) interacting with agents, by (ii) asking agents for opinions, and by using other information from the (iii) environment. Agent then conveys the computed trust values to its decision making mechanism where they are used in various decision making processes, such as deciding with whom to interact or who to ask for opinions.

Furthermore, agent a consists of the interpretation, the trust model and the decision making mechanism sub-components. The interpretation converts obtained information to a representation that is compatible with the trust model (in the schema this corresponds to converting interaction outcomes to experiences, obtained opinions to opinions, and environmental information to others). The trust model then uses this information to compute trust values. These are then conveyed to the decision making mechanism to (i) select interaction partners and to (ii) select opinion providers (and in some cases offer opinions to other agents).

The decision making mechanism is usually very complex and while trust values can be an important part of its input, the decision making mechanism also considers other factors. They are, however, domain specific and often independent of the trust model, which is why the majority of trust models do not provide any guidance on how to use the computed values in the decision making process.

8.2 Trust modeling based on key features of trust

Artz and Gil [63] categorize the notion of trust in computer science domain into three main categories: policy-based trust, reputation-based trust and general models of trust. Here it describes more detail about the trust model [64].

- **Policy-based trust**: Using policies to establish trust, focused on managing and exchanging credentials and enforcing access policies. Work in policy-based trust generally assumes that trust is established simply by obtaining a sufficient amount of credentials pertaining to a specific party, and applying the policies to grant that party certain access rights. The recursive problem of trusting the credentials is frequently solved by using a trusted third party to serve as an authority for issuing and verifying credentials.
- **Reputation-based trust**: Using reputation to establish trust, where past interactions or performance for an entity are combined to assess its future behaviour. Research in reputation-based trust uses the history of an entity's actions/behaviours to compute trust, and may use referral-based trust (information from others) in the absence of (or in addition to) first-hand knowledge. In the latter case, work is being done to compute trust over social networks (a graph where vertices are people

and edges denote a social relationship between people), or across paths of trust (where two parties may not have direct trust information about each other, and must rely on a third party). Recommendations are trust decisions made by other users, and combining these decisions to synthesize a new one, often personalized, is another commonly addressed problem.

- **General models of trust**: There is a wealth of research on modelling and defining trust, its prerequisites, conditions, components, and consequences. Trust models are useful for analysing human and agenized trust decisions and for operationalizing computable models of trust. Work in modelling trust describes values or factors that play a role in computing trust, and leans more on work in psychology and sociology for a decomposition of what trust comprises. Modelling research ranges from simple access control polices (which specify who to trust to access data or resources) to analyses of competence, beliefs, risk, importance, utility, etc. These subcomponents underlying trust help our understanding of the more subtle and complex aspects of composing, capturing, and using trust in a computational setting.

A model of trust should capture and relate essential aspects of the trusts. While all three subcategories of trust have been researched, it is well-accepted that in a social world, trust is modelled as reputation-based approach. To express trust and reputation information ontologies are usually used, allowing for expression and quantification of trust for use in algorithms to make a trust decision about any two entities [65].

8.2.1 Develop a trust model for a specific use case

Several interesting trust models and also systems, such as PolicyMaker, KeyNote and REFEREE have emerged. However, the focus has been on more comprehensive and concrete system having wider trust management elements, such as Poblano, Free Haven, SULTAN, TERM and SECURE.

8.2.1.1 Trust Networks on Sematic Webs

Golbeck first referred to such model as a Web-of-Trust. A Web-of-Trust is a directed-edge network between a group of entities (or resources), within which each link carries a trust value and, assuming a transitivity of trust, reputation can be collected and inferred for each single individual across such network. Within the context of Web-of-Trust, reputation can be defined as a measure of trust, within which individuals can gather and maintain reputation of other individuals across the network.

There are many measures of "trust" within a social network. It is common in a network that trust is based simply on knowing someone. By treating a "Person" as a node, and the "knows" relationship as an edge, an undirected graph emerges. If A does not know B, but some of A's friends know B, A is "close" to knowing B in some sense. Many existing networks take this measure of closeness into account. We may, for example, reasonably trust a person with a small Erdos number to have a stronger knowledge of graph theory than someone with a large or infinite number [66].

Techniques developed to study naturally occurring social networks apply to these networks derived from the semantic web. Small world models describe a number of algorithms for understanding relationships between nodes. The same algorithms that model the spread of disease in physical social networks, can be used to track the spread of viruses via email.

For trust, however, there are several other factors to consider. Edges in a trust network are directed. A may trust B, but B may not trust A back. Edges are also weighted with some measure of the trust between two people. By building such a network, it is possible to infer how much A should trust an unknown individual based on how much A's friends and friends-of-friends trust that person. Using the edges that exist in the graph, we can infer an estimation of the weight of a non-existent edge.

8.2.1.2 Beta Reputation System (BRS) [67]

Beta Reputation System (BRS) uses the expected value of the beta distribution to represent trust. Because of this, its trust degrees are real numbers from [0, 1]. BRS computes trust from agent’s own experiences and from opinions from third-parties. Such information comes in the form of 2-tuples <r,s> that represent the amount of positive and negative feedback, respectively.

BRS uses a simple discounting procedure for handling false opinions. The discounting is based on the level of trust the BRS places in the agents that provide opinions. For instance, if BRS considers an agent to be very untrustworthy as a service provider, it heavily discounts its opinions. Such assumption is sometimes called trust transitivity, because it states that if an agent is trustworthy to provide a certain service it can also be trusted to provide good (honest) opinions.

8.2.1.3 Abdul-Rahman, Hailes (ARH)

The trust model proposed by Abdul-Rahman and Hailes (ARH) [68] uses qualitative information for computing and representing trust. In ARH, domains of trust degrees and assessments are the same: X=K={vb < b < g < vg}, where elements denote 'very bad', 'bad', 'good', and 'very good' degrees (assessments), respectively.

ARH copes with liars by using a mechanism capable of correcting opinions. For instance, ARH can learn if an agent consistently badmouths other agents and adjusts its opinions accordingly. Additionally, ARH is the only tested trust model that separates trust by service types.

8.2.1.4 Travos (TRA) [69]

Travos (TRA) is a trust and reputation model for agent-based virtual organizations. Similar to BRS it is based on the beta distribution and represents trust degrees as its expected value. Moreover, feedback in Travos is also represented in the form of 2-tuples<m, n>, but contrary to BRS, Travos uses binary interaction outcomes. Thus (1, 0) represents a satisfactory and (0, 1) an unsatisfactory interaction. The interpretation component computes these tuples by thresholding the interaction outcomes; if the outcome reaches the threshold, we get (1, 0), if not, (0, 1). Like ARH, there are three thresholds; TRAL thresholds at 0.25, TRAM at 0.50, and TRAH at 0.75.

Travos expects opinions as tuples hr, si that contain the number of positive, r, and negative, s, past interactions. When a receives an opinion, say (ai, aj, s, t, 0.60, 0.05), the interpretation component simulates a number of interactions of ai with aj by using truncated normal distribution. It sets the mean to the opinion's internal trust degree, 0.60, and the standard deviation to the same value that is used for generating experiences, 0.10. Each sampled number is then compared against the threshold to determine whether the interaction is satisfactory. This procedure assures that a obtains the same tuple – adjusted for the correctness of the given opinion – that would have been obtained if agent ai had interacted with aj 10 times and then reported the number of positive and negative interactions. For instance, with threshold 0.50, the opinion above would most likely be transformed into hai, aj, s, t, h8, 2i, 0.05i.

Travos computes confidence in its experiences and if confidence is not sufficient, it combines experiences with opinions. Additionally, it also uses a complex mechanism to reduce the effect of false opinions. If an opinion provider is deemed as a liar, Travos reduces the weight of its opinions. Travos manipulates parameters of the beta distribution.

8.2.1.4 Eigen Trust [70]

EigenTrust is a trust model for P2P networks. It computes global trust values based on opinions from all peers in the system. An important aspect of EigenTrust is the notion of special peers that are pre-trusted. The trust in those peers has to be accurate, otherwise EigenTrust's computation method does not converge. EigenTrust paper does not specify how to determine such peers.

EigenTrust uses binary interaction outcomes and computes local trust values in the form of net difference between the number of positive and negative interactions. If the difference is negative - more negative than positive interactions - EigenTrust assigns a local trust value of 0 to such peer. Because of this, it is said that EigenTrust does not measure negative trust, since it cannot differentiate between peers with whom it has had bad experiences from those with whom it has not interacted.

EigenTrust also exchanges opinions in the form of tuples that contain the number of positive and negative past interactions. EigenTrust does not have any special mechanism to deal with false opinions. Similar to BRS, it considers trust to be transitive, and simply discounts opinions based on the level of trust it has in agents as service providers.

8.2.2 Specify trust attributes and trust relationships among entities

The trust model presented attempts to tie together all trust attributes. There is an attempt to capture the semantics of the trust relationship using a proposed trust model and design a trust ontology that serves as an upper level ontology for use across multiple domains. Using this trust ontology, there are the following questions like: What are the trust relationships that an agent is participating? Is there a trust relationship between agent X and agent Y? What is the scope of a trust relationship? What process was used to arrive at this trust value? These questions are formulated as queries using the trust ontology in the next part.

In this part, the trust model needs cover all aspects of the trust relationship. Following the general trust model, we can model the trust relationship between two agents as a six tuple relationship trustor, type, scope, value, process, trustee (as shown in Figure 19).

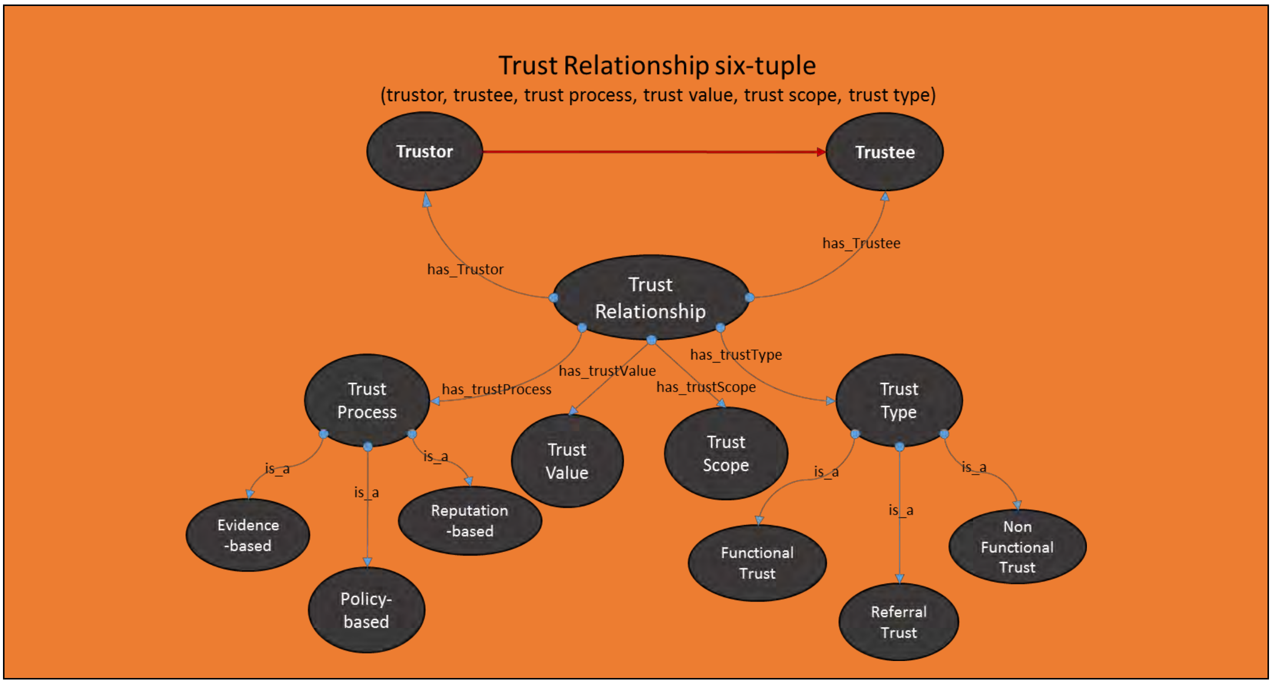


Figure 19 – Trust Model illustrating all the concepts and relationships between the concepts

The trust relationship between two agents is represented as a six tuple. The agent who trusts another agent is called the trustor and the agent being trusted is called the trustee. Each trust relationship is further qualified with [71]:

1) **Trust Type**: The trust type captures the semantics of the trust relationship. Trust type can be functional, referral or non-functional.

- Functional Trust: Trust relationship established with direct interactions between two agents. One agent trusts another agent's ability to carry out a particular task.
- Referral Trust: Trust relationship established for conceiving an agent's referral of another agent. An agent trusts another agent's ability to recommend a third agent.
- Non-Functional Trust: Distrust in agent's competence or behaviour established. Note that referral trust is transitive within the same scope, while functional trust is not.

2) **Trust Scope:** Trust Scope captures the context in which the trust relationship is valid. A trust relationship is valid only in a prescribed scope. An agent that trusts another agent in one scope may distrust the same agent in another scope. For instance, an agent A can have functional trust in agent B for music and, at the same time, have non-functional trust in agent B for books.

3) **Trust Value:** Trust value is a way to quantify or compare trust relationship. Value can be a natural number, real number in the range [-1, 1], or it a partial ordering [1] of trust relationships.

4) **Trust Process:** The process by which we arrive at trust values is termed as Trust Process. The trust process will indicate the way in which trust values are computed and updated, essentially leading to trust management. This can include specific trust computation algorithms and application specific techniques for trust computation, aggregation and management. Some examples of trust processes are described below:

- Policy Based Trust: An agent trusts another agent based on some policy or rules. For instance, if a company is ISO 9001 certified, then we can expect a certain quality enforcement in the products they deliver.
- Reputation Based Trust: If an agent has a record of previous interactions with another agent, then this can act as a basis for inferring trust and this is termed as reputation based trust process.
- Evidence Based Trust: Evidence-based trust is the process of arriving at trust values by seeking additional confirmatory evidence for a known fact in order to validate or invalidate what is already known.

The idea of trust process is to abstract the method of arriving at trust values and managing them. There is no universal trust algorithm that fits all domains and applications. This abstraction will allow us to talk about trust across domains and use application specific or domain specific trust algorithms for each class of problems. Reputation based algorithms and entropy based algorithms are some examples of trust processes used within sensor networks.

8.2.3 Implement an trust ontology based on trust modeling

Semantic vocabularies and semantic annotation

There should be formal means e.g. a formal semantic vocabularies, to semantically state (context)-specific trust expectations such as “I trust to services having a good reputation and being popular” or “I trust to services having high reputation, ensuring data confidentiality using Transport Security Layer (TSL)/ Secure Socket Layer (SSL) protocol, but better if TSL protocol, and having authorization in means of tokens”. Security is more relevant than reputation.

The service providers should have the same formal means to semantically state the trust guarantees (trust characteristics) of their respective objects and services - e.g. “Communication security and data confidentiality is ensured by encrypted TSL communication and OAuth 2.0 authorization and authentication mechanisms (RFC 6749)”. With a common language with formal semantics, the matching between the trust expectations and trust guarantees will likely have higher recall and precision.

Yet, there is no a semantic vocabulary suitable for annotating or describing trust expectations and guarantees in a common, standardized way, and with sufficient expressivity. However, there are certain semantic vocabularies and ontologies, in other domains, that can be reused. For example, W3C Semantic Sensor Network (SSN) Ontology [72] provides concepts such as Accuracy, Detection Limit, Drift, Frequency, Latency, Resolution, Response Time, and Sensitivity, that might be relevant in a perception of the trust towards the sensing devices (e.g. I trust to sensors that provide the data frequently and have a good sensitivity.) Unified Service Description Language (USDL)-Sec [73] vocabulary for describing service security aspects seems to be suitable for describing the security guarantees, such as authorization or confidentiality, in different levels of security details.

Then, there are trust ontologies present in the literature (e.g. [74], [75]), however, those are conceptual models of the trust relationship. They capture notions such as trustor, trustee, trust relation, or trust typology (reputation-based, evidence-based, policy-based), but no details for stating trust expectations and guarantees. QoS ontologies, such is WS-QoSOnto [76], previously built for annotating quality aspects of semantic web services can be reused to describe QoS-based trust expectations and guarantees.

The COMPOSE project [77] has developed a trust ontology (illustrated in Figure 20) and aim to integrated it with SSN, USDL-Sec, and other ontologies relevant for the trust considerations in the IoT. Among others, the ontology captures notions of TrustRelationship, TrustingParticipant, TrustorParticipant, Trust Criteria (trust expectations), TrustProfile (trust guarantees), TrustAttribute, Measurable TrustAttribute and NonMeasurable TrustAttribute.

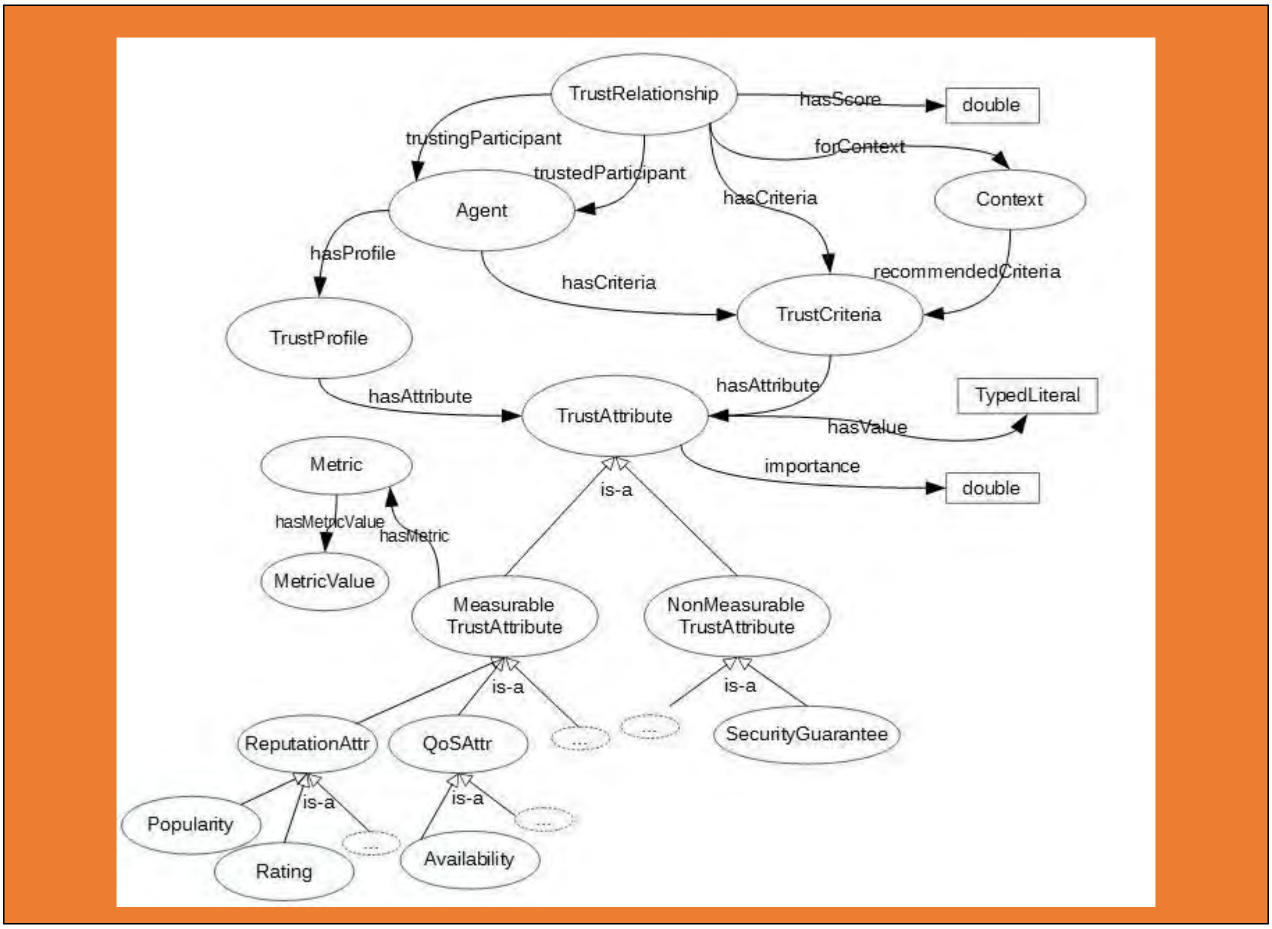


Figure 20 – Trust ontology [77]

Semantic Matchers

Discovery of the trustworthy products is a semantic matching or semantic search task. The trust expectations of a user are semantically matched with the trust guarantees of a service/product. The trust expectations and guarantees may match exactly, almost or be disjoint. If the trust guarantees match the trust expectations exactly or almost, the product classifies as trustworthy. If disjoint, the product classifies as distrusted. With the trust expectations and trust guarantees expressions communalized and formalized using semantic vocabularies and machine-processable semantic annotations, the trust-based discovery engines will be capable to do better job, thanks to the semantics.

There are many existing semantic matchers and semantic search engines available. The existing ones can be reused to develop a special-purpose engine for matching the trust expectations with trust guarantees. In particular [77] have developed a trust evaluation module on the top of a trust goal classification approach introduced in [78], which was designed for the trust-based discovery of semantic web services. In that approach, trust guarantees of the web services are matched against trust expectations by a classification technique to identify services that fit (classify) into the requirement. In addition to the classification, they have introduced the measure of similarity between the trust expectations and trust guarantees. The measure is a value between 0 and 1, and represents the trust level.

Importantly, the trust guarantees should be constantly or periodically verified and monitored, by users and/or by established central authorities, in order to help to increase accuracy of the trust evaluation. The monitoring is collecting the evidence for the claimed trust guarantees. The monitoring of trust guarantees requires sophisticated mechanisms over the Internet with possible involvement of trusted third parties for detecting, isolating and limiting the negative behaviours. It is a challenge on its own.

The evidence of trust guarantees may be coming from different sources including users reviews and ratings, from various estimations such could be an estimation of popularity, then from third party services assessing the QoS and data (e.g. detection of accuracy of a wind sensor by comparing the data with the data of other wind sensors in the same area) or performing static code analysis to detect possible negative effects of the execution, etc.

8.2.3.1 Trust Network in Friend of a Friend (FOAF) scheme [79]

Friend-Of-A-Friend (FOAF) is one project that allows users to create and interlink statements about who they know, building a web of acquaintances. The FOAF schema [24] is an RDF vocabulary that a web user can use to describe information about himself, such as name, email address, and homepage, as well as information about people he knows. In line with the security mentioned before, users can sign these files so information will be attributed to either a known source, or an explicitly anonymous source. People are identified in FOAF by their email addresses, since they are unique for each person.

In this project, a schema was introduced, designed to extend foaf:Person, which allows users to indicate a level of trust for people they know. Since FOAF is used as the base, users are still identified by their email address. Trust schema adds properties with a domain of foaf:Person. Each of these new properties specifies one level of trust on a scale of 1-9. The levels roughly correspond to the following:

1) Distrusts absolutely
2) Distrusts highly
3) Distrusts moderately
4) Distrusts slightly
5) Trusts neutrally
6) Trusts slightly
7) Trusts moderately
8) Trusts highly
9) Trusts absolutely.d

Trust can be given in general, or limited to a specific topic. Users can specify several trust levels for a person on several different subject areas. Users can specify topic specific trust levels to refine the network. For example, Bob may trust Dan highly regarding research topics, but distrust him absolutely when it comes to repairing cars. Using the trust ontology, the different trust ratings (i.e. "distrustsAbsolutely," "trustsModerately," etc.) are properties of the "Person" class, with a range of another "Person". These properties are used for general trust, and are encoded as follows:

```
<Person rdf:ID="Joe">
        <mbox rdf:resource="mailto:bob@example.com"/>
        <trustsHighly rdf:resource="#Sue"/>
</Person>
```

Another set of properties are defined for trust in a specific area. They correspond to the nine values above, but are indicated as trust regarding a specific topic (i.e. "distrustsAbsolutelyRe," "trustsModeratelyRe," etc.). The range of these topic specific properties is the "TrustsRegarding" class, which has been defined to group a Person and a subject of trust together. The "TrustsRegarding" class has two properties: "trustsPerson" indicates the person being trusted, and "trustsOnSubject" indicates the subject that the trust is about. There are no range restrictions on this latter property, which leaves it to the user to specify any subject from any ontology.

8.2.32 Konfidi – Trust Network using PGP and RDF [80]

A RDF schema is used with the FOAF to represent trust relationships and a rating system. The Kondifi is also same approach to Trust.

Konfidi uses Pretty Good Privacy (PGP) connections to determine authenticity and topical trust connections described in RDF to compute inferred trust values. Between yourself and some person X whom you do not know, Konfidi works to find a path of cryptographic PGP signatures to assure the identity of X, and estimates a trust rating by an algorithm that operates along the trust paths that connect you to X. The trust paths are formed from public person-to-person trust ratings that are maintained by those individuals.

Konfidi refers to the trust network design, the ontology used to encode it, and the software to make it usable. The central idea is that between yourself and person X whom you do not know, there is a path of PGP signatures to assure the identity of X. An estimated trust rating can then be computed by some algorithm that operates along the trust paths that connect you to X. The numbered paths indicate the steps in the process to form a Trust Network Figure 21:

1) A client makes a request to the Konfidi server, indicating the source and the sink.

2) The frontend passes the request to the PGP Pathfinder, which verifies that some path exists from the source to the sink in the PGP Web-of-Trust.

3) The Pathfinder returns its response.

4) If thre is a valid PGP Web-of-Trust connection, the frontend passes the request to the TrustServer, which traverses the Konfidi trust network that is built from data kept up-to-date by the FOAFServer.

5) The TrustServer responds with the inferred trust value or an appropriate error message.

6) The Frontend combines the responses of the Pathfinder and the TrustServer, and sends them back to the client.

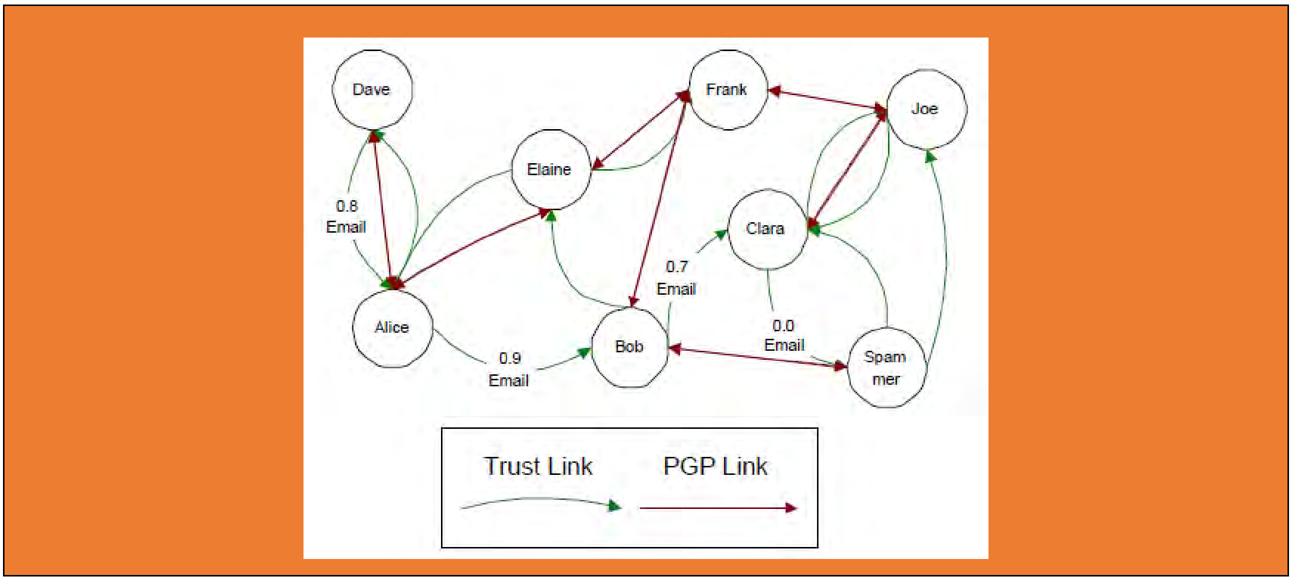


Figure 21 – Combined Trust Network Ontology in Konfidi

8.2.3.3 Trust Ontology for Data Usage Policy in Smart Cities

The trust ontology is used to define the trust policy formulated in the Data Usage Policy. It is possible to reuse related concepts proposed in data usage conceptual models in Smart Cities as illustrated in Figure 22, and extend more concepts in advance to define own trust ontology, called Trust Data Usage Ontology. Data usage is defined by using modal operators (Obligation, Forbidden, and Permission) on following conditions: (i) class of actors, (ii) constraints (Spatiality, Temporality, and Abstraction), (iii) class of purposes, and (iv) monetization.

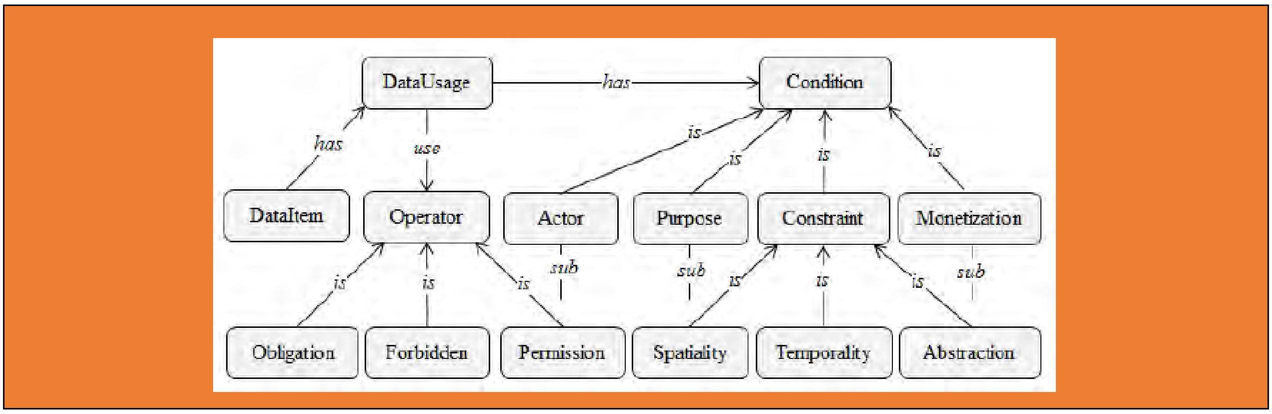


Figure 22 – A Trust Data Usage Ontology

8.3 Development of a static policy/rule-based trust-level decision making mechanism

Trust models with decision making mechanism are trust models that provide both (i) rules, formulas and algorithms describing how to compute trust, and also (ii) hints on how to use that information in the decision making processes. The evaluation protocol and the used metrics differ, depending on what the decision making mechanism does.

While the trust evaluation phase has been extensively studied, approaches for decision making mechanism often employ very simple models. Often, the agent who is 'most trusted' is automatically selected for delegation, without considering any other factors. Risks, rewards, and the potential for trustees to make deliberate choices, are often not considered.

8.3.1 Specify policy/rule for deciding trust levels

Once trust evaluations have been produced for a given set of individuals, the decision to trust must be made. This problem has been approached in different ways by some existing trust models, and neglected entirely by others.

The trust policy is used by the trustor as well as trust platform to define the diversity of personal preferences that they wish to impose on their perspectives of trust. There are many possible policies depending on the context, trust model and infrastructures.

Here are some trust policy and rules perspective depending on the trust model for decision-making mechanisms:

- **Cognitive View**: This cognitive approach explicitly considers the inseparable nature of trust, risk and context.

  While trust in another individual may be higher than for any other, the trustor may stand to lose too much to make delegation preferable. On the other hand, the trustor may have so little to lose and so much to gain, that he is willing to consider even those partners who are not especially trustworthy.

  The cognitive approach argues the need to keep separate the process by which an agent forms trust beliefs, and the process by which an agent decides to act on trust, by delegating. While the cognitive view is abstract and far richer than any existing computational model, the authors show that the different trust beliefs can be reduced to a single degree of trust suitable for use within a decision-theoretic framework.

- **Exploration and Thresholds**: The trustors who possess utility functions for each attribute of a service, and these are used when evaluating services after an interaction. Agents can, therefore, define a threshold of utility, here co-operation may be considered. As this is not a probabilistic model, this utility cannot be considered 'expected' in the decision-theoretic sense. In their evaluation, consumer agents are initially randomly distributed in the environment and have a preference for interacting with agents who are 'nearby' in the environment.

- **Decision Theoretic Approaches**: These approaches are built upon a strong foundation of probability theory and so their trust evaluations are compatible with standard statistical decision theory. That is an agent which can calculate its expected utility directly using the output of the model.

8.3.2 Develop a decision making algorithm for policy decision and enforcement [81]

- **Exploration and Threshold**

Griffiths et al. [82] employ a simple, threshold-based decision-making model. To this end, they define the concepts of untrust and undistrust (in addition to trust and distrust) to represent the notions that a degree of trust may be insufficient for deciding to delegate (or not, in the case of undistrust). Agents who are 'untrusted' are only considered for interaction if no explicitly trusted alternatives are available. The eventual decision to interact is made if the degree of trust exceeds a pre-defined threshold, provided by the system designer. In initial cases, the authors require that all trustors participate in a 'bootstrapping' phase of a fixed duration, whereby agents explore the society before beginning to use their trust models. While the particular exploration strategy is not discussed, Griffiths states that any partner has an equal chance of being selected during the bootstrapping phase.

The SULTAN model was developed primarily with a view to supporting secure interactions in internet applications, in the domain of trust management. These works can be distinguished from other works by their focus on security and implement ability within enterprise systems. Typical decisions necessitating trust, in this context, may be the decision to allow a user access to a sensitive or restricted system resource, or the decision to accept a user's authorisation key. Trust is generally specified as rules (or policies) provided by users, stating the preconditions of trust. By taking a probabilistic view of the possible contingencies, the authors quantify risks in terms of Expected Loss and Maximum Allowable Loss. The decision to trust is made using the policies together with a risk threshold, here an interaction will be considered too risky.

The FIRE model Huynh et al. employ a more sophisticated variant of the most-trusted strategy for selecting interaction partners which includes exploration. The decision mechanism of FIRE consists of two stages, and can be summarised as follows. The set of potential partners is initially divided into two subsets, based on the ability of the trustor to produce evaluations for those partners. These sets are termed hasTrustValue and noTrustValue. The most trusted candidate from the hasTrustValue is advanced to the exploration stage. In this secondary stage, the Boltzmann exploration strategy is used to make a decision between selecting the most trusted agent, or a random one from the noTrustValue set. In this model, the trustor always chooses to delegate.

The Boltzmann exploration strategy is useful for decision-making when nothing is known about the candidate set. Given an agent has a choice between a number of actions (i.e. delegation candidates) (a1, a2, …, an) with expected utilities (u1, u2, …, un), the Boltzmann strategy assigns a probability to each action according to the distribution in the equation:

$$P(a_i) = \frac{e^{u_i/T}}{\sum_{j=1}^{n} e^{u_j/T}}$$

- **Decision Theoretic Approaches**

Matt et al. present an approach which combines probabilistic measures of trustworthiness within the context of a logical argumentation framework. In this work, the authors assume the existence of contracts which specify certain guarantees about the interaction outcomes that can be expected. The probabilistic representation of trust is based on the model of Yu and Singh. An agent deliberates by advancing arguments regarding service parameters (e.g. reliability, security) that either attack or support a proposition T, representing the assertion that a particular trustee is trustworthy. A second kind of argument (called a mitigation argument) attacks contract arguments that support T. These arguments represent claims that a particular agent usually violates a contract clause which supports T. The decision to trust is eventually made on the basis of whether the proposition T is supported beyond some cautiousness parameter, which is equivalent to the trusting threshold of Yu and Singh.

The benefit of this approach is that it permits the use of explicitly stated expectations, such as contract clauses, in the decision about whether to trust. This approach needs not to be limited to contracts; social norms can equally be considered. With this in mind, this type of approach may be suitable for reasoning explicitly about the integrity of agents, as well as their competence, based on past performance with respect to norms and contracts.

The model proposed by Smith and des Jardins addresses the decision problem of agents by modelling interactions as Iterated Prisoner’s Dilemma games. These are a repeated variant of the classic Prisoner’s Dilemma game (Axelrod and Hamilton), where the ‘players’ have a personal incentive to behave in an untrustworthy way.

8.3.3 Implement a trust reasoner using rule languages [83]

Ontologies are formal definitions of concepts and the relationships between them. The Web Ontology Language OWL 2 is a W3C Recommendation since 2009. It is based on Description Logics (DLs), a family of knowledge representation formalisms. OWL 2 RL (Rule Language) reasoning systems allow for rule-based reasoning. OWL 2 Query Language (QL) supports conjunctive query answering against large volumes of instance data that is stored in relational database systems. OWL 2 EL aims at applications that employ large ontologies.

A reasoner is a program that infers logical consequences from a set of explicitly asserted facts or axioms and typically provides automated support for reasoning tasks such as classification, debugging and querying. For OWL 2 EL, scalable implementations of dedicated reasoning algorithms are available. A question is whether these implementations perform better on OWL 2 EL ontologies than traditional reasoning engines, which have been designed for much more expressive languages. Sematic tableau algorithms can be highly optimized, so that they are not necessarily outperformed by straightforward implementations of polynomial-time algorithms.

Here are some prospective reasoners that we can use for trust.

CB (Consequence-based reasoner, University of Oxford) is an implementation of a reasoning procedure for Horn Ontologies, i.e. SHIQ ontologies that can be translated to the Horn fragment of first-order logic. CB’s reasoning procedure can be regarded as an extension of the completion-based procedure for EL++ ontologies and works by deriving new consequent axioms. It is theoretically optimal for Horn SHIQ ontologies as well as for the common fragment of EL++ and SHIQ.

FaCT++ (Fast Classification of Terminologies, University of Manchester) is the new generation of the OWL DL reasoner FaCT. It supports OWL DL and a subset of OWL 2 that is more expressive than the ontologies in other ontologies. FaCT++ is implemented in C++ and based on optimized tableaux algorithms.

HermiT (University of Oxford) can determine whether or not a given ontology is consistent and identify subsumption relationships between concepts, among other features. HermiT is based on a “hypertableau” calculus.

TrOWL (Tractable reasoning infrastructure for OWL 2, University of Aberdeen) is the common interface to a number of reasoners. TrOWL Quill provides reasoning services over OWL 2 QL. TrOWL REL is an optimized implementation of the CEL algorithm that provides reasoning over OWL 2 EL. It employs a syntactic approximation from OWL 2 DL to OWL 2 EL to enable OWL 2 DL ontologies to be classified within polynomial time [41]. This approximation is soundness-preserving but sacrifices completeness. To support full DL reasoning, TrOWL allows for the use of heavyweight plugin reasoners, such as FaCT++, Pellet, HermiT and RacerPro.

8.4 A reputation and knowledge based trust model and decision making mechanism

There are numerous trust solutions have been proposed for each environment (e.g. P2P, MAS, e-commerce, etc.), in this section, it aims at developing a trust service platform that cooperates with applications and services to for the trust in future social IoT environments.

8.4.1 Trust in the Internet of Things

The IoT is considered as the network of devices such as household appliances, office appliances, and vehicles which are embedded with computing system, sensors, connectivity with self-configuring capability. These electronic devices, which are billions in number and varied in size and computing capabilities, are ranging from Radio Frequency Identification tags (RFIDs) to vehicles with Onboard Units (OBUs). IoT is expected to enable advanced services and applications like smart home, smart grid or smart city by integrating a variety of technologies in many research areas from embedded systems, wireless sensor networks, service platforms, and automation to privacy, security and trust. Recently, the convergence of two emerging network paradigms Social Networks and IoT as social IoT has attracted many researchers as a prospective approach for dealing with challenges in IoT. The benefit of social IoT is the separation in terms of the two levels of humans and devices; allowing devices to have their own social networks; offering humans to impose rules on their devices to protect their privacy, security and maximize trust during the interaction among objects. Indeed, some social IoT systems are currently taking advantages of social relationship models to offer secure and reliable services by using the reputation and trust such as eBay, Amazon and Google's Web Page Rankings.

There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism. Some important properties of trust are stated and discussed in this report. Previous research has shown that trust is the interplay among human, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation. The competence is measurement of abilities of the trustee to perform a given task which is derived from trustee's diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee.

A trust system covers a large number of trust-related research aspects ranging from Trust Relationship and Decision, Data Perception Trust to Identity Trust [14]. Several works focus on trust evaluation and trust assessment in IoT and in social IoT. The authors assume that entities in the systems are human-related or human-carried which are capable of establishing relations depending and cooperatively working together in accordance with their owners' relationships. They proposed distributed, encounter-based, and activity-based trust management protocols in which entities compute and update trustworthiness of the partners once mutual interactions occur. The entities also share trust evaluations to their friends as recommendations to help friends in their trust-related processes. Thus, a reputation-based mechanism is needed to incorporate with the trust systems.

However, some malicious entities, which is dishonest and socially uncooperative in nature, could exploit the principal reputation-based properties to break the functionalities of the system by means of trust-related attacks such as self-promoting, bad-mouthing, good-mouthing, ballot-stuffing, discriminatory and whitewashing. Several solutions were proposed to try to deal with these kinds of attack by validating the identity as well as recommendation information through some trust compositions such as honesty, cooperativeness, community-interest, relationship factor and centrality. However, these solutions are mostly built for P2P network, ad-hoc networks or WSNs.

Other works proposed fuzzy approaches to calculate trust score from some TMs such as Experience, Recommendation, and Knowledge, or based on technical properties extracted from physical layer, core layer, and application layer in IoT system as a mechanism for access control. The trust scores are then mapped to permission; and the access requests are accompanied accordingly. This approach of trust calculation is, however, impossible to deal with the scenarios that TMs are crossed-domain. Several TMs are derived from both physical layer and core layer and other TMs could only be extracted from both core layer and application layer. For instance, to reckon the Knowledge TM, it is needed to extract valuable information from data of both physical layer and application layer, which describes the trustee.

The catalyst for figuring out trust features is that when judging whether a trustee (a person, a device or a service) is trustable or not, the trustor "thinks" like human by taking its knowledge, recommendations from trustor’s relations; and trustee’s reputation into account. Thus, the human processing when assessing trust is imitated in trust model by modulating Reputation, Recommendation, and Knowledge as three basic TMs. Basically, a trust service platform continuously manages and updates the Reputation and Recommendations TMs of all entities in the social IoT network by the reputation system. For the Knowledge TM, the trust service platform will cooperate with each application or service for specific trust information such as Knowledge trust ontology and trustor preferences. Then, the final stage, called Trust Calculation, is to calculate the trustworthiness or trust score of the trustor to the trustee, based on all three TMs, the user preferences and the application/service context. It can be done by using an appropriate algorithm assigned by the trust analysis and management system.

8.4.2 Social IoT Environment

Social IoT concept is eventually formalized in some ways, mostly bases on the idea that objects in IoT belong to humans in the network and people offer services through their owned objects. Social IoT, thus, is considered as social networks in which any device is capable of establishing social relationships with others according to its owners. These entities are exposed their characteristics to public areas through not only themselves but also the owners’ behaviours.

Among several social IoT models proposed, Atzori et al. [11] proposed that every device has one or more owners who could also have some other devices. The social IoT model is based on social relationships among humans by applying some defined mechanisms and rules. For example, each owner has a list of friends with other owner, representing its social relationships. If the owners of two devices are friends, then it is likely they will be cooperative with each other. A device may be carried or operated by its owner in certain community-interest environments (e.g. work place, home, social club). Entities belonging to a similar set of communities likely share similar interests or capabilities. D2D communication is through overlay social network protocols, or underlying standard communication network protocols (P2P, M2M), forming an autonomous social relationship which is potential for the social IoT paradigm. As a result, forms of socialization among objects are foreseen; and types of social relationships are also established as illustrated in Figure 23.

According to the social IoT model, the trust service platform is able to instantiate on a collaborative basis allowing multiple entities to share their trust related opinions, as induced from their knowledge and experience, by submitting to a reputation system.

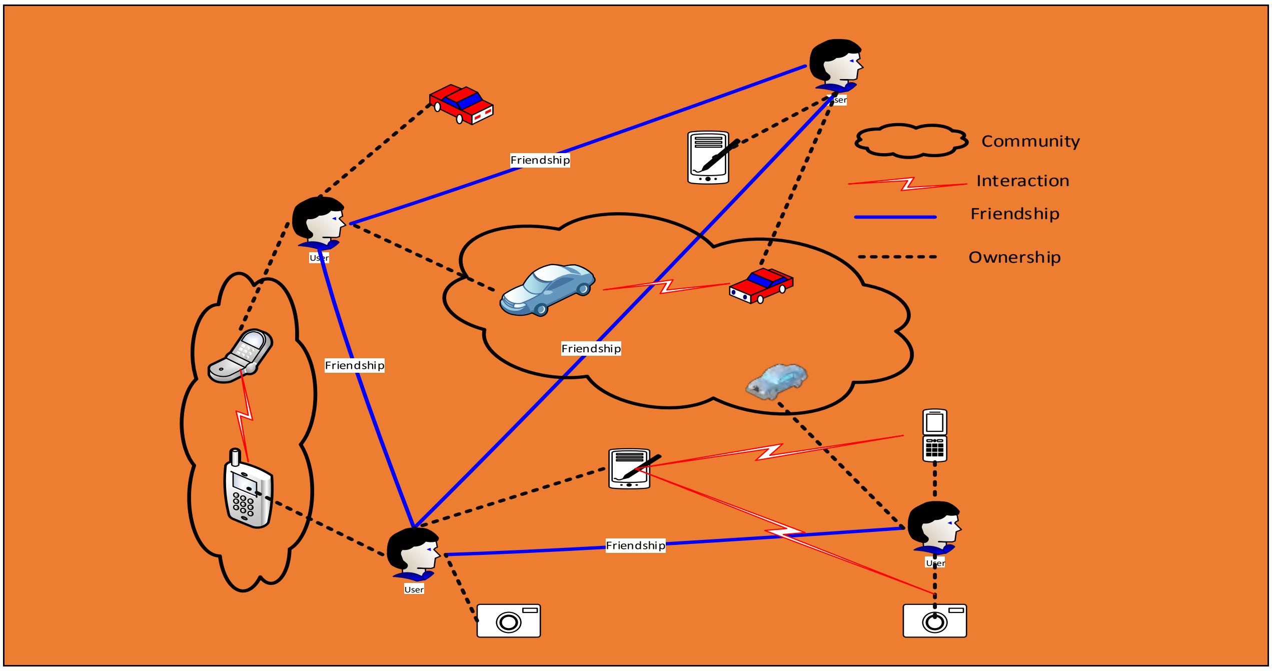


Figure 23 – Social structures of the IoT

8.4.3 Trust Models and Trust Metrics

Based on the approach mentioned in the Trust Model in previous sub-section, with the catalyst of imitating human trust processing as discussed above, a trust model comprises of three TMs namely Reputation, Recommendation, and Knowledge (See Figure 24).

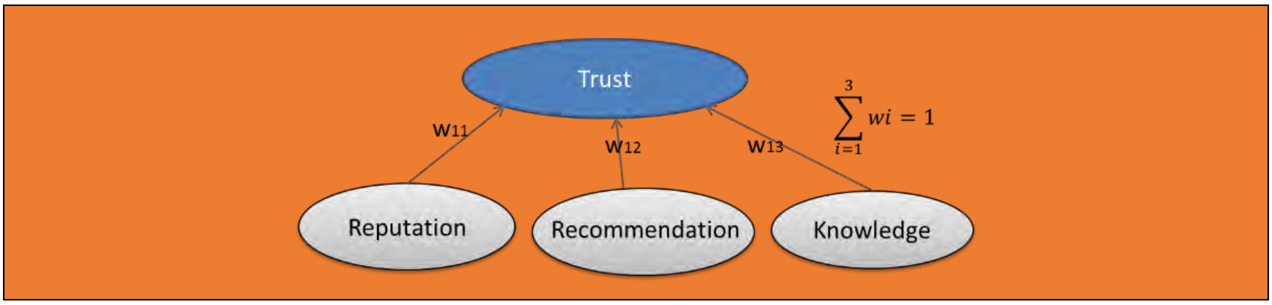


Figure 24 – A Trust Model with three Trust Metrics

This sub-section takes the trust-car sharing example for illustrating the policy mechanism reasoner. Generally, the Reputation and Recommendation TMs in the trust car-sharing example are similar to any other services; and can be get from the reputation system. The Human-to-Human knowledge can be also calculated depending on four TAs mentioned in the previous section. The Human-to-Object knowledge extraction algorithm and Trust Calculation mechanism are service-and-object specific.

Knowledge is the first party information provided by trustee to evaluate its trustworthiness and composed by some TAs depending on services and entities. Service providers are supposed to register their own information including both Knowledge TM ontology and requirements to the platform prior to use. These trust data has many dimensions and should be normalized and unified in order to be suitable for software oriented architecture (SOA) environment by using an ontology manager and an information model.

This report considers the platform for social IoT environment in which humans offer services through their owned items. Thus, when judging Knowledge TM of a service, a user needs to assess both device and device's owner as illustrated in Figure 25.

The Human-to-Human knowledge can be comprised of four TAs: Honesty, Cooperative, Community-Interest and Experience, inspired by ideas in [84].

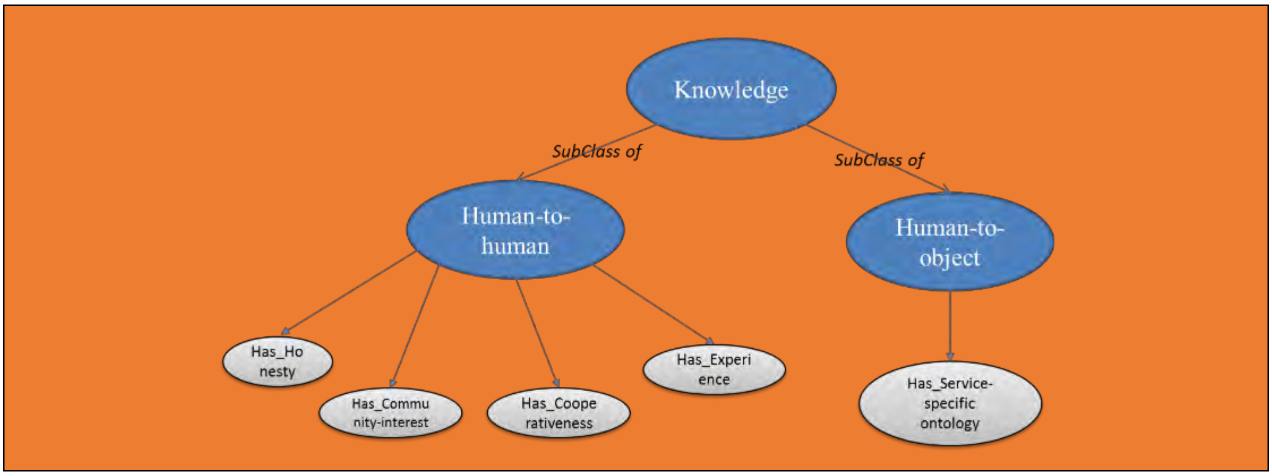


Figure 25 – The Knowledge TM is divided into two sub-ontologies

The honesty represents whether a human is honest. In social IoT, a malicious user can be dishonest when providing services or trust recommendations, resulting in disrupting the trust management and service continuity. Thus, honesty is chosen as a TA to prevent an entity from trusted-related attacks.

The cooperativeness represents the level of the social cooperation from the trustee to the trustor. The higher cooperativeness means the higher trust level. A user can evaluate the cooperativeness of others based on social ties and select socially cooperative users.

The community-interest represents whether trustor and trustee have close relationship in terms of social communities, groups, and capabilities. Two entities with a degree of high community-interest have more opportunities in interacting with each other, and thus can result in higher trust level.

The experience of trustor A to trustee B in particular context ‘c’ (service C) is based on the track record of previous interaction. If the interaction is successful then, experience value is +1, in case of failure it is -1. The record of the successful and unsuccessful interactions is valuable information for trust judgment.

The detail calculations of the three TAs Honesty, Cooperativeness and Community-Interest are presented in [85] whereas the TA Experience is achieved from the interaction record conducted by Trust Agent. By taking these trust properties, our trust service platform will be able to deal effectively with certain types of malicious behaviour aimed at misleading other entities.

The Human-to-Object knowledge depends on both service and object; and can be calculated using sufficient information provided from the service with appropriate reasoning methods and machine learning technique.

8.5 Autonomic trust management

The future ICT environment integrates a large amount of everyday life devices from heterogeneous network environments, bringing a great challenge into trust, security, and reliability management. In doing that, smart objects with heterogeneous characteristics should cooperatively work together. It is a known fact that the devices particularly in IoT very often expose to public areas and communicate through wireless, hence vulnerable to malicious attacks [89] [90] [91]. Migrating IoT application specific data into the Cloud offers great convenience, such as reduction of cost and complexity related to direct hardware management [92] [93] [94]. However, to evaluate the trustworthiness of their systems cannot use only the past experiences, since the novel autonomic systems nowadays are highly dynamic and the behaviors are unpredictable. These restrictions are detrimental to the adaptation of Trust Management Systems to today’s emerging IoT architectures, which are characterized with autonomic and heterogeneous nodes and services.

Clouds or cloud computing has picked up many researchers’ attention, as such it is being a part of IoT. Undoubtedly, trust management is the most challenging issues in emerging cloud systems where millions of services, applications and nodes deployed together under a single umbrella to serve each other [95]. Together with the current dynamism of the systems and the autonomous users’ behavior, the latter task has been too complicated [96]. In reality, autonomic trust management is hard to be realized because the cloud of things is hard to control due to the scale of deployment, their mobility and often their relatively low computation capacity [97] [98]. As a result, the trust manager itself should be adaptive to the autonomic conditions posed by the system.

This sub-section shows a framework for autonomic trust management based on Monitor, Analyse, Plan, Execute, Knowledge (MAPE-K) feedback loop to evaluate the level of trust in an IoT cloud ecosystem. Even though many research activities were carried out in the scope of autonomic trust management, non of them have addressed how an integration between IoT and cloud would work. It is necessary to utilize MAPE-K feedback control loops to enhance consistency of the system while improving robustness and scalability with the introduction of cloud concepts.

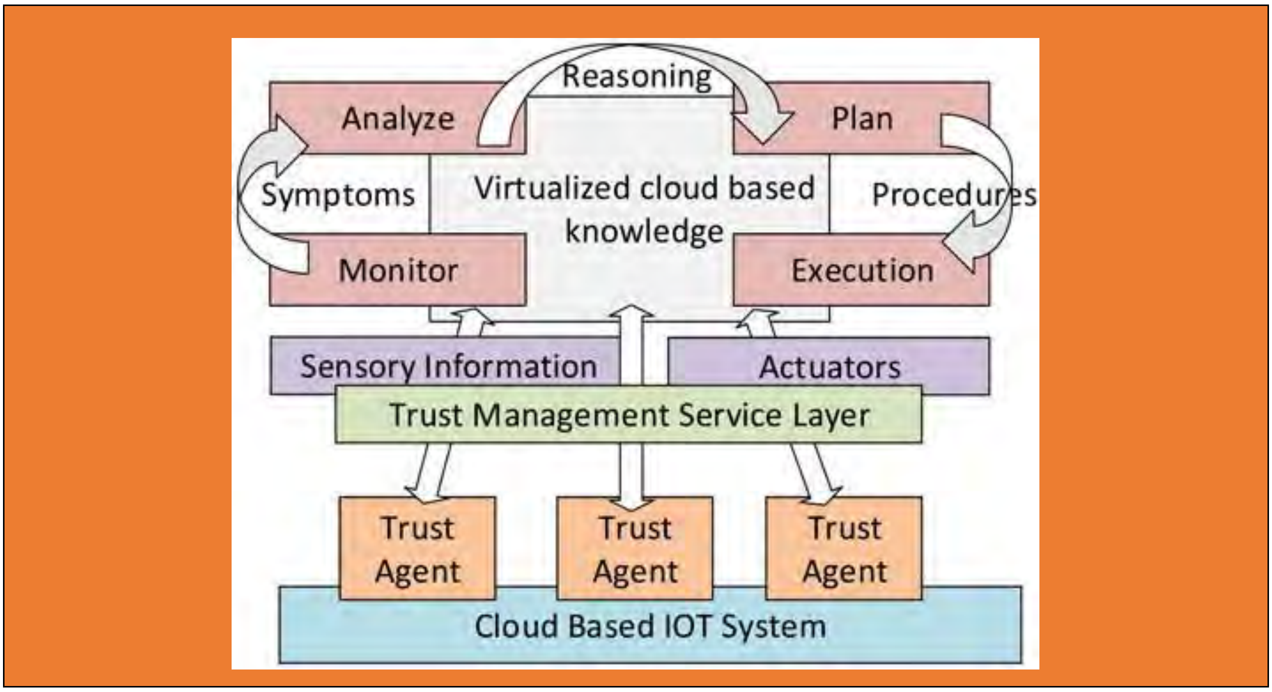


Figure 26 – MAPE-K feedback loops for adaptive trust agents

The system is highly dynamic which implies the need for adaptive decision making and autonomic agents with control loops to manage resources. A promising approach to handle such dynamics is self-adaptation that can be realized by a MAPE-K feedback loop. To provide an evidence that the system goals are satisfied, regarding the changing conditions, state of the art advocates the use of formal methods. However, it is important to remark that the trust agents in Figure 43 do not replace the monitoring phase of the MAPE-K, but instead it filters out the trust information from other information while holding the required knowledge to support the autonomic decision-making process.

The distributed nature of the trust agents assure quick responses and scalability of the solution. In Figure 43, the monitor function aggregates, correlates and further filters the information until it determines a symptom that needs to be analyzed. Analyze function performs complex data analysis and reasoning on the symptoms provided by the monitor function. Analyze function would be influenced by stored knowledge data which, in fact, virtually centralized but physically exists within the trust agents. If changes are required, a change request is logically passed to the plan function. The plan function structures the actions needed to achieve goals and objectives and creates or selects a procedure to enact a desired alteration in the managed resource. At the same time it can take on many forms, ranging from a single command to a complex work-flow. Execution phase changes the behavior of the managed resource using effectors, based on the actions recommended by the plan function. In fact, the executors are open APIs to the trust managers' feedback system.

The knowledge in Figure 26 is the standard data associated with the monitor, analyze, plan and execute functions. The knowledge here is shared among the trust agents and could be virtually centralized using cloud techniques to facilitate decision making. This would include data such as all trust related information, context information, topology information, historical logs, metrics, symptoms, policies, etc. This system now becomes self-adaptive based on MAPE-K feedback loops that deal with dynamic trust issues arising due to openness. It is important to notice that the particular focus is on adaptations that require elevating or downgrading the level of trust in a system.

8.6 Using Blockchain as Tool

Blockchain technology can assist smart devices to become autonomous agents, independently conducting a different of transactions. Blockchain technology in case of not existing of a centralized server brokering messages, enhancing file storage, transmissions and deciding roles any decentralized IoT. Applying the blockchain technology to the environment of IoT provides trustful potentials. Since the time an invention finishes final assembly, the M2M services provider into a universal blockchain representing its starting of life could register it. In addition, when sold a trader or end buyer could register it to a local blockchain public or private area. When registered, the device stays a unique entity within the blockchain during its life [106].

Consequently, in a blockchain relied on IoT, the ability of preserving product data, its history, product revisions, guarantee details and end of life in the blockchain becomes the Blockchain itself can mean the trusted product database. Therefore, we can use this technology in various IoT use cases as real example requirements to enhance trust among heterogeneous sensors with complicated service relationships.

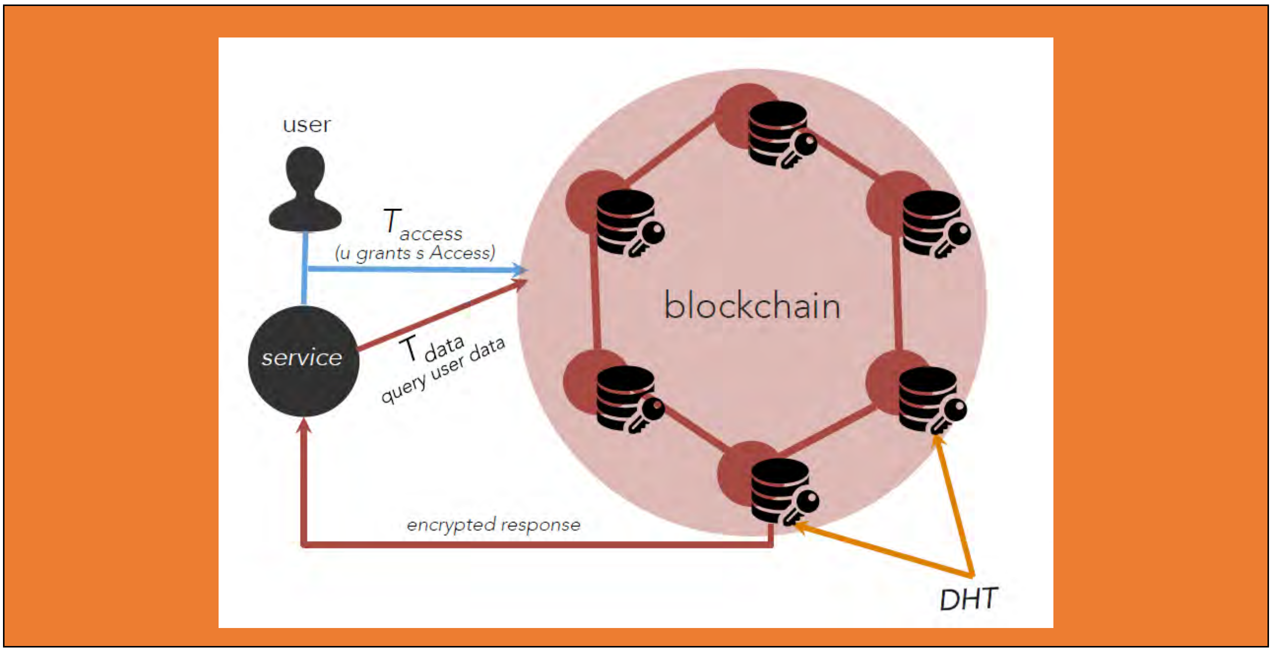


Figure 27 – Overview of the decentralized platform [114]

Figure 44 shows overview of the decentralized platform using blockchain technology. There are the three entities comprising the system: 1) mobile phone users, interested in downloading and using applications; 2) services, the providers of such applications who require processing personal data for operational and business related reasons (e.g., targeted ads, personalized service); and 3) nodes, entities entrusted with maintaining the blockchain and a distributed private key-value data store in return for incentives. The blockchain accepts two new types of transactions: Taccess, used for access control management; and Tdata, for data storage and retrieval. These network operations could be easily integrated into a mobile Software Development Kit (SDK) that services can use in their development process [114].

9 Roadmap and working priority for standardization

9.1 Related standardization activities in ITU-T

9.1.1 Correspondence Group on Trust (CG-Trust) in SG13

At the last April SG13 meeting, the CG-Trust was created for preliminary work on trust standardization after the workshop on future trust and knowledge infrastructure held in ITU-T.

Based on the agreement, Q16/13, as the parent group of CG-Trust, has made a lot of efforts to develop a technical report for trust provisioning in ICT infrastructure.

So far, 5 CG-Trust meetings in total have been held.

- 1st meeting (e-meeting, 17 June 2015): 4 contributions
- 2nd meeting (Geneva, 13 – 23 July 2015): 5 contributions

- 3rd meeting (e-meeting, 2 September 2015): 5 contributions
- 4th meeting (Geneva, 17-18 October 2015): 6 contributions
- 5th meeting (Geneva, 30 November – 11 December 2015): 12 contributions

There are key outcome of CG-Trust. So far CG-Trust has being developed a technical report through face-to-face and electronic meetings. From the CG-Trust activity, the group identified the following points while developing the technical report:

- The importance of trust in future ICT infrastructure towards knowledge society;
- A clear understanding of trust from different perspectives;
- Key challenges and technical issues;
- Various use cases for trust provisioning mostly in IoT environment;
- Key functionality from the generic architectural framework;
- Existing efforts for standardization on trust in related SDOs.

9.1.2 Trust related activities in cloud computing group of SG13

The cloud computing group (WP2) in ITU-T SG13 has been developing various standards on cloud. Recently this group has been developing the trust related recommendation.

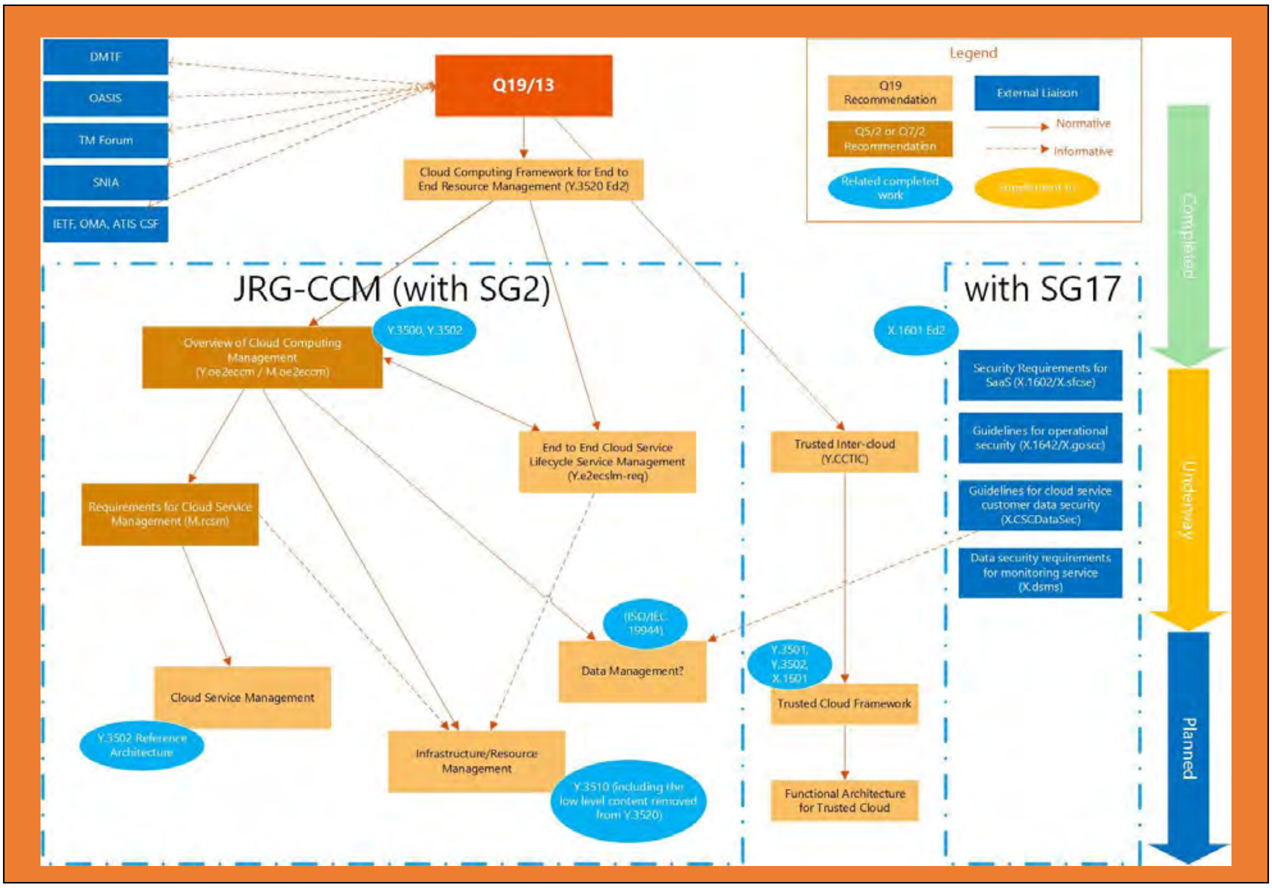

DMTF
OASIS
TM Forum
SNIA
IETF, OMA, ATIS CSF
Q19/13
Cloud Computing Framework for End to End Resource Management (Y.3520 Ed2)
Legend
Q19 Recommendation
External Liaison
Q5/2 or Q7/2 Recommendation
Normative
Informative
Related completed work
Supplement to
Completed
Underway
Planned
JRG-CCM (with SG2)
Y.3500, Y.3502
Overview of Cloud Computing Management (Y.oe2eccm / M.oe2eccm)
End to End Cloud Service Lifecycle Service Management (Y.e2ecslm-req)
Requirements for Cloud Service Management (M.rcsm)
(ISO/IEC 19944)
Data Management?
Cloud Service Management
Y.3502 Reference Architecture
Infrastructure/Resource Management
Y.3510 (including the low level content removed from Y.3520)
Trusted Inter-cloud (Y.CCTIC)
Y.3501, Y.3502, X.1601
Trusted Cloud Framework
Functional Architecture for Trusted Cloud
with SG17
X.1601 Ed2
Security Requirements for SaaS (X.1602/X.sfcse)
Guidelines for operational security (X.1642/X.goscc)
Guidelines for cloud service customer data security (X.CSCDataSec)
Data security requirements for monitoring service (X.dsms)

Figure 28 – The updated Roadmap diagram for Q19/13 in ITU-T (TD 478 Rev.1 (WP 2/13))

- Trusted Inter-Cloud (Y.CCTIC) - Cloud computing – Trusted inter-cloud computing framework and requirements

  This Recommendation specifies framework of trusted inter-cloud computing and relevant use cases, based on the framework specified in ITU-T Rec. Y.3511. The scope of this Recommendation includes: objectives of trusted inter-cloud computing, requirements for security of trusted inter-cloud, requirements for governance of trusted inter-cloud, requirements for resiliency of trusted inter-cloud.

The cloud group plans to develop trusted related documents such as trust cloud framework and functional architecture for trusted cloud, etc.

9.1.3 New Question proposal on security and trust provisioning in IoT in SG20

At the opening plenary of SG20 in October 2015, a contribution to initiate new Question for security and trust provisioning in IoT was presented. This Contribution highlights security and trust provisioning in IoT since only the IoT security is not enough to support future converged service environments. In alignment with the security matters led by SG17, it also provides the Question description for SG20 to have a leadership on all the IoT issues concerning security and trust matters. SG20 did not take any decision and invited related Contributions in the next meeting, which will be held in January 2016 for further detailed discussion.

9.2 Related standardization activities in other SDOs

9.2.1 Activities in Online Trust Alliance (OTA) for IoT

Introduction

This sub-section introduces the activities for IoT Trust by the Online Trust Alliance (OTA).

OTA is a non-profit organization with the mission to enhance online trust and address IoT risks comprehensively. The framework presents guidelines for IoT manufacturers, developers and retailers to follow when designing, creating, adapting and marketing connected devices in two key categories: home automation and consumer health and fitness wearables.

Through extensive research, this taskforce concluded that the safety and reliability of any IoT device, app or service depends equally on security and privacy, as well as a third, often overlooked component: sustainability.

Without addressing sustainability, devices that may have been secure off the shelf will become more susceptible to hacking over time. This could lead to hackers remotely opening garage doors and turning on baby monitors that are no longer patched to infiltrating fitness wearables to spy on health vitals, or creating mayhem by sabotaging connected appliances.

Although the IoT framework of OTA has identified various requirements, most of them can be seen as reinterpretation of traditional security and privacy issues. Therefore, we can notice that trust in OTA includes more broad range of scope covering security and privacy as well as regulatory issues.

Activities relating to Trust

The following requirements are the proposed baseline for any self-regulatory and/or certification program. It should be noted in addition to what is outlined below, companies must adhere to all regulatory requirements as they pertain to where their users or consumers reside, including but not limited to breach notification, disclosure requirements, child protection, anti-spam and related consumer protection laws and regulations [107],[108],[109].

(1) User should be informed about privacy policy prior to product purchase, download or activation and be easily discoverable to the user.

Target is to provide the consequences of declining or opt-in policies, including the impact to usage of main product features or functionality. This can be done in many ways including but not limited to following options, a short notice on product packaging, providing an online link to privacy policy or in welcome information pack.

(2) To maximize the clarity and readability, display of policy must be optimized to user interface.

The working group encourage a short-layered format to resent policies to match with the user interface.

(3) All personally identifiable data types and attributes must be evidently disclosed by the inventor.

Vital and personal information such as physical location, medical information (heart rate, pulse, and blood pressure), and user profile info are among such information for an example.

(4) Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for specified purposes.

Any sharing of personal data with third parties for other purposes must be revealed and require an agreement, including an explanation of the nature and scope of the data shared and limitations on the use of the data if any.

(5) The term and duration of the data retention policy must be disclosed.

As long as customer uses the product or service data can be retained and must be deleted upon account termination or expiration.

(6) Any ability to remove personal and sensitive data (other than purchase transaction history) must be informed to users by the manufacture upon discontinuing device use, loss, damage, sale or device end-of-life.

This option should be provided at no-charge.

(7) Personally identifiable and sensitive data must be encrypted or hashed when at storing in databases and when using available communication methods.

The idea is to achieve end-to-end encryption for all personal data. For direct wired connections, this is not mandatory and can be applied currently available encryption technologies to make sure to secure the integrity of data being communicated.

(8) Default passwords must be prompted to be reset or changed on first use or uniquely generated.

Best practise is to use two credentials for administrative and user access where ever possible and password reuse must be avoided. Furthermore randomly generated passwords are more encouraged.

(9) All user sites must adhere to SSL best practices using industry standard testing mechanisms.

Minimum of 90% site score is expected.

(10) By default all device sites and cloud services must exploit HTTP over SSL (HTTPS) encryption.

In general this is known as Always On Secure Sockets Layer (AO SSL) or HTTPS everywhere.

(11) Manufacturers must conduct penetration testing for devices, applications and services.

The goals of penetration tests are determine feasibility of a particular set of attack vectors, identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence, identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software, assess the magnitude of potential business and operational impacts of successful attacks, test the ability of network defenders to detect and respond to attacks and provide evidence to support increased investments in security personnel and technology.

(12) If there are any weakness in the product, manufacturers must have capabilities to rectify in a prompt and reliable manner either through remote updates and / or through consumer notifications and instructions.

Wherever this is not possible, manufacture must inform the user in advance. Alternatives could be device replacement or manufacturer upgrade, product recall or onsite service for connected home devices.

(13) Manufacturers must provide secure recovery mechanisms for passwords.

Recommendations are multi-factor verification (email and phone, etc.), lockout capability for multiple sign-on attempts among many.

(14) Device must provide a visible indicator or require user confirmation when pairing or connecting with other devices.

(15) Manufacturers must publish and provide timely mechanisms for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, account compromise, etc.

(16) Manufacturers must provide a mechanism for the transfer of ownership including providing updates for consumer notices and access to documentation and support.

(17) To avoid email frauds, configuration of all security and privacy related communications must adhere to authentication protocols.

Industry standards include SPF, DKIM and DMARC are some of the technologies to avoid email fraud, malicious emails and spear phishing exploits. Additionally organizations should consider STARTTLS and opportunistic Transport Layered Security (TLS) for email to aid in securing communications and enhancing the privacy and integrity of the message.

9.2.2 Activities in Trusted Computing Group (TCG) for Interoperable Trusted Computing Platforms

Introduction

This sub-section introduces the activities for interoperable trusted computing platforms by the Trusted Computing Group (TCG).

TCG is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.

TCG technologies do not provide an immediate solution to all IoT device and service security needs, but they enable existing and new IoT solutions to be fundamentally far more robust than today's state-of the art.

Solutions developed by TCG includes authentication, cloud security, data protection, IoT, mobile security and end-to-end security. Similar to OTA, TCG has also focused on various solutions from existing security and privacy issues while taking into account additional concepts of trust.

Activities relating to Trust

TCG has provided the following concepts for trust related terminologies in the architecture's guide for cyber security [110], [111].

- Trusted Network Connect (TNC)

  TCG's TNC network security architecture and open standards help businesses create and enforce security policies as well as facilitating communication between security systems. Using TNC standards, network managers gain better visibility into who and what is on their network, and whether devices remain compliant with policies. More than two dozen vendors of commercial and open source products support TNC standards in their products.

  TCG's TNC network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also enable network-based access control enforcement — granting or blocking access based on authentication, device compliance, and user behavior — and security automation.

  TNC provides security automation, Network Access Control (NAC), and interoperability in multi-vendor environments. Products from over two dozen commercial and open source vendors support and help implement TNC standards.

  Expanded efforts for enterprise security have resulted in open specifications including the Interface to a Metadata Access Point (IF-MAP). IF-MAP provides a standard way for information security products to rapidly share and respond to information about a variety of security-related topics and events.

- Self-Encrypting Drive (SED)

  Self-Encrypting Drives silently and automatically encrypt all user and system data, making sure this information doesn't fall into the wrong hands if the device or drive gets lost. Such drives may also be remotely wiped if they're lost or stolen.

- Trusted Platform Module (TPM)

  The Trusted Platform Module is a hardware security component built into a computing device that provides a hardware root of trust for user and device identity, network access, data protection, and more. TPMs are built into more than half a billion end systems, including many laptops and mobile devices.

  TPM Mobile is a scaled-down TPM designed for mobile environments, which retains the ability to cryptographically store passwords and digital keys, for example, to verify the device's identity. TPM Mobile is expected to be publicly available in the near future.

In addition, TCG has specified a set of fundamental security capabilities that will be required of many IoT devices. TSG has developed typical IoT security use cases and provides guidance for applying TCG technology to those use cases. Because IoT devices vary widely in their cost, usage, and capabilities, there is no one-sizefits-all solution to IoT security. The practical security requirements for different devices and systems will vary. Therefore, the list of solutions from TCG can be regarded as a menu from which the implementer can pick the options most suitable for their product or service.

9.3 Important work items for trust provisioning in ICT infrastructure

As a starting point of standardization for trust provisioning in ICT infrastructure, we should firstly consider the following work items.

- Overview of trust in ICT: It aims to provide a clear understanding of trust form different perspectives and identify key differentiations compared to security and privacy. It also highlights the importance of trust in future ICT infrastructure towards knowledge society.
- Service scenarios and capabilities: From various use cases analysis, considering sharing economy, it is necessary to develop service scenarios for trust provisioning and define required capabilities to support trust.
- Requirements for trust provisioning: Frome key challenges and technical issues, it is necessary to specify detailed requirements in terms of different viewpoints, considering various stakeholders.
- Architectural framework: It targets to identify core functions for the future trustworthy ICT infrastructure and develop architectural models including detailed functional architectures.
- Technical solutions for trust provisioning: It covers methodologies for specifying trust metrics and measuring trust. It also needs to develop protocol specifications for trust provisioning and mechanisms for trust-based decision making.
- Trust provisioning in IoT: From the perspective of IoT, it is necessary to develop specific technical solutions applicable to the IoT applications with the connected devices.
- Trust provisioning in data analytics: From the perspective of big data analytics, it is necessary to develop specific technical solutions applicable to the processing and analysis of the large amount of data through cloud computing.

For more specific technical items for standardization, the followings should be considered.

(1) Trust Management

Trust has interactions with all vertical layers – users, applications, computing, networks, things. Thus similar to security, trust management technology is necessary as a separate common layer which covers all vertical layers. It basically needs identity management to assure the identity of an entity and support business and trust applications.

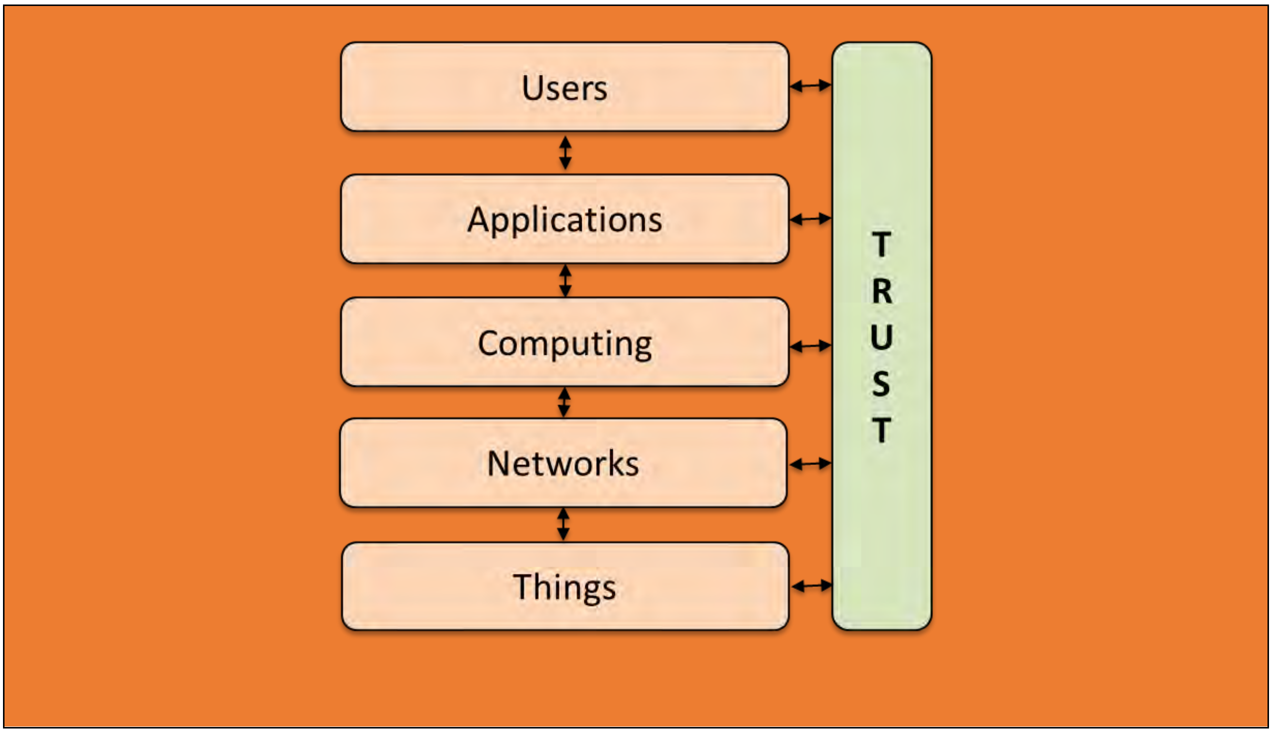


Figure 29 – Trust management (Trust as a cross domain relationship)

Trust management has the following key functionalities: monitoring management, data management, analytics management, expectation management and decision management. Specifically trust information for reputation and recommendation are exchanged to support these functionalities and adaptive knowledge based control for dynamics is further considered.

(2) Trust Measure & Calculate

For measurable trust, some mechanisms or solutions of trusts may be accounted by defining trust metric or trust index. There are several attributes for trust provisioning such as security, strength, reliability, availability, and ability, etc. Depending on services and applications, the required attributes of trust may vary. For example, for a particular application, trust attributes may be consisted of security, reliability and availability. Whereas, for other applications, security and reliability may be needed for such trust provisioning. The capability or attributes of trusts can be also classified into application types, costs, technical complexity, and human credibility/reputation. Depending on applications, most of trust solutions may be clarified and mapped.

(3) Trust-based Decision Making

In the IoT environments, data generated by devices and existing infrastructure must be able to be shared through databases for analysis. For trusted data exchange, each process from sensing to actionable knowledge requires trust enabled mechanisms such as data perception trust, trustworthy data fusion/mining and reasoning with trust related policies and rules (see Figure 47).

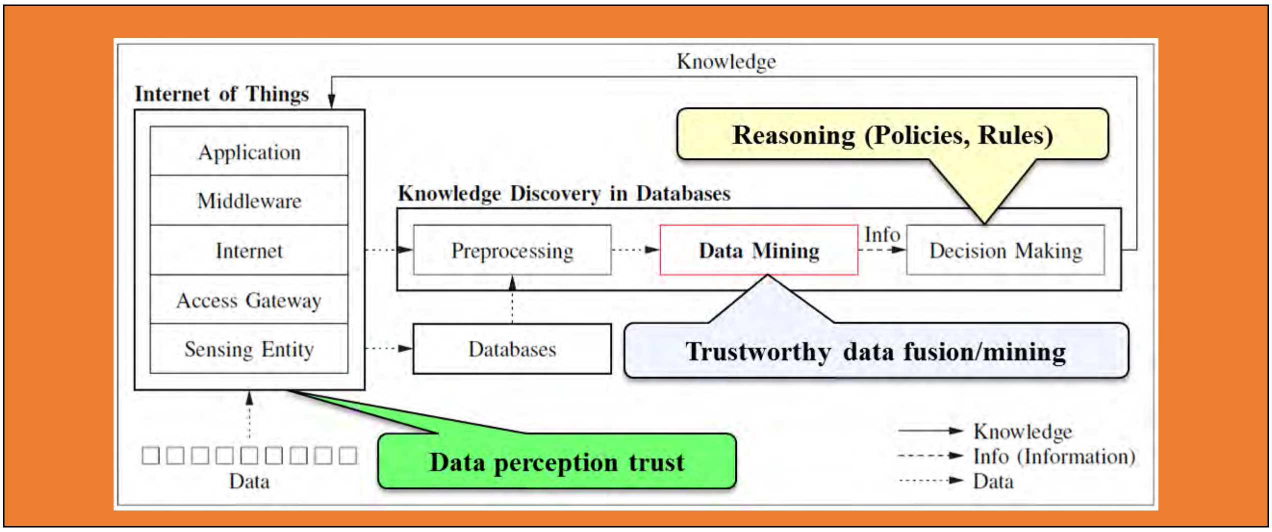


Figure 30 – Trust-based decision making

The state of entities changes dynamically, e.g., sleeping and waking, connected/disconnected, etc. as does their context, including location and speed. Moreover, the number of entities can change dynamically. For supporting these characteristics, autonomics through feedback loop control for handling trust requirements under dynamic conditions is required and recent advances like fog computing or edge computing can be a possible solution for distributed and localized trust-based decision making.

(4) Constraint Environment

For small-sized objects with limited power, their capabilities as communication objects are less (sometimes much less) than those of higher-end processing and computing devices. To cope with these constrained objects, performance, less energy consumption and heterogeneity should be considered. Trust solutions with lightweight mechanisms that remove unnecessary loads/messages and minimize energy consumption become a necessity.

(5) New Business Models

The platform services using big data and open platforms are becoming important to be provided by the automatic capture, communication and processing of the data of things based on the rules configured by operators or customized by subscribers. Trust-based services require more reliable techniques for trust related information and its processing (e.g., data fusion and data mining). Thus trust in new business models considering sharing economy will be quite an essential element for value added services.

9.4 Next step for future standardization

At the SG13 December 2015 meeting, SG13 has decided to extend the CG-Trust activity until April 2016 in order to further improve the current technical report on trust.

To progress related standardization on trust, we need to discuss the following possible ways at the coming SG13 meeting, April 2016.

- Option 1 (Establishment of a new group like Focus Group)

  If we need a new group to quickly develop specifications and invite external experts for trust standardization, it is necessary to establish a Focus Group for more dedicated work.

- Option 2 (Task assignment to related groups)

  If it's ready to go forward for developing related Recommendations, SG13 needs to assign tasks to related Questions based on the CG-Trust technical report. SG13 also needs to send liaisons to other SGs (e.g., SG20 for IoT, SG17 for security) for announcing the outcome of CG-Trust and stimulating related standardization work.

10 Conclusions and future work

This technical report first describes definitions, key characteristics and features on trust from different perspectives for a clear understanding of trust as standardization activities for trusted information infrastructure in ITU-T Correspondence Group on Trust (CG-Trust). Secondly, the report illustrates various use cases for trust provisioning based on the technical report of ITU-T CG-Trust and materials from other SDOs and related literature. In addition, this section also analyses these uses cases in terms of purpose, method, actors and considerations for measuring trust.

In addition, the report proposes trust taxonomy in different domains in order to identify important issues for trust provisioning in the ICT infrastructure and describe strategies for solving these issues, particularly considering trust provisioning process.

For a specific technical solution, report provides the demonstration of feasible methods to implement architecture for trust data analysis and a frame work for trust decision making for trustworthy IoT Eco-system. Furthermore, it emphasizes key functionalities, requirements and standard interfaces for autonomic decision making. And then, the report focuses on developing a generalized trust definition for all entities in Social IoT in which trust can be formalized and produced within our platform in future. Supporting to our goal, topics on trust provisioning strategies for services, applications and ICT infrastructure and ideas on trust ontology has been discussed. Finally report elaboration the suggestions on a framework for autonomic trust management based on Monitor, Analyse, Plan, Execute, and Knowledge feedback loop to evaluate the level of trust in an IoT cloud ecosystem.

From standardization point of view, until now, a number of standards focusing on network security and cybersecurity technologies have been developed in various standardization bodies including IETF. The scope of these standards needs to be expanded to take into consideration trust issues in future ICT infrastructures. There are a few preliminary activities taking place, for instance in OTA and TCG. However, as existing research and standardization activities on trust are still limited to social trust between humans, trust relationships between humans and objects as well as across domains of social-cyber-physical worlds should also be taken into account for trustworthy autonomous networking and services.

Based on this, one needs to first find various use cases considering user confidence, usability and reliability in ICT ecosystems for new business models which reflect a sharing economy. Then, a framework for trust provisioning including requirements and architectures should be urgently specified in relation to the relevant standards. In addition, global collaborations with related standardization bodies are required to further stimulate trust standardization activities.

More specifically, the following key items are identified as future work for standardization on trust.

- Overview of trust in ICT
- Service scenarios and capabilities
- Requirements for trust provisioning
- Architectural framework
- Technical solutions for trust provisioning
- Trust provisioning in IoT
- Trust provisioning in data analytics

Additionally, there is a need to incorporate trust issue into related SGs' activities in ITU-T.

- SG13: One of main roles of SG13 is to develop related Recommendations on ICT infrastructures. In this regards, so far SG13 has played significant roles for dealing with future knowledge and trust ICT infrastructures. Therefore, SG13 should take related work items on overall ICT infrastructures for future standardization. Especially SG13 needs to focus on trusted networking technologies.
- SG20: As the recently established SG20 is targeting IoT applications, services and platforms as well as smart cities infrastructure, SG20 should consider trust in IoT.
- SG17: As trust is tightly associated with security and privacy issues, a liaison with SG17 activities on security matters is required.

- Others: Depending on specific topics, a collaborative work is needed, for instance, identification issue with SG2.

Finally, a close collaboration with other SDOs and forums (listed below) is needed.

- Existing security solutions: IETF, W3C
- IoT: oneM2M, FI-WARE, OIC, AllSeen Alliance
- Cloud Computing: TCG, Cloud Security Alliance
- Other groups: OTA

Furthermore, there is a need to address lots of issues on governance and transparency while developing trust related standards.

11 References

[1] B. Alcalde, “Towards a Decision Model based on Trust and Security Risk Management,” Seventh Australasian Conference on Information Security, pp. 61-67, 2009.

[2] D. Gambetta, “Can We Trust Trust,” in Trust: Making and Breaking Cooperative Relations, 1990, pp. 213-238.

[3] M. S. T. Grandison, “A Survey of Trust in Internet Applications,” IEEE Communications Surveys and Tutorials, 2009.

[4] Entrust, “White Paper: The concept of trust in network security,” 2011.

[5] I. Pranata and R. A. Geoff Skinner, “A Holistic Review on Trust and Reputation Management Systems for Digital Environments,” International Journal of Computer and Information Technology, 2012.

[6] E. Chang, F. Hussain and T. S. Dillon, “Fuzzy nature of trust and dynamic trust modelling in service oriented environments,” in Workshop on secure web services, Fairfax, USA, 2005.

[7] E. Chang, T. Dillon and F. K. Hussain, “Trust Reputation for Service-Oriented Environments,” West Sussex, England, John Wiley & Sons Ltd, 2006.

[8] uTRUSTit-2012, “White Paper: Trust Definition “Defining, Understanding, Explaining TRUST within the uTRUSTit Project”, August 2012.,” 2012.

[9] C. M. a. L. C. Liam McNamara, “Trust and Mobility aware Service Provision for,” in In Proceedings of Workshop on Requirements and Solutions for Pervasive Software Infrastructures, Dublin, Ireland, 2006.

[10] A. C. &. J. P. &. C. Wolf, “SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation,” Toronto, Ontario, Canada, 2010.

[11] L. Atzori, A. Iera and G. Morabito, “SIoT: Giving a Social Structure to the Internet of Things,” Communications Letters, pp. 1193-1195, 2011.

[12] F. Bao and I. Chen, “Dynamic Trust Management for Internet of Things Applications,” in International Workshop on Self-Aware Internet of Things, Self-IoT, USA, 2012.

[13] C. D. D. O. N. S. P. Bonatti, “An integration of reputation-based and policy-based trust management,” in Proceedings of the Semantic Web Policy Workshop, 2005.

[14] T. Y. K. S. A. H. J. J. R. J. B. S. T. M. Winslett, “Negotiating trust on the web,” in IEEE Internet Computing, 2002.

[15] J. H. J. Golbeck, “Accuracy of metrics for inferring trust and reputation,” in Proceedings of the 14th International Conference on Knowledge Engineering and Knowledge Management, 2004.

[16] J. H. J. Golbeck, “Inferring reputation on the semantic web,” in Proceedings of the 13th InternationalWorldWideWeb Conference, 2004.

[17] P. R. e. al, “Reputation Systems,” Communications of the ACM, pp. 45-48, 2000.

[18] J. F. J. I. a. A. K. M. Blaze, “The KeyNote Trust Management System,” University of Pennsylvania, 1999.

[19] A. S. Aarti Singh, “Introducing Trust Establishment Protocol In Contract Net Protocol,” in International Conference on Advances in Computer Engineering, Bangalore, Karnataka, India, 2010.

[20] R. Neisse, “Trust and Privacy Management Support for Context-aware Service Platforms,” University of Twente, 2012.

[21] C. M. L. C. Liam McNamara, “Trust and mobility aware service provision for pervasive computing,” First International Workshop on Requirements and Solutions for Pervasive Software Infrastructures, 2006/5.

[22] C. P. Mouratidis H, “Practitioner’s challenges in designing trust into online systems,” Journal of theoretical and Applied Electronic Commerce Research, vol. 5, pp. 65-77, 2010.

[23] F. M. ,. M. N. Z. Paolo Giorgini, “Requirements engineering for trust management:model, methodology, and reasoning,” International Journal of Information Security, 2006.

[24] K. M. H. T. R. A. C. A. S. Jose E. Fadul, “A Trust-Management Toolkit for Smart-Grid Protection Systems,” IEEE TRANSACTIONS ON POWER DELIVERY,, vol. 29, no. 4, pp. 1768-1779,.

[25] J. Z. T. T. U. F. M. R. C. John Finnson, A Framework for Modeling Trustworthiness of Users in Mobile Vehicular Ad-hoc Networks, vol. 7379, Berlin: Springer, 2012, pp. 76-87.

[26] P.-T. C. a. C.-S. Laih, “A challenge-based trust establishment protocol for peer-to-peer networks,” SECURITY AND COMMUNICATION NETWORKS, p. 71–78, 2011.

[27] A. L. A. S. Laurent Gomez, “Trustworthiness Assessment of Wireless Sensor Data for Business Applications,” in International Conference on Advanced Information Networking and Applications, Bradford, 2009.

[28] W. Zhang, S. Das and Y. Liu, “A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks,” in IEEE SECON 2006 proceedings., Reston, VA, 2006.

[29] M. F. J. a. L. Blaze, “Decentralized Trust Management,” in IEEE Conference on Security and Privacy, 1996.

[30] S. B. Y. Y. N. X. Jingpei Wang, “Distributed Trust Management Mechanism for the Internet of Things,” in International Conference on Computer Science and Electronics Engineering, 2013.

[31] S. C. M. Bahtiyar, “Extracting trust information from security system of a service,” Journal of Network and Computer Applications, pp. 480-490, 2012.

[32] Z. F. Y. X. Li X, “A multi-dimensional trust evaluation model for large-scale P2P computing,” ournal of Parallel and Distributed Computing, pp. 837-847, 2011.

[33] Y. L. H. Z. Y. Sun, “A trust evaluation framework in distributed network: Vulnerability analysis and defense against attacks,” in IEEE Infocom, 2006.

[34] R. A. J. H. d. B. J. Shaikh, “Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems, pp. 1698-1712, 2009.

[35] A. W. J. a. R. A. T. Z. Liu, “A Dynamic Trust Model for Mobile Ad Hoc Networks,” in 10th IEEE Int’l Workshop on Future Trends of Distributed Computing Systems, China, 2004.

[36] M. M. Nima Dokoohaki, “Effective Design of Trust Ontologies for Improvement in the Structure of Socio-Semantic Trust Networks,” International Journal On Advances in Intelligent Systems, 2008.

[37] E. Dumbill, “XML Watch: Finding friends with XML and RDF,” IBM Developer Works, 2002.

[38] B. P. J. H. J. Golbeck, “Trust Networks on the Semantic Webs,” Trust Networks on the Semantic, Springer, 2003.

[39] G. D. S. Toivonen, “The Impact of Context on the Trustworthiness of Communication: An Ontological Approach,” in Workshop on Trust Security, and Reputation on the Semantic Web, 2004.

[40] B. A. J. Hradesky, “Elements for Building Trust,” in iTrust: A Conference on Trust Management, 1994.

[41] A. S. D. Brondsema, “Konfidi: Trust Networks Using PGP and RDF,” in WWW'06 Workshop on Models of Trust for the Web (MTW'06), Edinburgh, UK, 2006.

[42] M. W. M. V. S. a. G. L. Ricardo Neisse, “Trust Management Model and Architecture for Context-Aware Service Platforms,” in In Proceedings of the 2007 OTM confederated international conference on On the move to meaningful internet systems:, 2007.

[43] KCN, “Knowledge Centric Networking,” 2014. [Online]. Available: Available: https://www.ee.ucl.ac.uk/kcn-project/.

[44] A. I. G. M. a. M. N. L. Atzori, “The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization,” Computer networks,, pp. 3594-3608, 2012..

[45] F.-Y. Wang, “The Emergence of Intelligent Enterprises: From CPS to CPSS,” IEEE Intelligent Systems, 2010.

[46] e. a. Jay Lee, “A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems,” Elsevier Journal, 2015.

[47] G. Vanecek, “The Internet of Things, ambient intelligent and the moving towards intelligent systems,” IEEE Smart Tech, 2012.

[48] M. B. H. Susen Döbelt, “Defining, Understanding, Explaining TRUST within the uTRUSTit Project,” uTRUSTit – Usable Trust in the Internet of Things, August 2012.

[49] C. B. J. H. Soumya Kanti Datta, “Fog Computing Architecture to Enable Consumer Centric Internet of Things Services,” in EURECOM,, Biot, France .

[50] G. T. J. K. a. R. D. W.E. Walsh, “Utility Functions in Autonomic Systems,” in International Conference on Autonomic, 2004.

[51] D. B. K. B. H. C. P. K. M. Andres J. Ramirez, “Applying Genetic Algorithms to Decision Making in Autonomic Computing Systems,” in ICAC’09, , Barcelona, Spain, 2009,.

[52] H. H. M. D. S. L. Martina Maggio, “A Comparison of Autonomic Decision Making Techniques,” cambridge, 2011.

[53] R. S. S. a. A. G. Barto, Reinforcement Learning: An Introduction, London, England: The MIT Press , 2005.

[54] L. C. a. M. Musolesi, "Autonomic Trust Prediction for Pervasive Systems," in International Conference on Advanced Information Networking and Applications (AINA'06) , 2006.

[55] R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems," Transactions of the ASME - Journal of Basic Engineering,, p. :35–45, 1960.

[56] P. Z. ,. A. V. V. Zheng Yan, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, p. 120–134, 2014.

[57] F. M. SIMON DOBSON, "A Survey of Autonomic Communications," ACM Transactions on Autonomous and Adaptive Systems, p. 223–259., 2006.

[58] J. M. a. E. Ipek, "Dynamic multicore resource management: A machine learning approach," IEEE Micro, 2009.

[59] A. G. J. J. a. W. M. P. Ulam, "Using model-based reflection to guide reinforcement learning," In Proceedings of the 2005 IJCAI Workshop on Reasoning, Representation and Learning in Computer Games,, pp. 1-6, 2005.

[60] R. H. J. S.-M. D. T. David Jelenc, "Decision making matters: A better way to evaluate trust models," Knowledge-Based Systems, pp. 147-164, 2013.

[61] D. Trcek, "Towards trust management standardization," in Computer Standards & Interfaces, 2004.

[62] D. Trcek, "An integrative architecture for a sensor-supported trust management," in Sensors, 2012.

[63] Y. G. Donovan Artz, "A survey of trust in computer science and the Semantic Web," JOURNAL OF WEB SEMANTICS, 2007.

[64] Y. G. D. Artz, "A survey of trust in computer science and the sematic web," Web Semantics: Science, Services and Agents on the World Wide Web, pp. 58-71, 2007.

[65] N. D. M. M. Federica Cena, "Forging Trust and Privacy with User Modeling Frameworks: An Ontological Analysis," in International Conference on Social Eco-Informatics, 2011.

[66] N. D. M. M. Federica Cena, "Forging Trust and Privacy with User Modeling," in International Conference on Social Eco-Informatics, 2011.

[67] R. I. A. Jøsang, "The beta reputation system," in Proceedings of the 15th Bled Electronic Commerce Conference, 2002.

[68] S. H. A. Abdul-Rahman, "Supporting trust in virtual communities," in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000.

[69] J. P. N. J. M. L. W.T.L. Teacy, "Travos: trust and reputation in the context of in accurate information sources," in Autonomous Agents and Multi-Agents System, 2006.

[70] M. S. H. G.-M. S.D. Kamvar, "The eigentrust algorithm for reputation management in p2p networks," in Proceedings of the 12th International Conference on World Wide Web, 2003.

[71] C. A. H. K. T. A. P. S. Pramod Anantharam, "Trust Model for Semantic Sensor and Social Networks: A Preliminary Report," in Aerospace and Electronics Conference (NAECON), Ohio, US, 2010.

[72] M. Compton, "The SSN ontology of the W3C semantic sensor network incubator group.," [Online]. Available: http://www.w3.org/2005/Incubator/ssn/wiki/images/f/f3/SSN-XG_SensorOntology.pdf.

[73] SAP, 2014. [Online]. Available: http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.Security.USDL-.

[74] P. e. a. Anantharam, “Trust model for semantic sensor and social networks: A preliminary report,” in Aerospace and Electronics Conference (NAECON), , 2010.

[75] E. e. a. Chang, “International Journal of Intelligent systems,” Trust ontologies for e-service environments, pp. 519-545, 2007.

[76] V. X. Tran, “WS-QoSOnto: a QoS ontology for web services." Services,” Service-Oriented System Engineering, 2008.

[77] A. G. S. G. Marko Vujasinovic, Trust-based Discovery for Web of Things Markets, Berlin, Germany, 2014.

[78] S. G. A. a. J. D. Galizia, “A trust based methodology for web service selection,” in International Conference on Semantic Computing, IEEE, 2007.

[79] B. P. J. H. Jennifer Golbeck, “Trust Networks on the Semantic Web,” in In Proceedings of Cooperative Intelligent Agents, 2003, pp. 238-249.

[80] A. S. David Brondsema, “Trust Networks Using PGP and RDF,” in Workshop on the Models of Trust for the Web, 2006.

[81] C. Burnett, “Trust Assessment and Decision-Making in Dynamic Multi-Agent Systems,” University of Aberdeen. Doctor of Philosophy, 2011.

[82] N. Griffiths, “A fuzzy approach to reasoning with trust, distrust and insufficient trust,” Lecture Notes in Computer Science, 2006.

[83] R. C. A. t. T. a. N. d. K. Kathrin Dentler, “Comparison of reasoners for large ontologies in the OWL 2 EL profile,” Semantic Web, 2011.

[84] S. H. Z. Yan, “Trust Modeling and Management - from Social Trust to Digital Trust,” Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions IGI Global, p. 2008, 290-323.

[85] R. I. A. Josang and C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision,” Decision Support Systems, pp. 644-681, 2007.

[86] L. Zadeh, “ Fuzzy Logic, Neural Networks, and Soft Computing,” Communications of the ACM, 1994.

[87] A. H. a. N. Georganas, “A Comparison of Mamdani and Sugeno Fuzzy Inference Systems for Evaluating the Quality of Experience of Hapto-Audio-Visual Applications,” IEEE International Workshop on Haptic Audio Visual Environments and Games (HAVE), 2008.

[88] E. J.-L. a. J. Siskos, “Assessing a Set of Additive Utility Functions for Multi-criteria Decision-Making, the UTA Method,” European Journal of Operational Research, pp. 151-164, 1982.

[89] H. J. B. J. d. H. L. S. L. a. Y.-J. S. Riaz Ahmed Shaikh, “Group-based trust management scheme for clustered wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems,, p. 1698–1712, ,2009.

[90] I.-R. C. M. C. a. J.-H. C. Fenye Bao, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” IEEE Transactions on Network and Service Management,, p. 169–183, 2012.

[91] R. R. I. A. a. C. F.-G. “. Javier Lopez, “Trust management systems for wireless sensor networks: Best practices,” Computer Communications, p. 2010, 1086–1093.

[92] S. R. a. M. M. Sheikh Mahbub Habib, “owards a trust management system for cloud computing,” p. 933–939, 2011.

[93] J. B. J. a. G.-J. A. Hassan Takabi, “Security and privacy challenges in cloud computing environments,” IEEE Security & Privacy, pp. 24–31, 2010. .

[94] Kai Hwang and Deyi Li, “Trusted cloud computing with secure resources and data coloring,” Internet Computing, IEEE, p. 14–22, 2010.

[95] K. K. a. Q. Malluhi, “Establishing Trust in Cloud Computing,” IT Professional, p. 20–27, 2010.

[96] A. F. R. G. A. D. J. R. K. A. K. G. Michael Armbrust, “A view of cloud computing,” Communications of the ACM, pp. 50–58, 2010.

[97] S. P. a. A. Benameur, “Privacy, security and trust issues arising from cloud computing,” p. 693–702, 2010.

[98] P. J. M. M. S. P. M. K. Q. L. S. L. Ryan KL Ko, “TrustCloud: A framework for accountability and trust in cloud computing,” pp. 584–588,, 2011. .

[99] A. Dumbrow, “Secure by design: a healthcare IT imperative,” 29 October 2015. [Online]. Available: https://blogs.vmware.com/healthcare.

[100]] P. Giorgini, F. Massacci, J. Mylopoulos and N. Zannone, “Requirements engineering for trust management: model, methodology, and reasoning,” 16 August 2006.

[101] J. Brill, “The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control,” Fordham Law Review, vol. 83, no. 1, 2014.

[102] Y. G. D. Artz, ““A survey of trust in computer science and the semantic web,” in Web Semantics: Science, Services and Agents on the World Wide Web, 2007.

[103] “[uTRUSTit-2012] Trust Definition White Paper - “Defining, Understanding, Explaining TRUST within the uTRUSTit Project”,” 2012.

[104]] Siemens, Improving Performance with Integrated Smart Buildings www.usa.siemens.com [Accessed on 25/Nov/2015].

[105] IBM, Building a worldwide smart connected enterprise https://developer.ibm.com/iotfoundation/blog/recipe-page/sogeti-high-tech/[Accessed on 25/Nov/2015].

[106] IBM. ADEPT Practictioner Perspective - Pre Publication Draft - 7 Jan 2015.

[107] Leigh Ann Gilson. (2015). Internet of Things Lacks Safety Today, Opening Door to Major Threats Tomorrow, Warns OTA. Online Trust Alliance. Retrieved from https://otalliance.org/news-events/press-releases/internet-things-lacks-safety-today-opening-door-major-threats-tomorrow

[108] OTA. (2015, August 11). IoT Trust Framework – Discussion Draft. Retrieved from https://otalliance.org/system/files/files/initiative/documents/iot_trust_frameworkv1_2.pdf

[109] OTA. (2015, 10 28). OTA IoT Trust Framework – Pre-Release Draft. Retrieved from https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_lastcall.pdf

[110] TCG Published. (2013, October). Architect’s Guide: Cybersecurity. TCG Published. Retrieved from http://www.trustedcomputinggroup.org/files/resource_files/CA36D107-1A4B-B294-D08829372D5796E1/Architects Guide Cybersecurity.pdf

[111] TCG Published. (2015, September 14). Guidance for Securing IoT Using TCG Technology. 1.1. TCG Published. Retrieved from https://www.trustedcomputinggroup.org/files/resource_files/CD35B517-1A4B-B294-D0A08D30868AB3D1/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[112] Mahalle, P.N., Thakre, P.A., Prasad, N.R., Prasad, R., "A fuzzy approach to trust based access control in internet of things," Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2013 3rd International Conference on, June 2013.

[113] oneM2M Technical Report, "oneM2M Use cases collection," September 2013.

[114] Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," Security and Privacy Workshops (SPW), 2015 IEEE, May 2015.

[115] Jin-Hee Cho, Ananthram Swami, "Towards trust-based cognitive networks: a survey of trust management for mobile ad hoc networks," 14th ICCRTS, May 2009.

GLOBA
COMMUNICATIO

2.

Future social media and knowledge society

ITU-T Technical Paper, Future social media and knowledge society (2015)

Introduction

Smartphone addiction

Most mothers claim "my children are dying brain" since they use smartphones the whole day. They feel that smartphones are similar to "Digital Drugs". Even when children go to bed, they have their smartphones with them. If the battery is almost worn out, most children panic easily. Many couples too often fight to use the smartphone. Most people send and receive an unlimited number of short messages by using social networking services, such as Twitter and Facebook. Smartphone addictions are due to a hyper-connected society of Internet, and they are more serious than Internet addiction or video game addiction. The average usage time per day of smartphone addiction is more than eight hours, while normal users use three hours. The main purpose of using smartphones is chatting, news searching, listening to music, and games. In the near future, mobile phone manufacturers may have to attach mandatory warning on smartphones such as "Excessive use of smartphones is harmful to your health and family reconciliation".

Data explosion

In Cisco's report on visual networking index in 2013, the volume of global Internet traffic is expected to reach 1.6 zeta bytes. (Note that 1 zettabyte = 1021 bytes = 1 billion terabytes = 1000 exabytes [1].) It has been announced that global Internet protocol (IP) traffic is expected to increase by about three-fold during the next five years. Wireless mobile traffic will exceed wired traffic, and video traffic with high definition quality will be the best. The major factor of traffic increase is the increase of Internet users and mobile devices, which are the result of the increase of broadband network bandwidth and video watching. The traffic volume of mobile devices will exceed the volume of personal computer (PC) traffic. Moreover, wireless fidelity (WiFi) traffic will exceed wired traffic for the first time. The percentage share of video traffic with high definition quality of all the traffic is expected to increase to 79% in 2018 compared to 66% in 2013. Traffic for Internet of things/machine-to-machine (IoT/M2M) applications will increase sharply in the near future.

New habit of online society

While people frequently use the Internet, they develop new habits. Currently, Internet users are increasing drastically. More than 50% of the people in the world are plugged-in at the Internet. The penetration ratio of smartphones is also steeply rising to more than 50%. Such penetration is causing change in the daily lives of people. Lately, many people may have the habit of checking their smartphones first thing in the morning; they check their schedule of the day to decide what clothes they have to wear, depending on their meeting and business schedule. On their way to work, they check their e-mails and mobile messages. For their daily lives and businesses, most people always connect to the online environment by using smartphones.

If they have a question during a meeting or a conversation, they directly check the related websites by using the smartphone so that they can obtain the facts from the Internet without a serious debate. To get the opinion of faraway experts, people call them immediately during the meeting. Sometimes, the meeting makes a vote from the all the participants including those who participated remotely. In some strange cases during face-to-face meetings, people start the meeting by using the social networking services in order to record the meeting results even though all the members are present in the same location.

In their day-to-day life, people check their personal schedule by using the Internet. They fix dates with their girlfriends, and book movie tickets by using the smartphone. When a girlfriend does not find the exact meeting place, her boyfriend directs her from her current location. Sometimes, he asks his friends to find out a nice venue to meet. He may enjoy a major event nearby like a street parade or fireworks. He can receive a discount coupon for a nearby restaurant while he is looking for a nice place.

By using the smartphone, he meets with his family and friends every day even though he could not meet them physically. Most mothers worry about their daughters when they come back home late in the evening; they can contact their daughters by using the smartphone to ensure that they return safely.

Social effects of online connectivity

At least once a day, people visit their social networking service like Twitter and Facebook, etc. When people are excluded to join as a friend or be a member of the social networking services, they are very disappointed and they think that are being bullied. People may worry about such online as well as offline exclusion from these communities. When people post the latest news and gossip on their social networking sites, they observe and wonder how to appeal or how to react to their friends. People may want to learn about new cultures of online social communities regardless of where they are or what they are working at. They may exercise new skills on how to live in an open culture of an online society. This online culture may be similar to a community culture like the Confucian civilization of Far East Asia.

Impact of technology development toward future society

The recent new technologies such as cloud computing, the web, and social networking services over the Internet are just the beginning of a wide variety of technological developments for the future. The future society is ready to invite new technologies like big data analytics, deep learning, augmented reality/virtual reality (AR/VR) as well as Internet of things (IoT), etc. In the near future, network transmission speeds will be exceeding more than 1 terabits per second and network processing power will be more than several hundred petaflops. The storage capability of individual smartphones or personal computers will be more than 1 terabytes.

IBM Watson supercomputer wins over a human at the television quiz show of Jeopardy in 2011. The thinking capability of a computer is superior to that of humans while puzzling over a particularly hard question [2]. This means that humans may focus on how to think rather than on how to remember. Humans welcome to utilize the storage and processing capability of the cloud computing system. The computer with artificial intelligence may help with how to think and remember. To overcome the language barrier, real-time language translation may be available. For example, if people are discussing some outstanding issues, the searching machine displays in advance the relevant information on the screen from the websites.

Wind of changes

In human history, there is no memory more than several billions of people are simultaneously talking and sharing contents/documents together through the Internet. The real-time voting and instant collection of opinions give an insight that technological development leads to a new cultural revolution. It offers new challenges to individual human life such as dating, chatting, shopping, listening to music, and enjoying movies, etc. There will be new business styles during the purchase, and the business transactions, etc. This leads to social, cultural, and political changes of the human life. Digital technology may be asking to change national laws and regulations. It also requests to change individual rights and responsibilities at the human and business levels.

Many people may feel ashamed in such technological developments. New ecosystems of life and business may be unstable without a guarantee of the stability and reliability of technology. If people try to drive a car without the required skill or confidence, this causes car accidents. New technologies may introduce the build-up of an unacceptable value chain (e.g. monopoly) of industries and eventually may destroy the traditional business models. The development of new technologies may be sometimes undesirable if certain levels of controllability and credibility are not guaranteed.

The online connectivity of the Internet is stronger than our expectations since it may introduce a new society and create a new culture. However, online connectivity may awake a very unstable resonance in society where collective actions, demonstrations, and public heated debates can occasionally take place. Moreover, many people receive many spam e-mails and are attacked by short message service phishing (i.e. smishing), etc.

Table of contents

1 Scope

This Technical Paper focuses on what is the expected and hopefully the knowledge society. It analyses the impacts of the development of digital technologies, the social effects of online connectivity, and the trends of the new ecosystem. It recognizes that the information and communication technology (ICT) is a centre of wind of changes. The future knowledge society will be built on the basis of the ICT infrastructure since it is totally an artificial society created by humans. The ICT infrastructure is not only for the delivery of digital data, but it also provides the eco-platform to share data, information, and knowledge. The new innovative technologies will be developed for the future open and collaborative knowledge society. Therefore, this Technical Paper explains the minimization of the unexpected risks and the maximization of the survivability of the future knowledge society.

2 Definitions

A number of terms in this Technical Paper with definitions are being used to describe knowledge society and social media.

2.1 data serialization: It is the process of translating data structures or an object state into a format that can be stored (for example, in a file or memory buffer, or transmitted across a network connection link) and reconstructed later in the same format or in another computer environment.

2.2 explicit knowledge: It is knowledge that can be readily articulated, codified, accessed and verbalized.

2.3 extensible markup language (XML): It is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable. It is defined by the W3C specification [17].

2.4 fintech: Financial technology, also known as FinTech, is a line of business based on using software to provide financial services.

2.5 hypertext markup language (HTML): It is the standard markup language used to create web pages. Along with cascading style sheets (CSS), and JavaScript, HTML is a technology, used by most websites to create visually engaging web pages, user interfaces for web applications, and user interfaces for mobile applications [18].

2.6 linked open data (LoD): It is the linked data that is open content. The linked data describes a method of publishing structured data so that it can be interlinked and become more useful through semantic queries. It enables data from different sources to be connected and queried.

2.7 markup language: A markup language is a system for annotating a document in a way that is syntactically distinguishable from the text. Some markup languages, such as the widely used hypertext markup language (HTML), have predefined presentation semantics with meaning that their specification prescribes how to present the structured data.

2.8 metadata: Metadata is "data about data". Two types of metadata exist: structural metadata and descriptive metadata. Structural metadata is data about the containers of data. Descriptive metadata uses individual instances of application data or data content.

2.9 resource description framework (RDF): It is originally designed as a metadata data model. It has come to be used as a general method for conceptual description or modelling of information that is implemented in web resources, using a variety of syntax notations and data serialization formats. It is defined by the W3C specification [49].

2.10 smishing: It is a compound of 'phishing' and short message service (SMS). SMiShing (SMS phishing) is a type of phishing attack where mobile phone users receive text messages containing a website hyperlink.

2.11 social graph: It is a graph that depicts personal relations of Internet users. The social graph has been referred to as "the mapping of everybody and how they are related".

2.12 tacit knowledge: It is the kind of knowledge that is difficult to transfer to another person by means of writing it down or verbalizing it.

2.13 uniform resource locator (URL): It is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

2.14 extensible markup language (XML) schema: An XML schema is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of documents of that type, above and beyond the basic syntactical constraints imposed by XML itself. These constraints are generally expressed using some combination of grammatical rules governing the order of elements.

3 Abbreviations

This Technical Paper uses the following abbreviations:

5G	Fifth Generation mobile networks
API	Application Programming Interface
APT	Advanced Persistent Threats
AR	Augmented Reality
AVC	Advanced Video Coding
BEMS	Building Energy Management System
CapEx	Capital Expense
CCTV	Closed-Circuit Television
CD-ROM	Compact Disk – Read-Only Memory
CPS	Cyber Physical System
CSRF	Cross-Site Request Forgery
CSS	Cascading Style Sheets
CSV	Comma-Separated Value
DIKW	Data-Information-Knowledge-Wisdom
DNA	Deoxyribonucleic Acid
DTD	Document Type Definition
EAV	Entity-Attribute-Value
GPS	Global Positioning System
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
I/O	Input/Output
IoT	Internet of Things
IP	Internet Protocol
IPTV	Internet Protocol Television
IT	Information Technology
ITU	International Telecommunication Union

ITU-T	The ITU Telecommunication Standardization Sector
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
LOD	Linked Open Data
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAB	Multi-Author Blog
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
NoSQL	Non-Structured Query Language
OpEx	Operational Expense
PaaS	Platform as a Service
PC	Personal Computer
PDA	Personal Digital Assistant
PHP	Hypertext Preprocessor
RDF	Resource Description Framework
RFID	Radio Frequency Identification
SaaS	Software as a Service
SDO	Standards Development Organization
SMS	Short Message Service
SNS	Social Networking Service; Social Networking Site
SOAP	Simple Object Access Protocol
SPARQL	SPARQL Protocol and RDF Query Language
SQL	Structured Query Language
UDDI	Universal Description, Discovery and Integration
UHD	Ultra-High Definition
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USB	Universal Serial Bus
VR	Virtual Reality
WiFi	Wireless Fidelity
WSDL	Web Service Definition Language
WSIS	World Summit on the Information Society
XaaS	Everything as a Service
XML	eXtensible Markup Language

4 Vision and technology trends toward knowledge society

4.1 Vision toward knowledge society

History of knowledge

The term "knowledge society" and "knowledge worker" are used for the first time by Peter Drucker in his 1959 book "Landmarks of Tomorrow" [3]. Since then, knowledge society has become increasingly important in the business world. In addition, the idea of knowledge society is inseparable from studies on information society. The notion of information society realizes the new economy based on scientific knowledge and changes in the workplace. The information society is based on technical breakthroughs to handle massive data through the network. The information and communication technology (ICT) removes main technical obstacles to achieve the information society. For a deeper understanding of knowledge society, the history that the humankind has thought, invented, created, considered, and perfected from the beginning of civilization into the twenty-first century is highlighted by Charles Van Doren [4]. The effects of social networking and online connectivity though the ICT infrastructure are interestingly imagined to make the future knowledge society.

At the 15th ITU Plenipotentiary Conference in 1999, the World Summit on the Information Society (WSIS) was created to develop the information society. During the first phase of WSIS, the debates on the information society were mainly focused on the ICT infrastructure. The concept of knowledge societies is more all-embracing and more conducive, which simply "opens the way to humanization of the process of globalization". The notion of knowledge is central to changes of education, science, culture, and communication. Knowledge is recognized as the object of huge economic, political and cultural stakes, to the point of justifiably qualifying the societies currently emerging.

Compared with the invisible hand by Adam Smith in his 1776 book "Wealth of Nations" (regarded as the father of economics), knowledge is an invisible public good, available to each and every individual. Knowledge fosters universality, liberty, and equality as a concept of openness [5]. Nobody should be excluded from the knowledge society. Young people play a major role in using new technologies of knowledge in their daily lives. To accelerate knowledge production, information processing and communication have built a cumulative and recursive loop of innovation among people. The creativity and innovation will play a major part in knowledge societies. It leads to promoting new types of collaborative processes to achieve genuine knowledge societies.

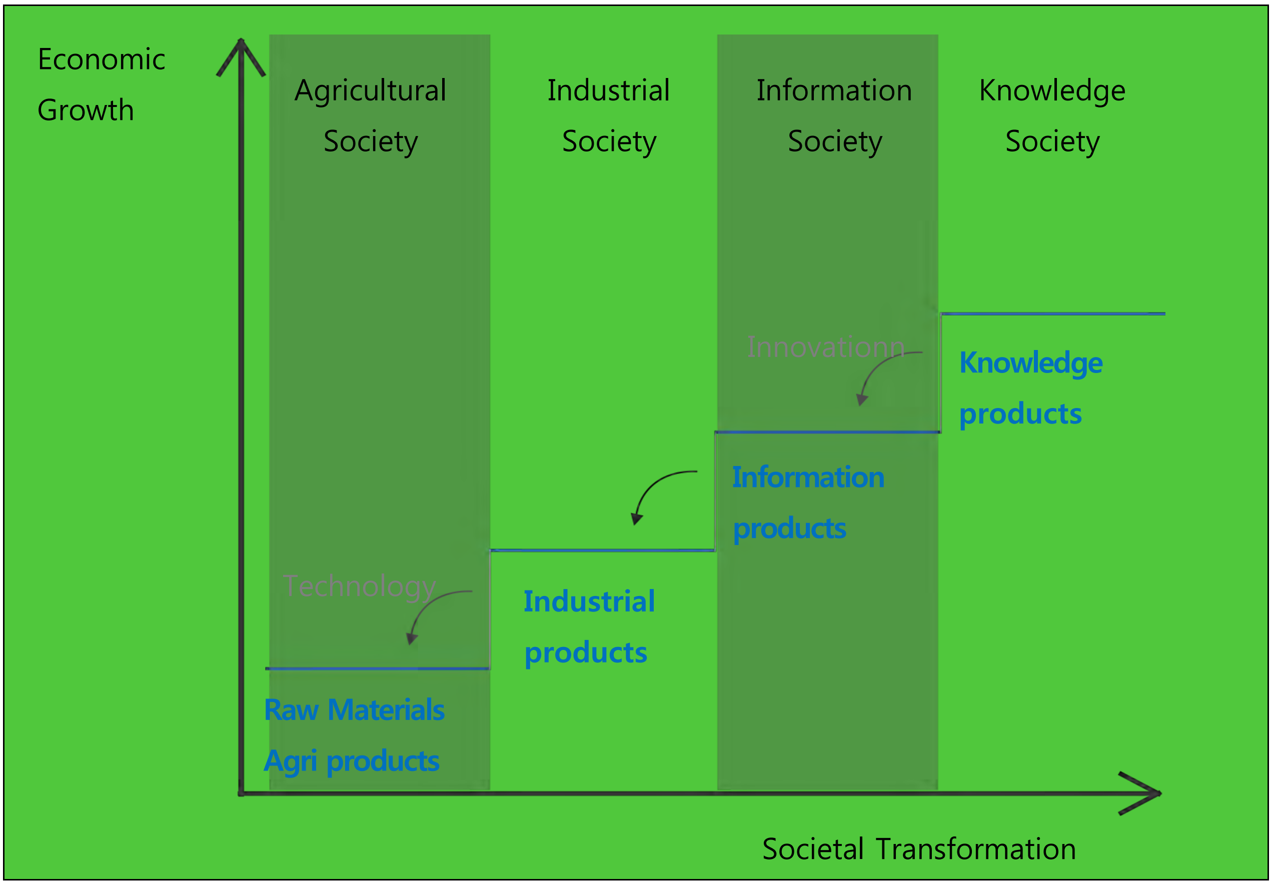


Figure 1 – From agricultural society to knowledge society

From agricultural society to knowledge society

To understand the evolution from the agricultural era to knowledge society, people interact with their environments and utilize technologies to satisfy their needs. During the agricultural revolution, people experienced a rapid improvement in agricultural production and farming technology. Farmers learned more practical and efficient farming technologies by using wheel and fertilizer. In the industrial revolution, the introduction of new power-driven machinery and other energy sources brought about a rapid and significant change of production. The steam engines, textile mills, and large scale equipment are capable of producing massive amounts of products.

Recently, in the information society, revolution is shifting from products to ideas and knowledge as shown in Figure 1 [6]. The ICT infrastructure is rooted to enable information society. The shifts are from hands-on skills to literacy skills and from industrial engineering to knowledge engineering. The decentralized and collective knowledge of the humankind will be a key factor to realize the new society. The power resides with people in charge of storing, sharing, and distributing information. New technologies and new knowledge products will be widely investigated to get new market opportunities.

What is the value of knowledge in information and communication technology?

For the value of knowledge, there are some statements: "All knowledge is of itself of some value" in Samuel Johnson in 1775, "The worth and value of knowledge is in proportion to the worth and value of its object" in Clodridge in 1825 [7]. Recently, and in relation to business, Firestone wrote "Thought, not money is the real business capital" [8]. Firestone observed that knowledge about how to produce products is more valuable than the products themselves. The value of knowledge exceeds the business values of industrial products and goods. Moreover, the shifts from tangible knowledge to intangible knowledge will be revolutionized by the way that knowledge is power in its own right.

In the information and communication world, characters, images, and symbols as well as audio/video signals can be used to indicate meaning and can be thought of as delivery of data. The transfer of data can be viewed as a process whereby knowledge can be transferred. The information and communication technology is used in all forms of recording and transfer of knowledge. The millions of books of knowledge in the libraries can be transferred in an electronic manner. The growth of information and communication technology has significantly increased the network capacity for creation and transfer of data. The evolution of the Internet and web technologies offers individuals tools to connect with each other worldwide. Innovation in mobile wireless digital technologies offers individuals a means to connect anywhere and anytime where digital technologies are accessible. ICT has the potentials to radically change education, training, employment for all members of human society.

However, the ICT infrastructure for individuals to produce and use data does not necessarily result in knowledge creation. Digital media delivers seemingly amounts of information. However, information alone does not create knowledge. For knowledge creation to take place, it is required to create awareness, meaning, and understanding of data and information. The critical analytic process of information is required to develop the knowledge that assists humankind. Information as such lacks reflection and critical thinking, and thus it can actually become "non-knowledge", which is false or inaccurate. The anticipated new technologies like big data analytics and semantic web will move both information and knowledge creations to use intelligence and create meaning.

Technology reduces the prices of telecommunication resources and enables the increase of transmission speeds and volumes of information. Technology has given birth to "networked societies". In a community, there is a set of networks within which individuals maintain special relationships whether they are family, ethnic, economic, professional, social, religious, political, or all of these simultaneously. Technological innovation helps in the emergence of new information and knowledge sharing systems that are shaped by the choices of a user or communities. The intelligence of knowledge and information sharing systems are enabled by a filtering principle that depends on the interaction of individual actions and processing of data. New information and communication technologies have created the emergence of knowledge societies. The International Telecommunication Union (ITU) as the United Nations top level standards organization relating to information and communication technologies may be concerned about future knowledge society.

Definitions of knowledge from ICT perspectives

Knowledge is a familiarity, an awareness or an understanding of someone or something such as facts, information, description or skills. Knowledge is acquired though experience or education by perceiving, discovering and learning [9]. Knowledge can refer to theoretical or practical understandings of a subject that is implicit (as with practical skills or expertise) or explicit (as with a theoretical understanding of a subject). It can be more or less formal or systematic.

Knowledge acquisition involves complex cognitive processes of perception, communication, and reasoning. From the ICT perspectives, knowledge is related to human perceptions of data streams of audio, video, image, and texts while transferring knowledge from people or organizations to others. By using e-mails or written documents for a meeting, knowledge is created and transferred by a dynamic acquisition and complex cognitive processes of the human brain like reasoning, observation, experimentation, formulation, and testing of hypotheses, etc. In scientific methods, knowledge has developed a broader view of the accumulated results of scientific experiments from discussions of communities or group of experts. For human behaviours in business, knowledge is related to a kind of decision-making process. Human behaviour is quite predictable when a certain level of experience and accumulated information are successfully collected through the network.

Types of intelligences

There is a theory of multiple intelligences rather than seeing intelligence as dominated by a single general ability which was proposed by Howard Gardner in his 1983 book "Frames of Mind: The Theory of Multiple Intelligences" [10]. He describes various types of intelligences as follows.

- **Logical/mathematical intelligence: NUMBER SMART**

This intelligence has to do with logic, abstractions, reasoning, numbers and critical thinking. This also has to do with having the capacity to understand the underlying principles of some kind of causal system. Scientists, engineers, computer programmers, and accountants are excellent in these kinds of intelligences. The key features of this intelligence are summarized as follows:

- Thinks conceptually;
- Skilled in reasoning, logic and problem solving;
- Explores patterns, categories, and relationships;
- Manipulates the environment to experiment in a controlled way;
- Questions and wonders about natural events.

- **Interpersonal intelligence (including emotional intelligence): PEOPLE SMART**

This intelligence has to do with interaction with others. Individuals who have high interpersonal intelligence are characterized by their sensitivity to others' moods, feelings, temperaments and motivations, and their ability to cooperate in order to work as part of a group. According to Gardner, inter- and intrapersonal intelligence are often misunderstood as being extroverted or liking other people. Those with high interpersonal intelligence communicate effectively and empathize easily with others, and may be either leaders or followers. They often enjoy discussion and debate. Gardner has equated this with the emotional intelligence of Goleman [11]. Emotional intelligence is the ability to recognize one's own and other people's emotions, to discriminate between different feelings, and to use emotional information to guide thinking and behaviour [12]. Counsellors, business people, politicians, and community organizers are excellent in this kind of intelligence. The key features of this intelligence are summarized as follows:

- Thinks and processes by relating, cooperating and communicating with others;
- Leaders among peers;
- Uncanny ability to sense feelings and intentions of others;
- Understands people, mediates conflict.

- **Bodily-kinaesthetic intelligence: BODY SMART**

The bodily-kinaesthetic intelligence is the control of one's bodily motions and the capacity to handle objects skilfully. Gardner elaborates to say that this also includes a sense of timing, a clear sense of the goal of a physical action, along with the ability to train responses. A person who has high bodily-kinaesthetic intelligence is generally good at physical activities such as sports, dancing, acting, and making things. Athletes, dancers, musicians, actors, builders, police officers, and soldiers are excellent of this intelligence. The key features of this intelligence are summarized as follows:

- Processes knowledge through bodily sensation;
- Excellent fine-motor co-ordination;
- Gut feelings about things;
- Great at mimicking your best or worst qualities and mannerisms;

- **Musical/rhythmic Intelligence: MUSIC SMART**

This intelligence has to do with sensitivity to sounds, rhythms, tones, and music. People with high musical intelligence normally have good pitch and may even have absolute pitch, and are able to sing, play musical instruments, and compose music. They have sensitivity to rhythm, pitch, meter, tone, melody or timbre. People for choirs, orchestra, bands, disc jockeys, and theatre are excellent in this kind of intelligence. The key features of this intelligence are summarized as follows:

- Thinks in sounds, rhythms and patterns;
- Sings, hums, whistles to themselves;
- Immediately responds to music;
- Performs and appreciates music and leads in songs;
- Sensitive to environmental sounds: crickets, bells, ambient music;
- Strong opinions of others' music.

- **Intrapersonal intelligence: SELF SMART**

This intelligence has to do with introspective and self-reflective capacities. This refers to having a deep understanding of the self; what one's strengths or weaknesses are, what makes one unique, being able to predict one's own reactions or emotions. Self-employed, researchers, theorists, and philosophers are excellent in this kind of intelligence. The key features of this intelligence are summarized as follows:

– Skilled in inner focusing;

– Displays a strong personality;

– Deep awareness of inner feelings, dreams and ideas;

– Reflective and analytical attitudes;

– Tends to shy away from team activities;

– Recognizes self-strength and weaknesses;

– Requires private space and time.

- **Linguistic/verbal intelligence: WORD SMART**

This intelligence has to do with high verbal-linguistic intelligence which displays at a facility with words and languages. People are typically good at reading, writing, telling stories and memorizing words along with dates. Verbal intelligence includes an ability of vocabulary, information, similarities, and comprehension. Teachers, journalists, writers, lawyers, and translators are excellent in this kind of intelligence. The key features of this intelligence are summarized as follows:

– Thinks in words;

– Highly developed auditory skills;

– Plays with sounds in language;

– Great storytellers, tells tales and jokes;

– Loves seeing, saying and hearing words;

– Heads are frequently stuck in a book;

– Likes to write.

- **Spatial/visual intelligence: PICTURE SMART**

This intelligence deals with spatial judgment and the ability to visualize with the mind's eye. Inventors, architects, engineers, and mechanics are excellent in this kind of intelligence. The key features of this intelligence are summarized as follows:

– Thinks in images and pictures;

– Clear visual images and representations;

– Knows the location of everything;

– Fascination with machines and contraptions.

Value of knowledge

The power of knowledge enables to create new add-on values to human business by combining some intelligence. All businesses have access to an extensive accumulation of knowledge since the understanding of customers' needs is combined with skills and experiences. By understanding what the customers want, combined with know-how, new chances of business may be obtained. By using knowledge in the right way and at the right time, the risks of new businesses are reduced and new opportunities are acquired.

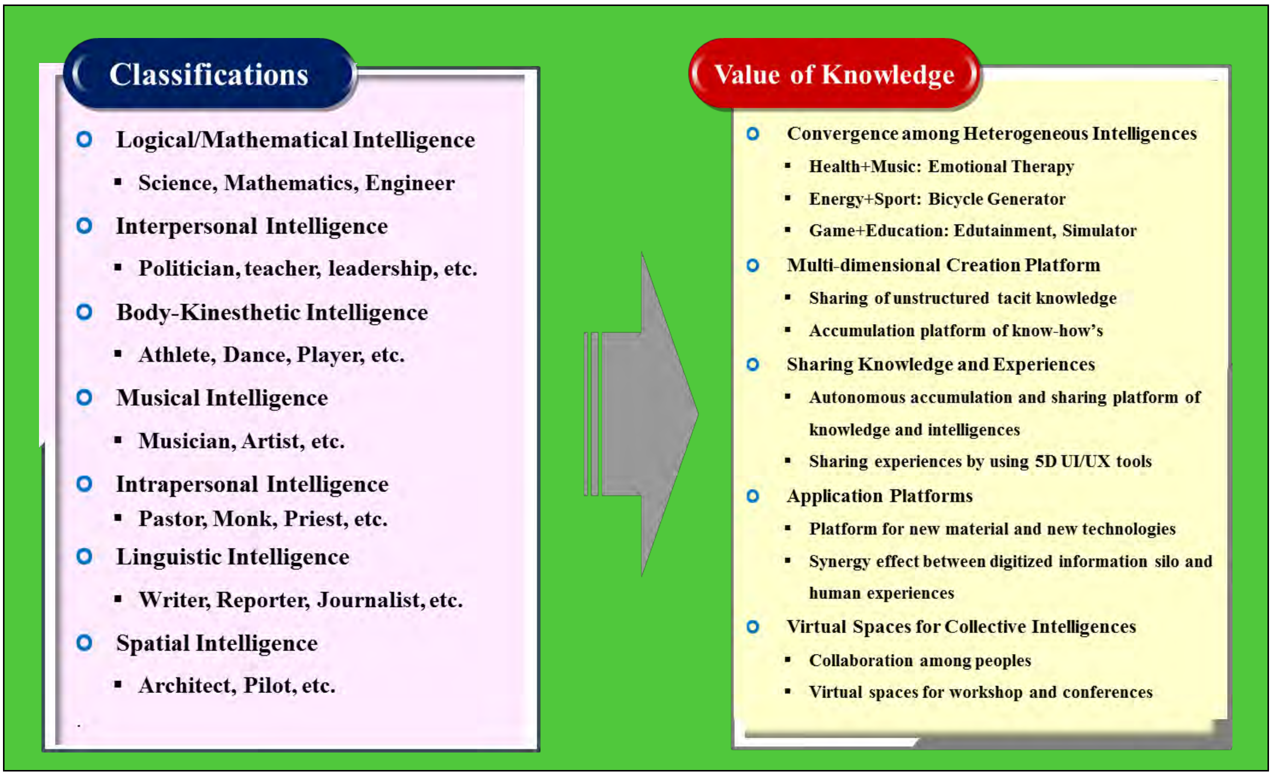
Knowledge has not only become one of the keys to economic development, but it also contributes to human development and individual empowerment. Knowledge is a source of power because it creates a capacity for action. One of the major advantages of knowledge is that it reduces costs by achieving economies of scale and avoiding useless duplication. The notion of "knowledge societies" holds out the possibilities for sustainable development, which may be also called "information society", "knowledge-based economies", "learning societies", and "risk societies".

In science and engineering domains, knowledge is essential to make fundamental theoretical or experimental researches. Since knowledge is fundamentally a matter of cognitive capability of problem-solving, skill, training, and learning, most research in the academic world is a hybrid of new knowledge generation and subsequent exploitation. Radical innovation is rarely possible without prior knowledge. Some collaboration between the academic world and industry is necessary both for the generation of new knowledge and its applications. New scientific knowledge is essential not only for fostering innovation and development of new technology, but also for creating new processes of education and collaboration of researchers. To accelerate knowledge creation, the collaborative research model of science and engineering is crucial.

The key ingredient of knowledge is understanding. The good understanding of basic theories and practice of experimental results are required among well-trained scientists and skilful engineers. Understanding means the ability to figure out a simple set of rules that explains a particular situation. For example, a teacher gives an explanation to his students of some features of a physical object. One understands reasoning, arguments, or language if one can consciously reproduce the information contents conveyed by the network. One understands a mathematical concept if one can solve problems using it, especially problems that are not similar to what one has seen before.

For the future knowledge eco-society, there are a lot of opportunities in order to accumulate the values of knowledge as shown in Figure 2. By converging heterogeneous intelligences as indicated by Howard Gardner, the disruptive innovation of knowledge may happen: for example, emotional therapy by converging health+music, bicycle generator by converging energy+sport, and edutainment by converging game+education, etc. The innovative convergence platform of knowledge will be open for multi-dimensional thinking which enables people to create clarity out of complexity. For innovation of science and engineering, the knowledge platform extends to factual and tangible dimensions where a wide variety of scientific data are collected and analysed. However, more intangible dimension including tacit knowledge and sharing experiences, which is not well formulated, can support the emotional and spiritual drivers of culture, lifestyle and consumption behaviour, alongside the dynamics of personal well-being. The future knowledge platform will be a comprehensive and integrated set of tools and technologies which maximize accumulation and collaboration of people's knowledge.

New virtual spaces with collective intelligences may replace the existing working spaces for workshops and conferences. A lot of researchers who have not actually participated at the workshop may be encouraged to investigate new business scenarios and technological solutions at the virtual space. The virtual space provides the possibility and challenges to design new activities of collaboration and learning.



Classifications

- Logical/Mathematical Intelligence
  - Science, Mathematics, Engineer
- Interpersonal Intelligence
  - Politician, teacher, leadership, etc.
- Body-Kinesthetic Intelligence
  - Athlete, Dance, Player, etc.
- Musical Intelligence
  - Musician, Artist, etc.
- Intrapersonal Intelligence
  - Pastor, Monk, Priest, etc.
- Linguistic Intelligence
  - Writer, Reporter, Journalist, etc.
- Spatial Intelligence
  - Architect, Pilot, etc.

Value of Knowledge

- Convergence among Heterogeneous Intelligences
  - Health+Music: Emotional Therapy
  - Energy+Sport: Bicycle Generator
  - Game+Education: Edutainment, Simulator
- Multi-dimensional Creation Platform
  - Sharing of unstructured tacit knowledge
  - Accumulation platform of know-how's
- Sharing Knowledge and Experiences
  - Autonomous accumulation and sharing platform of knowledge and intelligences
  - Sharing experiences by using 5D UI/UX tools
- Application Platforms
  - Platform for new material and new technologies
  - Synergy effect between digitized information silo and human experiences
- Virtual Spaces for Collective Intelligences
  - Collaboration among peoples
  - Virtual spaces for workshop and conferences

Figure 2 – Expecting value of knowledge by classification of intelligences

Sociality of knowledge

There is implicit knowledge (as with practical skill or expertise) or explicit knowledge (as with theoretical understanding of a subject). If a person has sufficient knowledge, he is thinking, making a judgement, and has an action for a subject. In order to collect sufficient information and knowledge, he searches for the related documents, discusses with colleagues, hears the opinions and shares the experiences of experts so that he can have a commonly accepted opinion on a topic. In a knowledge society, knowledge is recognized as the fundamentals of politics, economics, and culture. Individuals, communities, and organizations produce knowledge-intensive results. Peter Drucker viewed knowledge as a key economic resource in his 1969 book "The Age of Discontinuity" [13]. Knowledge is a commodity of knowledge workers to be traded for economic prosperity.

Similar to the recent social networking services, the heart of online knowledge sharing communities are the members who interact through technology and experience. The members discuss their community while constantly providing feedback that is used to shape and extend their knowledge. The social network provides best practices to ensure the synergy effects of knowledge in an area of a particular interest of each community. An interaction among people influences the development of knowledge. The collection and accumulation of knowledge drives to solve difficult problems that humans confront. For scientific matters, individual scientists are gathering ideas and opinions from communities based on some hypothesis and experimental results. The road to knowledge needs social networking environments via people, conversations, connections, and relationships. Therefore, all knowledge is socially mediated and access to it is achieved by connecting people. The social networking is to build a collection of human communities.

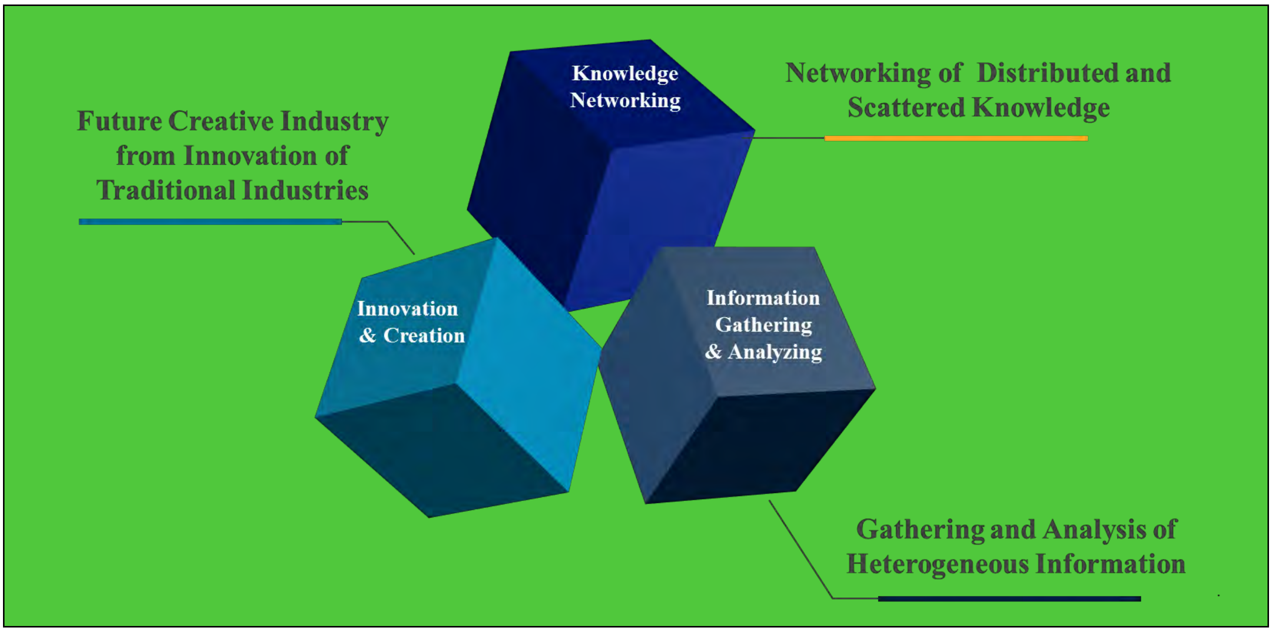

Knowledge Networking
Networking of Distributed and Scattered Knowledge
Future Creative Industry from Innovation of Traditional Industries
Innovation & Creation
Information Gathering & Analyzing
Gathering and Analysis of Heterogeneous Information

Figure 3 – Key features of knowledge society

Features of knowledge networking

From the perspectives of information and communication technology (ICT), knowledge is reusable information in a specific context. Knowledge networking is an effective way of combining individual knowledge, experiences, and skills in the pursuit of personal and community objectives. Knowledge is shared, developed, and evolved in the creation of new values. ICTs provide a new era of human thinking and knowledge processes. For knowledge workers, the use of ICTs has steadily changed from computation and communication. When people think about new concepts and patterns on real challenging issues, they can use the computing system to search in the local or external databases, use the e-mail and conference system, and discuss together with experts. The new work environments provided by ICTs attract highly motivated and knowledgeable individuals to address the detailed technical issues and engage in conceptual arguments. All the time through networking, knowledge is being continually evolved and developed. A lot of debate is invited and helpful criteria are suggested. To solve the outstanding problems, offline or one-to-one conversations can take place at the same time during the conference. Sometimes, within hours an expert solves the problems and then people make the decision with enough wisdom of the know-how.

Figure 3 shows the key features of knowledge society. First, knowledge networking is a collection of distributed and scattered knowledge. There is a rich and dynamic phenomenon of knowledge since it is more than access to information, more than the rules and inferences from theory, and more than tacit knowledge and wisdom of people's experiences. Second, from openness of communication, people gain information from experts in heterogeneous domains. They are willing to contribute their knowledge freely. The challenging problems are analysed by experts in different domains. The genuine process of cooperation is essential to share conclusions in harmony. Third, in knowledge society, a breakthrough innovation in a business matter helps to get patents. The scientific innovation leads to productive growth in related industries. The more radical and revolutionary innovations are easy to emerge from research and development through exchange of professional experiences. The information and communication technology can provide a new work environment favourable to innovation. With the help of ICTs, future new industries can be invented from creative idea generation.

Cross-disciplinary and interdisciplinary knowledge

One of the key characteristics of knowledge is seeking to synthesize broad perspectives, skill, experiences, and know-hows by crossing boundaries and thinking across traditional academic schools. Interdisciplinary knowledge is applied not only with education and training, but also with research and development. To solve the global common tasks on climate change and health, interdisciplinary studies are important to connect and integrate people with different knowledge disciplines such as physics, biochemistry, engineering, economics as well as information and communication technology.

Until now, the interdisciplinary studies are not easy if there is no agreement of soft and sufficient autonomy. Most experts with a specific knowledge in a certain domain may try to keep their own traditional methods and perspectives. Ideally, the synergy effects among people with broad dimensions and different experiences are promising. However, this contradicts the opinion that traditional disciplines are a barrier for experts who hesitate to commit themselves in interdisciplinary issues. Most organizations or scholarly journals build up their own silos of knowledge, where they store their disciplines to maintain the level of knowledge which is proudly accumulated in their own area.

The interdisciplinary activities are better suited for researchers with more than two disciplines to solve cross-domain problems. From the ICT perspectives, the research and development related to the Internet of things (IoT) and machine-to-machine (M2M) technologies are needed to collaborate with cultural and social sciences as well as in economics. In the scientific domain, the examples of interdisciplinary research areas include neuroscience, cybernetics, biochemistry and biomedical engineering. However, if the cooperative and collaborative procedures for interdisciplinary studies lack consensus, it would be difficult to carry out this interdisciplinary research.

To solve the global problems, the knowledge of eco-environments may consist of people, organizations, and processes that work together. The systematic framework would be defined with the belief that the component parts of a system can best be understood in the context of relationships with each other rather than in isolation. The ICT infrastructure can promote the interdisciplinary communication in order to avoid the silo effects of knowledge.

Knowledge accumulations

Knowledge accumulation is a step in creative thinking where information is gathered and analysed for a new idea. The societies possess huge knowledge accumulated by their own activities and experiences. Every society has its own knowledge assets. To envisage knowledge revolution of information and communication technology, the following issues are outstanding:

- **How to connect the different forms of knowledge**

There are many forms or types to represent knowledge or intelligences, and some forms are not represented by words. Tacit knowledge (or implicit knowledge) is difficult to transfer to other persons by means of writing it down in a document.

- **New forms of development, acquisition, and spread of knowledge**

The existing knowledge management relying on writing is quite restricted. New forms of capturing, developing, sharing, and effectively spreading knowledge would be needed by utilizing the ICT infrastructure as well as the computing and storage system. Texts and audiovisual forms of knowledge would be extended to the use of the five senses of human beings: sight, hearing, tasting, smelling, and touching.

- **New media as useful tools of the Internet and the web**

The existing file format across the Internet would be expanded to transfer various types of knowledge. The hypertext markup language (HTML) of the web technology is only designated to the text-based name of media types of software applications, audio, image, video and their mixed combinations. Digital technologies by using computer and the Internet can provide new means of communication and expression of knowledge. New media can replace the old media such as television, radio, movies, music, newspapers, magazines, books, and most printing materials.

- **Cultural and linguistic diversity of knowledge**

Languages, with their complex implications for identity, communication, social integration, education and development, are of strategic importance to create knowledge. Linguistic diversity plays a vital role in knowledge creation and accumulation to foster cultural diversity and intercultural dialogue. The multilingual forms of knowledge would be encouraged to preserve the existing cultural heritage.

Data → Information → Knowledge → Wisdom framework

"Knowledge Pyramid" refers to the representation of functional relationships between data, information, knowledge, and wisdom. "Typically information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge" [14]. From the ICT perspectives, data is simply defined as a string of bits which have no meaning or values because of lack of contexts and interpretation. When sensory signals of light, heat, sound, force, and electromagnetic are converged to digital forms, the data has a meaning with relevant description or additional explanation. Data itself cannot contain any information and it looks like noise without meaning or interpretation of empirical perception. Information is inferred from data and is defined as data that are endowed with meaning and purpose. If data to be sent is combined with interpretations from previous experiences and human cognitive intention, etc., the valuable information can be extracted. Also, when a lot of data streams are integrated or collectively analysed with other data, new information that could not be coming from individual data may be found. Knowledge is a difficult concept which is typically defined with reference to information. Humans can capture knowledge if information has been processed, organized, evaluated, or structured with combinations of experiences, insight, and intelligent cognitive decisions. Knowledge is only perceived by humans. By extending information inferred by data, knowledge is sometimes described as [14]:

- synthesis of multiple sources of information over time;
- organization and processing to convey understanding, experience and accumulated learning;
- a mix of contextual information, values, experience and rules.

One interesting issue is that knowledge has a recursive nature with data and information. When people write books and communicate with others, a set of data (i.e. texts, sounds, and images, etc.) is used to deliver information and knowledge. For voice telephony, tele-conferences or e-mails through the network, the digital bit stream can be interpreted to deliver information and knowledge together. It can be recognized depending on the level of interpretation and perception.

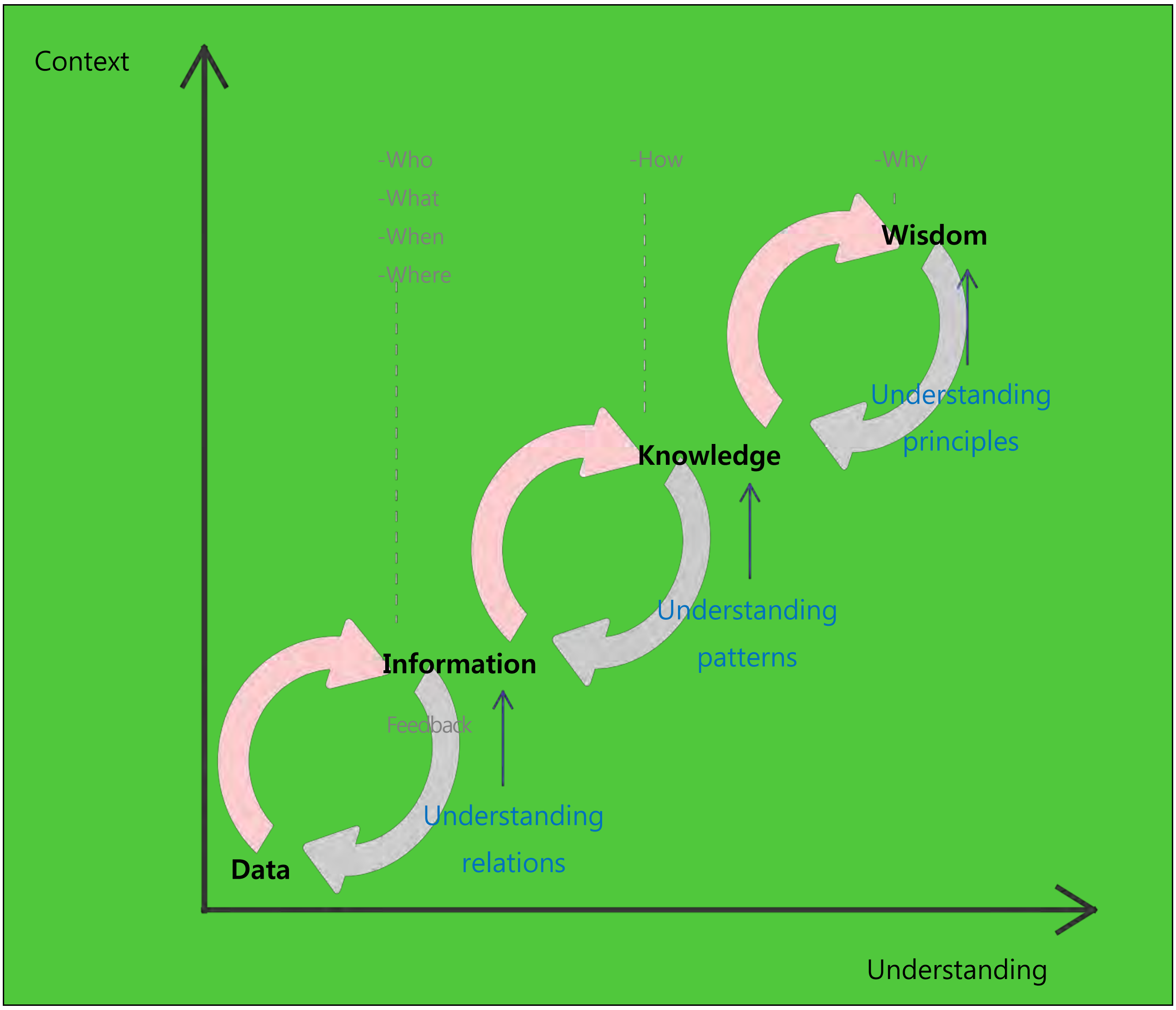


Figure 4 – Data-information-knowledge-wisdom (DIKW) process (ref. [14])

Better understanding of information versus knowledge

From the ICT perspectives, there are some additional interpretations of information and knowledge as follows:

– Information is a knowledge-generating tool.

– Information is only raw data, the basic material for generating knowledge. Information is not only raw data but also the product of an operation by which it becomes a shaping or packaging to make it manageable, transmissible and consumable.

– Information is a fixed stabilized form of knowledge, while exchange knowledge is achieved by transmission.

– Information is a commodity where knowledge is shared with certain rights or restrictions (e.g. intellectual property, traditional form of knowledge, etc.).

– Information is a useful set of data to master the available information with critical judgement and thinking, analyse, sort, and incorporate the items in a knowledge base.

– Through flows of information, everyone is able to develop cognitive and critical thinking skills to distinguish between useful and useless information.

– By the reflective nature of judgement required to convert information into knowledge, knowledge processing involves more than a mere verification of facts. It implies a mastery of certain cognitive, critical and theoretical skills.

- There are different information-use strategies based on useful knowledge.
- Knowledge is precisely what enables us to "orient ourselves in thought".
- To transform information into knowledge, the distinction between knowledge and information must also take into account the process whereby knowledge is shaped as information.

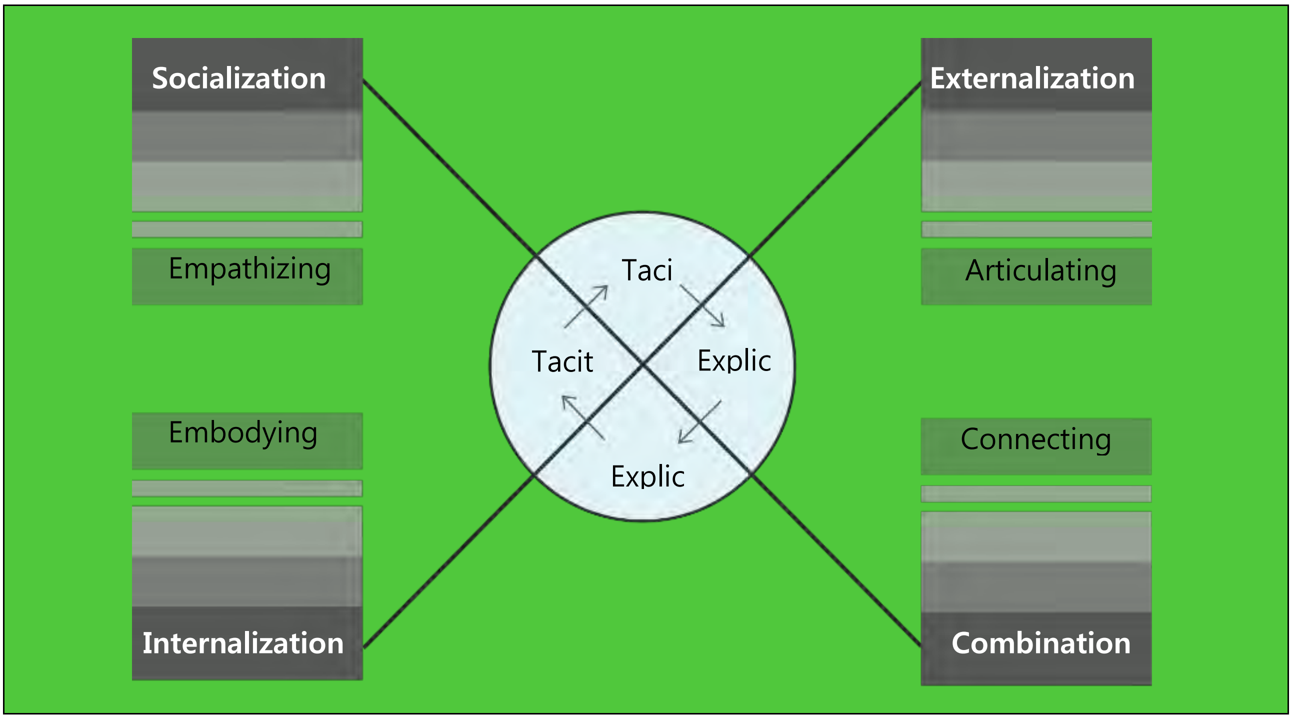


Figure 5 – Recursive cycle of knowledge creation (ref. [15])

Recursive natures of knowledge

Knowledge creation has an iterative and recursive nature between tacit knowledge and explicit knowledge [15]. "Tacit knowledge represents the internalized knowledge that an individual may not be consciously aware of, such as how he or she accomplishes particular tasks" with unexplainable know-how. "Explicit knowledge represents the knowledge that the individual holds consciously in mental focus, in a form that's easily communicated to others." [15]. When tacit knowledge is extracted to become explicit knowledge, explicit knowledge is re-internalized into the tacit knowledge. Based on the iterative nature of knowledge, there can be a continual evolution of knowledge through socialization, externalization, combination, and internalization. By understanding the process of how data and information is stored, related, and integrated (data layers) and how people will want to access and utilize the information (information and knowledge layers), the steps in addressing the technology needs of a knowledge creation in the ICT environment are clarified.

Knowledge platform for complex systems

To solve the human genome and complex systems, a large number of interacting processes are needed among all the components. Moreover, the activity of individual components are non-linear. The sciences of complexity systems such as the earth's global climate, human brain, and social organization are necessarily based on interdisciplinary researches. Almost all interesting processes in nature are highly cross linked. Many systems which interact non-linearly to form compound structures or functions require more explanatory devices to explain the building blocks. This process for new, complementary, modes of description is known as hierarchical self-organizing systems that are defined as complex. The complex system is comprised of a large number of strongly interacting entities, processes, or agents, which requires understanding new scientific tools and non-linear models without equilibrium descriptions. In addition, to solve the human genome, a lot of networking environments are needed: 1) the gene networks that direct developmental processes; 2) immune networks that preserve the identity of organisms and social insect colonies; 3) neural networks in the brain that produce intelligence and consciousness; 4) ecological networks; and 5) social networks comprised of transportation, utilities, and telecommunication systems, as well as economies. The ICT infrastructure with the help of cloud computing can provide massive computer simulations for complex systems.

A stepwise approach toward future knowledge society

For the networked society, knowledge is a source of all human beings including behaviours and building society. The networking of knowledge and the speeding up of information processing open up new possibilities for work according to their use and their ultimate purpose. The current Internet as a public network gives fresh opportunities to achieve equal and universal access to knowledge. True knowledge society is evolved from sustainable development of the ICT infrastructure.

Jeremy Rifkin in his 2011 book "The Third Industrial Revolution" said that there will be new information and communication technologies associated with a change in knowledge systems and patterns [16]. With the advent of virtual world during the digital revolution, the society of the intangible always confers greater strategic advantages and power over the tangible. Jeremy Rifkin explores how Internet technology and renewable energy are merging to create a powerful "Third Industrial Revolution". He asks us to imagine hundreds of millions of people producing their own green energy in their homes, offices, and factories, and sharing it with each other in an "Energy Internet", just like we now create and share information online. The Third Industrial Revolution by using Internet technology will create thousands of businesses and millions of jobs, and usher in a fundamental reordering of human relationships. It will impact the way we conduct business, govern society, educate our children, and engage in civic life. The revolution toward knowledge society improves thermodynamic efficiencies, dramatically increases productivity, and reduces the marginal cost of producing and delivering a full range of goods and services to near zero across the entire economy.

4.2 New technologies for knowledge society

Data formats depending on applications

Through the ICT infrastructure, there are various digital data types and formats including audio/video as well as files. In telecommunication and broadcast applications, the content formats are used in recording and transmission, which include analogue and digitized contents. The contents may be delivered via transmission channels, encrypted in digital forms, recorded in storage and processing methods, and displayed on the screen. The metadata provides the descriptive information of the data such as means, purpose, time and date, creator or author, and location, etc.

For Internet applications, there are many file types and formats that are encoded for digital storage in a computer. Some file formats such as hypertext markup language (HTML), scalable vector graphics, and source codes of computer language are used with defined syntaxes and possible control characters. The chunk-based file format are used for the Internet, in which the identifiers are human-readable and classify parts of the data such as "surname", "address", "rectangle", and "font", etc. The information that identifies a particular "chunk" may be called by "field name", "identifier", "label", or "tag". The data format with multipurpose Internet mail extensions (MIME) header, comma-separated value (CSV), extensible markup language (XML), and JavaScript object notation (JSON) are used on the Internet and the web. Recently, unstructured file formats of raw data are widely used by dumping memory or collecting sensing data of Internet of things (IoT) devices. The unstructured data is difficult for reading and writing without conversion to a structured format. To identify a file format, the internal metadata is stored inside the file itself. Typical file header contains metadata about content format, size, resolution, colour, and optional authoring information. Such metadata may be used by reading, interpreting, and displaying the file.

For the location-based applications, the geographic data format is used to capture, store, edit, analyse, share, and display spatial or geographical information. The geographical data are used for location-enabled services such as transport/logistics, real estate, public safety, crime mapping, national defence, and climatology. The global positioning system (GPS)-enabled mobile devices are used to display their location in relation to fixed objects (nearest restaurant, gas station, and fire hydrant, etc.) or mobile objects (friends, children, and police cars, etc.). The geographical data represent real objects such as roads, lands, trees, houses, buildings, and waterways, etc. Moreover, abstraction references like images, vectors, points, lines, and polygons are mapped to location attributes. A new hybrid method of data is identifying the physical location which combines three-dimensional vector points of physical space. This information is becoming more realistically visually descriptive. Recently, the web access to huge amounts of geographic data enables users to create customer applications and make complex spatial information, which is called mashup application of the web. An editable map of the geographical data is used to offer street maps, aerial/satellite imageries, geocoding, search, and car navigation, etc.

For the identification-related applications, the identification can mean the process of recognizing or identifying persons, objects, or animals, etc. The bar code is increasingly being used in the industry, and the radio frequency identification (RFID) is being used as an alternative. In these applications, the identification is used to reduce running out of stock or wasted products. Credit cards and passports in the wallet are to prove who you are. Recently, biometrics, iris recognition, and voice recognition technologies are used for identification. Theft and counterfeiting of critical or costly items such as drugs, food, repair parts, or electronic components will be reduced because manufacturers will know where their products are at all times. Product wastage or spoilage will be reduced because environmental sensors will alert suppliers or consumers when sensitive products are exposed to excessive heat, cold, vibration, or other risks. Supply chains will operate far more efficiently because suppliers will ship only the products needed when and where they are needed. Consumer and supplier prices should also drop accordingly.

For data intensive applications, a large volume of data typically terabytes in size and referred to as big data are processed. Computing applications requiring large volumes of data and their processing times to I/O are deemed data intensive. The rapid growth of the Internet led to vast amounts of information available online. Parallel processing can typically involve partitioning or subdividing the data into multiple segments which can be processed independently using the same executable application program in parallel on an appropriate computing platform. The data-intensive computing are managing and processing exponentially growing data volumes, significantly reducing associated data analysis cycles to support practical and timely applications. Information extraction and indexing of web documents can derive significant performance benefits on data parallel executions since the web can be processed in parallel. The semantic query language like SPARQL protocol and RDF query language (SPARQL) may be enabled to retrieve and manipulate data stored in RDF format of the web. Massive data from millions of IoT sensors may need the non-structured query language (NoSQL) database for storage and retrieval of data, making some operations faster than the relational database. The high-speed ICT infrastructure allows the data to be partitioned among the available computing resources and processed independently to achieve performance and scalability based on the amount of data. The cloud computing system controls the scheduling, execution, load balancing, communications, and movement of programs and data across the distributed computing cluster.

For science and engineering applications, various types of signals or information such as electromagnetic signals or biometric information are converted to digital forms. The weather conditions and chemical formula are represented by digital data. The conversion of analogue symbols or signals to digital is needed to relevant mapping methods or converting rules.

The data formats described above are summarized as follows:

- **Telecommunication and broadcast applications:**
  - Audio data encoding including analogue and digital audio;
  - Visual data encoding including film, colour, graphic, 3D display, and holographic format, etc.
  - Descriptive data encoding including metadata, etc.
- **Internet and web applications** (including semantic contexts):
  - File, image, documents, computer language, etc.
  - Chunk-based formats (e.g. MIME, CSV, XML, JSON, etc.).
- **Location-related applications:**
  - Geographical information including geographical map and physical 3D spaces;
  - Mainly used for transport and logistics industry (by using geolocation maps).

- **Identification-related applications:**
  - Sensor/radio frequency identification (RFID) code, product code, bar code, etc.
  - Used for trade, copyright, and ownership (e.g. shipping code, product value chain, security key, etc.).
- **Data intensive applications:**
  - NoSQL, SPARQL, big data analytics by using MapReduce and Hadoop;
  - Used for business intelligences in government and commercial solutions.
- **Science and engineering applications:**
  - Electromagnetic spectrum, traffic signal, time, weather, temperature standards;
  - Used for healthcare and medical data (e.g. deoxyribonucleic acid (DNA) sequence, biometric data including drugs, etc.).

Data models

The entity-attribute-value (EAV) model is a data model to describe entities where the numbers of attributes (properties, parameters) that can be used to describe them are potentially vast, but the number that actually applies to a given entity is relatively modest. In mathematics, this model is known as a sparse matrix. EAV is also known as object-attribute-value model, vertical database model, and open schema. This data representation is analogous to space-efficient methods of storing a sparse matrix, where only non-empty values are stored. The data type of EAV offers a limited set of data types: byte, Boolean, DateTime, double, and string, in addition to dividing numeric data into int, long, or float. It also defines custom data types such as a phone number, an e-mail address, geocode, and a medical record, etc. The cloud computing system offers data stores based on the EAV model, where an arbitrary number of attributes can be associated with a given entity. XML provides a framework on top of an EAV design and builds an application that has to manage data sets extremely complicated when using EAV models.

The data serialization model is used for computer science and communication network. The context of data serialization is the process of translating data structures or objects into a format that can be stored in a file or memory buffer, or transmitted across the network. For communication network, this process is not straightforward since data serialization is formatted by their associated protocol. In addition, a communication system running on a different hardware architecture should be able to reliably reconstruct a serialized data stream. Serializing the data structure prevents the problems of byte ordering, memory layout, or simply different ways of representing data structures.

The metadata model describes the contents and contexts of data or data files. Metadata was traditionally similar to the card catalogues of libraries. As information has become increasingly in digital form, metadata is used to describe digital data. For example, most files and documents include metadata specifying what language the page is written in, what format was used to create it, and where to find more information about the subject. There are two types of metadata: structural metadata and descriptive metadata. Structural metadata is the data about the containers of data. Descriptive metadata uses to describe individual instances of application data or the data contents. The main purpose of metadata is to facilitate in the discovery of relevant information, more often classified as resource discovery. Metadata also helps organize electronic resources and provide digital identification.

At the XML format, a set of rules to which an XML document must conform, called XML schema published as W3C, can be used to the processing of XML document [17]. Technically, a schema is an abstract collection of metadata, consisting of a set of schema components, mainly elements, attribute declarations, and complex and simple type definitions. These components are usually created by processing a collection of schema documents, which contain the source language definitions of the components. Schema documents are organized by namespace. All the named schema components belong to a target namespace which is a property of the schema document. A schema document may include other schema documents by using the same namespace and may import schema documents for a different namespace.

With the advent of web services, there are many markup languages, especially the hypertext markup language (HTML), which is the standard markup language used to create web pages [18]. It is a markup language that web browsers use to interpret and compose text, images and other materials into web pages. Web browsers can read HTML files and render them into visible or audible web pages. HTML describes the structure of a website semantically for presentation, making it a markup language, rather than a programming language. The HTML elements form the building blocks of all websites. HTML allows images and objects to be hyperlinked and can be used to create interactive forms. It provides a means to create the structured documents by denoting structural semantics for texts such as headings, paragraphs, lists, links, quotes, and other items. The language is written in the form of HTML elements consisting of tags enclosed in angle brackets like <html>. Browsers do not display the HTML tags and scripts, but use them to interpret the contents of the page. HTML can include scripts languages such as JavaScript which affect the behaviours of HTML web pages. Web browsers can also refer to cascading style sheets (CSS) to define the look and layout of texts and other materials.

If the metadata is stored in HTML format, it is very easy to share on the Internet. The files representing metadata can be grouped into three parts: structured texts from reference points to data, how the files can be accessed, and location information of files. HTML prescribes how the text will be formatted visually, which fonts will be used and on which place, where the image will be situated, and where the heading of the chapter is located, etc. However, it is typical for the descriptions of the documents that they can be classified into various categories. These categories form a certain hierarchy depending on their significance. The differences of content are not always represented visually in formatted documents, but they are very important for the mass processing of metadata.

The data models described above are summarized as follows:

- **Entity-attribute-value (EAV) models**
  - Making statements about resources.
    - (Examples) XML document type definition (DTD), tag, name, address, etc.
- **Data serialization models**
  - File, memory buffer, packets of communication protocol, and time-varying data, etc.
    - (Examples) binary/integer/real/exponent/character/string/Boolean/time, vector/matrix/array, 2D/3D graphics, recursive, audio/video stream, etc.
- **Metadata/schema/markup data models**
  - Specify the processing to be performed or the related actions (i.e. layout, activate, trigger, and invoke, etc.).

Data storage

There was a long history of writing, recording, and storing information. Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs. A storage device may hold information. Electronic data storage requires electrical power to store and retrieve data. Electromagnetic data may be stored in either an analogue data or digital data on a variety of media. This type of data is considered to be electronically encoded data, whether it is electronically stored in a semiconductor device. Most electronically processed data storage media (including forms of digital data) are considered permanent (non-volatile) storage, that is, the data will remain stored when power is removed from the device. In contrast, most electronically stored information is volatile memory while it vanishes if power is removed.

Except for printed data, electronic data storage is easier to revise and may be more cost effective than alternative methods due to smaller physical space requirements and the ease of replacing (rewriting) data on the same medium. However, the durability of printed data is still superior to that of most electronic storage media. The durability limitations may be overcome by the ease of duplicating (backing-up) electronic data. In this digital age, the long-term durability may be more significant since more than several zeta-bytes of the storage capacity may be needed within few years.

The information files stored on millions of servers constitute educational, cultural, and scientific resources. "Web culture" is characterized by the extreme rapidity of data-flows and rapid obsolescence. The average lifespan of an Internet page is less than one month. To preserve the accumulated information in a knowledge society, one of the possible solutions is to utilize electronic capturing devices and cloud computing storage on the web. To archive data in the cloud computing system, there is the problem of indexing files. By the uniform resource locator (URL) of the web, the successive version of the same documents should be lined up with its date of release. Digital storage is unlimited by time, geography, culture or format. It may be culture-specific but remains potentially accessible to every person in the world. The new storage technologies permit important advances regarding the accessibility and manageability of knowledge. The digital content itself has a subject to some degree of standardization without problems of incompatible formats.

Data classification and filtering

In the era of zeta-bytes, digital data would be well arranged, sorted, and prepared for searching, filtering, grouping and classification. Data classification is the process of organizing data into categories for effective and efficient use. A well-planned data classification makes essential data easy to find and retrieve. This can be of particular importance for access and search. The relevant procedures for data classification should define what categories and criteria people will use to classify data. If a data-classification scheme has been created, the appropriate handling procedures for each category should be addressed with data's life cyle requirements. It is essential that data classification is closely linked with data categories. Data classification is clustering the data sets by an iterative process of data category. New data sets can be categorized by new classification rules of knowledge and intelligence. The effectiveness of data classification is measured by predictive accuracy, speed of sorting and clustering, scalability on large amounts of data, and robustness of data quality.

In scientific and engineering fields, data classification raises the issues of identifying new observations from the existing categories of knowledge. It is considered as a kind of researching, analysing, and learning. It involves grouping data into categories based on the measure of inherent similarity. Data clustering for pattern recognition from a large amount of statistic data of images and speeches is used to identify a member of possible classes with the highest probability. Probabilistic algorithm with statistical inference is to find a best instance. In experimental and statistical analysis, data classification is done with logistic regression or a similar procedure. New observations on experimental results are referred to create new categories of possible values or outcomes.

Meaning of hyperlink, linked data, and linked open data

The outstanding difference of the web page compared with other plain documents is the hyperlink, which points to a specific web page or to a specific element within a document [19]. The hyperlink is used to link information to any other information over the Internet. It is integral to the creation of the World Wide Web. Web pages are written in the hypertext markup language (HTML). Hypertext is the text with hyperlinks. The hyperlink is a reference to data that the reader can directly follow by clicking. Users navigate or browse the web page following the hyperlinks. On the web page, most hyperlinks cause the target document to replace the document being displayed. The effect of the hyperlink may vary with the hypertext system. A link from one domain to another for a common destination anchor is a uniform resource locator (URL) used in the World Wide Web. It is achieved by means of an HTML element with a "name" or "id" attribute at the HTML document. A web browser usually displays a hyperlink in some distinguishing way, e.g. in a different colour, font or style. The behaviour and style of links can be specified using the cascading style sheets (CSS) language.

In a graphical user interface of web browsers, the hyperlinks are displayed in underlined blue texts when they have not been visited, but are displayed in underlined purple texts when they have been visited. When the user activates the hyperlink (e.g. by clicking on it with the mouse), the browser will display the target of the link. If the target is not an HTML file, depending on the file type and on the browser and its plug-ins, another program may be activated to open the file. The document containing a hyperlink is known as its source code document. For example, in an online reference work such as Wikipedia, many words and terms in the text are hyperlinked to definitions of those terms. Hyperlinks are often used to implement reference mechanisms, such as tables of contents, footnotes, bibliographies, indexes, letters, and glossaries.

The linked data builds upon standard web technologies such as hypertext transfer protocol (HTTP), resource description framework (RDF) and uniform resource identifier (URI). It describes a method of publishing structured data and enables data from different sources to be connected and queried. The linked open data (LOD) is the linked data that is open content. Tim Berners-Lee outlined four principles of the Linked Data in his "Design Issues: Linked Data note", paraphrased along the following lines [20]:

– Use URIs to name (identify) things.

– Use HTTP URIs so that these things can be looked up (interpreted, "dereferenced").

– Provide useful information about what a name identifies, when it is looked up, using open standards such as RDF, SPARQL, etc.

– Refer to other things using their HTTP URI-based names when publishing data on the web.

Metadata technology

The two groups of data are created during the digitization processing:

– digital copies of documents;

– the supporting structure, mostly textual, which enables access to the first group of data.

Let us call the first group data and the other one metadata. The data are, for example, images of the manuscript pages, while the metadata are descriptions of these pages. The distinction between these two groups is rather imprecise, because the digital copy can often be directly a component part of the description. In this case, the point of the end-user view is decisive and the metadata can be taken as the whole description including various preview images which are component parts of the texts, while the data is not a visible part of description and is referenced from it as an external file.

The metadata has two important functions to describe data and to provide access to data. Two groups of data must be decided by data formats, especially the metadata. The data format including metadata should comply with the following requirements [22]:

1) It is independent of software which will enable the user to work with metadata.

2) It should enable to classify metadata into various categories such as author, shelf-number, and page number in case of the description of a book. This classification is very useful for the mass processing of data.

3) It should enable the hierarchical classification of metadata in order to make the difference between the description of a book as a whole and the description of a page.

4) It should enable an easy transition from metadata to data.

Advantages of the web browser

With the rise of the web, the communication capacities and cognitive skills of humans are extended as active and interactive manners where individuals are not passive recipients and are capable of constituting, quite autonomously, virtual communities. The web can work to provide a gigantic pool of ideas, whether it is a matter of pieces of information or of knowledge itself. With a browser, the web is quite obvious for people to open their preferred websites multiple times a day. The web browsers are running on almost all types of computers and running on all kinds of operating systems. Many people are using the web to get the news, weather forecasts, cooking recipes, medical diagnoses, book reviews and the like. They are also using the web to book flights, plan vacations, buy and sell goods, and express opinions, etc. The major advantages that the web holds relative to the other media include [18]:

– **Time**: With radio and TV, the rare events that are important to a broad group of viewers could be reported live or in minutes. More typically, the delay is hours to a day. With newspapers, it takes closer to a day, sometimes more, before the news is received by the readers. With the web and smartphones, people are reporting on (e.g. through Twitter, crowd-sourcing, etc.) and reading about events about when the events occur. People get pictures and information almost instantaneously.

– **Localization**: The traditional media such as newspapers, radio and TV reports information relevant to a relatively large geographical region. It is more difficult to find localized information at the small community level. With the web, a village, independent of size and any community (even though it is separated geographically), can share information relevant to their members and citizens wherever web access is possible.

– **Universality**: Radio, TV, and newspapers usually cover a relatively large geographic area, and they are typically available only to people living in that area. It is difficult for people outside of the area to access those media. The web is universal and available anywhere in the world. It allows people today to book a hotel and prepare vacations on the other side of the world.

– **Focus**: There are today millions of communities specialized on specific themes (languages, hobby, nature, etc.). When there are thematic radio, newspaper, TV, and magazines, their diffusion is geographically limited. When these communities are spread over the web, the web enables people with shared interests to exchange their resources independently of their respective locations.

– **Search**: Mechanisms such as libraries, guides, reviews, and word-of-mouth can help people to find information that they seek in traditional media. On the web, search engines, as well as easier access to guides and reviews, facilitate the quest for information. The volume of information on the web and the ability to assess the quality of information are surprisingly remarkable.

– **Linking**: A person can change channels on the radio or TV, or pick up one newspaper and then move to another. On the web, links allow people to move easily from one web page to related information elsewhere on the same page, on the same site or one a different site half-way around the world. The emergence of the semantic web promises to extend this capability to linking data and ascribing greater meaning to data and relationships across the web.

Knowledge structure

Humans understand knowledge from a combination of data, information, experience, and individual interpretation. Knowledge is the sum of what is known and resides in intelligence and competence of people. There are various definitions of knowledge as "things that are held to be true in a given context and that drive us to action if there were no impediments", "capacity to act", "justified true belief that increases an entity's capacity for effective action", and "the perception of the agreement or disagreement of two ideas" [9]. There are three basic schemes of knowledge to be organized:

– **Declarative knowledge**: How and why the things work the way they do. It includes information about concepts and elements of particular subjects.

– **Procedural knowledge**: Detailed steps or activities required to perform a task or job. It allows a task to be performed into automatic (habitual) processes with repetition.

– **Structural knowledge**: A basis for problem solving. It is required in the creation of plans and strategies by analysing what to do, when failure occurs, or when a piece of information is missing. The conceptual elements in the knowledge structure are the key to having a "deeper understanding".

A typical example of tacit knowledge are know-how results from experience, information, knowledge, learning, and skills of humans and human communities. Knowledge creates the longest lasting competitive advantage and is an essential component of the human capital. It may consist entirely of technical information (as in science and technology area) or may reside in actual experiences or skills acquired by the individuals (as in manufacturing or medical industries).

In scientific and technological fields, the various types of knowledge are also identified as [23]:

– **Conceptual knowledge**, such as the concept of momentum or energy, or that the velocity of an object changes when it accelerates, or that the gravitational potential energy of an object decreases as it falls.

– **Factual knowledge**, such as the value of the gravitational constant g, the radius of the moon, or the density of iron.

– **Representational knowledge**, such as how to draw and use graphs.

- **Strategic knowledge**, such as the ability to recognize the applicability of a concept, for example, momentum is conserved when there are no external forces, or that energy is conserved when there are no non-conservative forces.
- **Meta-cognitive knowledge**, for example, the awareness of underlying assumptions, or that an answer should be checked by solving the problem a different way.
- **Self-knowledge**, such as knowing one's likely sources of mistakes, or knowing that one should be more procedural when solving problems.
- **Operational knowledge**, such as how to take the cross product or dot product of two vectors, or how to take the determinant of a matrix, or how to draw a free-body diagram.
- **Procedural knowledge**, such as when to use conservation of energy (i.e. when all forces are conservative), or when to specify a coordinate system (e.g. when finding potential energy), or when to draw a free-body diagram (e.g. when applying Newton's laws).
- **Problem-state knowledge**, which are the features of a problem used for deciding how to solve it. Examples are: knowing that there are no external forces in a particular problem, or that there are no non-conservative forces in the problem, or that an object is at rest initially, or that the object is on the incline.

Problem solving and decision-making

Recently, most problems raised by the industry or academia are not easy to solve. Problem solving and decision-making are important skills for business and life, and they are especially important to get consensus among individuals or groups of people. To improve the quality of their decisions, decision-makers need to be more decisive in acting upon the assessments.

In the problem solving and decision-making process, the creativity of individuals is essential. The brainstorming technique among people is particularly useful. Good decision-making requires a mixture of skills which includes creative development and identification of options, clarity of judgement, firmness of decision, and effective implementation. For teams and organizations, a perspective of group profiles and human resources can assist in making decisions. The decision-making may be different according to categories of people, especially in a large group of human resources, since some people may have different knowledge backgrounds and different understanding of things.

There are various techniques of problem solving from finding and defining the problems to selecting the best option. To improve the problem solving process, all the members share the current situations and the challenging issues, and seek an optimal solution. The leader encourages a group of members to develop options and select a solution. The social networking technologies may be used to get a consensus among people efficiently and effectively.

Cognitive process of knowledge creation and learning

Most knowledge is conceptual in nature. The relevant cognitive processes are required for acquisition of conceptual knowledge and construction of the useful knowledge structure. As an example, the following activities can be used by teachers to stimulate the cognitive processes needed to develop a conceptual understanding of science and technology [23]:

- **Use multiple representations**: A representation may be linguistic, abstract, symbolic, pictorial, or concrete. Using many different representations for the same knowledge helps people to interrelate knowledge types and relate knowledge to physical experiences. It encourages the formation of links between knowledge elements and promotes a rich clustering of knowledge.
- **Make forward and backward references**: Concepts require a long time to be formed. Thus, students completely learn one topic before moving on to the next. By making forward references, new materials are prepared. By making backward references, the new materials with established (or partially established) material are also linked, thus making knowledge interconnected rather than linear.

- **Explore extended contexts**: Concepts are extremely context dependent and do not become useful until they are well abstracted and recognized. Investigating a broad context of applicability helps people to refine and abstract concepts. It also avoids incorrect or oversimplified generalizations.
- **Compare and contrast**: Essence to the process of structuring (or re-structuring) knowledge is the classification and interrelation of knowledge elements. Comparisons and contrasts sensitize people to categories and relationships, and help people perceive the commonalities and distinctions needed to organize their knowledge store.
- **Categorize and classify**: In parallel with comparisons and contrasts, people are aware of categories and classification. People may practice creating and recognizing categorization. By classifying items, to choose names for their categories, and to explain their system, people can restructure their knowledge store.
- **Predict and show (inadequacy of old model)**: Carefully selected demonstrations and experiments can be used to bring out inconsistencies. When experimental apparatus are being set up, people should be asked to predict what will happen when something is done. By making predictions beforehand, people may have a chance to choose alternative solutions if their own model fails.
- **Explain (summarize, describe, discuss, define, etc.)**: The typical problems of learning are what students do not understand. Even when students get a problem right, there can still be confusion about the applicability of the equations used. When the teachers ask students how they will solve a problem, they recognize the misunderstandings and misconceptions of students, and they help the students reorganize their knowledge structure. By seeing the experts' standard demonstrations and experiments, the students can explain and discuss what they think they have seen, so that the teachers can interact with the students' views. Furthermore, the process of explaining (or summarizing, describing, discussing, etc.) helps students become aware of their own models as well as the models of other students.
- **Generate multiple solutions**: The students have difficulties to choose a solution when there is a set of valid solution paths. By solving problems in more than one way, students learn to prioritize elements of their knowledge.
- **Plan, justify, and strategize**: To avoid their impatience of solving a problem, students should be asked to plan (and then explain) how they will solve the problems. Students must learn how to determine which concepts are relevant (and which are irrelevant) for any particular problem situation and how to implement the relevant concepts to solve that problem. By generating their own strategies, students can learn how concepts are used to solve problems.
- **Reflect (evaluate, integrate, extend, generalize, etc.)**: After completing most activities, students can get a benefit from looking back on what they have done. What experiences have they perceived? What general rules can be constructed? Other types of activities give students tips of know-hows needed to create a coherent picture of science and technology, but some sort of reflective activity is usually needed to "put the pieces together".
- **Meta-communicate about the learning process**: To learn science and technology (or any other complex subject), students should become self-involved. They should be exposed to other people (teachers and students) models. By communicating with each other, they must be informed of common pitfalls and misinterpretations and be ready to restructure their knowledge. Students must learn how they learn best. The collective and cooperative learning platforms between students and teachers are needed through ICT infrastructure.

Knowledge platform

The sources of knowledge may include documents, files, database, and recording of best practices or activities. A knowledge platform may need capturing, developing, sharing, and effectively using organizational knowledge. It may be a multidiscipline platform to achieving organizational objectives by making the best use of knowledge. A knowledge platform covers the fields of business strategy, information systems, management, and data and information sciences. More recently by utilizing information and communication technologies, a knowledge platform for other fields such as media, computer science, education, health, and public safety is investigated. In order to encourage the sharing of knowledge, a knowledge platform may focus on the value-added objectives such as the improved performance, competitive advantage, innovation, the sharing of lessons learned, integration and continuous improvement of human society.

Impacts of cloud computing platform

Cloud computing is to share computing resources. Cloud computing and storage provide users and enterprises to store and process their data. It relies on sharing of resources to achieve coherence and economies of scale and maximize the effectiveness of the shared resources. Cloud resources are not only shared by multiple users but are also dynamically reallocated per demand. The key technology for cloud computing is virtualization. Virtualization separates a physical device into one or more "virtual" devices, each of which can be easily used and managed to perform tasks. The key benefits of cloud computing is to increase utilization, efficiency, and productivity when multiple users can work on the same data simultaneously without suffering peak loads, rather than waiting for it to be saved, transferred, and e-mailed. With concepts of service-oriented architecture as "everything as a service" (XaaS), cloud computing providers offer their "services" which happen to form a stack: software-, platform-, and infrastructure as a service (SaaS, PaaS, and IaaS, respectively).

In the evolution of technologies and paradigms toward the knowledge society, cloud computing allows users to share data for specific applications, allows open source software, and gets new opportunities for the connected business among a large group of people, and creates deep knowledge collectively. To reshape the sharing concepts among people and communities, the cloud computing platform is very useful to extract information and knowledge from raw data.

Cloud computing has the ability to develop and design new applications through human knowledge and awareness. It provides a knowledge-based approach for end users to create new values. User's knowledge is stored in the cloud and is accessible everywhere. The essential characteristics of cloud computing are summarized as:

- **On-demand self-service**: Computing capabilities, such as server time, networked storage, and communication and collaboration services, are being provided automatically without requiring human interaction.
- **Seamless broad network access**: It can be accessed by heterogeneous mobile phones, laptops, and personal digital assistants (PDAs) anywhere and anytime. The seamless connectivity with high availability as well as high bandwidth is critical in the cloud computing environments. From the customer's point of view, users are reluctant to use cloud computing platforms if there are service disruptions or a stream of packet loss.
- **Resource pooling**: Physical and virtual resources are dynamically assigned according to user demands.
- **Rapid elasticity**: The resources of cloud computing are rapidly and elastically provisioned, quickly scaled out and scaled in.
- **Measured service**: Resource usages of cloud computing can be monitored, controlled, and reported.

From the viewpoint of multiple stakeholders, there are some benefits of cloud computing. From the viewpoint of network providers, the cloud computing platform provides a rich set of communication services such as voice and video calls, audio, video and web conferences, messaging, and unified communications, which may be recently implemented by mashup applications with web technologies. From the perspectives of service providers, cloud computing provides a lot of benefits as follows:

- Cost saving by virtualization of computing resources;
- Improvement of total cost of ownership and risk reduction, which is shifted from capital expense (CapEx) to operational expense (OpEx) by sharing information technology (IT) resources;
- Highly scalable and flexible infrastructure;
- Efficiency and flexibility of resource management;

- Business agility with rapid service deployment;
- Reliability of service with high availability;
- High support of third-party business.

From the user's perspectives, the cloud computing platform provides some benefits as follows:

- **Optimized and rapid provisioning**: Optimal application software for each business process;
- **Anywhere application with any device**: Connect online with any device, not only via the desktop but also via a mobile device;
- **Pay-per-use pricing**: Pay-as-you-go model similar to the subscription-based pricing;
- **Low migration costs**: Easy to switch to a competing solution by signing a new contract, transferring data, and retraining users;
- **Secure important data**: Easy back-up and storage of important data in multiple sites.

Impacts of Internet of things technologies

With the development of Internet of things and sensor networks, various types of data are being produced from sensors. In people's life and environments, more and more sensors are expected to detect location, measure temperature and air pressure, and record communication log. In the home, there are smart household appliances with sensors that can collect status about these appliances. They can extract status or presence information from raw data of IoT sensors. This represents some facts or context information about users and recognizes the environment which extends the ability of people's perception. This context information can be organized as the basis of effective reasoning. Users may upload a part of their perceived knowledge to the cloud environment in a certain form of rules. When Internet of things technologies are organized in the cloud computing system, the reasoning and perception processes are running and they invoke some actions for users. Moreover, the cloud provides composed web services which are connected to users and IoT sensors together.

Evolution of cyber physical systems

A cyber physical system (CPS) is a system of collaborating computational elements controlling physical entities which is bridging the physical world to the cyber world. The concept of cyber physical systems can be applied in diverse areas such as aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances, etc. In the CPS environments, the functions and processes of the physical elements are mapped to objects or tasks in the cyber domain. With the evolutions of Internet of things (IoT) and machine-to-machine (M2M) technologies, the sensor networks link between computational objects and physical elements. The intelligent IoT/M2M technologies can dramatically increase adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of cyber physical systems. The applications of the cyber physical system, for example, include:

- the medical systems with high confidence, assistance to patients and disabled people;
- the advanced automotive systems with intelligent traffic control and safety;
- the manufacturing and robot systems with intelligent process control;
- the smart grid with energy balance of supply and demand;
- the ubiquitous city with environmental control; and
- the water resources and defence systems with infrastructure control, etc.

However, the cyber physical systems will be more deterministic, predictable, and understandable with the help of IoT/M2M technologies as well as information and communication technologies. The physical world is highly concurrent with cyber objects, which is the abstractions of software. The predictable concurrent computation is possible to satisfy performance and integrity of the system.

To realize the cyber physical system as described above, top-down solutions can complement the existing bottom-up approaches. However, there remain many challenges and opportunities in developing the immature technologies of the cyber physical system. Technically, for the first phase of the evolution of the cyber physical system, all the functions and processes of the physical system could not be mapped to the cyber system. In addition, the physical world is not entirely predictable. Within a certain reliability and predictability, the cyber physical system can be operating in a controlled environment. It should be robust to unexpected conditions and adaptable to system failures. The software in the cyber world should be predictable and reliable in the contexts of the cyber physical system since small deviations of expected operations may cause catastrophic failures. It is important to determine whether the system has performed correctly. The certain mechanism of the cyber physical system should be developed to compensate for the loss of predictability and reliability.

Second, an abstraction of objects and tasks is well defined to hide the detailed physical implementations from the cyber world. The real-time operating system in the cyber system should be hidden from the details of the concurrent operations of the physical systems. Timing in the physical implementation should be tolerant in the software operation of the cyber system. Since the cyber physical system is presumably concurrent, the physical processes coupled with the computing system are also concurrent. They have to control multiple sensors and actuators concurrently.

Third, there are security risks in the distributed applications of the cyber physical system. The proper security technologies should effectively be exploited to improve robustness in the distributed cyber physical system. For example, the distributed denial of service attacks bring about some difficulties in the realization of the cyber physical system. Therefore, the outstanding technical issues should be solved to apply the concepts of the cyber physical system to the real business market.

5 Vision and technology trends of social media

5.1 New trends of social media

Definition of social media

Wikipedia defines social media as the computer-mediated tools that allow people to create, share or exchange information, ideas, and pictures/videos in virtual communities [24]. Social media is defined as "Internet-based applications that allows the creation and exchange of user-generated contents." In another definition, social media has been broadly defined to refer to "the many relatively inexpensive and widely accessible electronic tools that enable anyone to publish and access information, collaborate on a common effort, or build relationships" [25]. Furthermore, social media depends on mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated contents.

The rise of social media has fostered an unprecedented expansion of networks along two axes: the horizontal axis is the transmission speed and the vertical axis is the number of connections. People can communicate more and more and, above all, more and more rapidly. Interactivity is another characteristics of this new digital media. Social media introduces substantial and pervasive changes of communication between organizations, communities, and individuals. Social media differs from traditional or industrial media in many ways including quality, reach, frequency, usability, immediacy and permanence. This is in contrast to traditional media that operates under a single transmission model (one source-to-many receivers).

Social networking services and new ecosystem

A social networking service (also social networking site or (SNS)) is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. By using the web technology, social network services provide means for users to interact over the Internet, such as e-mails, instant messaging, photo/video sharing, and blogging, etc. Social networking services allow users to share ideas, pictures, posts, activities, events, and interests with people in their network.

Social networking technologies take on many different forms including blogs, business networks, enterprise social networks, forums, microblogs, photo sharing, product/service reviews, social bookmarking, social gaming, and video sharing, etc. There are many social networking services such as Facebook, Twitter, or

YouTube [24]. The purpose of the social networking service is to connect between individuals and groups of people who share something in common and are interested in learning from the lives of others. As there are many ways of connecting with people in the real world, there are also a number of social networking services in the virtual world where people communicate with each other in slightly different ways. Some of these networking services are file sharing, traditional and/or voice-video chats, messaging, e-mails, and blogging. There are categories of social networking services like former/current classmates, co-workers, and business groups, friends, dating, or suggested reading usually via some sort of customizable pages that include pictures, lifestyle information, likes/dislikes and more.

With the advent of user-generated contents and sharing features, social ecosystem platforms are very important in social media: the publishing media (with Blogs), the sharing media (with Facebook and Twitter), and the curating media (with Pinterest). The preferences in social media depend on the amount of contents. The value-added content is currently in the curating media. The interesting users' behaviour is the evolution of users' expectations: the more they use social media, the more sophisticated their needs are. As users can experience social media every day, the social media platforms like Facebook and Google are changing with a dense ecosystem of niche players. By using various social media platforms, users are involved in conversations and interactions with various device types (desktop, tablet, smartphones) as well as more sophisticated usages (publishing, sharing, playing, networking, buying, and localization). While social networking services consistently rise, new technologies are observed with the concepts of "real-time web" and "location-based". Real-time web allows users to contribute contents which are then broadcast as they are being uploaded. These concepts are analogous to live radio and television broadcasts. Twitter sets the trends as "real-time" services, wherein users can broadcast to the world what they are doing. Facebook follows suit with their "Live Feed" where users' activities are streamed as soon as they happen. Another real-time service focuses on group photo sharing wherein users can update their photo streams with photos while at an event. The image-based social media has become one of the social networking services. By merging cloud computing platforms with social networking concepts, interactive communities connect individuals based on the shared business needs or the shared experiences. The specialized networking applications can be accessed via their websites, which are closely tied to individual networking relationships based on social networking principles.

Evolution of digital book

For a very long time ago, books have been recognized as the useful material to write, print, and illustrate works of literature or human history. There is a long history of writing from papyrus to electronic books. Recently, most books are now printed in an electronic format which is fed by a continuous roll of paper and consequently more copies are printed in a short time. By adopting new digital printing technology, electronic books are widely distributed for educational, living and business purposes.

One of the problems of traditional books is the make-ready materials when the authors decide that the contents are correct. In periodicals such as magazines, journals, or newspapers, the publishing date is important, but for other types of books (for example, biographies), it is robust like carving in wood. If books are typeset for printing, any changes of contents are not possible. Only reprinting or discarding takes place.

Recent developments in book manufacturing include the development of digital printing. Digital printing has opened up the possibility of print-on-demand with relevant updates, whereas paper books are printed only until after the whole content of the book has been received from the author. It should be noted that digital books should not be modified or changed after their electronic publication. To face an ever-increasing rate of publishing, sometimes called data explosion, new contents and information are readily updated during the electronic printing of books. Since it is available online via the Internet, an online book is a digital medium for an unlimited redistribution and infinite availability in the public domain. Therefore, if digital technology is used in book design, there will be a new art of incorporating content, style, format, design, and sequence of a book. New digital books will be hyperlinked with interdisciplinary knowledge, ready for academic discussion, and collecting various opinions from social networking services. Digital books may be constantly updated and hyperlinked with the advances of contents, which is similar to publication on websites.

Electronic journals on science and technology

In academic publishing, a scientific journal is a periodical publication intended to further the progress of science, usually by reporting new researches. There are thousands of scientific journals in publication. Most journals are highly specialized and have been peer reviewed to ensure that articles meet the journal's standards of quality and scientific validity across a wide range of scientific fields. The publications of scientific research are an essential part of the scientific method. If they describe experiments or calculations, they should supply enough details that an independent researcher could repeat the experiments or calculations to verify their results. Such an article in a journal becomes part of the permanent scientific records.

Articles in scientific journals can be used in research and higher education. Scientific articles allow researchers to keep up to date with the developments of their research field. An essential part of a scientific article is the citation of earlier works. The impact of articles and journals is often assessed by counting citations. Some studies are partially devoted to the explication of classic articles. The seminar by each researcher may consist of the presentation of classic or current papers. Schoolbooks and textbooks have been written usually only on established topics while the latest researches and more obscure topics are only accessible through scientific articles. In scientific research groups or academic departments, the standards that a journal uses to determine publication can vary widely. In many fields, an informal hierarchy of scientific journals exists; the most prestigious journal in a field tends to be the most selective in terms of the articles that it will select for publication.

Electronic publishing is a new area of information dissemination. In an electronic (non-paper) form, scholarly scientific results are written or created for publication or dissemination. The electronic journal is specifically designed to be presented on the website. The electronic journal will exist alongside the paper version because the latter is not expected to disappear in the future. The output on a screen is important for browsing and searching. Many journals are electronically available in formats readable on the screen via the web browsers. Electronic publishing of scientific journals is not costly, is accessible to many people, and is doable due to the availability of supplementary materials (data, graphics, and video).

There is usually a delay of several months after an article is written before it is published in a journal. Paper journals are not an ideal format for announcing the latest researches. Many journals now publish the final papers in their electronic version as soon as they are ready, without waiting for the assembly of a complete issue, as is necessary with a paper publication. In many fields in which even greater speed is wanted, the role of the journal in disseminating the latest researches has largely been replaced by electronic databases. An increasing number of electronic journals are available as open access. Individual articles from electronic journals may be found online and stored either in personal or community archives, or posted on websites as blogs.

Meaning of social connectivity

In the ICT world, connectivity is the ability to make a connection between two or more interfaces in a telecommunication system. Many terminals including machines, appliances, and facilities are used to connect and exchange information with each other. Internet connection may be available to access from home, school, and workplace as well as public places such as libraries and Internet cafes. Coffee shops, shopping malls, and other venues increasingly offer wireless Internet connection. A whole campus or an entire city can be enabled to build a wireless community. There is a gap between people with effective connectivity and those with very limited or no connection, which is one of the digital divide.

In human life, connectivity has changed the way in which many people think, and it also allows them to take advantage of the "political, social, economic, educational, and career opportunities". A social structure composed of individuals, business partners, friends or other organizations is connected by utilizing social media technologies. Human connection is dependent on the intelligence that one brings into it. It influences thought and action, whether to do good or bad things. The needs for human connection can be perceived as physical, spiritual or emotional interactions with others. Humans are supposed to be more responsible and arguably more intelligent. José van Dijck contends in her book "The Culture of Connectivity" (2013) [26] that to understand the full weight of social media, their technological dimensions should be connected to the social domain and the cultural domain. She critically describes six social media platforms:

– three concepts of technology, users and usage, and content as platforms as techno-cultural constructs;

– ownership, governance, and business model as platforms as socio-economic structures.

Environments for crowdsourcing and collective intelligence

In theory, collective intelligence attempts to describe the phenomenon in which large, loosely organized groups of individuals come together to solve problems in highly effective ways. With the new environment of ICT connectivity, it is possible for individuals in separate locations, who may even be anonymous to each other, to work together on the same idea. Together, the concepts are attempting to understand the "wisdom of the crowd". The large network of people to solve problems can extend more broadly as an open innovation which consists of shifting the innovation process from inside the organization to generate ideas with those outside the organization. One of the benefits of collective intelligence is the diversity of ideas to be produced. When an individual tackles a problem alone, he or she may approach it with certain biases. Collective intelligence mitigates these biases by collecting a wide range of viewpoints and then aggregating them to reduce the effects of individual bias. The famous tools for collective intelligence are Wikipedia as a free encyclopaedia and Wiki as a collaborative website.

Crowdsourcing, the best-known example of technology-enabled collective intelligence, refers to the practice of an organization with a large population to solve a problem. To produce better ideas, crowdsourcing is to generate solutions, products and/or ideas that are superior in quality, quantity and effectiveness to those generated by the closed problem-solving methods. The word "crowdsourcing" is a combination of the words "crowd" and "outsourcing". Crowdsourcing is a process of getting work or funding, usually online, from a crowd of people. The idea is to take work and outsource it to a crowd of workers. By definition, crowdsourcing combines the efforts of numerous self-identified volunteers or part-time workers, where each contributor, acting on their own initiative, adds a small contribution that combines with those of others to achieve a greater result. Crowdsourcing can involve division of labour for tedious tasks split to use crowd-based outsourcing, but it can also apply to specific requests, such as crowdfunding, a broad-based competition, and a general search for answers, solutions, or a missing person.

New trends of social media

- **Smartphones or social networking services replacing your wallets or credit cards**

Recently, by using smartphones and/or social networking services, several millions of users send money to each other by just using their debit card information, free of charge. Meanwhile, the smartphone has also rolled out new payment features. It allows users who save their credit card information to check out with a lot of e-commerce applications across the network. As a result, many business players are battling it out in the mobile payment system, which is known in financial technology as FinTech. The smartphone or social networking services may eventually charge for their money transfer services, leverage customer purchasing data to rival traditional credit cards like Visa and Mastercard.

- **Shopping plugs into social media**

New buttons labelled as "buy" appear on certain tweets and posts on the social networking services. They allow users to make purchases with just a click which integrates e-commerce and social media. While happily chatting with friends, browsing the latest trends, sharing photos and videos, etc., their payment details are on file and purchases are a tap on the screen. Since most social networking services are real time, the short-term deals are with fleeting trends. With time-sensitive offers, consumers may be inclined to act quickly and make a deal. There are major benefits to advertisers. With the advent of "buy" buttons, concrete revenue figures can be attached to specific social networking messages in a way that has not been possible until now.

- **Increasing advertising and privacy problems**

A number of niche social networking services are built specifically with the lack of privacy, the collections of demographic and psychographic data, and the increasingly pervasive advertising. They allow users to exchange fully anonymous posts with people who are not physically nearby. The social networking service has promised to share advertisement revenues with users based on the popularity of their posts. New social platforms try to replace the existing social networking services with fewer advertisements or more privacy. The technical challenge is to provide privacy to the global community.

A number of anonymous social networking services with more privacy surge in popularity. Not everyone wants every conversation over the social media to be broadcast to the world, after all. Some users are concerned about ways the personal data is being collected, sold to advertisers, manipulated in tests, or accessed by government agencies.

A few social media fulfil their mandates on privacy issues. Some of them have been hacked with sensitive user photos posted. Real anonymity and privacy is extremely difficult to achieve. For privacy, some social media allows users to create chat rooms around shared interests with no requirement to reveal their names or locations. They allow users to conceal their identity, location, and browsing history.

- **Smart devices with IoT sensors are more social**

In the near future, cheap IoT sensors are included in smartphones. There is an explosion of smart devices in home appliances like thermostats, bathroom scales and refrigerators to wearables like fitness bracelets and smart watches. Many IoT devices are now collecting data and push notifications to smartphones. The challenge becomes how to more intelligently integrate the fast-growing Internet of things technologies with social media. Smart devices need to improve their social intelligence. By tapping users' social graph on their unique network of friends or listening to social media, it is easy to track users' activities and interactions with friends and followers.

Emergence of new media

By reviewing the existing types of media described above, there is some evidence of the emergence of new media with advances of information and communication technology. The rise of new media has increased communication between people all over the world. It has allowed people to express themselves through blogs, websites, videos, pictures, and other user-generated media. New media most commonly refers to contents available on-demand through the Internet, accessible on any digital device, usually containing interactive user feedbacks and creative participation [27]. New media includes the existing social media such as online newspapers, blogs, wikis, video and games. New media enables people around the world to share, comment on, and discuss a wide variety of topics. One of the key features of new media is denoted as interactivity among communities.

New media represents the digital forms with technologies that are manipulated, networkable, dense, compressible, and interactive. Wikipedia, an online encyclopaedia, combines Internet accessible digital texts, images, and video with web-links, creative participation of contributors, interactive feedback of users, and formation of a participant community of editors and donors for the benefit of non-community readers. Facebook is an example of the social media model, in which most users are also participants. As a result of the evolution of new media technologies, virtual communities are being established online by eliminating geographical boundaries and social restrictions. People in virtual communities use words on screens to exchange information for life and business. New media has the ability to connect like-minded people worldwide and feeds into the process of guiding their future development.

Although traditional social media offers a variety of opportunities for companies in a wide range of business sectors, mobile social media makes use of the location- and time-sensitivity aspects in order to engage into marketing research, communication, sales promotions/discounts, relationship development, and loyalty programs. Mobile social media offers data about offline consumer movements to online companies. Any firm with new media can know the exact time at which a customer entered one of its outlets, as well as the comments made during the visit. Mobile social media communication takes two forms, the first is a company-to-consumer relationship whereby a company may establish a connection with a consumer based in its location and provide reviews about locations nearby. The second type of communication is the result of user-generated contents. Mobile social media allows companies to tailor promotions to specific users at specific times. In order to increase long-term relationships with the customers, companies are able to create premium service programmes that allow customers who check in regularly at a location to earn discounts. Mobile social media applications are influencing an upward trend in the popularity and accessibility of e-commerce or online purchases. Almost half of smartphone owners visit social networks every day via their mobile applications. With the rapid adoption of mobile devices, social media has a symbiotic relationship with the mobile consumer.

Although there are several ways that new media may be described, Lev Manovich, in an introduction to "*The New Media Reader*", defines New Media by using eight propositions [28]:

1 **New media versus cyberculture** – Cyberculture is the various social phenomena that are associated with the Internet and network communications (blogs, online multi-player gaming), whereas new media is concerned more with cultural objects and paradigms.

2 **New media as computer technology** – New Media are the cultural objects which use digital computer technology for distribution and exhibition, e.g. websites, computer multimedia, and Blu-ray disks, etc.

3 **New media as digital data controlled by software** – New media is based on the assumption that all cultural objects rely on digital representation and computer-based delivery. New media is the digital data that can be manipulated by software. New media can create several versions of the same object. As an example, an image stored as matrix form can be manipulated and altered according to the additional algorithms implemented, such as colour inversion, grey-scaling, sharpening, and rasterizing, etc.

4 **New media as the mix between existing cultural conventions and software** – New media can be understood as the mix between older cultural conventions and newer conventions for data representation, access, and manipulation. Software using computer animation can help representations of visual reality and human experience.

5 **New media as the aesthetics** – If many aesthetic strategies may reappear, a much more comprehensive analysis on new media would correlate the history of technology with social, political, and economical histories.

6 **New media as faster execution of algorithms** – High performance computers can make many new forms of media art such as interactive multimedia, 3D virtual reality, and video games.

7 **New media as meta-media** – New media is about new ways of accessing and manipulating information (e.g. hypermedia, databases, search engines, etc.). Meta-media is an example of how quantity can change into quality as in new media technology. The manipulation techniques can recode modernist aesthetics into a very different postmodern aesthetics.

8 **New media as parallel articulation of post art and modern computing** – Post art or "combinatorics" involves creating images by systematically changing a single parameter. This leads to the creation of remarkably similar images and spatial structures. It means that algorithms as an essential part of new media do not depend on technology, but can be executed by humans.

5.2 New technologies for social media

Media technologies

Media is to transport information that is meant for communication like newspapers, radio, and television. It disseminates information to a large number of people, which is called mass media. However, to indicate the means of human communication such as language, reading, writing or audio/video/music, there are technologies and methods that support communication over distances in time and space. Media is physically stored content (in the case of files) or transferred content (in the case of messages), audio/video/music, film, photos or more generally of data. It is based on today's media, for example, newspapers, radio, TV, and cinema, etc. Current media technologies are described as follows:

- Mobile media: the smartphone is rapidly advancing to be the new platform of mass media;
- e-paper: certainly replaces traditional newspapers and magazines;
- wearables: tomorrows clothes are a part of the new media;
- tangible interface: a new way to use your personal computer (PC) while reading, writing, and playing games, etc.
- organic input/output (I/O): help human organs to see, hear, touch, and smell, etc.

As in science and engineering, media technology is to create cost-effective solutions to help human intelligence by applying various scientific knowledge such as electronics, telecommunication, computer science, mathematics, physics, material science, human-machine interaction, cognitive science, perception psychology, sociology, and economics, etc. However, today's media technologies are mainly built on electronic and computer systems, which are called digital media or multimedia. Digital media is stored in compact disk – read-only memory (CD-ROMs), hard disks, and flash memory. Digital cameras and video recorders are used to capture photos and record real scenes.

Online newspapers

An online newspaper is the online version of a newspaper, either as a stand-alone publication or as the online version of a printed periodical. Online newspapers such as those competing with broadcast journalism can present breaking news in a timelier manner. The credibility and strong brand recognition of well-established newspapers are also seen by the newspaper industry as strengthening their chances of survival. No printing process can help decrease costs.

Online newspapers are more or less like hard-copy newspapers and have the same legal boundaries, such as laws regarding libel, privacy and copyright. A blog or a wiki is nevertheless not clear to the public. News reporters are being taught to shoot videos and to write the Internet news pages. They attempt to write stories for both print and online publications.

Wiki (as a kind of social media)

A wiki is a website which allows collaborative modification of its content and structure directly from the web browser. "Wiki" is a Hawaiian word meaning "quick". Wikipedia is by far the most popular wiki-based website, and is in fact one of the most widely-viewed sites of the world. In a typical wiki, text is written using a simplified markup language, running on wiki software. There are at least tens of thousands of other wikis in use, both public and private, including wiki functions as knowledge management resources, notetaking tools, community websites and intranets. Some wiki engines are open source, whereas others are proprietary. Some permit control over different functions (levels of access), for example, editing rights may permit changing, adding or removing materials. Others may permit access without enforcing access control. Other rules may also be imposed to organize contents. Ward Cunningham, the developer of the first wiki software, WikiWikiWeb, originally described it as "the simplest online database that could possibly work." [29]

The essence of the wiki concept is as follows:

– "A wiki invites all users to edit any page or to create new pages within the wiki Web site, using only a plain-vanilla Web browser without any extra add-ons.

– "Wiki promotes meaningful topic associations between different pages by making page link creation almost intuitively easy and showing whether an intended target page exists or not.

– A wiki is not a carefully crafted site for casual visitors. Instead, it seeks to involve the visitor in an ongoing process of creation and collaboration that constantly changes the website landscape."

"A wiki enables communities to write documents collaboratively, using a simple markup language and a web browser." A single page in a wiki website is referred to as a "wiki page" which is usually well interconnected by hyperlinks. "A wiki is essentially a database for creating, browsing, and searching through information." A wiki allows evolving, complex, and networked texts with argument and interaction. A characteristic of wiki technology is the ease to find which pages can be created and updated. Generally, there is no review before modifications are accepted. "Many wikis are open to alteration by the public without requiring registration of user accounts. Many edits can be made in real-time and appear almost instantly online. However, this feature facilitates abuse of the system. Private wiki servers require user authentication to edit pages, and sometimes even to read them."

Blog (as a kind of social media)

A blog is a personal online journal that is frequently updated and intended to the open public, which is a discussion or an informational site published on the World Wide Web [30]. Blogging can be seen as a form of a social networking service. A key characteristic of blogs is interactive, allowing visitors to leave comments and even messages to each other on the blogs. The interactivity of blogs distinguishes them from other static websites. "Bloggers do not only produce contents to post on their blogs, but also build social relations with their readers and other bloggers." The one is more personal online diaries and the other is more of an online brand advertising of a particular individual or company. Many blogs provide commentary on a particular subject. "A typical blog combines text, images, and links to other blogs, Web pages, and other media related to its topic. The ability of readers to leave comments in an interactive form is an important contribution to the popularity of many blogs. Most blogs are primarily textual, although some focus on art (art blogs), photographs (photoblogs), videos (video blogs or "vlogs"), music (MP3 blogs), and audio (podcasts). Microblogging is another type of blogging, featuring very short posts."

Recently with the rise of Twitter and other "microblogging" systems, "multi-author blogs" (MABs) have been developed, in which the posts written by large numbers of authors are professionally edited. "MABs from newspapers, other media outlets, universities, think tanks, advocacy groups, and similar institutions account for an increasing quantity of blog traffic." There are many different types of blogs: personal blogs, collaborative blogs, group blogs, microblogging (the practice of posting small pieces of digital content which could be texts, pictures, links, short videos, or other media on the Internet), corporate and organizational blogs. It is noteworthy to mention that the future direction of the news is all blogosphere, all opinions with no serious fact-checking, no serious attempts to put stories in contexts, but not a lot of mutual understanding.

Wikipedia (as a kind of social media)

Wikipedia is a free, open content online encyclopaedia created through the collaborative efforts of a community of users. It is a special type of website designed to make collaboration easy, called a wiki. Jimmy Wales and Larry Sanger co-founded Wikipedia [42]. As of January 2008, the encyclopaedia offered over four million articles. At that same time, Wikipedia is ranked as the eighth-most popular site on the Internet. Wikipedia was the only non-commercial site of the top ten. Criticisms of Wikipedia include assertions that its openness makes it unreliable and unauthoritative. Because articles do not include by-lines, authors are not publicly accountable for what they write. Similarly, because anyone can edit any article, the site's entries are vulnerable to unscrupulous edits.

Facebook (as a kind of social media)

Facebook is a popular free social networking website that allows registered users to create profiles, upload photos and video, send messages, and keep in touch with friends, family, and colleagues. This site includes public features such as:

– Marketplace – allows members to post, read, and respond to the classified advertisements;

– Groups – allows members who have common interests to find and interact with each other;

– Events – allows members to publicize an event, invite guests, and track who plans to attend;

– Pages – allows members to create and promote a public page built around a specific topic;

– Presence technology – allows members to see which contacts are online and chat.

Within each member's personal profile, there are several key networking components. The most popular feature is arguably the Wall which is essentially a virtual bulletin board. Messages left on a member's Wall can be texts, videos or photos. Another popular component is the virtual photo album. Photos can be uploaded from a desktop or directly from a smartphone camera. An interactive album allows the member's contacts (who are generically called "friends") to comment on each other's photos and identify (tag) people in the photos. Another popular profile component is status updates. A microblogging feature allows members to broadcast short announcements to their friends. All interactions are published in a news feed, which is distributed in real time to the member's friends.

Facebook offers a range of privacy options to its members. A member can make all his communications visible to everyone. He can block specific connections and keep all his communications private. Members can choose whether or not to be searchable, decide which parts of their profile are open to the public, decide what not to put in their news feed, and determine exactly who can see their posts. For those members who wish to use Facebook to communicate privately, the messages closely resemble e-mails.

Facebook represents a potentially useful tool in educational contexts. It allows for both asynchronous and synchronous dialogues and supports the integration of multimodal contents such as user-created photographs, video, and URLs to other texts. Furthermore, it allows students to ask minor questions when they might not feel like visiting a professor during office hours. Facebook is one alternative means for shyer students to be able to voice their thoughts in and outside of the classroom. It allows students to collect their thoughts and articulate them in writing. In addition, it can encourage more frequent student-instructor and student-student communications.

Twitter (as a kind of social media)

Twitter is a free social networking microblogging service that allows the registered members to broadcast short posts called tweets. Twitter has been called "the SMS of the Internet". Twitter members can broadcast tweets and follow other users' tweets by using multiple platforms and devices. Tweets can be sent by cell phone text messages. Twitter was created in March 2006 by Jack Dorsey, Evan Williams, Biz Stone and Noah Glass and launched in July 2006 [31].

The default settings for Twitter are public. To weave tweets into a conversation thread or connect them to a general topic, members can add hashtags to a keyword in their post. Tweets, which may include hyperlinks, are limited to 140 characters due to the constraints of Twitter's short message service (SMS) delivery system. Because tweets can be delivered to followers in real time, they might seem like instant messages to the novice user.

YouTube (as a kind of social media)

YouTube is a video-sharing website headquartered in San Bruno, California, United States [32]. The site allows users to upload, view, and share videos. It makes use of WebM, ITU-T H.264/MPEG-4 advanced video coding (AVC) [50] to display a wide variety of user-generated and corporate videos. Available contents include video clips, TV clips, music videos, and other contents such as video blogging, short videos, and educational videos.

Most of the contents on YouTube have been uploaded by individuals, but some media corporations offer their materials via YouTube. The unregistered users can watch videos and the registered users can upload videos to their channels. YouTube is the most frequently used social media tool in the classroom. Students can watch videos, answer questions, and discuss contents. Additionally, students can create videos to share with others. YouTube also provides an opportunity for peer learning and problem solving since videos keep students' attention, generate interests in the subject, and clarify course contents. Additionally, the videos help students recall information and visualize real world applications to understand course concepts.

Both individuals and large production companies have used YouTube to grow audiences. Old media move into the websites that witness early content creators and perceive audience volumes larger than that attainable by television. Online video will dramatically accelerate scientific advances. It can do for face-to-face communication which has been "fine-tuned by millions of years of evolution". However, at the time of uploading a video on YouTube, the copyright issues are controversial since there are still many unauthorized clips of copyrighted materials.

Key features of social media

In comparison with other media, social media has a variety of business opportunities to engage into marketing, research, communication, sales promotions/discounts, and relationship development. Social media are a blending of technology and social interaction for the co-creation of values. People obtain information, news, and other data from electronic media. They enable anyone to publish information as a type of user-generated contents. Social media have provided an open environment where people are free to exchange ideas on technologies, applications, brands, and products.

One characteristic shared by social media is the capability to reach small or large audiences, for example, either a blog post or a television show may reach some people or millions of people. The differences of social media from traditional media is described as follows [24]:

1 **Quality**: The main challenge posed by contents in social media sites is the fact that the distribution of quality varies from very high quality to low quality, to sometimes abusive contents.

2 **Reach**: Social media are more decentralized, less hierarchical, and distinguished by multiple points of production and utility.

3 **Frequency**: The number of advertisements is immediately displayed on social media platforms.

4 **Accessibility**: The social media tools are generally available to the public.

5 **Usability**: Most social media production requires skills or tools to be open, and anyone can commonly operate the means of social media production.

6 **Immediacy**: Social media can be capable of virtually instantaneous responses.

7 **Permanence**: The contents of social media can be altered almost instantaneously by comments or editing.

In addition, the features of social media can be classified with the following functional blocks [24]:

– **Identity**: This block represents the extent to which users reveal their identities in a social media setting. It includes metadata information such as name, age, gender, profession, location, and also additional information that portrays users in certain ways.

– **Conversations**: This block represents the extent to which users communicate with other users. Many social media sites are designed primarily to facilitate conversations among individuals and groups. People tweet and blog to meet new like-minded people, to find true love, to build their self-esteem, or to be on the cutting edge of new ideas or trending topics.

– **Sharing**: This block represents the extent to which users exchange, distribute, and receive contents. The term 'social' often implies that exchanges between people are crucial. In many cases, however, sociality is about the objects that mediate these ties between people.

– **Presence**: This block represents the extent to which users can know whether other users are accessible or not. It includes knowing where others are, in the virtual world and/or in the real world, and whether they are available.

– **Relationships**: This block represents the extent to which users can be related to other users. Two or more users have some form of associations that lead them to converse, share objects of sociality, meet up, or simply just list each other as a friend or fan.

– **Reputation**: This block represents the extent to which users can identify the standing of others, including themselves. Reputation can have different meanings on social media platforms. In most cases, reputation is a matter of trust. Since the current information technologies are not yet good at determining such highly qualitative criteria, social media sites rely on automatic aggregation of user-generated information to determine trustworthiness.

– **Groups**: This block represents the extent to which users can form communities and sub communities. The more 'social' a network becomes, the bigger the group of friends, followers, and contacts.

Recently, the new add-on features of social media technologies are investigated as follows:

– (**Secret**) The users share their feeling and thoughts only inside their own contacts. They do not want to share without knowing who they are.

– (**Snap shot**) By using smartphones, mobile social networking services can share photos or videos with private messages. A series of photos and videos can be composed of a variety of storytelling. A nice collection of photos can be tagged from others.

– (**Voice message**) The smartphone is useful to send voice messages as well as texts. Through voice calls, photos and videos can be shared with others.

– (**Dating**) People can chat about their mutual feelings on photos and basic information of others.

- (**Microblogging**) If someone wants to publish stories or ideas, others can recommend the related stories and give a view of their favourites.
- (**Like**) Users can click the "like" button with a comment. Some symbols like a heart and bubble can be posted on photos and messages.
- (**Direct message**) A direct message can be sent to an anonymous person for advice or just for a chat. It allows people to anonymously share secrets.

Web technologies for social media

Many people recognize that web technology is a web page by using the web browser. A web browser displays a web page on a monitor or mobile device. With graphic user interface, the web page is what is displayed, usually written in HTML or comparable markup language. Web browsers coordinate the various web resource elements for the web page such as style sheets, scripts, and images [33]. Typical web pages provide hypertexts which include the navigation menu to other web pages via hyperlinks. A web browser can retrieve a web page from a remote web server. The web browser uses the hypertext transfer protocol (HTTP) to make requests to the web server. The web server may restrict access to only a corporate network. A static web page is delivered exactly as stored in the web servers, while a dynamic web page is generated by a web application that is driven by server-side software or client-side scripting. Today, web pages are becoming more dynamic as in many popular forums, online shopping, and even on Wikipedia. A dynamic web page is created at the server side when it is requested and served to the end users. These types of web pages typically do not have a permanent link, or a static URL, associated with them. The design of a web page is personal according to one's own preferences. Many people edit the contents of a web page by using web templates. They rely on web hosting services for a quick and easy creation of a web page.

A web document is similar in concept to a web page, but a web document has its own uniform resource identifiers (URIs). It should be noted that a web document is not the same as a file. A single web document can be available in many different formats and languages. A single file, for example a hypertext preprocessor (PHP) script, may be responsible for generating a large number of web documents with different URIs. A web document is defined as HTML, Joint Photographic Experts Group (JPEG), or resource description framework (RDF) in response to HTTP requests. As for the resources identified by URI, the user gets a readable representation of the web, in which the resources are not only web documents, but also real world objects such as cars, buildings, sensors, and non-existing things.

There are various definitions of the web: web service, web applications, web page, web protocol, web operating systems, and web data, etc. First, W3C defines a web service as a software system designed to support interoperable machine-to-machine interaction over a network. Technically, a web service describes a standardized way of integrating the web-based applications using the XML, simple object access protocol (SOAP), web service definition language (WSDL) and universal description, discovery and integration (UDDI) open standards, which is defined as [34]:

- A web service has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the web service prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other web-related standards.

- **Social graph for knowledge representation**

The social graph is a graph that depicts personal relations of users. In the relational representation of social networking services, the social graph has been referred to as "the global mapping of everybody and how they're related." [35] The graphic model of knowledge has structured the relationships with lines connecting objects to indicate knowledge. To solve problems of very complex systems, social graphs are used to find rules and relations of sets and subsets of problems. Various kinds of reasoning from individual views or opinions automate their logics into a graphical form. Knowledge representation by using social graph incorporates the findings about how humans solve problems and represent knowledge that will make complex systems easier to design and build. In a graphic form, knowledge representation goes hand in hand with automated reasoning because representing knowledge explicitly by graphic form is to be able to reason about that knowledge, to make inferences, and assert new knowledge, etc. All knowledge representation methods like social graphs have a reasoning or inference engine.

Similar to a social graph, a mind map is also used to visually organize information based on hierarchies and tree structures denoting relationships with a concept. A mind map is created and drawn as an image to which representations of ideas are added. The concept maps connect multiple words or ideas which has text labels on their connecting lines.

- **Emerging technologies for structured media**

For the future of media structure, the documents with website usability are very important to enable content sharing, creating ideas collectively, and accumulating business intelligence. The web technology with a cloud-based platform provides the controlled way to share and store documents with the collaboration of users. The emerging features of future structured media will be based on web technologies as follows:

- (**Voice**) For voice interaction, document formats representing speech dialogue and specific markup language for speech recognition are defined in a form of XML. With voice interface at the web document, it is possible to create new interactive voice applications like a voice browser.
- (**Image**) For image representation, the colour format of images and the animated format of objects can be defined as an emerging document, which are natural for interpretation and suitable for user interaction. To search for image library, the techniques for tagging and indexing images are needed in the web documents. The images or symbols with textual contents are indexed by the search engines. In addition, the extraction of text strings from images and symbols of the web documents is used to represent colour code and indicate real physical components connected to animated symbols. A fraction of images may contain texts for a specific query.
- (**Table**) To lay out the contents with table format, the techniques for indexing and analysing tables are investigated at the web format. The sequence of strings of columns and rows in the table structure can appear in a graphical form.
- (**Graph**) The graph representation in the web documents is used to deliver the logical structure of tasks, algorithms, functionalities, or heuristics, etc. The graph model for HTML documents includes the tree-structured hierarchy when parsing the tags. To connect nodes in the hierarchy of a graph model, there are the incoming/outgoing links for query and process. The hyperlink in a graph model is used to distinguish nodes of external references.
- (**Index**) The documents in the database or the directory would be well formatted and indexed. The string of texts in the documents is hyperlinked to the specific URIs of the web. Some images may be linked with real geographical locations.
- (**Semantics**) Technically, the semantic web with tags will be coming to mark up semantics on HTML and XML as well as traditional word-like documents. Most contents have various ontology/XML standard formats, which are stored in databases with label.
- (**Multimodal**) The multimodal interface of future web documents is one of the outstanding issues to be solved in the near future.
- (**Language**) For exploiting knowledge from documents on the web, the integration of XML technologies is used for natural language processing. With syntactic and semantic analysis of language, the self-explaining XML tags can be used to recognize concepts and extract knowledge from the document.

To cultivate new emerging media, the content authoring tools are also needed to develop. Until now, there are many ways for authoring multimedia documents. A video description with the structured model is used for the composition of video elements (character, shot, scene, etc.) with other media objects (text, sound, image, etc.). The multimedia documents have more complex and sophisticated presentation. For example, a character in a video is introduced by displaying a textual description when that character occurs. A word in a text sentence is highlighted when an audio plays out. A hyperlink is set on a video object or on a particular region of an image. A start time of the video object in the video sequence coordinates the word in the texts and time location of word pronunciation in the audio or coordinates the video objects and the image regions. The structured media whose information content is described will make the content information available for composition process. A structured media contains not only raw data, but also a hierarchical description of this media content information. Multimedia documents have more complex presentation scenarios and require more flexible presentation services including interactions. For the multimedia documents with XML description, the web browsers can implement the temporal and spatial models to present the documents.

6 Risks of knowledge society

Negative effects of social media

Social media relies on trustworthiness and reliability of information presented. The impacts of social media include an individual's concentration, ownership of media content, and the meaning of interactions. Although some social media offers users the opportunity to cross-post simultaneously, some social media platforms have been criticized for poor interoperability or disparity of information, which leads to the creation of information silos-isolated collections of data contained in a social media platform. Sometimes, it is argued that social media have negative effects while allowing individuals to advertise themselves and form friendships. The term "social" cannot account for positive features and hence the level of sociability should be determined by the actual performances of users.

Since the dramatic decrease of face-to-face interactions, more social media platforms have been introduced with the threat of cyber-bullying and online sexual predators being more prevalent. Social media may expose children to images of alcohol, tobacco, and sexual behaviours. In regards to cyber-bullying, it has been proven that individuals who have no experiences with cyber-bullying often have a better well-being than individuals who have been bullied online.

Twitter is increasingly a target of heavy activity of marketers. Their actions, focused on gaining massive numbers of followers, include use of advanced scripts and manipulation techniques that distort the prime idea of social media by abusing human trustfulness.

British-American entrepreneur and author Andrew Keen criticizes social media in his book "The Cult of the Amateur" [36] writing: "Out of this anarchy, it suddenly became clear that what was governing the infinite monkeys now inputting away on the Internet was the law of digital Darwinism, the survival of the loudest and most opinionated. Under these rules, the only way to intellectually prevail is by infinite filibustering." This is also relative to the issue of "justice" in the social network.

Social networking threats

Social networking tools have changed the way people interact in their personal life and business. Increasingly, these tools play a significant role in how business gets done; however, they are also a high risk. Below are top 10 social networking threats/risks that enterprises must consider when developing their policies [37]:

1 **Social networking worms**: While a multi-faceted threat challenges the definition of "worm", it is specifically designed to propagate across social networks, enlist more machines into its botnet, and hijack more accounts to send more spam to enlist more machines.

2 **Phishing bait**: Many users of the social networking services had their accounts compromised. Although this was only a "tiny fraction of a percent," it is still a significant number considering that famous social networking services have over several million users. To their credit, the social networking services acted quickly, working to blacklist that domain, but many copycat efforts ensued.

3 **Trojans**: Social networks have become a great vector for Trojans: Zeus – a potential and popular banking Trojan that has been given new life by social networks. There have been several recent high-profile thefts blamed on Zeus. URL zone can calculate the value of the victim's accounts to help decide the priority of the thief.

4 **Data leaks**: Social networks are all about sharing. Unfortunately, many users may share too much sensitive information about their organizations such as projects, products, financial, organizational changes, and/or scandals, etc.

5 **Shortened links**: People use URL shortening services (e.g. bit.ly and tinyurl) to fit long URLs into tight spaces. They may be clicking on a malware since the shortened links are easy to use and are also ubiquitous.

6 **Botnets**: Recently, the accounts of a social networking service are used as the command and control channel for a few botnets. It is shutting these accounts down given the ease of access of infected machines via the social networking service.

7 **Advanced persistent threats**: One of the key elements of advanced persistent threats (APT) is the gathering of intelligences of persons of interest, for which social networks are a data source. Perpetrators of APTs use this information to further their threats by placing more intelligence gathering (e.g. malware, Trojans), and then gaining access to sensitive systems.

8 **Cross-site request forgery (CSRF)**: CSRF attacks exploit the trust that a social networking application has in a logged-in user's browser. Consequently, as long as the social network application is not checking the referrer header, it is easy for an attack to "share" an image in a user's event stream that other users might click on to catch and spread the attacks.

9 **Impersonation**: The social network accounts of several prominent individuals with thousands of followers have been hacked. Furthermore, several impersonators have gathered hundreds and thousands of followers.

10 **Trust**: The common thread across almost all of the threats is the tremendous amount of trust that users have in social applications. Like e-mail or instant messaging, people trust links, pictures, videos and executables when they come from "friends".

Political dangers and personal safety of blogs

Blogging can sometimes have unforeseen consequences in politically sensitive areas. Blogs are much harder to control than broadcast or even print media. As a result, some authorities and communities often seek to suppress blogs and/or to punish those who maintain them. For example, a blogger was found guilty and sentenced for a three-year prison term for insulting Islam and inciting sedition.

One consequence of blogging is the possibility of attacks or threats against the blogger, sometimes without apparent reason. While a blogger's anonymity is often tenuous, Internet trolls who would attack a blogger with threats or insults can be emboldened by anonymity. Therefore, the Blogger's Code of Conduct which is proposed by Tim O'Reilly for bloggers enforces civility on their blogs by being civil themselves and moderating comments on their blog. A proposed list for blogging behaviours is as follows [30]:

1 Take responsibility not just for your own words, but for the comments you allow on your blog;

2 Label your tolerance level for abusive comments;

3 Consider eliminating anonymous comments;

4 Ignore the trolls;

5 Take the conversation offline, and talk directly, or find an intermediary of who can do so;

6 If you know someone who is behaving badly, tell them so;

7 Do not say anything online that you would not say in person.

Human right in knowledge society

Human right and inclusive participation are characteristics of knowledge society. Freedom of expression implies freedom of opinion, freedom of speech and of the written word, freedom of the press, free access to information, and the free flow of data and information. Human right is summarized as [38]:

- Freedom of opinion and expression as well as freedom of information, media pluralism and academic freedom.
- Freedom of expression is a fundamental human right. Everyone has the right to freedom of opinion and expression.
- Closely linked with the essential freedom of scientific research and artistic creation.
- The right to education towards free access to other levels of education.
- The right to "freely to participate in the cultural life of the community, to enjoy and share in scientific advancement and its benefits."

- The freedoms described in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights also guarantee that individuals throughout the world will not allow themselves to be submerged by the mass of confused data. It is for relevant information, exchange, sharing, discussion and scientific or free creative activity that such information can become knowledge.
- Freedom of expression is moreover the guarantee of access for all to contents that are as diversified and reliable as possible.
- From the point of view of fundamental rights, the political safeguarding of those rights and the diversity of contents that circulate in the global information society.

Knowledge societies is risk societies

Knowledge resources have become strategic, but if exploited for ill-intentioned purposes they could inflict irreparable damage. By making such resources accessible to the world at large, unknown dangers will be opened up. On the contrary, the accelerated spread of knowledge is to confront risks and to boost the self-regulating capacity of human societies. The risks that threaten people arise from the complexity of their interaction and the mechanisms required to cope with those risks. Knowledge societies may precisely constitute the most effective means of dealing with the new complexity of technological developments. Eventually, some mechanisms are needed to cure the ills of ignorance and error, to free the individual from fears and constraints represented by nature, to lessen uncertainty and to control risks.

Knowledge societies will have to meet instability and insecurity that are often social and political consequences of scientific progress and technological innovation. In nature, any technological innovation and any technical system generates risks. However, not all risks are equal and some are unacceptable. The distinction between risks taken intentionally and risks incurred passively is an ethical debate on inequalities with regard to risk.

Risks on data integrity

Data integrity refers to maintaining and assuring the accuracy and consistency of data. It is critical to design, implementation, and usage of any system which stores, processes, or retrieves data. Data integrity is the opposite of data corruption, which is a form of data loss. Data integrity as protecting data from unauthorized parties is not to be confused with data security. It aims to prevent unintentional changes to information. The failure of data integrity results from any unintended changes to data as the results of storage, retrieval, processing operation, including malicious intent, unexpected hardware failure, and human error, etc. If the changes are the results of unauthorized access, it may also be a failure of data security. Data integrity can be lost because of programming errors (e.g. good data is processed by incorrect programs), processing errors (e.g. transactions are processed more than once against the same master file), or management/process errors (e.g. poor management of the systems maintenance process).

The risks of data integrity pervasively apply to an application system used to support a work process in multiple places and at multiple times throughout the network. However, they are principally manifest in the following components of risks:

- **User interface**: Risks in this area relate to whether there are adequate restrictions of user interfaces to be authorized to perform system functions. Other risks relate to the adequacy of preventive or detective controls of user interfaces to ensure that only valid data can be entered into a system.
- **Processing**: Risks relate to whether there are adequate preventive or detective balancing and reconciliation controls to ensure that data processing has been timely completed. It includes risks associated with the accuracy and integrity of decisions-making.
- **Error processing**: Risks in this area relate to whether or not there are adequate processes and other system methods to ensure that any data entry or processing exceptions that are captured are adequately corrected, and reprocessed accurately, completely and on a timely basis.
- **Data interface**: Risks relate to whether there are adequate preventive or detective controls to ensure data that is adequately and completely transmitted to be processed by another system.

- **Change management**: This risk is associated with inadequate change management that includes user involvement and training. It includes the process changes of a system that are both communicated and implemented.
- **Data**: This risk is associated with inadequate data management controls which include both the security/integrity of processed data and the effective management of databases and data structures.

Focusing on data integrity, attacks result from intentional, and unauthorized modification of data. There are several attacks on data integrity such as abuse of trust, forgery, and unauthorized use, etc. The loss of data integrity is triggered by the following situations [39]:

- Changes to access permissions and privileges;
- Inability to track the use of privileged passwords, particularly when passwords are shared;
- End-user errors that impact production and manipulation of data;
- Vulnerable code-in applications (e.g. backdoors);
- Weak or immature change control and accreditation processes;
- Misconfiguration of security devices and software;
- Incorrectly or incompletely applied patches;
- Unauthorized devices connected to the private network;
- Unauthorized applications on devices connected to the private network.

In order to improve data integrity, the adoption of best practices needs to be complemented by formalizing accountabilities for data processes that support and enhance data security. For the ICT service environments, the good practices for data integrity include [39]:

- **Taking ownership of data and accountability for data integrity**: When IT services and operations are outsourced, and when these are provided in-house, it is easy to believe that the data are owned by the IT service providers. In this situation, the IT service provider is responsible for maintaining confidentiality and integrity. Ownership requires a value assessment in an estimation of the potential cost of lost data integrity, including direct financial losses (as is the case in fraud or major operational disruption), legal costs, and reputational damage.
- **Access rights and privileges**: The principles of "need to know" and "least privileged" are good practice and, in theory, are not difficult to apply. The social networking concept that everyone is an information producer allows greater openness and sharing. It forces to resist and challenge the implementation of these principles. The processes for requesting, changing, and removing access rights should be formalized, documented, regularly reviewed, and audited. It is common for organizations not to have a complete and updated inventory of who has access and what is a complete list of user privileges.

Against transparency: Risks of open data

Open data is a growing class of available information assets that increasingly provides additional big data analytics. It offers a lot of business benefits including strategy insights, market and trend awareness, and even direct monetization. By consuming open data, people expose themselves to a variety of risks during the purchase of syndicated data from information brokers and the use of internal enterprise data.

There are many potential gains for a wide range of data to be used from financial transactions with business partners to high-level information such as tacit knowledge or know-hows, for example, on how bumblebees respond to different flowers. Open data enables accountability if the facts are there for all to see. Open data empowers communities from inputs of the truth about crime rates, educational achievement, and social services, etc. Open data even drives economic growth while more small companies are springing up that extract useful information from data. Open data may even lead to more accurate and better decisions since a wider variety of interested parties have the opportunity to examine the facts.

However, open data also raises some concerns. The potential threat to privacy is probably the foremost risk. There is no personal data to be shared with any third party. However, it is questionable whether this can be achieved by the use of multiple sources of data which can be combined to yield information about individuals.

Risks on Internet and digital technologies

Digital communication has a number of specific characteristics that make it so popular. Digital media are primarily characterized by an exceptional ease of receiving and sending messages. A message sent by e-mail or in the form of short message service (SMS) is received almost instantaneously regardless of geographic distance. Experts warn that specific characteristics of digital communication entail risks that may easily be overlooked or be underestimated and that affect young people in particular. The Internet and digital technologies can enable some authorities to monitor telephone conversations, to close down a website, to ban the illegal use of a radio frequency or even to filter out specific flows of spams or advertisement messages. The access of a large number of users to information resources is full of promise, but it can also cause irreparable damage and create unpredictable dangers. The growth of knowledge societies might precisely be one of the most effective means to reduce risks.

As far as technological hazards are concerned, the man-machine system has always proved unpredictable and fallible, whereas the nature of the system is to function normally. The drawbacks and risks in the system may be passed off while the inescapable failure down takes place. The network development gives increasing importance to knowledge. It relies on technological dependency which accentuates risks and threats. Misuse of knowledge can be utilized by terrorists. The potential consequences of misuse of knowledge may accelerate terrorist activities. Scientists and engineers have a duty to protect the public safety from those hazards.

Greater openness, combined with hiding one's real identity and impersonating a false one, increases the risks of people making contacts with malicious individuals and becoming victims of deception. In more extreme cases, young people may fall prey to "sexual predators", become members of cults, be exposed to dangerous ideologies, and start gambling or carrying out illegal activities, etc. With all emerging technologies, there are potentials for misuse. Risks associated with user interactive actions include cyberbullying and abuse by online predators. They also include identity theft and exposure to inappropriate contents including self-harm, racism, and adult pornography, etc. The risks to children and young people watching video games may be subject to be reviewed by governments. In order to understand the potential risks and encourage safe and responsible use of the Internet, there are crucial steps of risk management to be taken to keep children and young people safe online. The ICT experts may develop the safeguarding processes and relevant technologies to protect children and young people.

Security and privacy on cloud computing

Cloud computing poses privacy concerns because the service providers can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete some portions of the data. Many cloud providers can share data and information with third parties while a requisite for the purposes of law and order should be needed. This should be permitted in privacy policies that users have to agree to before they start using the cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how the data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. There is the risk that end users do not understand the issues involved when signing on to a cloud service (for example, persons sometimes do not read the many pages of the terms of service agreement, and just click "Accept" without reading).

In a cloud computing platform being shared by different users, there may be a possibility that information belonging to different copyright owners resides on the same data server. Therefore, information leakage may arise by mistake when information belonging to one customer is given to others. Additionally, hackers are spending substantial times and efforts looking for ways to penetrate the cloud. There are some real Achilles' heels in the cloud computing infrastructure that are making big holes for bad guys to get into. Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of a huge database of information through a single attack.

There is also the problem of legal ownership of the data. Many terms of service agreements are silent on the question of ownership. Physical control of the personal computer equipment (that is private cloud) is more secure than having the equipment offsite and under someone else's control (that is public cloud). Fundamentally, the private cloud is being seen as more secure with a higher level of control; however, the public cloud is being considered to be more flexible and requires less time and money investments from users. Public cloud computing service providers have great incentive to prioritize building and maintain a strong management of secure data. Some small businesses that do not have expertise in IT security could find it more secure to use a public cloud.

Risk identification, protection, and management

It is very difficult to prevent risks that people have not identified beforehand. Knowledge societies seem well protected than ever to undertake such a task. The information and technological revolution are indisputably a great advantage for researchers who have access to a vast amount of resources. Such proliferation may make it difficult to identify and manage risks. The knowledge-based process like big data analytics may be emerging to expose risks from the undifferentiated flows of available data.

As a matter of fact, risk identification is a matter of good governance. Information is of no value if people are unable to gather and use it. Risk identification requires the efficient activity of data analytics whose technical and scientific abilities must be recognized by the public and private decision-making entities. Risk identification has the priority to ensure that key information is passed up to the highest decision-making levels, in particular in cases of hacking or natural disasters. In order to handle risks, the relevant risk management system should report the incident quickly to the decision-makers. The precautionary principle on risk is to recommend a proactive approach.

The monitoring of the predefined risks can also be set up both at the domestic and international levels. In the war against terrorism, knowledge on risks becomes a strategic resource. Governments may monitor contents, identify access points, and block websites to avoid potential risks. To restrict illegal contents, the sophisticated surveillance techniques can be developed.

Risk management takes information feeds from one or more sources that detect deviations, defects, or other patterns from security or business applications. This can include active sensor technologies to protect, monitor, and manage information networks and systems. For risk management, it is important to bear in mind the prevention of risks. Sufficient countermeasures are required rather than excessive, unnecessary, and pointless measures. Sometimes, the good intentions of risk management become wasteful expenditure or impediments to growth, innovation, and opportunity for ICT markets. By combining information and communication technologies such as web-based information security management systems, the defences against cyberattacks are enhanced in real time. The information and communication technologies for risk protection and management include [40]:

- host-based intrusion detection, vulnerability assessment, configuration and policy compliance, database logs, website logs, and file accesses;
- hosts for penetration testing, e-mail scanning, and spam filters;
- network intrusion detection and prevention, netflow, and firewall/router/other network devices logs;
- access and identity for successful or failed logins, new users, deleted users, privilege escalation, and biometric identities;
- website vulnerability detection (cross-site scripting, structured query language (SQL) injection, etc.), pages visited, and referred from;
- end-point monitoring such as permitted user activity, not permitted user activity, data leakage monitoring, universal serial bus (USB) usage monitoring and reporting;
- anti-virus, anti-phishing, and malware detection;
- audit logs of activity, and audit log collection for operating systems, etc.

Governance of knowledge society

If everyone is able to find their place and their presence, without distinction of any kind – race, sex, language, religion, political or philosophical convictions, income or class, knowledge as a most valuable resource will increasingly determine who has access to profit from it. Knowledge sharing requires an effort of thinking and understanding, an ability to question one's own certainties, openness to the unknown, a desire to cooperate, and a sense of solidarity. In knowledge-based economies, the human capital is the main source of profit.

The emergence of a knowledge society may bring about new forms of relationships between its citizens, on the one hand, and between its citizens and institutions, on the other hand. With the progress of information and communication technology, some members directly control entire organizations and communities by managing information flows over their own hierarchical structure of management. Governance activities ensure that critical management information is sufficiently complete, accurate and timely to enable appropriate management decision-making, and provide the control mechanisms to ensure that strategies, directions, and instructions are carried out systematically and effectively.

In addition, data governance addresses specifically the information resources that are processed and disseminated. Data governance has an important function for public data of government and private data of business, which is setting the parameters for data management and usage, creating processes for resolving data issues, and enabling users to make decisions based on high-quality data and well-managed information assets. The key elements of data governance can be categorized into major areas of data accessibility, data availability, data quality, data consistency, data security, and data auditability.

New policies on privacy and copyright

The right to think and to say what one thinks is not the right to disclose what one knows. Thus, some information, for example, from the cartography of strategic sites to the publication of certain scientific discoveries can be seen as sensitive. It may be excluded from the information that may be freely circulated. The protection of privacy of personal data has arisen as a new fundamental right of the individual [38]. In the name of openness and free circulation of information and knowledge, there is a growing confusion between private knowledge and public knowledge. The separation between the public and private domain protects people against too intrusive an interest by others. Too much knowledge may be harmful. Secrecy is an important mode of social regulation because it protects privacy. In relation to private life, the counterpart of the right not to know is a right that the others shall not know. "Expression" and "commoditization" obey logics that can be contradictory.

Trademark protection can also entail a restriction on freedom of expression. It requires a balanced approach combining protection of intellectual property and promotion of the public domain. Paying process royalties to the copyright holder may lead to a violation of the copyright.

7 New opportunity of knowledge society and social media

Evolution of social media markets

Social media has become a ubiquitous part of daily life. From primitive days of traditional news and chat rooms, social media has changed the way we communicate, gather and share information, and has given rise to a connected global society. There was the social innovation that started with the first crowdsourced encyclopaedia, Wikipedia. While Facebook and Twitter are the two top social media platforms today, there will be other great steps of social media with combinations of IoT/M2M and cloud computing technologies. The mobile smartphone will open the additional playground of social media.

For interaction behaviours of social media, the users read blogs, Facebook and Twitter, listen to podcasts, visit social websites, watch and upload audio, music, and video, publish blogs and web pages, and comment on someone else's blog, etc. However, there will be new markets of social business as shown in Figure 6. While the current social media are mainly for information and entertainment, the new social media will shift their capabilities to drive business including mission critical applications. There will be new types of engagements of customer relationship to bridge the gap among human knowledge and experiences, and obtain new revenues from customers. By connecting people including customers, employees, and partners, new productive and efficient ways of business will be launched. By collectively sharing information among people, more exact actions to drive better business results will be aligned.

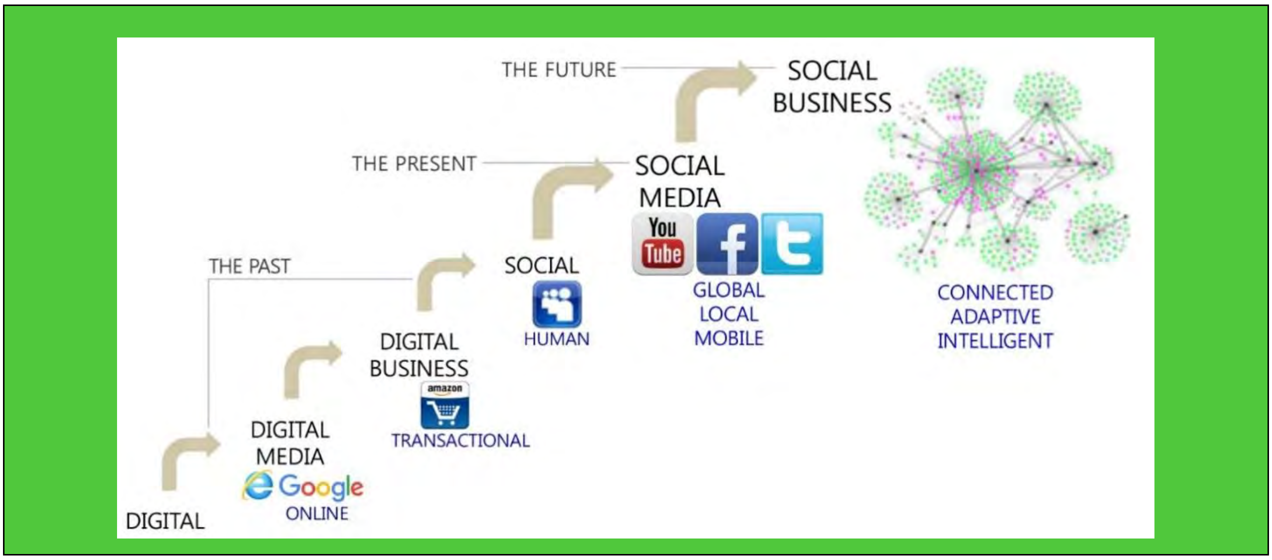


Figure 6 – Evolution of social business [41]

When the IoT/M2M technologies are combined with social media, there is an amazing opportunity to create better, more useful experiences. There are new ways of human life and business by utilizing sensor technologies such as smoke detectors, motion detectors, thermostats, and closed-circuit television (CCTV) cameras, etc. The situations captured by many sensors are visualized in the smartphones of individuals and/or groups of communities, which invoke reactions and feedback from people. The evolutions of the Internet of things (IoT) applications will take the same path as those of social media applications. The open application programming interface (API) technologies allow the IoT devices to become a member of social communities. For example, the building energy management system (BEMS) can be implemented and operated by collaborations of humans and a lot of sensors. It seems that the IoT sensors are a member of the social community to manage the building energy consumption. If IoT devices are open to invite new technologies, social IoT applications will be created, which is similar to those of social media applications.

Emergence of knowledge society

The creation and dissemination of knowledge is increasingly the key to success, and thus to sustainable economic and social development. Creative knowledge is a key factor in global competitiveness, which fuels new job creation and economic growth. The most important property of knowledge is now intellectual property. It is essential to growth and prosperity rather than traditional labour. Moreover, knowledge has been a driver of economic and social development as well as productivity of manufacturing industry. Knowledge innovation fundamentally means coming up with new ideas about how to do things better or faster.

By utilizing information and communication technologies, the emergence of the knowledge society is bringing about a fundamental reshaping of the existing industrial society. It introduces a transformation of global economy. The information and communication technologies are facilitating a new intensity in the application of knowledge to economic activity, to the extent that it has become the predominant factors in the creation of wealth.

To cope with the upcoming zeta-byte era toward knowledge society, the market potential of telecommunication and broadcast is gradually declining even though smartphones, TVs, and PCs are the major source of traffic [1]. The fastest growing traffic is coming from Internet of things/machine-to-machine (IoT/M2M) applications. The high traffic growth is due to more video applications combined with IoT/M2M applications such as e-health and self-driving cars. With the increasing usage of WiFi and long term evolution (LTE) technologies, video applications are becoming the largest portions of upstream traffic, which is mainly coming from user-created contents as the user has a role of content producer. The following are the tangible lists of sharing information and knowledge via the ICT infrastructure:

- Information of science and technologies;
- Bio and medical information;
- Energy, automobile related information;
- Nano, semiconductor, and component information;
- Education, culture, and art information;
- Public information of government;
- Society and life related information.

Social information infrastructure via ICTs

A large volume of data among human-to-human, human-to-machine, and machine-to-machine is delivered, shared, processed, and consumed through the ICT infrastructure. The concept of social information infrastructure is shown in Figure 7. To explain the left-hand side of this figure, more than seven billion people may connect to build up their own human relationships and communities through the ICT infrastructure. The traditional telecommunication services and the recent social networking services are connecting people. The right-hand side of the figure illustrates the concept of the cyber physical system consisting of building, transport, energy, water, manufacture, health, surveillance, and environment through the ICT infrastructure. All the physical entities are mapped to the corresponding objects in the cyber world through the ICT infrastructure. The actual behaviours and presence of the physical world are connected to the equivalent objects in the cyber world. Human intelligences accumulated by social communities are reflected on the objects in the cyber world. Therefore, the future social information infrastructure can consist of both the human platform among people and the platform for the cyber-physical system.

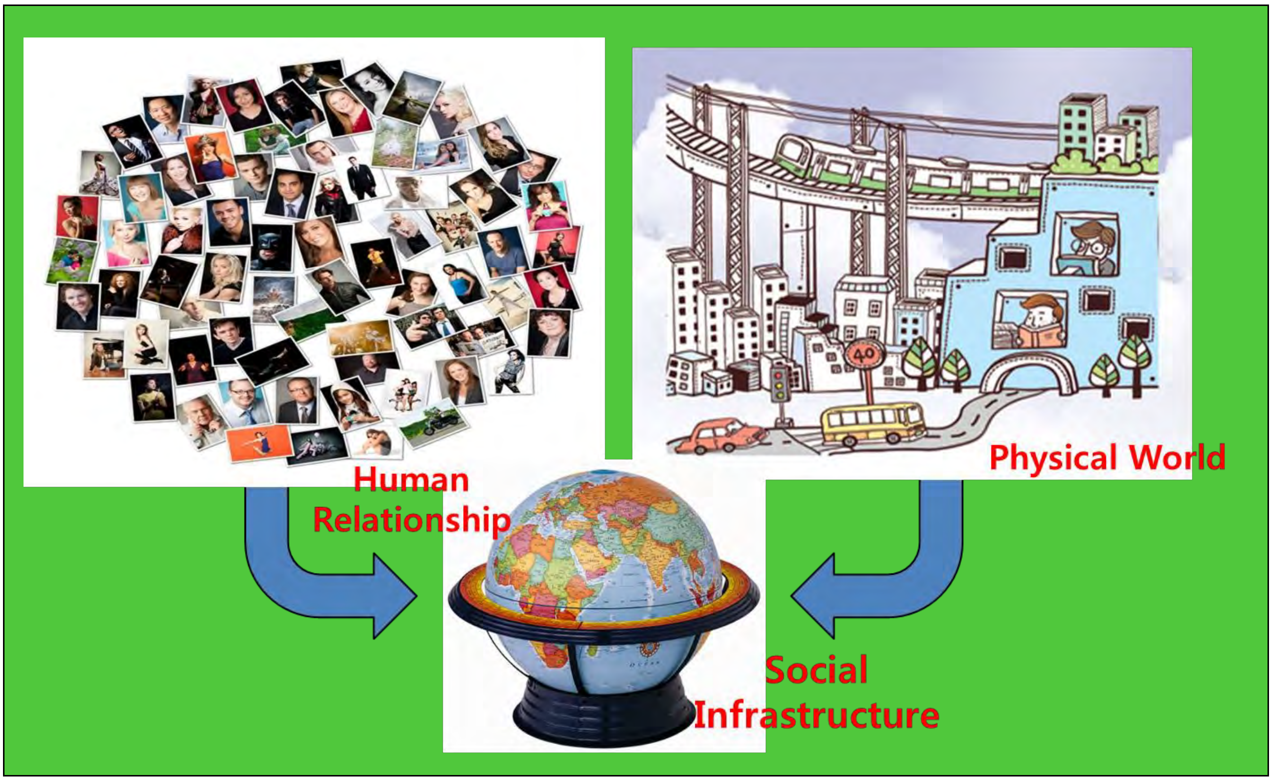


Figure 7 – Social information infrastructure via ICTs

Conceptual visions of future ICT infrastructure

With layering concepts, the future ICT world consists of the physical world and the cyber world as well as of the data world and knowledge world, as shown in Figure 8. The integration of the physical world and cyber world is done by ICT convergence which is interlinking the information and communication technology and other industrial technologies for energy, transportation, health, and public safety, etc. System information and physical operations are logged at software entities in the cyber world. The parameters of software entities in the cyber world are tuned with the corresponding parameters of the physical system, for example, for testing or manufacturing process. The software function in the cyber world has a mirror image of the real physical system which is able to continuously record and track the physical operation. Therefore, the integrated intelligent functions in the cyber world are applied to the physical world.

If the operation and maintenance of the cyber world are inconsistent with those of the physical world, there are some challenging issues to be solved by the creative innovation of the cyber physical system. For the design of the cyber physical system, the physical systems can be collaboratively and interdisciplinary implemented by using intelligent software engineering. The physical system should be robust and stable while there are the interruption of controllability and the failures of software functions. Also, the unexpected results and harmful failures of the physical system can be simulated by software engineering. For stable operations of the physical system, the proactive algorithms running in the cyber world can be applied to avoid unpredictable risks or deadlocks.

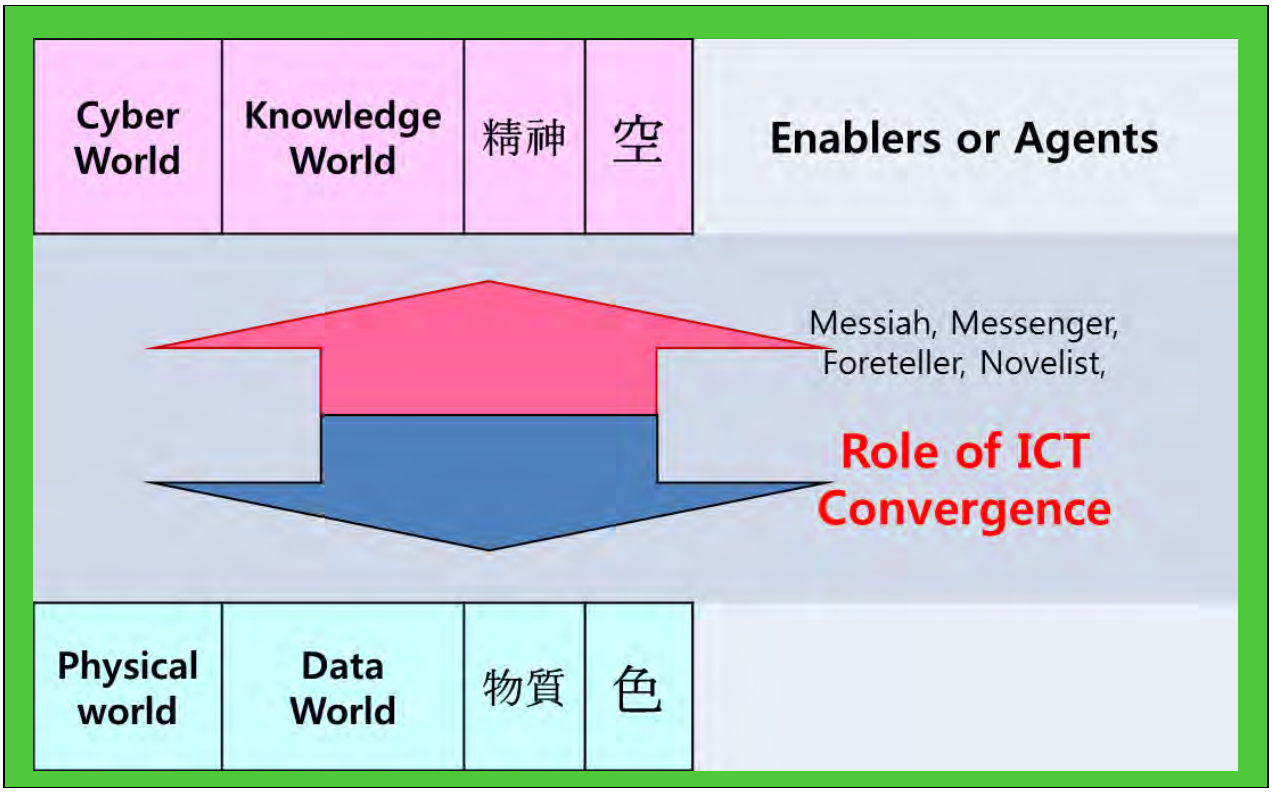


Figure 8 – ICT conceptual vision of future ICT infrastructure

Key trends of the future ICT eco-society

The key trends of the future ICT infrastructure are to build creative, trustworthy, and a knowledge eco-society. All people invent their own ideas for improvement of their life and business. If someone creates new ideas that wants to share with his/her friends, the communication channel should be secure and reliable. By accumulating the existing activities for a future knowledge society, the key trends are identified as "hyper connected society", "mobile native", "free economy", and "the third industrial revolution". The essence of the key trends for the future knowledge society is summarized as follows:

– "**Hyper connected society**" for coexistence, consensus, and sharing:
  - Technology breakthroughs by using smartphones and IoT/M2M technologies;
  - Information resonance effects of smart networking and social media;
  - New opportunities of explosion of digital information and big data analytics.

- "**Mobile native**" for global digital nomads:
  - Global citizenship/community and digital native/immigrants/nomad;
  - Smart seniors in an aging society;
  - Cultural convergence by utilizing information and communication technologies;
  - Accumulation of people's knowledge: expecting new democracy and virtual space for new agora world.
- "**Free economy**" on collaborative consumption:
  - Sharing culture and economy by utilizing social networking services;
  - Privacy collapse and new opportunity of statistics information from community interests.
- "**The third industrial revolution**" for sharing information (by Jeremy Rifkin [16]):
  - Energy Internet and industrial Internet, great escapes from telecommunication and broadcast business;
  - Global integration of online/offline markets and e-commerce;
  - Global reorganization of job/labour markets and human resources.

For the establishment of a creative, trustworthy, and knowledge eco-society, first the information and communication technology can help enormously increase the overall productivity of other industries such as energy, transportation, education, health, safety, and environment, etc., as shown in Figure 9. Second, the new paradigm toward the connected world will be open to realize communication among human-to-human, human-to-machine, and machine-to-machine. In addition, virtual reality technologies may be used to bridge between the physical world and the cyber world. Interdisciplinary activities among people are expected to search for new discoveries of knowledge and intelligence. The ICT infrastructure should be well structured to open new windows of discovery relying on human intelligence. It should also enable new innovations on education, energy, transportation, nano-, and bio-technologies, etc.

From the perspective of productivity, the information and communication technologies enable to improve the productivity of traditional industries. During the last ten years, the growth of the global economy is primarily due to utilizing ICTs. ICTs can provide significant benefits on convergence industries which are abbreviated by energy+ICT, health+ICT, and transport+ICT, etc. Until now, the lack of investments in the ICT infrastructure might have been the cause in the slow process of the economy. This is why ICT is an important enabler to drive the add-on values on productivity.

Second, from the perspective of communication, there is a wide range of ICT applications such as telephony and television as well as e-mail, etc. Recently, with the progress of IoT/M2M technologies, the human-to-machine and machine-to-machine communication are widely under development. Some software and devices help people record, store, process, retrieve, transfer, and receive information. To help public safety in metropolitan regions, some IoT devices enable new peer-to-peer services and location-based applications. Humans can communicate with sensors by abstraction or artefact of objects. Data visualization can help communication between humans and objects.

Third, from the perspective of new discovery based on human intelligence, ICTs can provide a more efficient and effective platform to explore new science and technology areas. In some specific areas, people find it difficult to learn a certain knowledge. By an optimum utilization of the computing and storage systems, people can get great help to find, compare, and analyse the facts and experimental results. A group of people among different communities can make a discussion and collect their opinions from various principles and theories. ICTs provide a collaborative platform for billions of people with unlimited storage and processing capacity, which can open new windows to discover knowledge for education, energy, transportation, nano- and bio-technology, etc. The complex system which has been almost impossible to handle by analytical and statistical methods of the existing science and technology can be solved, for example, to forecast the weather and analyse the human genome.

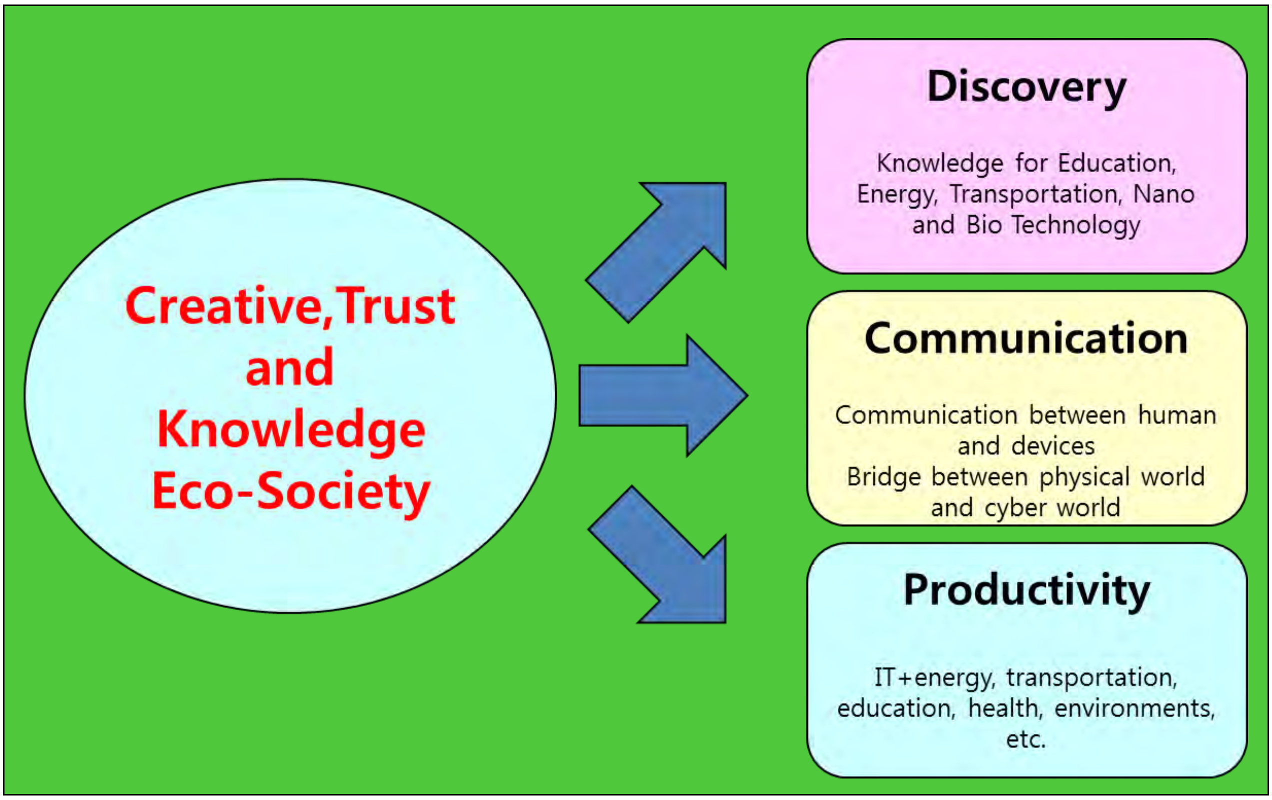

Creative,Trust and Knowledge Eco-Society
Discovery
Knowledge for Education, Energy, Transportation, Nano and Bio Technology
Communication
Communication between human and devices
Bridge between physical world and cyber world
Productivity
IT+energy, transportation, education, health, environments, etc.

Figure 9 – Key trends of future ICT eco-society

Value-added services of future ICT infrastructure

From a narrow perspective of ICTs, the expected market potentials of telecommunication and broadcast services are not so great even though 5G technology and ultra-high definition TV technology may appear in the market. The high speed and high quality of ICTs may be not significantly interesting since network performance is counting on the law of marginal utility. However, there are more productive, competitive, and innovative ICT markets if the value-added services and the discovery of new technology can be cultivated, as shown in Figure 10. The web- and app-services on cloud environments will be continuously upgraded and added to deliver new values. The wide variety of social media services can create a new life style and a new business model (we call this trend 2nd class of ICT industries). Finally, if future knowledge platforms are well organized to invoke collective intelligence and crowdsourcing among people, this will be very useful also for other industries such as education, energy, health, and transportation, etc., (we call this trend 3rd class of ICT industries). Therefore, new market volumes of future ICT services will be greater than those of traditional telecommunication and broadcast services.

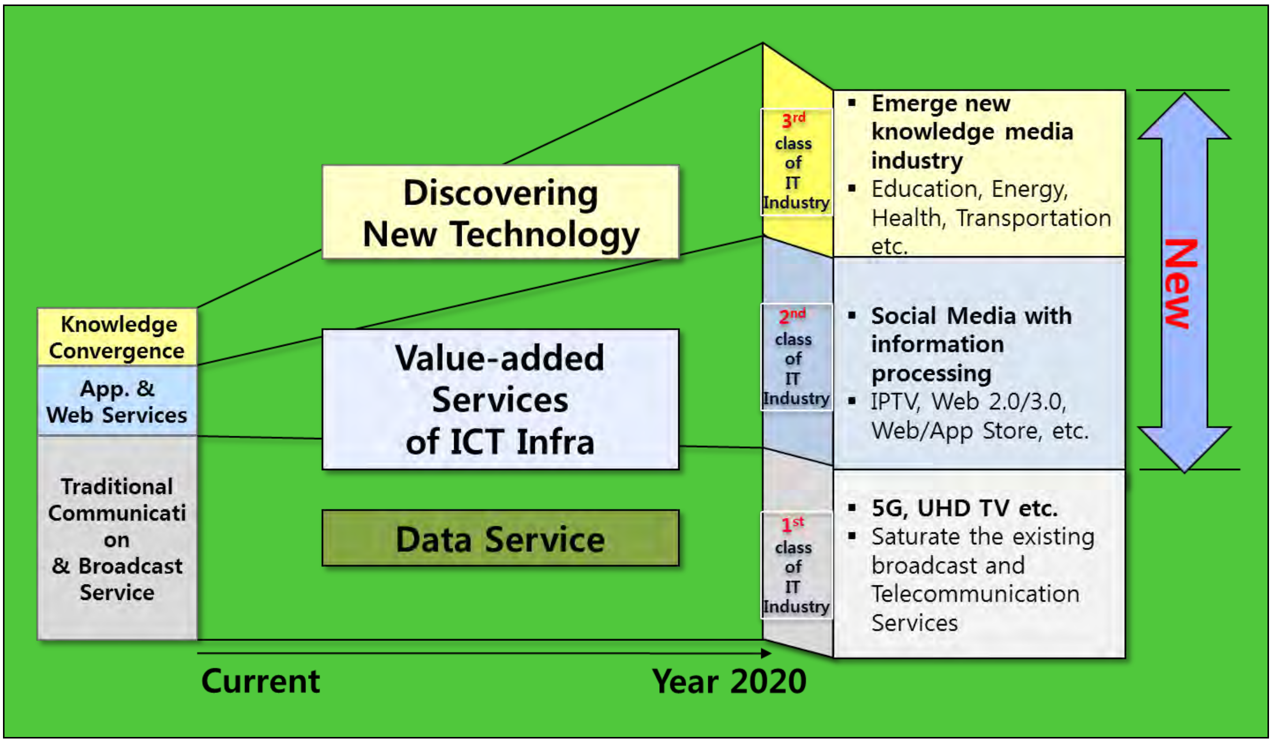

Knowledge Convergence
App. & Web Services
Traditional Communication & Broadcast Service
Discovering New Technology
Value-added Services of ICT Infra
Data Service
3rd class of IT Industry
2nd class of IT Industry
1st class of IT Industry
Emerge new knowledge media industry
Education, Energy, Health, Transportation etc.
Social Media with information processing
IPTV, Web 2.0/3.0, Web/App Store, etc.
5G, UHD TV etc.
Saturate the existing broadcast and Telecommunication Services
New
Current
Year 2020

Figure 10 – Value-added services of future ICT infrastructure

Emerging applications of future ICT infrastructure

If the ICT infrastructure is well designed and deployed, many applications will be accelerated. The new possibility will appear in the outstanding application areas in the environment, ageing, knowledge media, and information prediction, as shown in Figure 11. First, to cope with climate change, CO_2 emissions should be reduced by a global consensus. ICTs are a source of as much carbon dioxide in the atmosphere, while at the same time, they provide the solutions that save energy both in the industry and in-house applications. The energy-efficient data centres and software virtualization for dynamic capacity management are essential for green ICTs. When the green ICT is combined with relevant communication solutions, such as video conferences, this reduces carbon emissions by avoiding unnecessary travelling. The benefits of green ICTs can reduce energy consumption by installing more efficient hardware systems.

For better ageing and e-health, the information and communication technologies can improve the quality of life of the elderly and help people remain healthy. From e-health to intelligent care system, ICT promotes the well-being of the aged in their whole lifetime.

The multimedia applications and web-based contents are used for future education including training, presentation, and exercise, etc. The computer-based training and three dimensional simulation programs can help students get indirect experiences. The collective platform for teaching and learning is needed to support the creation of ideas among students. Teachers can be encouraged to use new education platforms equipped with multimedia sharing tools.

As a part of big data analytics, information prediction will be one of the emerging markets. By collecting statistics and analysing user behaviours, some events can be predictive to happen with certain probability. With risks of uncertainty, the probability of an event is closer than the average before. With the progress of IoT/M2M technologies, information prediction will be a steadily emerging market to predict natural disasters, protect public safety, and reduce traffic accidents and air pollution.

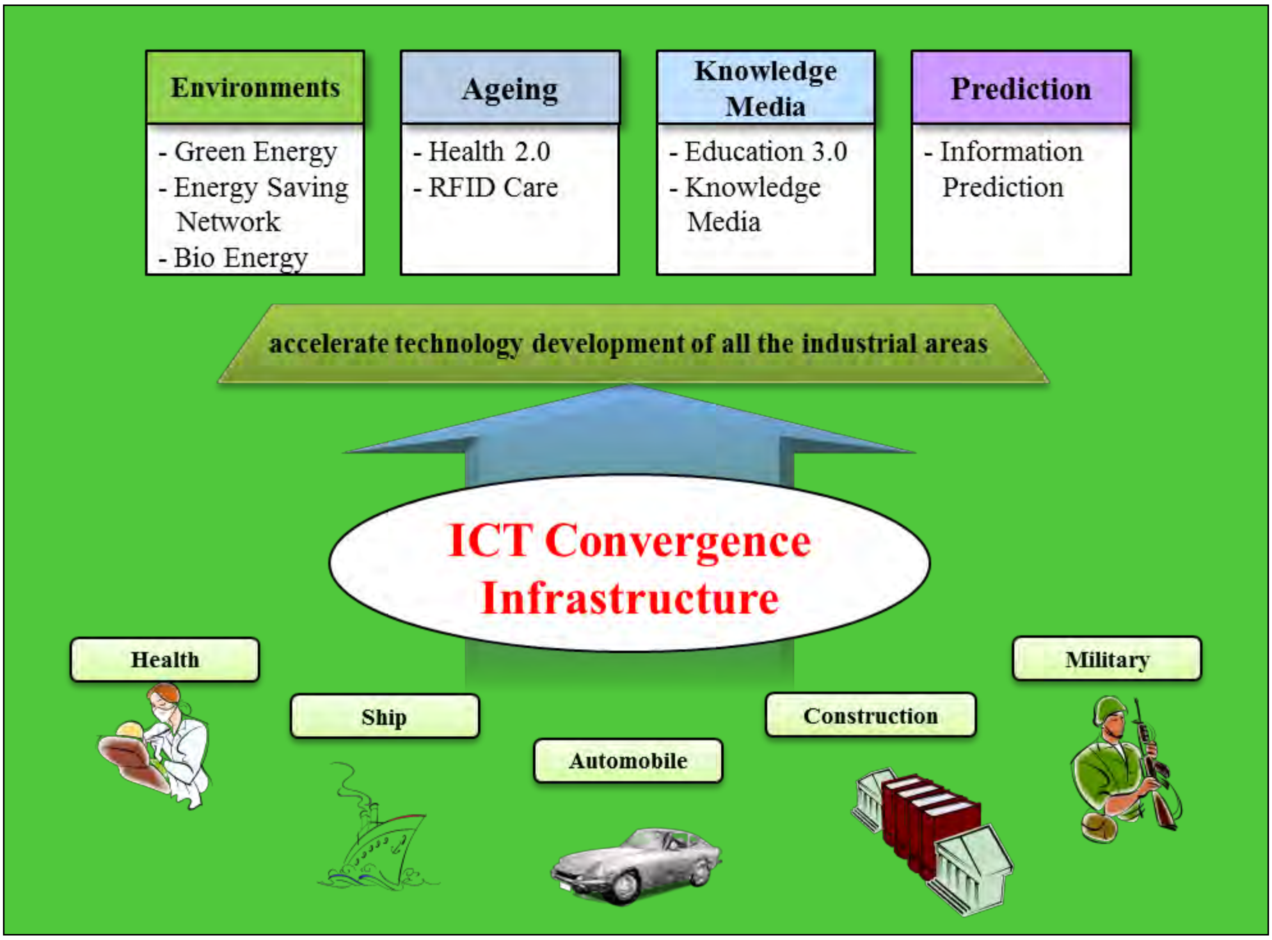


Figure 11 – Emerging applications of future ICT infrastructure

Convergence markets with energy, transportation, and healthcare, etc.

When information and communication technologies are applied to other industries like energy, transportation, health, education, and public safety, new behaviours and benefits will appear for individuals and communities in their own work environments. People working in other industries may have a chance to get new practices and experiences by using ICT and social media. When IoT/M2M devices plug-in at the network, these physical entities will become a partner of people in the same business domain, and they will be ready to connect people, activate systems, and process tasks.

For example, when the smart grid adopts social media technologies, overall energy consumptions are collaboratively controlled with the help of communities by being aware of energy generation and delivery status. To reflect the status of power generations including solar cells and wind turbines, the collaborative behaviours among people can make a shift of energy consumption to reduce peak energy consumption. The social network can measure the status of energy generation and consumption in real time. It acts properly to reduce peak energy consumption with the help of social communities.

For intelligent transportation management in a smart city, traffic signals at the crossroad are adaptively controlled according to the numbers of vehicles and driving behaviours of people. People may call a taxi or ride a bus at the nearest location with the help of social media. The new functionality of social media, combined with IoT/M2M technologies, makes transport easier and safer to people. To allow for seamless usage and on-time availability of transport means, an ideal solution may be a mix of individual vehicles, vehicle sharing, and railway.

For health applications with social media, smart monitoring equipment reports health conditions of patients and individuals periodically. The healthcare systems are equipped with the identification systems for tracking patients and individuals. The social media platform can gather health data of individuals and report to doctors. When a medical emergency happens, the social network can help call the 911 centre, drive an ambulance, assist patients, advice doctors, and notify the hospital simultaneously.

Strategic trends for deployment of future ICT infrastructure

In order to deploy future ICT infrastructure successfully, there are three strategic issues as shown in Figure 12. First, the well-organized wireline/wireless network will be a good basis to construct the future ICT infrastructure. From traffic demands and application types, user equipment and sensor devices will be plug-in the network mostly by using 5G or WiFi wireless technologies. At the edge and core network, optical systems with more than 100 Gigabits/s per wavelength will be available in the near future. The passive optical network system of more than 10 Gigabits/s will replace the existing copper cable and unshielded twisted pairs at the access network. Second, from the viewpoint of information sharing platform, all the data created by users and collected by machines are efficiently and effectively stored at certain servers. From this platform, the public information for human life and business may be easily accessed within a few seconds. Moreover, some of the government-owned information may be freely and easily obtained. The design guideline of the information sharing platform is how to access data with acceptable scalability and confidentiality. The cloud computing platform will be a good candidate to be a future information sharing platform.

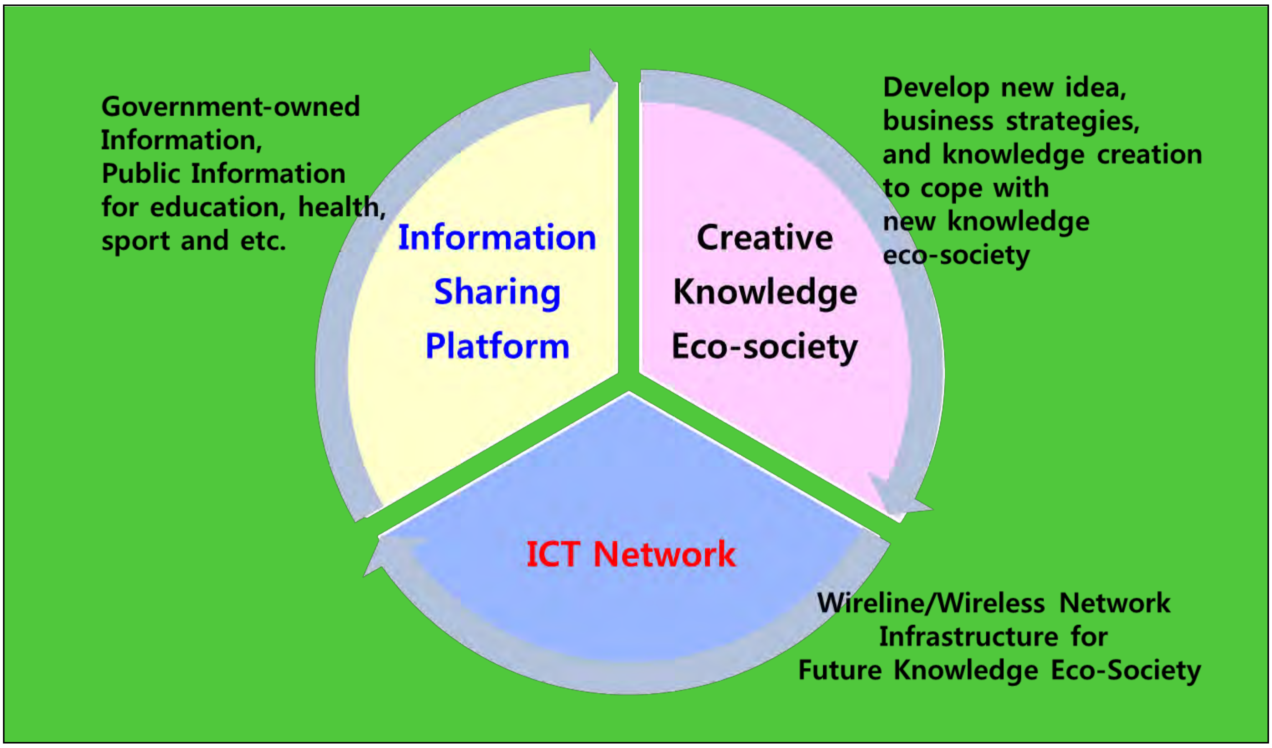

Government-owned Information,
Public Information for education, health, sport and etc.
Information Sharing Platform
Creative Knowledge Eco-society
Develop new idea, business strategies, and knowledge creation to cope with new knowledge eco-society
ICT Network
Wireline/Wireless Network Infrastructure for Future Knowledge Eco-Society

Figure 12 – Strategic trends for future ICT infrastructure

Third, from the viewpoint of knowledge creation, the most outstanding issues are how to support a creative knowledge eco-society with innovative ideas. Here, it is noted that all the relevant information and knowledge are created, shared, processed, and utilized originally by human beings. If some people raise questions, interests, and/or curiosity, they can share the relevant information and knowledge easily at that instance. However, unfortunately, the current cloud computing system is mainly designed only for efficiency of storage and processing. This means that the cloud computing platform will be evolved to help people's curiosity. In addition, the digital data format which is used to display video screening and deliver audio/sound/voice signals should be evolutionally tuned with the human organ and human perception mechanism. Until now, the data structure and formats are defined and classified according to the spectrum of long-lived knowledge silo as in education, transportation, energy, health, science, and engineering, etc. New integrated data formats based on semantic ontology may be challenging, which are easily interpreted and perceived by users.

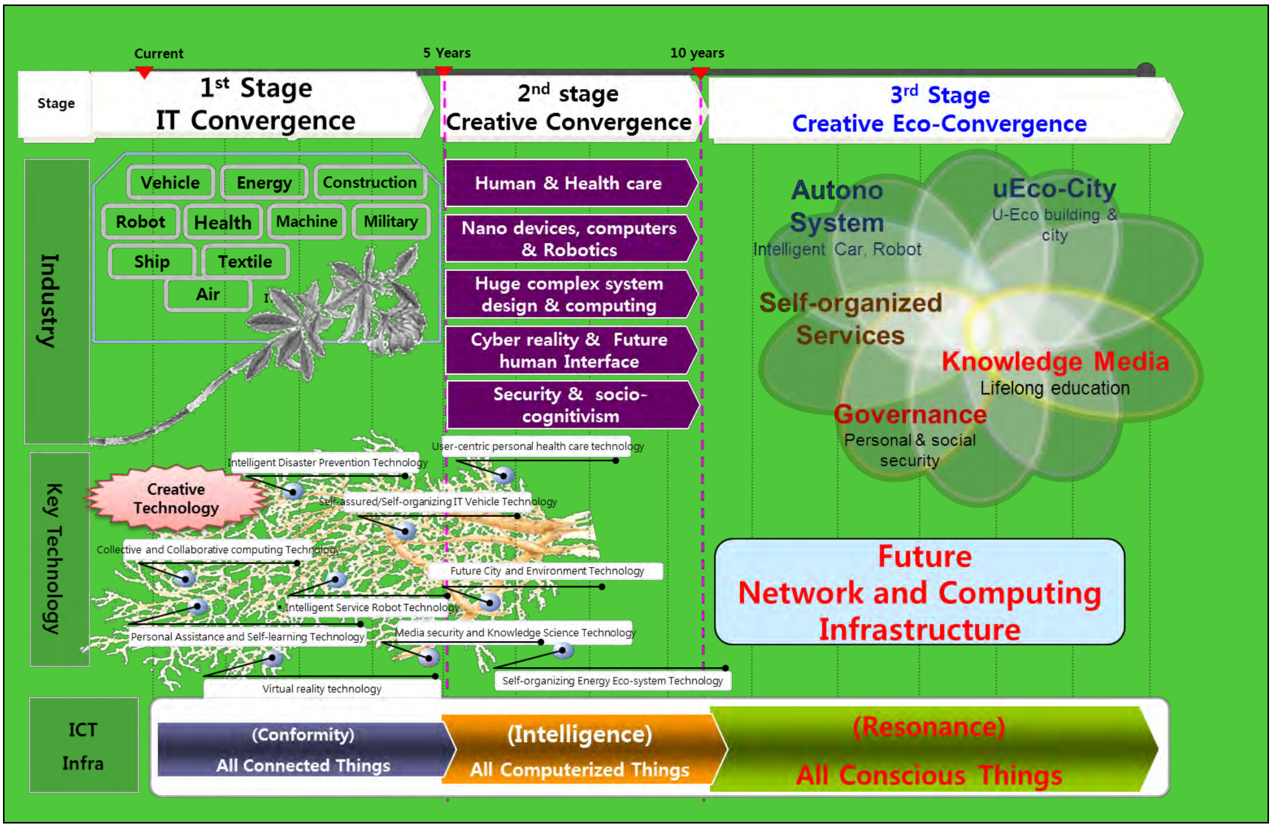

Current
5 Years
10 years
Stage
1st Stage
IT Convergence
2nd stage
Creative Convergence
3rd Stage
Creative Eco-Convergence
Industry
Vehicle
Energy
Construction
Robot
Health
Machine
Military
Ship
Textile
Air
Human & Health care
Nano devices, computers & Robotics
Huge complex system design & computing
Cyber reality & Future human Interface
Security & socio-cognitivism
Autono System
Intelligent Car, Robot
uEco-City
U-Eco building & city
Self-organized Services
Knowledge Media
Lifelong education
Governance
Personal & social security
Key Technology
Creative Technology
Intelligent Disaster Prevention Technology
User-centric personal health care technology
Self-assured/Self-organizing IT Vehicle Technology
Collective and Collaborative computing Technology
Future City and Environment Technology
Intelligent Service Robot Technology
Personal Assistance and Self-learning Technology
Media security and Knowledge Science Technology
Virtual reality technology
Self-organizing Energy Eco-system Technology
Future Network and Computing Infrastructure
ICT Infra
(Conformity)
All Connected Things
(Intelligence)
All Computerized Things
(Resonance)
All Conscious Things

Figure 13 – Step-wise evolution toward future ICT infrastructure

Figure 13 shows the overall roadmap of evolution toward the future convergence era relying on ICT infrastructure. In the first stage, the evolution of traditional industries such as energy, health, robots, machines, and vehicles simply utilize the data delivery capability of the existing network and computing infrastructure. The new technologies like IoT/M2M are applied to increase the productivity of traditional industries. The collaborative and interdisciplinary methods among various fields of knowledge are triggered to open a new convergence era in the second stage of evolution. Many key technologies are integrated with a certain level of intelligence. In the third stage of evolution, a new industrial structure is organized and constituted toward a future knowledge convergence society, which is quite different from the existing classification of industries. Conceptually, the future industrial structure toward a new creative eco-convergence era may be classified into five types: autono system, uEco-city, self-organized services, knowledge media, and governance:

1 **Autono system**: It is realized that autonomy is applied to all the eco-systems as well as individual systems like intelligent robots. It is used to refer to the self-governing system.

2 **uEco-city**: The uEco-city means the evolution of an eco-friendly ubiquitous city. The current metropolitan environments may be transformed to eco-cities in which the information and communication technologies enhance quality and performance of urban life and reduce costs and resource consumptions on transport, energy, healthcare, water, and waste.

3 **Self-organized services**: The self-organized services mean that all the operations of the physical system and software platform have the characteristics of a self-organized and self-sufficient systems. The software running at a specific system has a capability of self-organization and self-correction in cases of faults and abnormal situations. In the cloud computing environments, a self-organized service is crucial to discover and consume the service autonomously. Precise and robust service discovery algorithms are desirable.

4 **Knowledge media**: Future lifelong education needs a self-motivated pursuit of knowledge for either personal or professional reasons. Knowledge media is incorporated over the existing education and media with cognitive and learning sciences. Knowledge media is about the processes of generating, understanding and sharing knowledge using several different media.

5 **Governance**: Toward a future safe and sustainable knowledge society, governance is essential to reduce global risks and increase human sustainability. New forms of governance are inevitable to continue economic growth and regulate markets and technologies.

The future network and computing infrastructure will provide the fundamental facilities and environments to realize the concepts of all conscious things. Key concepts toward a new knowledge society are coming from understandings on how information and knowledge/intelligence via the ICT infrastructure are used to change human life and business behaviours.

8 ICT standardization for future knowledge society

Principles for knowledge eco-society

Knowledge society is based on the needs of knowledge distribution, access to information and capability to transfer information into knowledge. Knowledge distribution is one of the key requirements of the knowledge society. All the members have to understand the role of the knowledge society in the future development of human society. A knowledge society promotes human rights and offers equal, inclusive, universal access to all knowledge creation. There are basic principles that are essential for the development of knowledge society:

– (**Equal access and open interface**): A public and an open accessible knowledge has uncountable values in various areas of science and technology as well as in the business domain. It provides an opportunity for all to access local and global information in a more equitable manner. From the viewpoint of standardization, "open" means that the public information including ITU-T documents is available and is within the reach of the public (online), with low to no barriers for its reuse and consumption. Anonymous access to knowledge must be allowed for the public. Public data should not be hidden behind "walled gardens". Therefore, the knowledge society provides open and equal access, and universal access to ITU-T documents though better networking.

– (**Trust**): Trust including security and privacy is a prerequisite for the development of the future knowledge society. Published documents should be digitally signed or should include publication/creation date, authenticity, and integrity. Digital signatures help the public validate the source of the data they find so that they can trust that the data has not been modified since it was published. Trust needs to share the environmental knowledge for sustainable development to reduce all kinds of risks. The certification or trust to ensure user access of reliable and relevant ITU-T documents is inevitable.

– (**No privileges and universal access**): The benefits of the information and communication technologies are evenly distributed and widely open to a new digital opportunity to realize the future knowledge society. All knowledge extracted by data is made available to the public since knowledge is an invisible public good. Public data including ITU-T documents is not subject to valid privacy, security or privilege limitations. Public data is not subject to any copyright, patent, trademark or trade secret regulation. Reasonable privacy, security and privilege restrictions may be allowed with certain consensus or agreement. Therefore, the knowledge society provides a collaborative and an equal opportunity of knowledge in the public domain. Some harmony may be needed between the private sector and the public/social/government organizations to achieve a future knowledge society.

– (**Lifelong learning**): Pursuit of knowledge for either personal or professional reasons is ongoing, voluntary, and self-motivated. Lifelong learning recognizes that learning is not confined to childhood or to a classroom but that it takes place throughout life and in a range of situations. Learning can no longer be divided into a place and time to acquire knowledge (school) and a place and time to apply the knowledge acquired (workplace). Learning can take place on an ongoing basis from our daily interactions with others. There are several forms of learning: formal learning, informal learning, or self-directed learning.

- (**Diversity**): There are cultural and linguistic diversities that play a role in the supply of creative work. The promotion, affirmation and preservation of diverse cultural identities and languages will further enrich the future knowledge society.
- (**Social connectivity**): Everyone has the freedom of opinion and expression without interference. Communication is a fundamental social process. The information and communication technology can accelerate the social nature of individuals and communities.
- (**Linked chain**): Data consists of a set of data records linked together and organized by links or references. The linked data structure with linked lists or search trees is very useful to retrieve and identify their properties. Metadata includes the descriptive or related information of links. With the help of links and metadata information, the relationships among data, information, and knowledge will be defined.
- (**Technology**): The development of ICT technologies ensures free and common benefits of knowledge. It encourages innovation with collaboration, and research and developments with better scientific knowledge sharing. It is important to promote thinking about technical and legal feasibilities of knowledge certification and standards by ensuring users' access to reliable and relevant contents. In order to promote the spread and sharing of knowledge by developing ICT technologies (e.g. tools, freeware, common hardware, etc.), the step-wise plans of standardization with priority are essential.

Types of standards and open standards

There is a distinction between formal, *de facto*, and de jure standards. Formal standards are elaborated by standardization bodies. Both ITU and ISO/IEC are formal standardization bodies according to such a classification. *De facto* standards are technologies standardized through market mechanisms, and de jure standards are imposed by law. In addition, there are three levels of standards: reference, minimum quality and compatibility/interoperability standards. The compatibility/interoperability standards ensure that one component may successfully be incorporated into a larger system given an adherence to the interface specification of the standard.

De facto standards are often developed by industrial consortia or vendors. Examples of such standards are the World Wide Web (W3) consortium currently developing a new version of the HTML format for the web. The W3 consortium is independent of, but closely linked to, the standardization process of IETF. Some of the consortia operate independently of the international standardization bodies. Therefore, there may be some conflicts in governmental regulations or industry-specific requirements caused by fundamental climatic, geographical, technological, or infrastructural factors, or the stringency of safety requirements that a given standard authority considers appropriate.

An open standard is publicly available and has various rights to use associated with it, and may also has various properties of how it was designed (e.g. open process). The different meanings of openness are associated with their usage including the openness of the resulting specification, the openness of the drafting process, and the ownership of rights in the standard. If some standards are sometimes proprietary and only available under restrictive contract terms from the organization that owns the copyright on the specification, such specifications are not considered to be fully open; therefore, they cannot be called open standards. They may satisfy "reasonable and non-discriminatory" patent licensing fee requirements in order to be accepted by ITU-T standards.

Conceptual framework for standardization of knowledge information infrastructure

Standardization is a simple and straightforward process with a necessary basis for far-reaching technical consensus. The development of the ICT infrastructure including the standards should be recognized as a highly complex socio-technical negotiation process. The understanding of how to build the ICT infrastructure with social, economic, political and technical considerations is interacted with the overall design of the knowledge society which classifies and conceptualizes to grasp the role of standards in the development of future information infrastructures.

Before making a clear consensus of the future information infrastructure, discussion among people may be used to make conceptual distinctions and organize ideas. The conceptual framework identifies their priority and chooses initial action items. The conceptual framework is abstract representations, connected to the research that directs the collection and analysis of data. By collecting data and assessing the evidence, formal hypotheses take place with possible explanations. Finally, the conceptual model of the ICT infrastructure for the knowledge society is characterized without regard to their underlying assumptions and technologies. The abstract model may partition a set of functions or layers with certain classifications of the knowledge information infrastructure. An open, voluntary, and consensus-based standardization process will be critical to build the ICT infrastructure toward a future knowledge society.

When the ICT infrastructure may extend to other convergence industries, it may provide computing, storage, and networking resources for energy, transport, health, education, and environments, etc. Since people relating to other industries have their own data formats to share and distribute their idea, the data sharing platform is very important to access data with confidence. For the future ICT industry, the collective intelligence framework is essential to accumulate data from various sensors, networking systems, and cloud servers, etc. The location and presence information of the IoT systems are used to extract the context-aware information from raw data. However, there are some limitations in these types of data. All the data sources have their own output format by given types. In the current Internet and web, for example, only URL/URI/uniform source name (URN) are available to identify data types for certain Internet protocol (IP) domains of the Internet. There are only available for the telephone numbering and addressing structure for fixed and mobile telephony. Toward future convergence services, the data types including identification, numbering, and addressing should be extended to support IoT/M2M devices and equipment of other convergence industries.

Moreover, data sources are mainly classified into private data and public data. For private data, malicious threats may attack to obtain user sensitive information for identification, detection, and tracking, etc. The malicious activity may be based on IP addresses, numbering, and URLs. Some data may be discovered through an incident monitoring process which is shared with private communities. Therefore, the trust framework for the future knowledge society should be built to observe data from any source and protect against malicious activities.

Technically, in order to get a common understanding of the future knowledge society, the following outstanding issues for standardization can be investigated as follows:

– **How to connect the forms of knowledge in relationship to data**:
  - Writing books and documents is not enough. The recursive mechanism to accumulate individual knowledge and opinions including tacit knowledge are needed to create new forms of knowledge.

– **Metadata is like a glue to connecting data, information, and knowledge**:
  - Various types of metadata may be defined when data is created, delivered, processed, shared, and consumed by users and communities. It may be called source metadata, content metadata, service metadata, user metadata, and application-specific context metadata, etc.
  - Metadata may be parsed to extract the useful meanings of data, a capability which is part of the intelligent processing of data.
  - Metadata may be created after pre-processing or post-processing of data with related context-aware information such as condition, situation, and environment.
  - The discrimination between information and knowledge from raw data is the understanding and interpretation of their contents, which may be described as metadata.

– **New forms of development, acquisition, and spread of knowledge**:
  - The new tools to create, collect, accumulate, share and distribute data, information, and knowledge are needed to invent new forms of knowledge. This may evolve from social media with the progress of user interface and human perception technologies.

- **New web as a useful tool for knowledge society**:
  - The existing web technology based on HTML has some limitations to help convergence service environments including IoT/M2M applications. New markup languages to communicate and share data, information, and knowledge may be needed.
  - The concepts of the web application programming interface (API) for binding and sharing contents/documents/files with their corresponding software may be enhanced. Also, new sharing and communication mechanisms between human-to-machine and machine-to-machine are needed to support IoT/M2M applications in the environment of the web services and web applications.

Pre-standardization approaches toward knowledge information infrastructure

In spite the fact that there are many definitions on knowledge and knowledge society, the two terms are still ambiguous. From the perspective of information and communication technologies, the knowledge information infrastructure is difficult to realize as the famous philosopher Plato defined knowledge as: "justified true belief". Designing an accurate and efficient knowledge and trust model are a key research challenge. Various types of knowledge and trust models may be suggested as a pre-standardization process. The collective and crowdsourcing behaviours among people are supposed to collect knowledge from human reasoning and will be a basis to develop the relevant standards. The process of developing a standard is based on a fair and equitable way that typically ensures the high quality output and market relevance.

Standardization can be achieved on many different levels expanding from a uniform and integrated system over similar and harmonized process flows. As a result, harmonization is a preliminary stage of standardization which allows the exchange of information between different organizations without additional training. The right level of standardization varies depending on the individual member's conditions, working structure, management maturity, and the objectives of technical standardization. The formal working methods of ITU-T standardization may be not efficient if there are many views, opinions, and technical solutions. Brainstorming of ideas may be needed to get rough and common consensus.

In addition, the other standards development organizations (SDOs) may have their own working methods to produce documents, reports, and implementation agreements. The harmony between the working methods of formal standard bodies and the mission-oriented working methods of other SDOs may be needed. If the action items are well specified and the working methods including collaborations with other SDOs are clearly agreed, the formal working process of ITU-T can be initiated. Therefore, before standardization in ITU-T, a common understanding and consensus for knowledge are needed.

The following items are recommended for pre-standardization activities in ITU-T, which may be intended to initiate a joint research or coordination group for collaboration with other SDOs:

- Concept and basic principles of data, information, and knowledge in terms of the ICT world:
  - Review the concepts and understanding of data, information, and knowledge;
  - Identify the definition, property, and functional capability of data, information, and knowledge;
  - Analyse the relationship and the linked mechanism among data, information, and knowledge;
  - Investigate the use cases and examples of data, information, and knowledge.
- Data classification, types, and formats in terms of the ICT world:
  - Review the existing data types and formats both in digital and analogue forms, which are available in the real world;
  - Investigate the definition, property, and classification of data types and formats;
  - Investigate the data description methods according to common and specific applications;
  - Identify the definition, property, and description methods of metadata;
  - Investigate the relationship between data and metadata;
  - Investigate the linked types and formats of data (e.g. linked data and linked open data);

  - Investigate the data formats for specific applications (e.g. web application, file, database, 2D/3D geographical information, anatomy information of human body, composition of texts, image, symbol, and audio/visual information, etc.);
  - Investigate description format and processing methods of data, information, and knowledge (e.g. pre-processing and post-processing of data with the help of metadata).

– Functional architecture of knowledge information infrastructure:

  - Review the existing ICT architecture to handle data, information, and knowledge;
  - Investigate the service concepts and principles of the knowledge information infrastructure;
  - Investigate the requirements and functional architecture of the knowledge information infrastructure;
  - Identify the use cases and application models of the knowledge information infrastructure;
  - Investigate the step-wise deployment scenarios of the knowledge information infrastructure.

– Social media services and technologies for the knowledge information infrastructure:

  - Review the existing social media services and technologies;
  - Investigate service concepts and principles of social media toward the knowledge society;
  - Investigate the definition, requirements, and functional architecture of social media for the knowledge information infrastructure;
  - Investigate the web technologies and web services as a part of social media;
  - Investigate how to integrate web services and application software for the knowledge information infrastructure;
  - Investigate the step-wise deployment scenario and roadmap of social media.

– Trust provisioning for knowledge information infrastructure:

  - Review the existing security and privacy solutions;
  - Investigate service concepts and principles for trust provisioning;
  - Investigate the requirements and functional architecture for trust provisioning;
  - Investigate the relationship between trust, security, and privacy;
  - Investigate the step-wise scenarios of trust provisioning for knowledge information infrastructure.

Recursive standardization process for knowledge information infrastructure

In summary, Figure 14 may propose the conceptual model for a new standardization process toward the knowledge information infrastructure. In order to configure a conceptual framework of the knowledge information infrastructure, three key issues are well identified and analysed: knowledge definition, social media and the web, and trust provisioning. In the definition of knowledge, the basic concepts of data, information, and knowledge are specified. The data model and format including metadata are also critical to make progress. Standardization will take place with a common understanding and a certain consensus of knowledge, social media, and trust provisioning. However, the recursive process of standardization may be applicable to reflect some feedbacks from human understanding and the related markets after publishing standard documents, since knowledge, in nature, has a recursive form of human perception and intelligence.

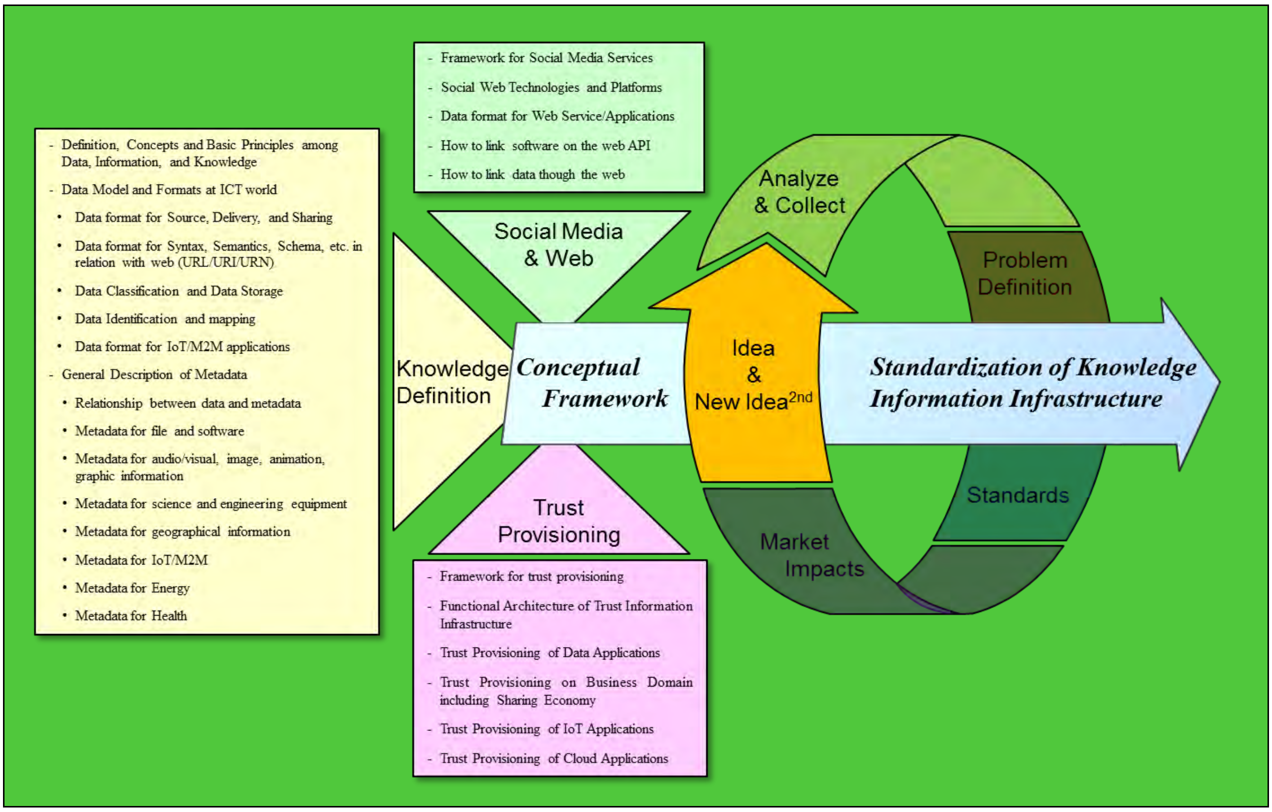

- Definition, Concepts and Basic Principles among Data, Information, and Knowledge
- Data Model and Formats at ICT world
• Data format for Source, Delivery, and Sharing
• Data format for Syntax, Semantics, Schema, etc. in relation with web (URL/URI/URN)
• Data Classification and Data Storage
• Data Identification and mapping
• Data format for IoT/M2M applications
- General Description of Metadata
• Relationship between data and metadata
• Metadata for file and software
• Metadata for audio/visual, image, animation, graphic information
• Metadata for science and engineering equipment
• Metadata for geographical information
• Metadata for IoT/M2M
• Metadata for Energy
• Metadata for Health
- Framework for Social Media Services
- Social Web Technologies and Platforms
- Data format for Web Service/Applications
- How to link software on the web API
- How to link data though the web
Social Media & Web
Knowledge Definition
Conceptual Framework
Trust Provisioning
- Framework for trust provisioning
- Functional Architecture of Trust Information Infrastructure
- Trust Provisioning of Data Applications
- Trust Provisioning on Business Domain including Sharing Economy
- Trust Provisioning of IoT Applications
- Trust Provisioning of Cloud Applications
Analyze & Collect
Problem Definition
Idea & New Idea2nd
Standardization of Knowledge Information Infrastructure
Standards
Market Impacts

Figure 14 – Recursive standardization process for knowledge information infrastructure

Collaborations with outside ITU-T

For acceleration and collaboration with outside of ITU-T, the following new working methods for the knowledge information infrastructure are recommended:

– Harmony between the public sector (ITU-T) and the private sector (implementation and market deployment):
  - (Public) Open, common, mutual benefits for all mankind;
  - (Private) maximize the revenues and help the public sectors;
  - Create new value-added markets without any harm and unhappiness;
  - Protect the negative effects of new technologies and the new ecosystem.

– Collaborations with academia for new ideas and technical breakthroughs:
  - Pre-standard collaborative processes are essential such as forums, workshops, and hackathon events of idea collection, etc.
  - Build open common collaborative platform and interoperability tests among people and communities;
  - Accumulate and share documents, opinions, and tacit know-hows, etc.

– Recursive standardization process with collective intelligence and crowdsourcing:
  - Idea → analyse, collect → problem definition → standards → market impacts → new ideas.

– Review the technical classifications of the current ITU-T study groups:
  - Functional decompositions (including pros and cons);
  - Identify the changing or evolving value-chains of technology and markets;
  - Establish a task force for special missions.

9 Conclusions

The year 2015 was ITU's 150th anniversary starting from the first international Telegraph Convention and the creation of the International Telecommunication Union. During the last 150 years, the information and communication technology (ICT) is one of the key drivers of innovation and technological breakthroughs in the world. Recently, the surprising news is that the penetration ratio of Internet access in the world was more than 40 % in 2014. Moreover, the number of mobile subscribers has already exceeded more than 3.6 billion in 2014. To cope with the future knowledge information infrastructure, this Technical Paper will be summarized as follows:

– Knowledge society will be realized by the developments of information and communication technologies:
  - Information and communication technology is a key enabler to open a future knowledge society since knowledge society is a kind of artificial world created by human minds.

– Online connectivity introduces new cultural experiences of human life and business:
  - Online connectivity has changed the way in which many people think and allows them to take advantage of the "political, social, economic, educational, and career opportunities";
  - Reflecting on human history, a totally new ICT culture relying on massive connectivity between human-to-human and human-to-machine may take place.

– New habits of human life and business via smartphones and social media:
  - Smartphones play the role of the personal assistant or guidance to help schedule meetings, ticket reservations, and information search, etc.
  - Social media may create a new window of cyber industry and open new social markets.

– Accumulation of human intelligence including tacit know-hows:
  - With the help of data and knowledge engineering, all human intelligence and experiences will be accumulated and shared with others;
  - Since all the experiences and experimental results are collectively and interdisciplinary accumulated, problems of a complex nature like climate change and human genome may be solved.

– New knowledge products and new social media markets relying on human intelligence:
  - Simulator or virtual space to experience the real physical world;
  - Virtual reality for practices and new experiences of tacit knowledge;
  - New markets for the cyber physical system by combining with the IoT/M2M technologies.

– ITU-T has a responsibility to get a consensus for the knowledge information infrastructure:
  - ITU may have a leadership role to introduce the future knowledge society by getting a global consensus for the future ICT infrastructure;
  - Standards for future knowledge-aware industries are critical to realize a knowledge eco-society.

– On the other hand, the future knowledge society should be a safe and sustainable society:
  - It encourages the positive effects of online connectivity and social media.
  - It protects user privacy and unexpected dangers to minimize the unexpected risks.
  - It maximizes human survivability in the future.

Finally, ITU-T may get a chance to lead the future knowledge society in terms of standardization. As a top level of formal standards body, ITU-T may try to initiate new working methods for the standardization of the future knowledge information infrastructure. In addition, ITU-T may have a leadership role to collaborate with the private sectors and academia which are outside of ITU-T. The pre-standardization and conceptual framework activities may be encouraged with collective intelligence and crowdsourcing.

11 References and bibliography

[1] Cisco® Visual Networking Index™ Global Forecast and Service Adoption for 2013 to 2018.

[2] http://www.techrepublic.com/article/ibm-watson-the-inside-story-of-how-the-jeopardy-winning-supercomputer-was-born-and-what-it-wants-to-do-next/, 2015 CBS Interactive.

[3] Drucker, Peter (1957), Landmarks of Tomorrow, Harper & Row, New York, ISBN 978-1-56000-622-0.

[4] Van Doren, Charles (1991), A History of Knowledge: Past, Present, and Future, Ballantine Book, ISBN: 978-0-345-37316-8.

[5] Smith, Adam (1776), An Inquiry into the Nature and Causes of the Wealth of Nations, (1 ed.), W. Strahan, London.

[6] http://www.slideshare.net/SD_Paul/science-and-technology-capacity-and-the-knowledge-society, LinkedIn Corporation © 2015.

[7] https://en.wikipedia.org/wiki/Knowledge_value, last modified on 5 November 2015.

[8] Firestone, Harvey (1868-1938), Thoughts on Wisdom, Forbes (1997) p. 108.

[9] http://www.businessdictionary.com/definition/knowledge.html, 2015 WebFinance, Inc.

[10] Gardner, Howard (1983), Frames of Mind: The Theory of Multiple Intelligences.

[11] Goleman, Daniel (1998), What Makes a Leader? Harvard Business Review.

[12] Coleman, Andrew (2008), A Dictionary of Psychology (3rd), Oxford University Press, ISBN 9780199534067.

[13] Drucker, Peter (1969), The Age of Discontinuity, Harper & Row, New York, ISBN 978-1-56000-618-3.

[14] Rowley, Jennifer (2007), The wisdom hierarchy: representations of the DIKW hierarchy, Journal of Information and Communication Science 33 (2): 163-180.

[15] http://www.cioupdate.com/cio-insights/implementing-knowledge-management-part-i-concepts-approach-1.html, 2015 QuinStreet Inc.

[16] Rifkin, Jeremy (2011), The third industrial revolution.

[17] XML and Semantic Web W3C Standards Timeline, W3C, 2012-02-04.

[18] https://en.wikipedia.org/wiki/HTML, last modified on 30 November 2015.

[19] http://www.merriam-webster.com/dictionary/hyperlink, 2015 Merriam-Webster, Incorporated.

[20] Berners-Lee, Tim (2006), Linked Data – Design Issues, W3C, Retrieved on 18 Dec. 2010.

[21] https://en.wikipedia.org/wiki/Linked_data, last modified on 30 November 2015.

[22] http://www.unesco.org/webworld/mdm/czech_digitization/doc/digitiz.htm, 2015.

[23] https://www.srri.umass.edu/topics/knowledge-structure, 2015 University of Massachusetts Amherst.

[24] https://en.wikipedia.org/wiki/Social_media, last modified on 2 December 2015.

[25] Murthy, Dhiraj (2013), Twitter: Social Communication in the Twitter Age, Polity, Cambridge, ISBN 978-0-7456-6510-8.

[26] van Dijck, José (2013), The Culture of Connectivity: A Critical History of Social Media, Oxford University Press.

[27] https://en.wikipedia.org/wiki/New_media, last modified on 28 November 2015.

[28] Manovich, Lev, New Media From Borges to HTML, The New Media Reader, Ed. Noah Wardrip-Fruin & Nick Montfort, Cambridge, Massachusetts, 2003, 13-25. ISBN 0-262-23227-8.

[29] Cunningham, Ward (2002), What is a Wiki, WikiWikiWeb, retrieved on 10 April 2008.

[30] https://en.wikipedia.org/wiki/Blog, last modified on 2 December 2015.

[31] https://blog.twitter.com/2012/twitter-turns-six, 2015 Twitter, Inc.

[32] https://en.wikipedia.org/wiki/YouTube, last modified on 3 December 2015.

[33] https://en.wikipedia.org/wiki/Web_page, last modified on 2 December 2015.

[34] Web Services Glossary, W3C, Retrieved on 22 April 2011.

[35] https://en.wikipedia.org/wiki/Social_graph, last modified on 23 October 2015.

[36] Keen, Andrew, The Cult of the Amateur, Random House, ISBN 978-0-385-52081-2.

[37] http://www.networkworld.com/article/2213704/collaboration-social/top-10-social-networking-threats.html

[38] Towards Knowledge Societies, UNESCO Publishing, ©UNESCO 2005, ISBN 92-3-204000-X.

[39] https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation.aspx, 2015 ISACA.

[40] https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance, last modified on 9 July 2015.

[41] http://www.dr4ward.com/dr4ward/2012/05/how-has-digital-and-social-media-evolved-into-social-business-and-what-is-next-infographic.html, Posted on 7 May 2012.

[42] https://en.wikipedia.org/wiki/History_of_Wikipedia, last modified on 2 December 2015.

[43] Hilbert, M., and Lopez, P. (2011), The world's technology capacity to store, communicate, and compute information, Science, 332 (6025) 60-65.http://www.martinhilbert.net/WorldInfoCapacity.html

[44] Weinberger, David (2011), Too Big To Know, Basic Books, Leader's Books Publisher.

[45] Schmidt, Eric, and Cohen, Jared (2013), The New Digital Age, Google Inc.

[46] Drucker, P.F. (1969), The age of discontinuity: Guidelines to our changing society, New York, NY: Harper & Row.

[47] Sanou, B. (2013), The world in 2013: ICT fact and figures, Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

[48] Gross, M. (2010), Ignorance and Surprise: Science, Society, and Ecological Design, Cambridge, MA, MIT Press.

[49] https://en.wikipedia.org/wiki/Resource_Description_Framework, last modified on 26 May 2016.

[50] Recommendation ITU-T H.264 (2016), Advanced video coding for generic audiovisual services.

3.

Trust Provisioning for future ICT infrastructures and services

ITU-T Technical Report, Trust Provisioning for future ICT infrastructures and services (2016)

Summary

This technical report provides an overview of trust provisioning for future ICT infrastructures and services. It describes the importance and necessity of trust from potential risks toward knowledge societies in terms of ICT and provides the concepts and key features of trust. After identifying key challenges and technical issues, it also presents architectural overview of trusted ICT infrastructures. And then, it introduces trust based ICT service models and summary of use cases, and it proposes strategies for future standardization on trust. The trust related activities in other standardization bodies, backgrounds for ICT service model analysis framework and detailed use cases are also provided in informative appendices.

Keywords

Trust provisioning, ICT infrastructure, ICT service, Knowledge society

Change Log

None

Foreword

This Technical Report has been developed by Mr Hyeontaek Oh, Mr Tai-won Um, Mr Jun Kyun Choi.

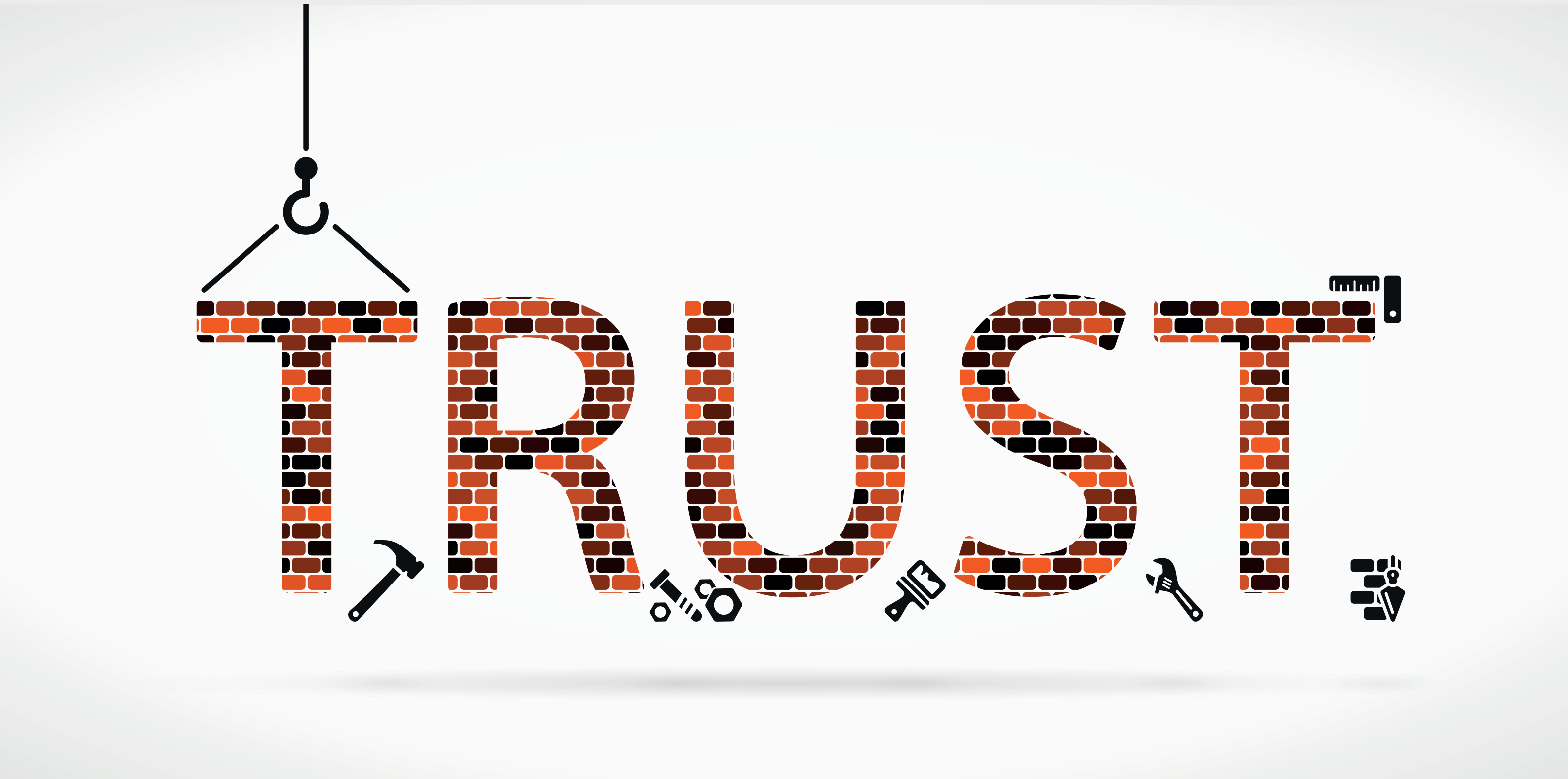

TRUST

Table of Contents

1 Scope

This technical report provides an overview of trust provisioning for future trusted ICT infrastructures and services. More specifically, this technical report covers the following:

– The importance and necessity of trust toward knowledge societies;

– Concepts and key features of trust;

– Key challenges and technical issues for trusted ICT infrastructures;

– Architectural overviews of trusted ICT infrastructures;

– Trust based ICT service models;

– Summary of use cases for trusted ICT infrastructures;

– Strategies for future standardization on trust.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in the text of this technical report form basis and help understanding the topic of trust provisioning in ICT. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; readers are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[ITU-T M.3410]	Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.
[ITU-T X.509]	Recommendation ITU-T X.509 (2012), *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.*
[ITU-T X.1163]	Recommendation ITU-T X.1163 (2015), *Security requirements and mechanisms of peer-to-peer-based telecommunication networks.*
[ITU-T X.1252]	Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*
[ITU-T Y.2701]	Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*
[ITU-T Y.2720]	Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 Cloud computing [b-ITU-T X.1601]: A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration.

3.1.2 Internet of Things [b-ITU-T Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.3 Knowledge society [b-UN]: The knowledge society is one in which institutions and organizations enable people and information to develop without limits and open opportunities for all kinds of knowledge to be mass-produced and mass-utilized throughout the whole society.

3.2 Terms defined here

3.2.1 Trust: Trust is an accumulated value from history and the expecting value for future. Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making.

NOTE 1 – Trust is applied to social, cyber and physical domains.

NOTE 2 – Trust [ITU-T X.509]: Generally, an entity can be said to "trust" a second entity when it (the first entity) assumes that the second entity will behave exactly as the first entity expects. The key role of trust is to describe the relationship between an authenticating entity and an authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates.

NOTE 3 – Trust [ITU-T X.1163]: The relationship between two entities where each one is certain that the other will behave exactly as it expects.

NOTE 4 – Trust [ITU-T X.1252]: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

NOTE 5 – Trust [ITU-T Y.2701]: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

NOTE 6 – Trust [ITU-T Y.2720]: A measure of reliance on the character, ability, strength, or truth of someone or something.

4 Abbreviations

API	Application Programming Interface
B2B	Business-to-Business
B2C	Business-to-Customer
CoI	Community of Interest
CPS	Cyber-Physical System
D2D	Device-to-Device
DDoS	Distributed Denial-of-Service
DIKW	Data, Information, Knowledge and Wisdom
DPI	Deep Packet Inspection
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IdM	Identity Management
IETF	Internet Engineering Task Force
IoT	Internet of Things
ITU	International Telecommunication Union
LBS	Location Based Service
M2M	Machine-to-Machine
NFC	Near Field Communication
OAM&P	Operations, Administrations, Maintenance, and Provisioning

OBD	On-Board Diagnostics
OIC	Open Interconnect Consortium
OS	Operating System
OTA	Online Trust Alliance
PaaS	Platform-as-a-Service
PIN	Personal Identification Number
QoE	Quality of Experience
QoS	Quality of Service
QoT	Quality of Trust
SaaS	Software-as-a-Service
SDO	Standards Development Organization
SG	Study Group
SLA	Service Level Agreement
SNS	Social Network Service
TA	Trust Agent
TAMP	Trust Analysis and Management Platform
TCG	Trusted Computing Group
TLA	Trust Level Agreement
TSB	Trust Service Broker
TSE	Trust Service Enabler
WAN	Wide Area Network
WSIS	World Summit on the Information Society
WWW	World Wide Web
W3C	World Wide Web Consortium

5 Introduction to Trust toward Knowledge Societies

5.1 Toward knowledge societies

At the 15th International Telecommunications Union (ITU) Plenipotentiary Conference, year 1999, the World Summit on the Information Society (WSIS) was created to develop the information society. During the first phase of the WSIS, the debates on the information society are mainly focused on information and communication technology (ICT) infrastructures. The concept of knowledge societies is more all-embracing and more conducive, which is simply "opens the way to humanization of the process of globalization." The notion of knowledge is central to changes of education, science, culture, and communication. Knowledge is recognized as the object of huge economic, political and cultural stakes, to the point of justifiably qualifying the societies currently emerging.

Knowledge is defined as a familiarity, awareness or understanding of someone or something such as facts, information, description or skills. Knowledge is acquired through experience or education by perceiving, discovering and learning. It can refer to theoretical or practical understandings of a subject that is implicit (as with practical skill or expertise) or explicit (as with theoretical understanding of a subject). It can be more or less formal or systematic.

In the networked society, knowledge is a source of all human being including behaviours and building a society. The networking of knowledge and the speeding up of information processing open up new possibilities for work on databases, irrespective of their size, their use and their ultimate purpose. The current Internet as a public network gives fresh opportunities to achieve equal and universal access to knowledge. Like Internet, new ICTs have created for emergence of knowledge societies [b-UNESCO]. Future knowledge societies will be built on the basis of ICT infrastructures since it is not only for delivery of digital data, but also provides the eco-platform to share data, information, and knowledge.

Accordingly, as a top level standard organization relating to ICTs as well as the United Nations agency, the ITU should concern about future knowledge societies.

5.2 Potential risks in ICT infrastructures

Knowledge societies will have to cope with instability and insecurity since the accelerated spread of knowledge will be confronted with risks in ICT infrastructures. There are many potential risks in ICT infrastructures as follows.

- **In nature**
  - **New technology development**: Any scientific progress and technology development may incur potential risks. New technologies may not be stable without guarantee of stability and reliability. Without acceptable confidence, it may cause unexpected accident and destroy the existing value chain of business. The development of new technologies may be sometimes undesirable if the certain levels of controllability and credibility are not guaranteed. Furthermore, the adaptation of new technologies may cause instability and insecurity since new technologies always have uncertainty. In the ICT infrastructure, new technological revolution may provide great advantages for utilizing networking resources. However, it confronts unidentified risk beforehand.
- **Human behaviours**
  - **Human-human interactions**: If there is no trust among peoples, their interactions (e.g., exchanging data and information) have meaningless due to lack of confidence with each other. If the people are not trustworthy, personal interactions do not invoke any response. The unclear decision making or unrealistic situation may be happening from low or broken trust in human relationships.
  - **Human-machine interactions**: When a human cannot trust a machine (e.g., delivering imprecise data from a machine to a human), human-machine interactions cannot be established and potential benefits on system performance will be lost. The human-machine systems have always proved unpredictable and fallible, whereas the nature of the system is to function normally. It relies on technological dependency which accentuates risks.
  - **Human interactions in cyber-physical system (CPS) environments**: The CPS cannot be fully operable if a physical world and a cyber world have some mismatch. If the malfunction of a physical system does not notify at the responsible entities in a cyber world, there are some risks to prevent safety in a physical world. An intelligent human in a cyber world can avoid or reduce the risk of failures and minimize the unacceptable situation in a physical world. The time critical convergence applications such as smart grid and intelligent transportation systems require high trust between a cyber world and a physical world. Greater openness, in combination with hiding one's real identity in a physical world and making a false object in a cyber world, increases the risks that people are becoming victims of deception. They also include identity theft and exposure to inappropriate actions.
  - **Human errors**: Without recognizing a set of rules and external conditions of a physical system, human actions may result on risks or failures. Human errors may be a primary cause or a contributing factor in risks and accidents. Intentional or unintentional human errors may cause serious problems in ICT infrastructures.

- **Complexity of ICT infrastructures**
  - **A numerous number of ICT resources**: Risks threaten us to cope with complexity of interactions and mechanisms of ICT infrastructures. The access of a large number of ICT resources causes irreparable damages and creates unpredictable dangers. It is essential to make ICT resources accessible to all the people with promises but with unknown dangers.
  - **Complexity of network operation**: There are a lot of algorithms for network resource optimization including efficient routing, congestion avoidance, and guaranteeing Quality of Service (QoS)/Quality of Experience (QoE). When the unpredictable situations are happened in a network, the out-of-service possibility is increasing. Natural disaster and distributed denial-of-service (DDoS) attacks are also a part of risks. While network control functions can arrange the by-pass or de-tour route to cope with overflowed traffic, the unexpected side effects like traffic fluctuation and domino effect may bring additional risks. To increase network survivability during network operation, networking protocols and OAM&P (Operations, Administrations, Maintenance, and Provisioning) functions should be re-designed to be trustworthy. Moreover, when a network infrastructure includes a cloud platform with large volume of storage and processing capabilities, network instability is not coming only from traffic congestion. The operation of the cloud platform and high level applications are additional harmful sources to increase network risks. The existing security functions including firewall and Deep Packet Inspection (DPI) may be replaced to provide the certain level of trust, through the implementation by a trust gateway system and trust-guaranteed network OAM functions.
  - **Data, information and knowledge process**: Since future ICT infrastructures should provide data, information and knowledge process, the trust provisioning is quite essential. Data integrity refers to maintain and assure the accuracy and consistency of data. The failure of data aggregation is coming from any unintended changes to data as the results of storage, retrieval and processing operation for further information and knowledge. For example, if data stored in a cloud platform are shared by anonymous users, there may be a possibility to happen undesirable situations. With a certain level of trust, data delivery and cognitive data, information, knowledge and wisdom (DIKW)1 process may be effective and meaningful.
  - **Complexity of convergence services and applications**: ICT based services and applications will continue to be heterogeneous, and this may lead to increase a number of convergence services that cover multiple service domains. Especially, in Internet of Things (IoT) and CPS environments, people, platforms and devices will be highly inter-connected by a dynamic network of networks and operated in heterogeneous environments. These kinds of highly connected environments increase the complexity of services and applications (which consume data and information from connected sensors, devices, etc.), and the unknown potential risks may be incurred due to complex interactions. As ICT based applications and services will scale over multiple domains and involves multiple stakeholders, methods for assessing trust are needed to enable the users to have confidence to these services and applications.

5.3 Trust for future ICT infrastructures and services

For evolving toward knowledge societies, ICT will be mainly used for the creation, dissemination and utilization of knowledge in an open and collaborative manner. Although recent advances in ICT have brought changes to our everyday lives, various problems exist due to the lack of trust. The large scale collection and analysis of data from sensors and devices in physical spaces imposes difficult issues, ranging from the risks of unanticipated uses of consumer data to the potential discrimination enabled by data analytics and the insights offered into the movements, interests and activities of an individual. If knowledge is exploited for

[1] *DIKW (Data, Information, Knowledge and Wisdom): This refers loosely to a class of models for representing purported structural and/or functional relationships between data, information, knowledge, and wisdom. "Typically information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge". (Source: https://en.wikipedia.org/wiki/DIKW_Pyramid)*

malicious intentions, it could suffer from irreparable damage and uncertain dangers. However, it is difficult to identify and prevent risks of knowledge in complicated ICT infrastructures.

The convergent services have been required to obtain reliable knowledge from raw data. As an aim of intelligent service provision is to make autonomous decisions without human intervention, trust has been highlighted as a key issue in the processing and handling of data, as well as the provisioning of services which comply with users' needs and rights. Therefore, we need to find a way to minimize the unexpected risks and maximizing the survivability of future knowledge societies. Within certain reliability and predictability, the ICT infrastructure can be operating in a controlled environment. It should be robust to unexpected conditions and adaptable to system failures.

Based on the significant efforts made to build converged ICT services and a reliable information infrastructure, ITU-T has recently started new work on future trusted ICT infrastructures. These infrastructures will be able to accommodate emerging trends in ICT, while taking into account social and economic considerations. Thus, this report addresses trust provisioning for future ICT infrastructures and services which act as the glue for integrating physical, cyber and social worlds with ICT as a basis for knowledge societies. It provides the trust conceptual model and the trust architectural framework to cope with potential risks due to the lack of trust. The aim is to create a trusted ICT infrastructure for sharing information and creating knowledge and to stimulate activities for future standardization on trust with related Standards Developing Organizations (SDOs).

6 Understanding of Trust

6.1 Generic definitions of trust

As a lexical-semantic, trust means reliance on the integrity, strength, ability, surety, etc., of a person or object. Generally trust is used as a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates.

Trust concept itself is a complicated notion with different meanings depending on both participators and situations and influenced by both measurable and non-measurable factors. There are various kinds of trust definitions leading to difficulties in establishing a common, general notation that holds, regardless of personal dispositions or differing situations. Generally, trust is considered as a computational value depicted by a relationship between trustor and trustee, described in a specific context and measured by trust metrics and evaluated by a mechanism.

Previous research has shown that trust is the interplay among human, social sciences and computer science, affected by several subjective factors such as social status and physical properties; and objective factors such as competence and reputation [b-Alcalde]. The competence is measurement of abilities of the trustee to perform a given task which is derived from trustee's diplomas, certifications and experience. Reputation is formed by the opinion of other entities, deriving from third parties' opinions of previous interactions with the trustee.

Trust revolves around assurance and confidence that people, data, entities, information or processes will function or behave in expected ways. At the deeper level, trust is regarded as a consequence of progress towards security or privacy objectives.

Trust is crucial that it affects the appetite of an entity to use services or products offered by another entity. This trust may come from our past experience of using these brands' products (termed "belief") or from their reputations that are perceived from people who bought items and left their opinions about those products (termed "reputation"), or from suggestions of your surrounding such as families and friends (termed "recommendation").

It is challenging to concisely define "trust" of an entity due to its uniqueness to each individual entity. From a sociological point of view, trust is defined as the trusting behaviour that one person has on another person in a situation where an ambiguous path exists. In such definition, trust is used to mitigate the risks of the dealings with others. Trust is also considered as the capacity and belief of an entity that the other entity would meet its expectations.

6.2 Trust in ICT Environments

As trust can be interpreted in different ways, there are various meanings from literature for more clear views on trust in terms of telecommunication systems and ICT.

The term trust in the context of ICT world differs from the concept of trust among people. This notion of trust stands in contrast to some more intuitive notions of trust expressing that someone behaves in a particular well-behaved way. Trust in ICT is an important concept in the sense that a trusted resource is one that you are forced by necessity to trust. The failure of this resource would compromise the function, integrity or security of a system which are not in expected ways.

Nevertheless, trust is an important feature in the decision-making process not only used by humans in daily life but also by applications and services in ICT environment.

Trust in computer science in general can be classified into two broad categories: "user" and "system". The notion of "user" trust is derived from psychology and sociology, with a standard definition as "a subjective expectation an entity has about another's future behaviour." "System" trust is "the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose."

Trust in an on-line transaction can be divided into two types: direct (personal) trust and third party trust. Direct trust is a situation where a trusting relationship is nurtured by two entities. This type of trust is formed after these entities have interacted with each other. The entity A inherently trusts entity B after a number of successful transactions that involved both entities. On the contrary, third-party trust is a trust relationship of an entity that is formed from the third party recommendations. For example, entity A trusts entity B because B is trusted by entity C and C recommends that B is trustful. In this example, entity A derives trust of B from C, and A also trusts entity C does not lie to him.

Due to dynamics of network configuration and resources, trust issue occurs not only in the human to human network, but also in machine to machine and human to machine and vice versa. In other words, trust is needed not only for people to maintain social network service benefit, but also for machine to be connected safely to network. System/network-related trust is the beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible [b-McKnight].

Trust is a broad concept used in many disciplines and subject areas but until now, there is no commonly agreed definition. Therefore, ITU-T CG-Trust has newly defined the terms "trust" Clause 3.2.1. As per the definition, trust in the ICT world is defined as "Trust is an accumulated value from history and the expecting value for future. Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making." Trust value is applied to social, cyber and physical domains. Figure 6-1 shows various related attributes for trust in social, cyber and physical domains.

NOTE 1 – Clause 7 presents the details of social, cyber and physical domains.

NOTE 2 – Appendix I provides the summary of trust definitions from various viewpoints.

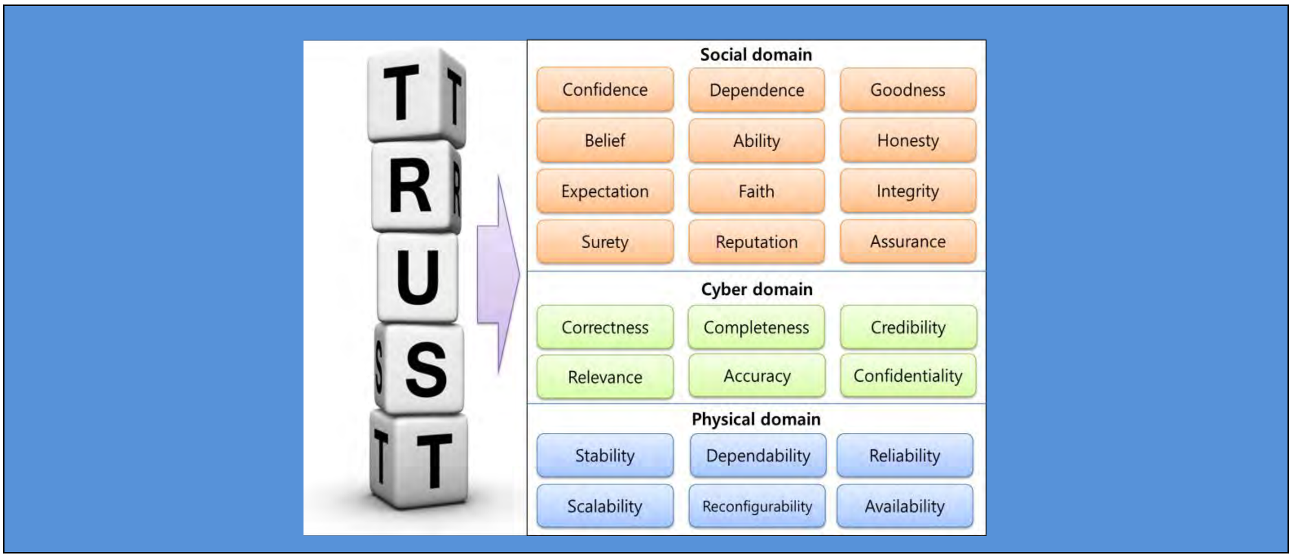


Figure 6-1 – Attributes for trust

6.3 Relationship among security, privacy and trust

- **Security**: systems need a variety of methods to prevent behaviours with malicious intents. Security mainly concerns technological aspects such as the confidentiality, availability and integrity. It also includes attack detection and recovery/resilience.
- **Privacy**: users need the protection of their personal information related to their behaviours and interactions with other people, services and devices. Privacy mainly concerns user aspects to support anonymity and restrictive handling of personal user data.
- **Trust**: trust is broader concept that can cover security and privacy (Figure 6-2). Trust revolves confidence that people, data, devices will function or behave in expected ways. Trust can be used to build new value-chain for future ICT infrastructure and services.

For example, security and privacy have controlled a system and data securely in social-cyber-physical domains. However, traditional secure system concerns about how to authorize the entities as well as how to provide data to the authorized entities. Trust can give reliability to security and privacy as a parameter by measuring a discrepancy between observation and objective or subjective expectation of the reliable entities and data.

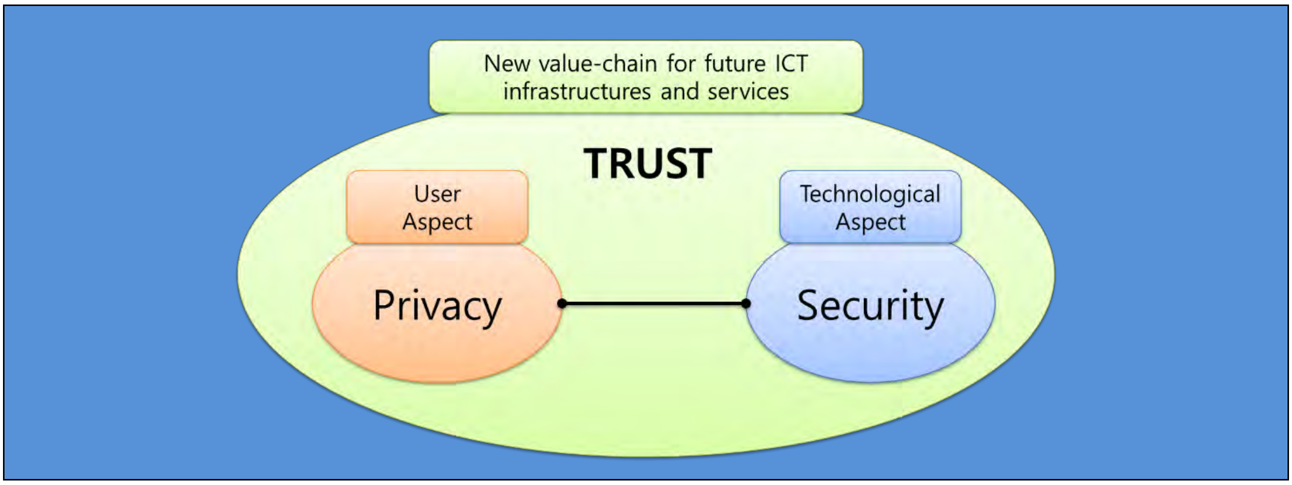


Figure 6-2 – Relationship among security, privacy and trust with different aspects

6.4 Relationship between knowledge and trust

To understand trust, it is required to analyse the collected data from entities, extract the necessary information for trust, understand the information, and then create the trust-related knowledge.

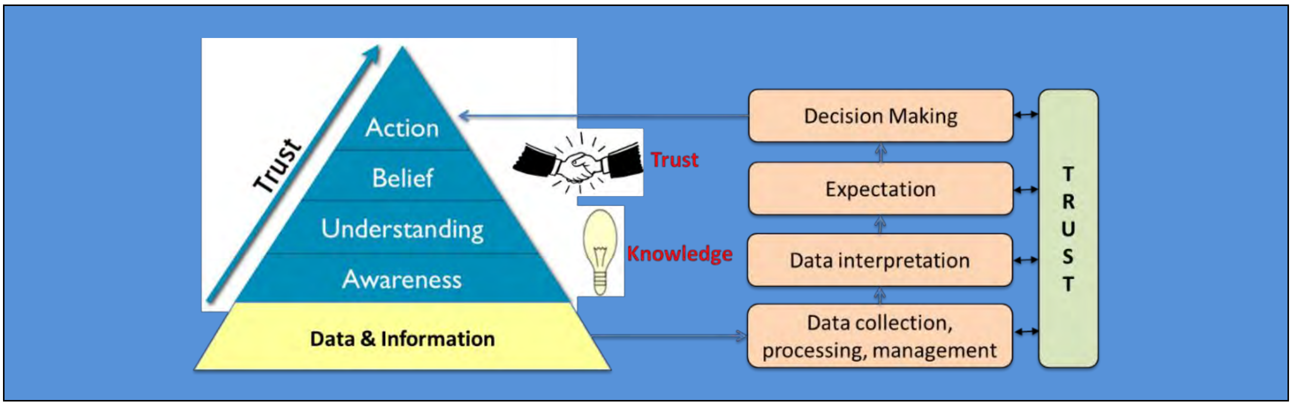


Figure 6-3 – Knowledge and Trust[2]

The social and economic value of data is mainly reaped during two moments: first when data is transformed into knowledge (gaining insights) and then when it is used for decision making (taking action). The knowledge is accumulated by individuals or systems through data analytics over time. So far data processing, management and interpretation for awareness and understanding have been considered as fundamental processes for obtaining the knowledge. As shown in left hand side of Figure 6-3, trust is strengthened from accumulated knowledge and it mainly has a significant role as a belief between knowledge (i.e., awareness and understanding) and action. It means that the expectation process for trust should be additionally considered before decision making. As shown in the right hand side of Figure 6-3, trust should be further considered to the whole process from data collection to decision making.

7 Features, Challenges and Technical Issues for Trusted ICT infrastructures

7.1 Trusted ICT infrastructure

Figure 7-1 shows high-level overview for a trusted ICT infrastructure. A physical domain mainly consists of physical devices which interwork with each other through information and communication networks. A cyber domain is responsible for the delivery, storage and processing of data and information. A social domain has become popular to people for sharing and showing their knowledge and become a new medium for connecting people in cyberspace.

[2] Illustration compiled from trust pyramid: http://www.johnhaydon.com/how-make-people-trust-your-nonprofit/

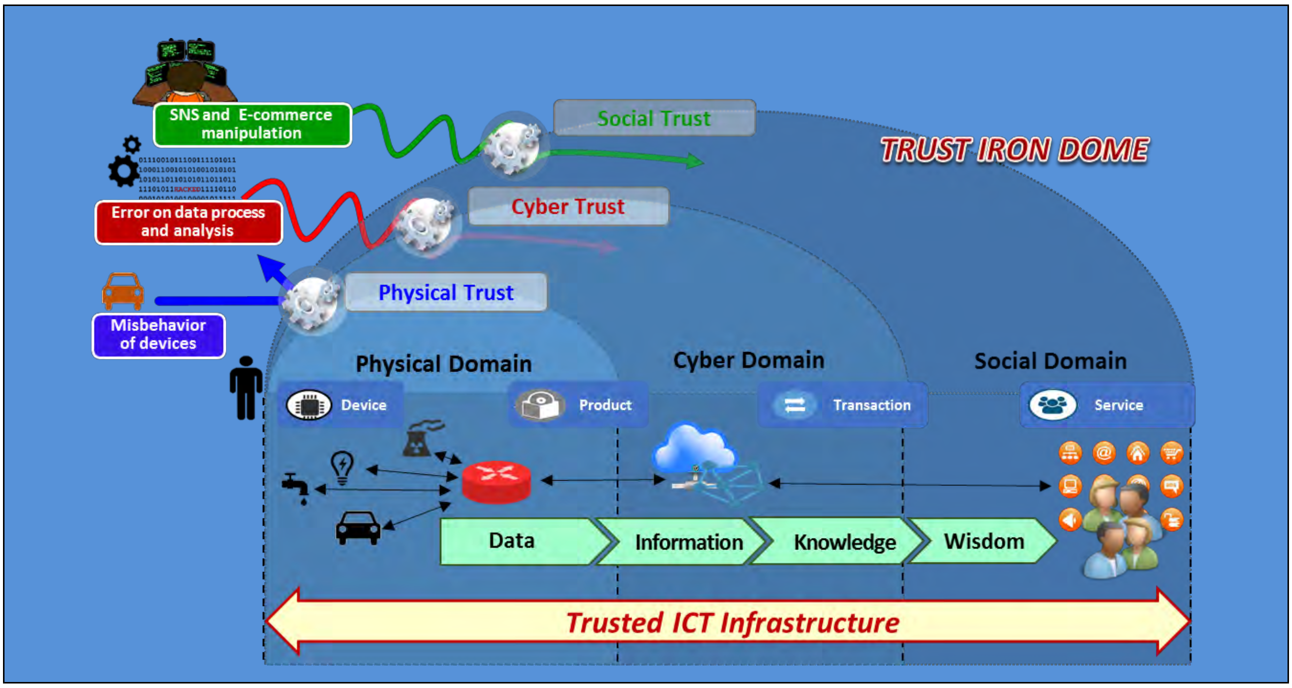


Figure 7-1 – High-level overview of a trusted ICT infrastructure

The trusted ICT infrastructure comprise objects from the physical domain (physical objects), the cyber domain (virtual objects) and the social domain (humans with attached devices), which are capable of being identified and integrated into information and communication networks. All of these objects have their associated information, which can be static and dynamic.

NOTE – Clause 8.1 provides detailed explanations on physical trust, cyber trust and social trust.

7.2 Key features of trust

- **Trust** characteristics

There are several important characteristics of trust that further enhance our understanding about trust digital environments.

– **Trust is dynamic**: as it applies only in a given time period and maybe change as time goes by. For example, for the past one year Alice highly trusts Bob. However, today Alice found that Bob lied to her, consequently, Alice no longer trusts Bob.

– **Trust is context-dependent**: trust applies only in a given context. The degree of trust on different contexts is significantly different. For example, Alice may trust Bob to provide financial advice but not for medical advice.

– **Trust is not transitive in nature but maybe transitive within a given context**. That is, if entity A trusts entity B, and entity B trusts entity C then entity A may not trust entity C. However A may trust any entity that entity B trusts in a given context although this derived trust may be explicit and hard to be quantified.

– **Trust is an asymmetric relationship**. Thus, trust is a non-mutual reciprocal in nature. That means if entity A trust entity B, then the statement "entity B trusts entity A" is not always true.

The nature of trust is fuzzy, dynamic and complex. Besides asymmetry and transitivity, there are additional key characteristics of trust: implicitness, antonym, asynchrony, and gravity [b-Chang-2005, b-Chang-2006].

– **Implicit**: It is hard to explicitly articulate the confidence, belief, capability, context, and time dependency of trust.

- **Antonym**: The articulation of trust context in two entities may differ based on the opposing perspective. For example, entity A trusts entity B in the context of "buying" book, however from entity B to entity A the context is "selling" book.
- **Asynchrony**: The time period of trusting relationship may be defined differently between the entities. For example, entity A trusts entity B for 3 years, however, entity B may think that the trust relationship only last for the last 1 year.
- **Gravity**: The degree of seriousness in trust relationships may differ between the entities. For example, entity A may think that its trust with entity B is important, however, entity B may think it differently.

- **Trust among multiple trust domains**

Trust domain is a set of information and associated resources consisting of users, networks, data repositories, and applications (or services) that manipulate the data in those data repositories. For providing a trust-based service, multiple trust domains are involved. Different trust domains may share the same social-cyber-physical components. Also, a single trust domain may employ various levels of trust, depending on what the users need to know and the sensitivity of the information and associated resources [ITU-T M.3410].

- **Quality of Trust (QoT)**: Due to the diversity of applications and their inherent differences in nature, trust is hard to be formalized in a general setting. However, it is important to quantify a level of trust in ICT infrastructures. A certain level of trust should be derived from the associated devices, services, applications and users of trust. The level of trust can be measured and classified objectively or subjectively. The concept of QoT, which is similar with QoS as an objective manner (e.g., measured quantitatively) or QoE as a subjective manner (e.g., counted qualitatively), represents different classes in terms of levels of trust in multiple domains (e.g., physical, cyber, and social domains). It can be used to understand the degree of trust among multiple trust domains.
- **Trust Level Agreement (TLA)**: Depending on what QoT the users need, including those related to sensitivity of information and associated resources, there may be a lot of TLAs – similar to the concept of Service Level Agreement (SLA).

Figure 7-2 shows an example of different classes of QoT among multiple trust domains in an ICT infrastructure. A service domain may consist of multiple trust domains (e.g., three trust domains in this figure). Depending on levels of trust for each component, a trust domain may have different classes of QoT. For example, trust domain A provides physical trust (QoT Class 1), trust domain B provides physical and cyber trust (QoT Class 2), and trust domain C provides physical, cyber and social trust (QoT Class 3). Then, TLA is established, based on the agreement of all involved trust domains using the QoT information to provide a trust-based ICT service.

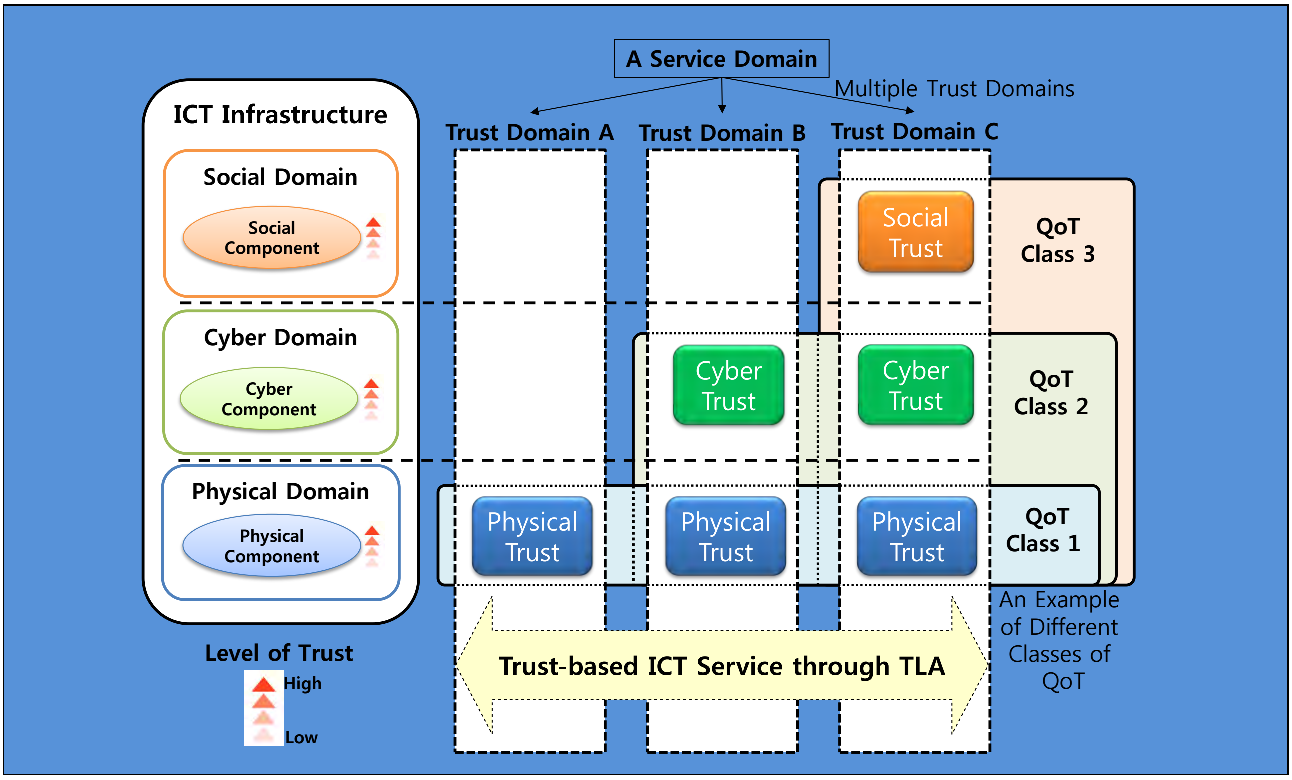


Figure 7-2 – An example of QoT and TLA among multiple trust domains

From the concepts of trust domains in the previous figure, Figure 7-3 illustrates several interactions among entities for trust provisioning in a real world. These interactions are based on trust relationships of each entity in social, cyber and physical domains according to different classes of QoT.

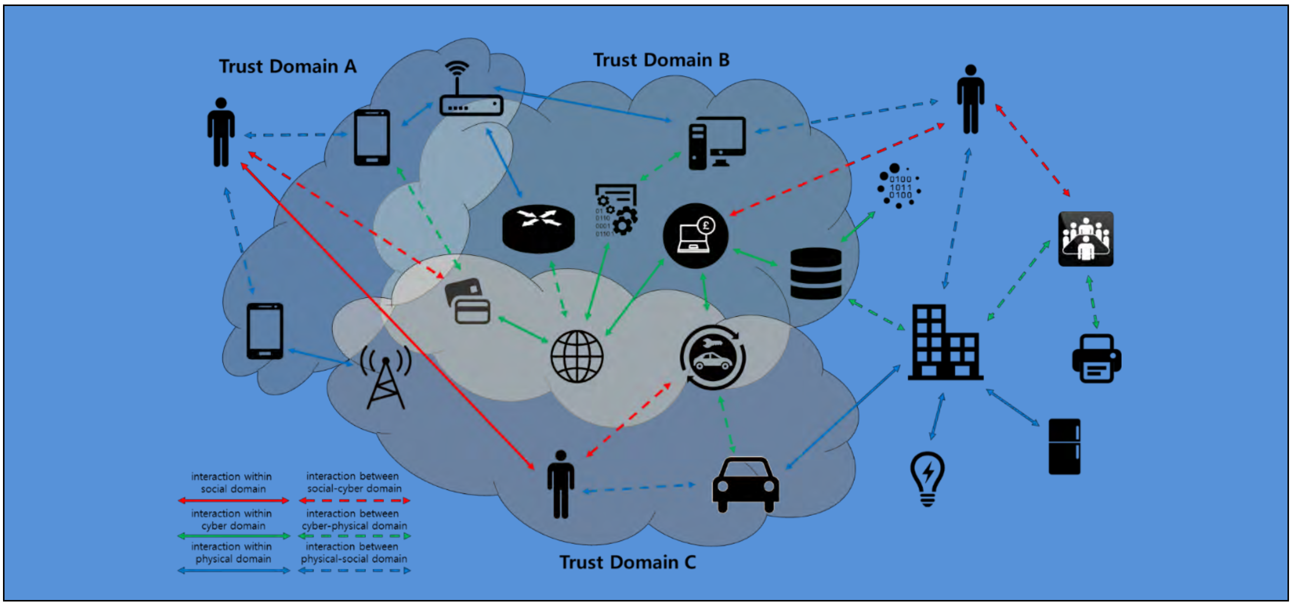

Trust Domain A
Trust Domain B
Trust Domain C
0100
1011
0100
interaction within social domain
interaction between social-cyber domain
interaction within cyber domain
interaction between cyber-physical domain
interaction within physical domain
interaction between physical-social domain

Figure 7-3 – Illustration of interactions among entities for trust provisioning in a real world

7.3 Key challenges for trust provisioning

This clause describes key challenges for trust provisioning for ICT infrastructures.

Trust relationship may be human to human, object to object (e.g., handshake protocols negotiated), human to object (e.g., when a consumer reviews a digital signature advisory notice) or object to human (e.g., when a system relies on user input and instructions without extensive verification) as shown in Figure 7-4. For social-cyber-physical relationships, trust is taking into consideration coexistence, connectivity, interactivity and spatio-temporal situations across domains.

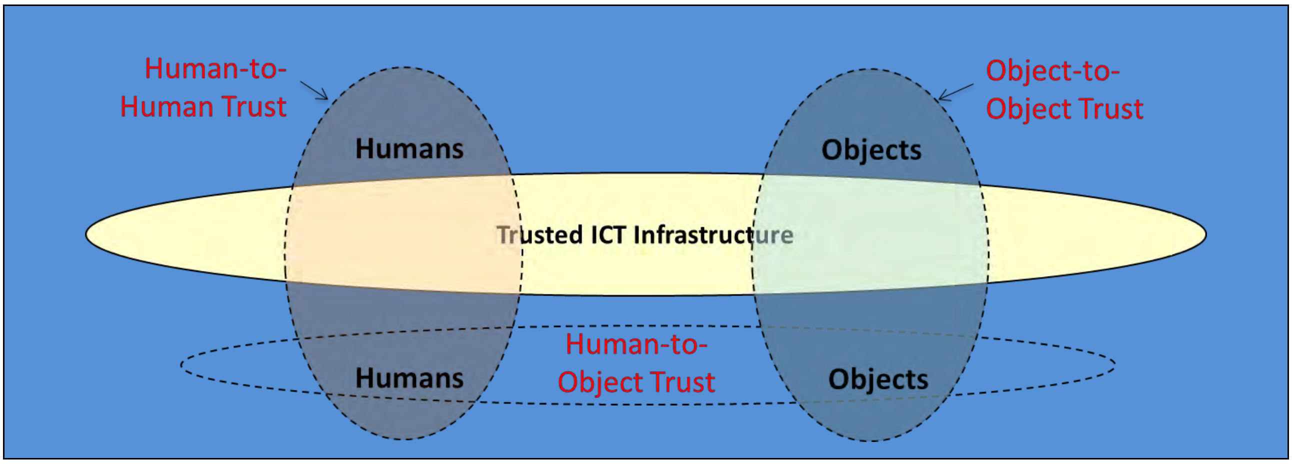


Figure 7-4 – Trust relationships in a trusted ICT infrastructure

In this highly interconnected ICT infrastructure, a number of independently developed, operated and managed objects are autonomously networked, yielding a new kind of complex system that provides various services. Furthermore, services and applications are now open their platform through common interfaces. Such characteristics of interconnected systems lead to the introduction of security vulnerabilities that can be very hard to find and analyse. If it is not properly handled, the stability and safety of the overall system can be seriously threatened.

Assuring continuous trustworthiness, taking into account such characteristics for trusted ICT infrastructures with highly interconnected systems, is becoming a key challenge. Trust must be addressed and evaluated in all services and infrastructures, as well as in all system and component levels, in a holistic manner. Trust management is required to apply between heterogeneous systems and stakeholders, while focusing on the relationships and dependencies between them. Also, the state of objects changes dynamically in the ICT infrastructure, (e.g., sleeping and waking, connected/disconnected, and node failure etc.) as does their context, including location and speed. Moreover, the number of entities also fluctuates. That is, trust is situation-specific and trust changes over time.

On the other hand, for scalability and complexity of ICT infrastructures due to the huge number of different links and interactions, trust, security and privacy become tightly coupled because system features increasingly depend on networks, computation and processing. Trustworthiness requires cooperation and co-engineering with security and privacy. It is not sufficient to address one of them in isolation, nor is it sufficient simply to combine components of trust, security and privacy. In order to address these issues, a unified approach is needed towards trust, security and privacy co-analysis, design, implementation and verification. In case of small-size sensor devices, because of its severe resource constraints and dynamics, conventional security approaches cannot fully cover security demands of the IoT domain, and trust technologies can be used as additional complementary features to support the security demands.

Trust provisioning is desirable to combine features from different domains for developing inter-domain trust provisioning which is able to cover social-cyber-physical trust relationships. For trust provisioning for ICT infrastructures, these key challenges are considered to new trust provisioning technology.

7.4 Technical issues for trust provisioning

This clause describes technical issues for trust provisioning for ICT infrastructures. Following technical issues should be considered: i) trustworthy data collection and aggregation, ii) trustworthy data process and analysis, iii) trust metric and modelling, iv) dissemination of trust information, v) trust index and vi) trustworthy system lifecycle management.

7.4.1 Trustworthy data collection and aggregation

As the number of data sources and types are dramatically increased, the trustworthiness of data itself is regarded as important. Because collection and aggregation of false data will lead to a degradation of service quality and waste of system resources, it is a significant issue to detect wrong or polluted data. Trust metrics and models can be used as criteria for checking trustworthiness to achieve trusted data collection and aggregation.

7.4.2 Trustworthy data process and analysis

When the huge amounts of data are collected to a system, these data should be processed and analysed in trustworthy ways. Data process and analysis mainly occurs in cyber domain (e.g., utilizing cloud computing for big data analysis), however, it also can be done in a physical domain as well as a social domain. Each domain has its own intelligence to process incoming data to create new useful information. This information is usually propagated to different entities and domains, so there are some ways to check whether given data process and analysis mechanism is trustworthy or not. Measurable trust value should be defined to analyse trust of entities, and it is also important to find appropriate trust evaluation mechanisms for analysing trust values for a specific domain.

7.4.3 Trust metric and modelling

A trust metric is a measure to evaluate a level of trust by which a human or an object can be judged or decided from trustworthiness. It can be differently defined in each human or each object. Trust metrics might be separately defined in each of domains, but the key issue is to describe qualitative and quantitative metrics across the domains, to determine the attributes in the different domains. For measurable trust, some mechanisms and solutions may be established by defining trust metric. There are several attributes social-cyber-physical domains for trust provisioning. Attributes in each domain of Figure 6-1 are examples. Depending on the services and applications, the required attributes of trust may vary.

A trust model is the method to specify, build, evaluate and ensure trust relationships among entities. The trust model is used for the processing trust data. Most existing trust models are based on the understanding of trust characteristics, accounting for factors influencing trust. Trust modelling is domain-specific and there exists numerous ways to define trust model for each domain. It is a critical issue to select a suitable trust model for a particular domain.

7.4.4 Trust index

A trust index is a composite and relative value that combines multiple trust related indicators (e.g., objective trust metrics and subjective trust attributes) into one benchmark measure, which is similar to ICT Development Index (IDI) or stock market index. It can be used to compare trust among stakeholders when they create a new trust relationships or a trust value chain. The trust index should be designed to quantify a trust value of each stakeholder, and the methodology used to compute trust index should be clearly defined. In order to apply the trust index to a real world, common indicators for covering different stakeholder characteristics and comparing methods for trust indices of different stakeholders should be developed.

7.4.5 Dissemination of trust information

Trust dissemination means to distribute or broadcast trust information. There could be many ways of disseminating trust information in different domains. In case of a social domain, recommendation and visualization methods are considered as main approaches to disseminate trust information [b-Sherchan]. The efficient, effective and suitable trust dissemination methods should be developed.

7.4.6 Trustworthy system lifecycle management

In order to achieve trustworthy systems, we need a systematic methodology to cover all relevant trust aspects of operation life cycle. At the design phase, the definition, metrics and goals of trust for the target system should be determined and the system should be developed while trust measures are considered to fulfil the design goals in the development phase. The maintenance phase has to properly monitor the normal operation of the running of a trustworthy system and the dynamics of the execution environment to verify the trust provisions at runtime.

8 Architectural overview for trust provisioning for ICT infrastructures

8.1 Generic ICT trust conceptual model

From the concept of trust provisioning for a trusted ICT infrastructure described in Clause 7, a generic ICT trust conceptual model is shown in Figure 8-1 to clarify architectural overview for trust provisioning for ICT infrastructures. The model comprises three different domains vertically (i.e., social, cyber and physical domains) and three different horizontal components (i.e., humans & objects, networking & environment and data). In addition, there are multiple service domains for supporting a multiplicity of applications. This model intends to illustrate the complex relationships and required roles for trust provisioning between and across domains which are associated with an individual entity of ICT infrastructures and services.

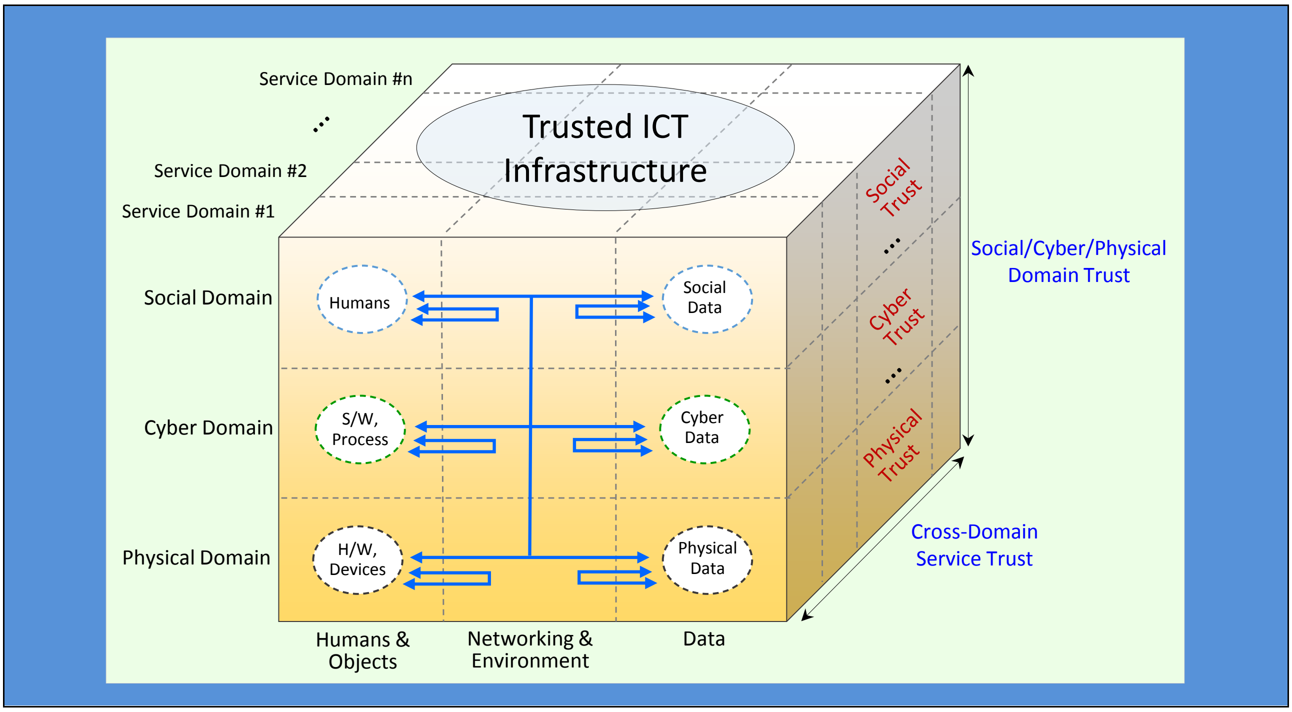


Figure 8-1 – A generic ICT trust conceptual model

Physical trust

A physical domain contains a huge number of objects (i.e., H/W or device) including sensors, actuators, mobile terminals, which generate data by using sensing technologies to sense physical objects and their behaviours within their environments (e.g., temperature, pressure, etc.). Collecting secure and reliable data from physical objects is the first step to provide trustworthy ICT services and applications because the propagation and process of false data will cause service degradation and waste system resources.

In order to detect trust problems in the physical domain such as injections of obstructive signals, malfunctions of systems, shutdowns or accidents, the operations of the physical objects and their data must be examined. Since many data are created from constrained devices, lightweight trust mechanisms are needed for data processing trust (e.g., efficiency, accuracy, reliability, etc.).

Cyber trust

A cyber domain includes virtual objects such as software agents, services and applications working over computing, storage and networking components. These virtual objects are seamlessly interconnected and cooperated for data coding, transmission, fusion, mining and analysing to provide information and knowledge to humans independent of location in fixed/mobile environments.

In order to safely cooperate between virtual objects, they have to distinguish malicious and non-malicious objects. One way to resolve this challenge is to evaluate the trust with their specific goal to decide which virtual objects to cooperate with. On the other hand, when huge amount of data is collected in the cyber domain, they should be processed and analysed accurately and transparently.

Data should be also transmitted and communicated in a reliable way via networking systems. Existing advances in networking and communications can be applied in order to achieve data transmission and communication trust. In particular, the trustworthy networking and communication protocols can support heterogeneous and specific networking contexts.

Social trust

Social networks are popular for sharing information and knowledge. Trust is an important feature in social networks because it relies on the level of trust that users have with each other, as well as with the service provider. Social trust actually depends on the behaviour and interactions of humans in the social networks. If humans fail to build trust, then they may not wish to share their experience and knowledge with others because of anxiety that their knowledge and privacy will be misused.

Social-Cyber-Physical domain trust

In the ICT infrastructure, there are interactions among the social, cyber and physical objects, as well as data transmission between them. Actually, the objects in the physical and cyber domain interoperate closely with each other and form a system organization around its user (human) in the social domain. Human interactions with cyber-physical objects should be performed in a trustworthy way.

Furthermore, because most smart devices are human-related or human-carried devices, the social relationships between humans can spread through their devices. To define and manage trust among physical, cyber and social domains, appropriate trust models for the interactions among social, information and communication networks are required while taking into account the severe resource constraints, and dynamics. Trust evaluation and trust management are especially challenging issues in the social-cyber-physical domain trust.

Cross-domain service trust

Trust management is service and domain specific, and it may be desirable to combine features from different trust management systems for developing cross-service trust management which is able to cover social-cyber-physical trust relationships between different service domains.

To disseminate trust information from one service domain to another service domain, a trust service brokering mechanism can be used for efficient, effective and suitable trust dissemination.

8.2 Trust Architectural Framework

Based on the generic ICT trust conceptual model, an architectural framework for strengthening trust in the ICT infrastructure is presented in Figure 8-2. It consists of four major parts as follows.

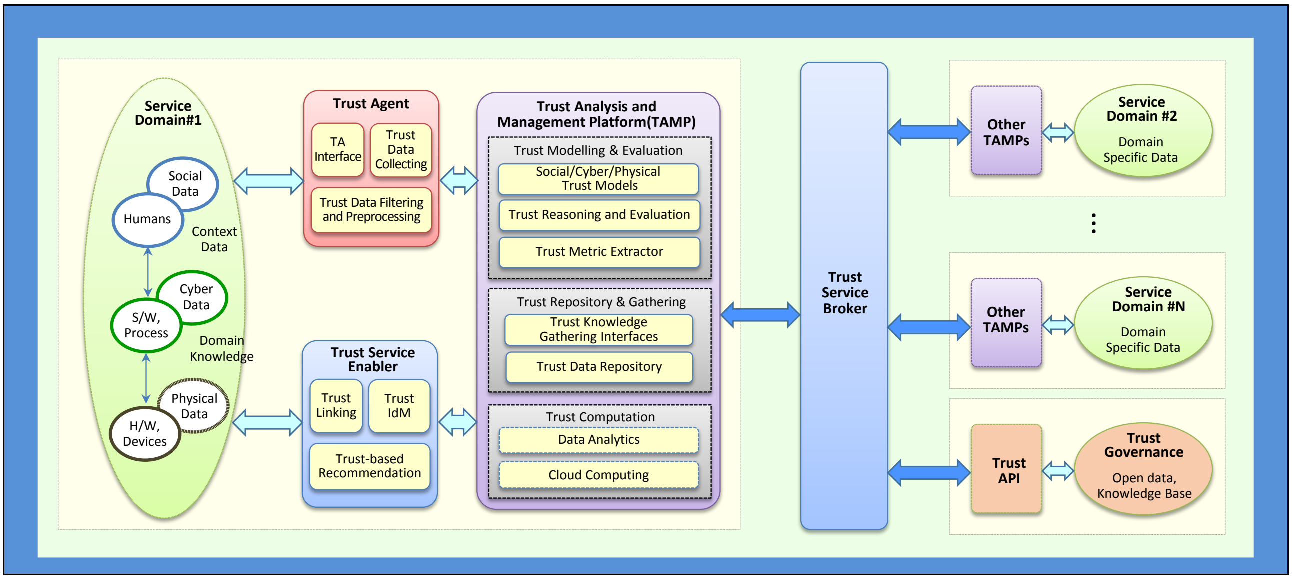


Figure 8-2 – An architectural framework for trust provisioning for ICT infrastructure

8.2.1 Trust Agent (TA)

TA is used to collect trust-related data from the social-cyber-physical environments with the following modules.

– **TA Interface**: TA provides lightweight interfaces to collect trust-related data from various types of objects. Furthermore, TA interfaces need to be easily connected to existing platforms and devices in order to extract the required data.

– **Trust Data Collection**: This module is responsible for gathering the data required for evaluating a trust level of an object. The Trust Analysis and Management Platform identifies the required trust metrics for the object and informs to this module.

– **Trust Data Filtering and Pre-processing**: This module is used to refine trust data sets without including other data that can be repetitive, irrelevant or even sensitive for trust evaluation.

8.2.2 Trust Analysis and Management Platform (TAMP)

TAMP is used for modelling, reasoning and managing trust data collected from TAs to check whether social-cyber-physical objects satisfy certain trust criteria.

– **Trust Modelling**: A trust model is used to specify, annotate and build trust relationships between objects for the purpose of reasoning trust data. Trust modelling is social-cyber-physical and service domain-specific, and there are social, cyber and physical trust models to define a trust model for each domain in the ICT infrastructure. According to its domain and a particular service domain, a suitable trust model is selected and applied for trust modelling. The trust-related data collected from TAs can be transformed to structured and annotated formats by using semantic and ontology technologies through this trust modelling module.

– **Trust Reasoning and Evaluation**: Trust evaluation is used to analyse and assess trust levels based on the trust model. There are various types of reasoning methods which depend on the social-cyber-physical domains, and a proper reasoning method will be chosen for the specific object. For example, policy-based trust reasoning makes a binary decision according to which an object is trusted or not. Because trust status could change with time and circumstantial context, a trust reasoning method must handle such dynamics of trust.

– **Trust Metric Extractor**: The trust metric extractor recognizes trust characteristics, accounts for factors influencing trust and determines proper trust metrics for the trust modelling and reasoning by analysing the metadata or semantic ontologies.

- **Trust Knowledge Gathering Interface:** This module is used to gather related trust knowledge regarding on object's trust aspects from related service domains via the Trust Service Broker.
- **Trust Data Repository**: The trust data including operations of objects and the history of interactions between objects can be maintained in the trust data repository. For trust evaluation, the necessary data will be loaded from this repository to the computation module.
- **Trust Computation**: This module is used for data processing for trust evaluation. Trust computation happens when the state of an object is changed or an interaction occurs between objects. To process a large amount of data related to trust evaluation, it can adopt data analytics and cloud computing technologies for calculation of the trust level of objects according to the change of the trust state of objects based on direct observation.

8.2.3 Trust Service Enabler (TSE)

TSE is used to provide trust knowledge of social-cyber-physical objects for a service based on the ICT infrastructure. It also provides trust-adapting capabilities to enable effective and efficient adaptation of trust knowledge to services.

- **Trust Linking**: Trust linking is a module capable of creating a link between social-cyber-physical objects based on trust metrics.
- **Trust IdM**: The identity management (IdM) can be used to manage digital identification/authentication of social-cyber-physical objects. Trust IdM assures the identity of trustworthy objects and support trust-based services.
- **Trust-based Recommendation**: This module provides recommendations to other objects. This module aims at providing a recommendation for selecting a suitable object that meets the required level of trust.

8.2.4 Trust Service Broker (TSB)

An object has a number of trust aspects which are related to other service domains in general. For instance, a human may have different trust levels at home, office, bank, social communities, etc. Each service domain has an effective trust evaluation mechanism specialized to analyse the domain-specific trust-related data. TSB provides a brokering service to share and disseminate domain-specific trust knowledge across service domains. TSB also provides a brokering service from trust governance information through trust API. When various kinds of trust aspects of a certain object are needed to investigate and judge their multifaceted trustworthiness, TAMP can gather an object's trust knowledge of other service domains from TSB and evaluate the whole trust knowledge to determine the object's multifaceted trustworthiness.

9 Trust based ICT Service Models

Today, it is known that almost everything can get hacked. If someone is going to get our data, tools like encryption and tokenization of that data become important defence methods. Any users including enterprises needs to follow some simple best practices to protect themselves online. Therefore, many business opportunities may exist if we further consider trust.

Trust based new ICT service models are a good positioning that builds trust with ICT service users by enabling them to control and leverage their own personal data. In doing so, trust based ICT service models give ICT service providers a sustainable business strategy for disrupting current ICT "Big Data primes" as well as delivering a permission-based personal data pipeline and services. A trust based ICT service model is a "game-changing" disruptive strategy that enables firms using big data to provide incremental trust improvements to existing big data deployment. To exploit customer data more comprehensively, businesses must develop a much greater level of trust with their customers. The primary concern is to overcome the gap between the personal controllability of privacy and business benefits of ICT services in terms of human and service related trust.

This clause firstly discusses some mistrust drivers in current ICT environments. Then, it presents a framework for analysing trust based ICT service models on new market disruption and symmetric ICT environment based on a new market disruptive innovation model.

9.1 Mistrust in current ICT environments

There are some mistrust drivers in current ICT environments:

- **Privacy infringements and errors**: The endless supply of so-called big brother stories is slowly shifting people's views on privacy and personal data, making them more open to tracking blockers and privacy products. Government agencies' programs used to collect ICT users' materials, including searches, the content of emails, file transfers, instant messages, and live chats. This puts the "Safe Harbor" agreement with the EU at risk [b-EU-Safeharbor]. In a company level, corporate annexation of consumer rights can be as easy as a new sentence in a company's privacy policy.
- **Security breaches**: The growing regularity of news reports about online security breaches is likely to lead a higher proportion of the population to change their behaviours. Consumers are now looking for improved security. It provides richer opportunities for security and privacy players.
- **Government mass surveillance**: A surveillance software provides users worldwide with the tangible evidence that comprehensive, population-wide surveillance is systemic in many countries. The surveillance covers every medium, and has been almost totally outsourced to a dozen of ICT major service providers.

The result of 'mistrust' is the "asymmetric ICT environment" as follows:

- **Information asymmetries**: Firms have an overload of user information, but consumers suffer from information scarcity in terms of their own data.
- **Solution asymmetries**: Firms have sophisticated analytics for optimizing customer lifetime value, but consumers have no analytics for minimizing vendor lifetime cost.
- **Control asymmetries**: Consumers are comparatively powerless to control the collection and use of their personal data. In some cases, firms have full control on personal data which firms have.

NOTE – Appendix III describes theoretical and industrial backgrounds about trust based ICT service models.

9.2 A framework for analysing a trust based ICT service model

A trust based ICT service model is a positional strategy building trust not only with consumers by defending their social economy and by enabling their control of their own devices and data, but also making ecosystem with business partners by defending their sharing economy and by enabling creation of their products and services. In doing so, trust gives a new business strategy for disrupting the legacy economy and delivers a more high-quality, permission-based data pipeline and profitable services with trust attributes (e.g., integrity, ability, benevolence, reliability, and helpfulness, etc.). This analysis framework is focusing on three major asymmetries:

- **Information asymmetries**: Companies have an overload of user information (mostly social and transaction data), but consumers suffer information scarcity in terms of their own data and that relating to companies. It is trust about product and service (product and service level).
- **Solution asymmetries**: Companies have sophisticated analytics for optimizing customer lifetime value, but consumers have no analytics for minimizing vendor lifetime cost, which is the flip side of customer lifetime value. It is trust about log, social and business transactions, etc. (software level).
- **Control asymmetries**: Consumers are comparatively powerless to control the collection of their data and the operating system (OS), but corporations have full control of data storage and OS which they provide. It is trust about data source, storage, network, and software **(software and network level)**.

Trust attributes of product & service, customer and process of ICT service models based on the theoretical background, new value chains of markets are as follows:

- **Product & Service**: Privacy, Safeness, Security, Convenience, Simplicity, etc.;

- **Customer & Market**: Satisfaction, Life cycle of service, Developer ecosystem, etc.;
- **Business model process** (infrastructure): Mobile, Social, Cloud, Data analytics, Interoperability, Standardization, etc.

With these backgrounds, this clause intends to categorize new market disruption into three platform types of products, market and software. In fact, on the road of disruptive innovation, the related researches are almost about the platform strategies and the meaning of platform business has been expanded from the products & services to market & software ecosystem. In these three types of platforms, there are rationalities specific for each platform as follows [b-Sandberg] and the rationalities are related to the trust attributes [b-Mayer, b-McKnight]:

- **Rationality of product platform** (Integrity, ability and functionality): Modularity allows re-use and decreases complexity, standardization of platform combined with customization allows economies of scale and scope. The overarching goal is product efficiency and functionality;
- **Rationality of market platform** (Integrity, ability and benevolence): Re-use of infrastructure allows efficient transactions. Focus on market efficiency and transaction costs. Competitive advantages are achieved by attracting a large number of providers and customers through strategic decisions;
- **Rationality of software ecosystem platform** (Integrity, reliability and helpfulness): Shared functionality in codebase allows specialization, distribution of development costs and access to users. Commonality achieved through shared platform rather than application area.

Based on disruptive model theory and ICT symmetry following Table 9-1 is presented, and detailed examples are shown in Appendix III.

Table 9-1 – A framework for analysing a trust based ICT service model

Types of Symmetric ICT	New Market Disruptions (platform type)		
	Products & Services (Product platform)	Customer & market (Market platform)	Business model Process (Software platform)
Information Symmetries	Ability	Ability	Reliability
Solution Symmetries	Functionality	Benevolence	Helpfulness
Control Symmetries	Integrity	Integrity	Integrity

10 Use cases of Trust Provisioning for ICT infrastructures and services

This clause discusses six use cases of trust provisioning for ICT infrastructures and services. The use cases can be shown in wide range of service domains requiring trust. Although each use case has different purposes and consists of different actors, it is true that trust can play an important role of mitigating risks of violation of security as well as privacy and mediating interactions among actors.

Use case #1: Trustworthy smart home service

Trustworthy smart home service is a service to monitor, control and manage home appliances and smart devices by using trust information. This use case focuses on a trust provisioning at home. The home gateway collects personal data from the household devices. After aggregating the personal data, the home gateway sends data to the remote service platform and service platform generates trust information from data and provides trust information to service providers for managing home appliances and other devices.

Use case #2: Trustworthy smart office service

This use case allows users utilizing various facilities in office based on the trust level of users. For the trust management, various properties like social/business relationship and membership of each user can be considered to determine each user’s trust level. Smart office provider offers office facilities to users based on the users’ trust level estimated by trust management platform.

Use case #3: Trustworthy document sharing service

This use case focuses on sharing the document among co-workers using social trust value among them. Trust management platform estimates social trust values between co-workers by using the collected social data from intermediate entities (e.g., smartphone) of co-workers and then, these values will be used to judge whether the receiver has enough qualification to get the document or not. If the document receiver has enough qualification to get the document, an entity transfers the document to receiver.

Use case #4: Device selection for data transmission

This use case focuses on selecting the device for data transmission in multi-hop Device-to-Device (D2D) environment using social trust value among devices. Trust management platform calculates the trust value using the collected social data from intermediate entities of users and then, these trust value will be used to judge whether that device has enough reliability to receive and transmit data or not.

Use case #5: Trustworthy car sharing service

The car sharing service offers a new business model for automobile transportation. This use case is particularly designed for two user groups – first of all, people who live in cities but do not drive a car every day, and secondly tourists who travel in cities but do not bring their car. Thus, people who need a car at short period can take this alternative without purchasing it. Trust management platform can provide the evaluated trust levels of users or cars by using collected data of cars as well as users who use the car sharing service.

Use case #6: Trustworthy used car transaction service

This use case focuses on buying a used car in trustworthy procedure. Buying a used car involves high levels of uncertainty and risk because there exists inevitable distrust in used car transactions between entities. Trust management platform can play an important role in mediating entities who participate in a used vehicle market by sharing trustworthy information between entities in a transaction. Trust management platform evaluates each actor's trust by collected data from various sources such as insurance company, public organization, social network services, and vehicle itself.

NOTE – The detail features and operations of each use case are described in Appendix IV.

Table 10-1 summarizes six use cases discussed in Appendix IV. In Table 10-1, it is observed that the uncertainty and risks can be mitigated by providing trust information.

Table 10-1 – Summary of use cases

No	Use case	Purpose	Method	Actors
1	Trustworthy smart home service	Managing home facilities	Trustworthy home-related data → Providing personal information to service platform	– User – Service provider – Service platform – Home gateway – Home appliance
2	Trustworthy smart office service	Managing office facilities	Trust level of users → Determining facility usage right	– User – Smart office – Smart office provider – Trust mgmt. platform
3	Trustworthy document sharing service	Sharing document with appropriate users	Trust level between users → Determining authority of accessing document	– User A – A's Device – User B – B' device – Trust mgmt. platform

Table 10-1 – Summary of use cases *(end)*

No	Use case	Purpose	Method	Actors
4	Device selection for data transmission	Selecting trustful device for D2D communication	Trust level between devices → Selecting appropriate device for transmission	– User A – A's device – User B – B's device – Trust mgmt. platform
5	Trustworthy car sharing service	Promoting trustworthy car sharing	Trustworthy data about a shared car and users' data → Providing an information of shared car and its user	– User A – A' device – Sensor attached in sharing car – Service platform – Service provider
6	Trustworthy used car transaction service	Mediating transparent used car transaction	Trustworthy data about a used car → Providing transparent car history information	– Seller (User A) – Seller's car – Service broker – Trust mgmt. platform – Buyer (User B)

11 Strategies for future standardization on trust

Until now, a number of standards focusing on network security and cybersecurity technologies have been developed in various standardization bodies including Internet Engineering Task Force (IETF). The scope of these standards needs to be expanded to take into consideration trust issues in future ICT infrastructures. There are a few preliminary activities taking place, for instance in Online Trust Alliance (OTA) and Trusted Computing Group (TCG). However, as existing research and standardization activities on trust are still limited to social trust between humans, trust relationships between humans and objects as well as across domains of social-cyber-physical domains should also be taken into account for trustworthy autonomous networking and services.

Based on this, we need to first find various use cases considering user confidence, usability and reliability in ICT ecosystems for new business models which reflect sharing economy. Then, a framework for trust provisioning including requirements and architectures should be urgently specified in relation to the relevant standards. In addition, global collaborations with related SDOs are required to further stimulate trust standardization activities.

More specifically, the following key items are identified as future work for standardization on trust.

- **Overview of trust in ICT**

It aims to provide a clear understanding of trust from different perspectives and identify key differentiations compared to security and privacy. It also highlights the importance of trust in future ICT infrastructures towards knowledge societies.

- **Service scenarios and capabilities**

From various use cases analysis, considering sharing economy, it is necessary to develop service scenarios for trust provisioning and define required capabilities to support trust in ICT.

- **Requirements for trust provisioning**

From key challenges and technical issues, it is necessary to specify detailed requirements in terms of different viewpoints and various stakeholders.

- **Architectural framework and functional architectures**

It targets to identify core functions for future trusted ICT infrastructures and develop architectural models, including detailed functional architectures. Relevant trust models should be based on key concepts of trust domains, levels of trust, TLA and trust index, taking into account social, cyber and physical domains.

- **Technical solutions for trust provisioning**

It covers some methodologies for specifying and measuring trust metrics. It also needs to develop protocol specifications for trust provisioning, and mechanisms for data gathering, filtering, analytics, reasoning and decision making.

- **Trust provisioning for convergence applications**

For trust provisioning, it is necessary to develop specific technical solutions applicable to convergence applications (e.g., smart grid, healthcare, intelligent transport systems, and logistics, etc.).

- **Trust provisioning for cloud computing**

For trust provisioning, it is necessary to develop specific technical solutions applicable to the processing and analysis of the large amount of data through cloud computing.

Additionally, we need to incorporate trust issue into related Study Groups' (SGs) activities in ITU-T.

– **SG17**: As trust is tightly associated with security issues, a liaison with SG17 activities on security matters is **required**.

– **SG20**: As the **recently** established SG20 is targeting IoT applications, services and platforms as well as smart cities infrastructure, SG20 should consider trust in IoT.

– **Others**: Depending on specific topics, a collaborative work is needed, for instance, the identification issue with SG2, trust in financial services with Focus Group on Digital Financial Services.

Finally, we need to closely collaborate with other SDOs and forums listed below.

– **Existing security solutions**: IETF, W3C

– **IoT**: oneM2M, FI-WARE, Open Connectivity Foundation, AllSeen Alliance

– **Cloud Computing**: TCG, Cloud Security Alliance

– **Other groups**: OTA

ITU-T has a responsibility to get a consensus for trust and knowledge information infrastructures. ITU-T may have a leadership to introduce future knowledge societies by getting global consensus of future ICT infrastructures. Standards for future all the industries as well as ICT industries are critical to realize knowledge eco-societies.

Finally, ITU-T may get a chance to lead future knowledge societies in terms of standardization. As a top level of formal standard body, ITU-T may initiate new work methods for future knowledge information infrastructures including pre-standardization and conceptual framework. Also, ITU-T may have a leadership to collaborate with private sectors and academia which are outside of ITU-T.

Appendix I
Trust definitions

This appendix provides various trust definitions from different viewpoints as shown in Table I.1.

Table I.1 – Trust definitions

	Definitions	References
Lexical-semantic	**Reliance** on the integrity, strength, ability, surety, etc., of a person or thing; **confidence**	Dictionary
	Reliance on and confidence in the truth, worth, reliability, etc., of a person or thing; **faith**	Dictionary
General aspects	**Trust** is a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates.	[b-Sherchan]
Psychology	**Trust** is considered to be a psychological state of the individual, where the trustor risks being vulnerable to the trustee based on positive expectations of the trustee's intentions or behaviour.	
	Trust is considered to have three aspects: cognitive, emotive, and behavioural.	
Sociology	**Trust** is defined as "a bet about the future contingent actions of the trustee". This bet, or expectation, is considered to be trust only if it has some consequence upon the action of the person who makes the bet (i.e., trustor).	
	Trust is considered from two viewpoints: individual and societal. At individual level, similar to the perspective from psychology, the vulnerability of the trustor is a major factor.	
	Trust is differentiated from cooperation in the presence of assurance (a third party overseeing the interaction and providing sanctions in case of misbehaviour). However, cooperation in the presence of the shadow of the future (i.e., fear of future actions by the other party) is considered to be trust. In this respect, social trust has only two facets, cognitive and behavioural, with the emotive aspect building over time as trust increases between two individuals.	
	At societal level, **trust** is considered to be a property of social groups and is represented by a collective psychological state of the group. **Social trust** implies that members of a social group act according to the expectation that other members of the group are also trustworthy and expect trust from other group members. Thus, at societal level, social trust also has the institutional or system aspect of trust.	
Computer Science	Trust in computer science in general can be classified into two broad categories: **"user"** and **"system"**. The notion of **"user" trust** is derived from psychology and sociology, with a standard definition as "a subjective expectation an entity has about another's future behaviour".	
	"System" trust is "the expectation that a device or system will faithfully behave in a particular manner to fulfil its intended purpose".	
	System trust is "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited"	[b-uTRUSTit]
Specific context (Trust in IoT)	**Interpersonal trust** is a relationship between a trustor and a trustee arising in uncertain and (potentially) risky situations, affecting trustors behaviour, emotion and cognition. It is evoked by the perception of trustworthy characteristics (such as ability, benevolence and integrity) of the trustee.	
	In the context of IoT, **trust** is reliance on the integrity, ability or character of an entity. **Trust** can be further explained in terms of confidence in the truth or worth of an entity.	
	Trust is an internal status of the user that may possibly become in the users behaviour as well as in the users' affect and cognition and therefore is partly accessible. Furthermore, **trust** is evoked by trustworthiness characteristics of the technology.	
	Trust is "a user's confidence in an entity's reliability, including user's acceptance of vulnerability in a potentially risky situation".	

Appendix II
Standardization Activities on Trust in related SDOs

This appendix introduces standardization activities on trust in related SDOs such as IETF, OTA and TCG.

1 Activities in Internet Engineering Task Force (IETF) for Internet Trust

To discuss a trust and knowledge ICT infrastructure, it is required to review a data lifecycle – its production, process and consumption. Therefore, it is important to deal with trust issues focusing on Internet. For this purpose, this clause introduces IETF's activities on trust to identify trends and main issues from perspective of Internet.

In IETF, currently 11 working groups (WG) are dealing with issues on trust.

– DNSOP (Domain Name System Operations)

– DNSSEC (Domain Name System Security Extensions)

– DNSExt (Domain Name System Extensions)

– NEA (Network Endpoint Assessment)

– OAUTH (Web Authorization Protocol)

– HTTPbis (HyperText Transfer Protocol)

– WPKOPS (Web Public Key Infrastructure Operations)

– ECRIT (Emergency Context Resolution with Internet Technologies)

– SDNRG (Software Defined Networking Research Group)

– ICNRG (Information Centric Networking Research Group)\

– SIDR (Secure Inter-Domain Routing)

Figure II.1 shows individual WGs and its related OSI layer.

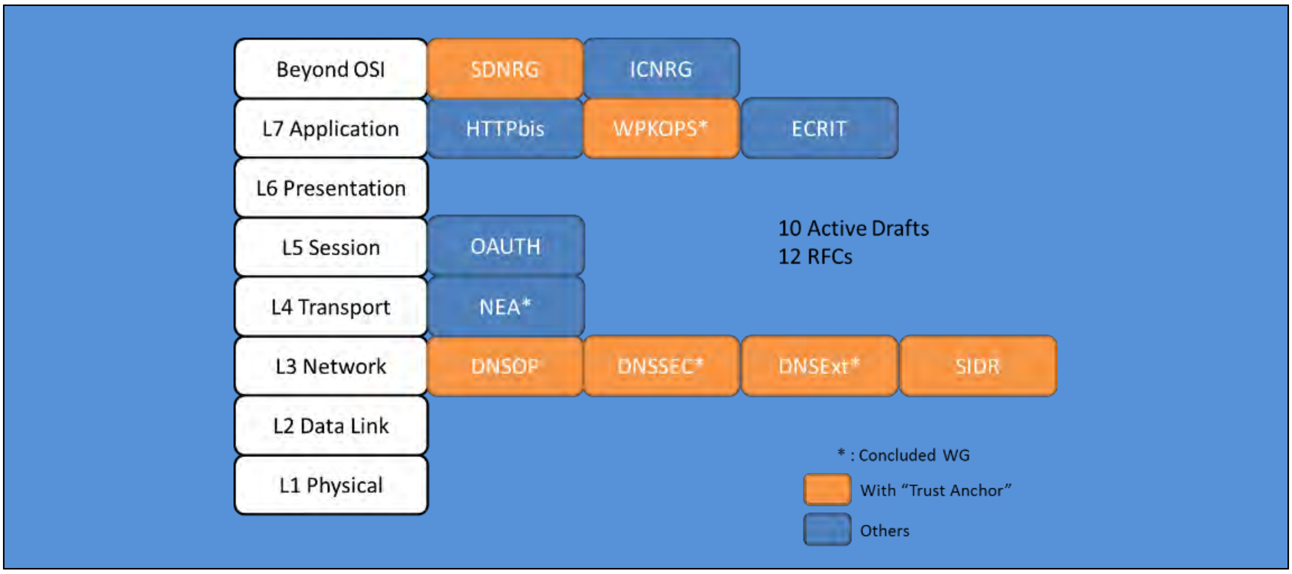


Figure II.1 – Classification of IETF WG based on OSI Layer

Figure II.2 shows a brief categorization of WGs into trust technical issues.

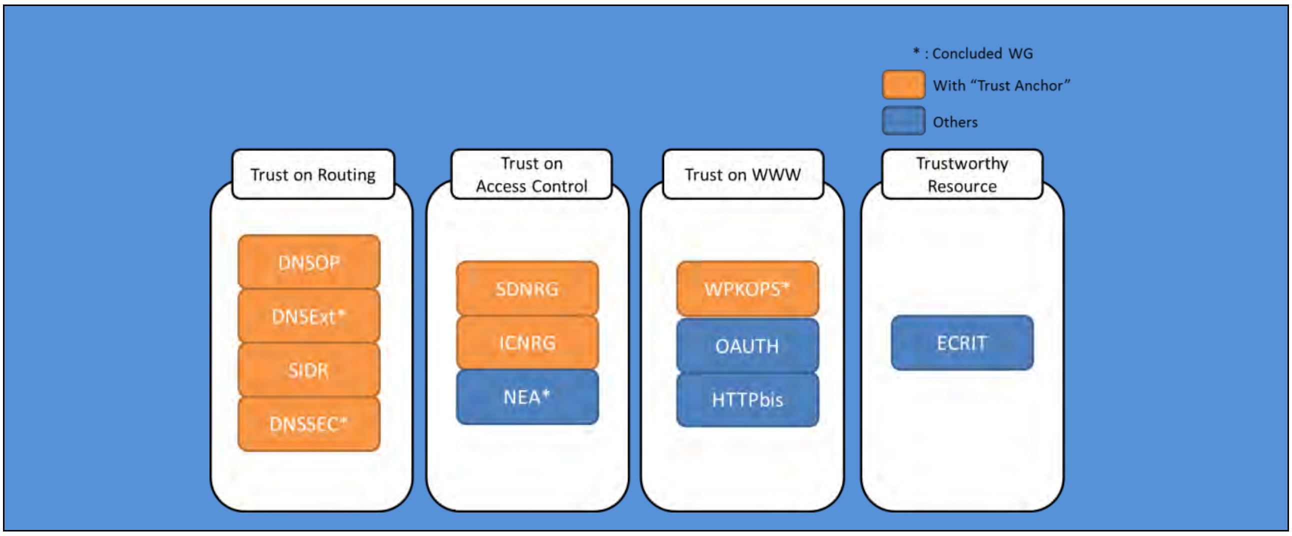


Figure II.2 – Trust domains of IETF WGs

2 Activities in Online Trust Alliance (OTA) for IoT

OTA is a non-profit organization with the mission to enhance online trust and address IoT risks comprehensively. The framework presents guidelines for IoT manufacturers, developers and retailers to follow when designing, creating, adapting and marketing connected devices in two key categories: home automation and consumer health and fitness wearables.

Through extensive research, this taskforce concluded that the safety and reliability of any IoT devices, Apps or services depend equally on security and privacy, as well as a third, often overlooked component: sustainability.

Although the IoT framework of OTA has identified various requirements, most of them can be seen as reinterpretation of traditional security and privacy issues. Therefore, it is noticed that trust in OTA includes more broad range of scope covering security and privacy as well as regulatory issues [b-Gilson, b-OTA-2015].

3 Activities in Trusted Computing Group (TCG) for Interoperable Trusted Computing Platforms

TCG is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.

TCG technologies do not provide an immediate solution to all IoT device and service security needs, but they enable existing and new IoT solutions to be fundamentally far more robust than today's state-of the art.

Solutions developed by TCG includes authentication, cloud security, data protection, IoT, mobile security and end-to-end security. Similar to OTA, TCG has also focused on various solutions from existing security and privacy issues while taking into account additional concepts of trust.

TCG has provided the following concepts for trust related terminologies in the architecture's guide for cyber security [b-TCG 2013, b-TCG 2015].

- Trusted Network Connect (TNC)

TCG’s TNC network security architecture and open standards help businesses create and enforce security policies as well as facilitating communication between security systems. Using TNC standards, network managers gain better visibility into who and what is on their network, and whether devices remain compliant with policies. More than two dozen vendors of commercial and open source products support TNC standards in their products.

- Self-Encrypting Drive (SED)

Self-Encrypting Drives silently and automatically encrypt all user and system data, making sure this information doesn’t fall into the wrong hands if the device or drive gets lost. Such drives may also be remotely wiped if they’re lost or stolen.

- Trusted Platform Module (TPM)

The Trusted Platform Module is a hardware security component built into a computing device that provides a hardware root of trust for user and device identity, network access, data protection, and more. TPMs are built into more than half a billion end systems, including many laptops and mobile devices.

Appendix III
Backgrounds for Trust based ICT Service models

This appendix describes some theoretical and industrial backgrounds about a framework for analysing trust based ICT service models in business perspective.

Many firms already see and manage high volumes of security incidents, breaches, malware, and hackers and early security offerings tended to focus on the network (e.g., WAN and Internet service security), but such managed security services are expanding now into other areas like Internet data, mobile, web, and cloud-based ICT, IoT services and business models.

Especially, people are connected with each other and with objects as well, and expect always-on connectivity. It is expected to see 'trusted ICT infrastructures from all parts of the ICT ecosystem, not only devices and networks, but also applications and services. The EU (European Union)'s focus on Trust & Security in "Europe 2020 Strategy," researches about 'trust' in projects of FP7's uTRUSTit, ABC4Trust, and USA's application of 'Trust & Security' on the industry level (NIST & DARPA), research about trust technology in projects like Smart America, and HACMS (High-Assurance Cyber Military Systems) are verifying the importance of the trust and security in the emerging business models in e-commerce, Social Network Service (SNS), IoT services and so on.

In business area, some leading firms also are pursuing the same way in financial technology area. Despite of such efforts of leading companies, recent big data based business models are not trusted by personal consumers. There is 'mistrust' in many ICT service domains. Some companies launched permission-based business models to use personal data, a more sustainable strategy to put consumers in control of their personal data. It is a kind of disruptive innovation in the new market.

Human/service-related trust is beliefs that the other party has suitable attributes for performing as expected in a specific situation irrespective of the ability to monitor or control that other party [b-Mayer]. It composed to three attributes of integrity, ability and benevolence. The integrity refers to the beliefs that the trustee adheres to a set of principles that the trustor finds acceptable. The ability is the beliefs that the trustee has the group of ability, skills and characteristics that enable them to have influence within some specific domain [b-Mayer, b-McKnight 2002]. Lastly, the benevolence is the beliefs that the trustee will want to do good to the trustor, aside from an egocentric profit motive.

There are three innovation models to creating new-growth businesses: 1) sustaining innovation, 2) low-end disruption, and 3) new market disruption: [b-Christensen]

1) **Sustaining innovation model**: A sustaining innovation does not create new markets or value networks but rather only evolves existing ones with better value, allowing the firms within to compete against each other's sustaining improvements.
   - **Disruptive innovation model**: An innovation that creates a new market by applying a different set of values, which ultimately (and unexpectedly) overtakes an existing market.
2) **Low-end disruption**: targets customers who do not need the full performance valued by customers at the high end of the market.
3) **New market disruption**: targets customers who have needs that were previously unserved by existing incumbents.

The characteristics of each innovation models are presented in Table III.1.

Table III.1 – Three approaches to creating new-growth businesses

Dimension	Sustaining innovations	Low-end disruption	New market disruption
Targeted performance of the product or service	Performance improvement in attributes most valued by the industry's most demanding customers. These improvements may be incremental or break-through in character.	Performance that is good enough along the traditional metrics of performance at the low end of the mainstream market.	Lower performance in "traditional" attributes, but improved performance in new attributes - typically simplicity and convenience.
Targeted customer or market application	The most attractive (i.e., profitable) customers in the mainstream markets who are willing to pay for improved performance.	Over-served customers in the low end of the mainstream market.	Targets non-consumption: customers who historically lacked the money or skill to buy and use the product.
Impact on the required business model (processes and cost structure)	Improves or maintains profit margins by exploiting the existing processes and cost structure, and making better use of current competitive advantages	Utilizes a new operating or financial approach or both, a different combination of lower gross profit margins and higher asset utilization that can earn attractive returns at the discount prices required to win business at the low end of the market.	Business model must make money at lower price per unit sold, and at unit production volumes that initially will be small. Gross margin dollars per unit sold will be significantly lower.

Several studies have examined the conditions or rules of the platform and its effects on competitive strategy in a variety of industrial contexts. Recently, it is suggested that digitizing and its affordance of convergence is one of the primary drivers for platform change [b-Yoo 2012]. They note "from one perspective, in order to harness the convergence and generativity made possible by pervasive digital technology, firms now innovate by creating platforms rather than single products." The penetration of digital technologies into products and services and their success as witnessed by the history of existing online markets has heightened the role of platform strategies in firms' innovation activities [b-Yoo 2010, b-Tilson 2010]. Also, [b-Sandberg] complements this understanding of platform evolution by analysing qualitative changes in platforms rules and architecture and how they relate to strategy (i.e., how the platform is positioned with regard to its use and production contexts).

More innovative firm tends to be platform providers in order to harness the convergence made possible by digital technology, firms innovate by creating platforms rather than single products [b-Yoo 2012]. The firm needs to source its products or services across multiple innovation domains (e.g., devices, networks, contents, and services) in order to increase its innovation complexity and diversity [b-Yoo 2010]. Platform evolution has been also explored in the context of market-based competition on two-sided markets [b-Eisenmann], and related concerns for strategy management [b-Gawer].

In Table III.2, an example of use case (or business model) analysis framework is shown.

Table III.2 – An example of use case analysis framework

Types of Symmetric ICT	New Market Disruptions		
	Products & Services	Customer & Market	Business model Process
Information Symmetries	Reputation service	Messaging service	Identity management as SaaS
Solution Symmetries	IoT device whose goal is efficiency and functionality	IoT based application service for specific market allowing efficiency and transaction cost	IoT PaaS, IoT server security as PaaS, IoT SaaS, IoT IaaS, etc. allowing shared functionality in codebase. Commonality can be achieved through shared platform.
Control Symmetries	Email, personal cloud	Universal platform	Personal cloud as SaaS, Cloud as IaaS, Security as SaaS, LBS as SaaS, M2M B2B

1) **Information symmetries**

- Targeted product and service
  - Reputation related services: provide privacy and reputation management for private individuals, their families and their businesses.
- Targeted customer and market
  - Messaging services: provides ephemeral messaging service (i.e., messages are deleted and disappeared after recipients read them).
- Business model process
  - Identity management as Software as a Service: provides simplified identification (or authentication) methods using various technologies (simple PIN code, one time password, etc.).

2) **Solution symmetries**

- Targeted product and service
  - Simple IoT device with integrity and interoperability
- Targeted customer
  - IoT based service applications allowing market efficiency and transaction costs by building two- or multi-sided market.
- Business model process
  - IoT platforms as Platform as a Service: provides the possibility to analyse and visualize the Internet of Things. It can be used to interconnect different devices over the Internet and can store a history of measured values and can display it with graphs, etc.
  - IoT server security as Platform as a Service: provides secure IoT device management servers, which are connected with many IoT devices, for maintenance and support operations.
  - Commonality can be achieved through shared software and network platform like big data analytics and cloud computing rather than application service area.

3) **Control symmetries**

- Targeted product and service
  - Email services: provides security and privacy email exchange methods using cryptographic technologies.
  - Personal cloud (e.g., cloud storage services): provides additional security mechanisms for authentication to help ensure users are protected against data or credential breaches.

- Targeted customer and market
  - Universal platform
- Business model process
  - Personal cloud as Software as a Service: provides personal cloud as SaaS to other companies for developing a solution to synchronize any data with any connected devices.
  - Cloud as Infrastructure as a Service: provides trusted cloud as IaaS to other companies which develop various applications on cloud.
  - Security as Software as a Service
  - LBS (Location Based Service) as Software as a Service: provides location based service to other companies as SaaS.
  - M2M B2B (Business-to-Business): provides the supply of connectivity for embedding in an enterprise's processes/service/products, even if the product ends up in the hands of a consumer.

Appendix IV
Use cases of trust provisioning for ICT infrastructures and services

This appendix describes the use cases of trust provisioning for ICT infrastructure, which can be shown in wide range of the trust domains. In this appendix, use cases on smart home, smart office, document sharing, device selection for data transmission, car sharing, and used car transaction services are introduced. Each use case describes following items:

– Description: describes its background including high level description and illustration;

– Actors: play a role in each use case;

– Detailed service flow: describes a service flow for a use case;

– Trust matrix: represents trust relationship between actors;

– Analysis: explains details about trust relationship in trust matrix.

1 Smart home service

1.1 Description

This use case is to manage connected devices at home. Trust-based smart home service is to enable users to monitor, control, and manage the home appliances and the devices remotely and safely at anywhere and anytime. For this service, it is important for users that trusted data collection, process, analysis, decision-making on the appliances and communication. Since the data, collected and generated at home contains personal life cycle information, trustworthiness is the key factor for users to adopt the service. The use case focuses on a trust provisioning at the home gateway that collects information from the electrical home network and communicates it to a system for aggregating and processing the data on the smart home service management platform. Services can then be developed from the collected data.

The home gateway performs an initial treatment of the data received from various sources (sensors, context) as follows:

– Aggregating and processing the collected data;

– Sending data to the remote service platform.

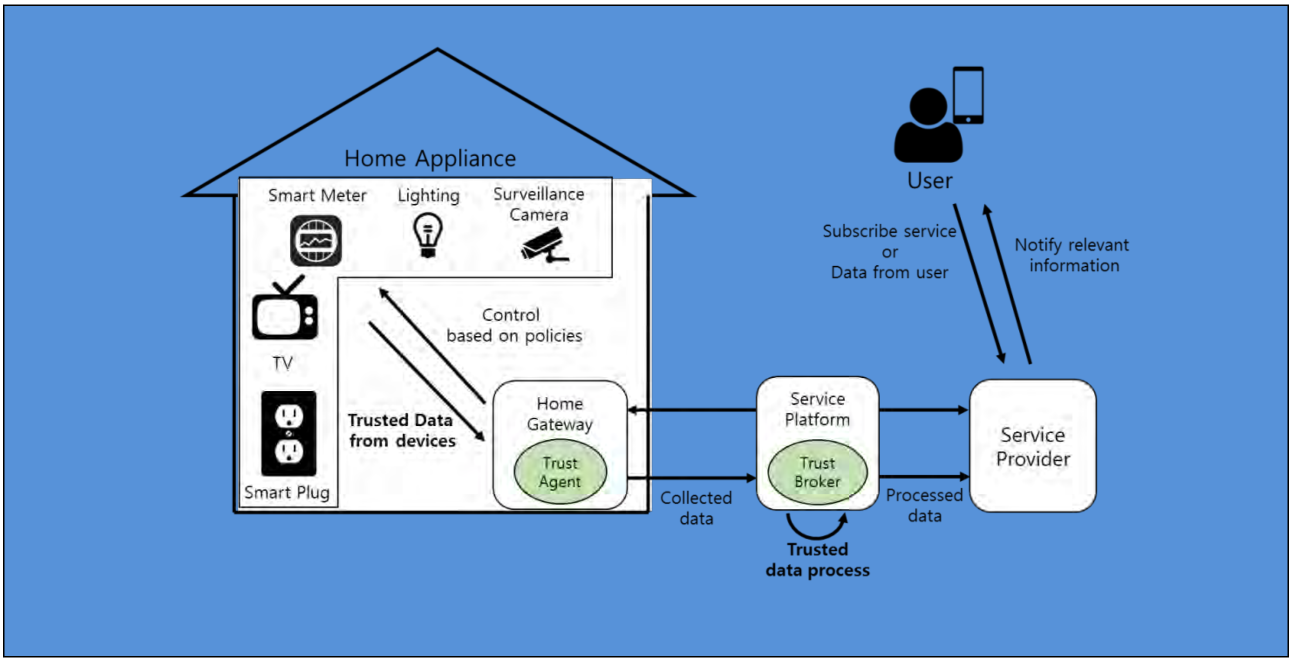


Figure IV.1: Smart home service high level illustration

1.2 Actors

- User: user who are able to control home appliance with terminal devices (e.g., laptop, smartphone, etc.).
- Home Appliance: various appliances from multiple vendors.
- Home Gateway: a device installed in the user's home and receives remote control commands from the management server.
- Service Platform: a service platform is in charge of providing services/common functionalities for applications to user.

1.3 Detailed service flow

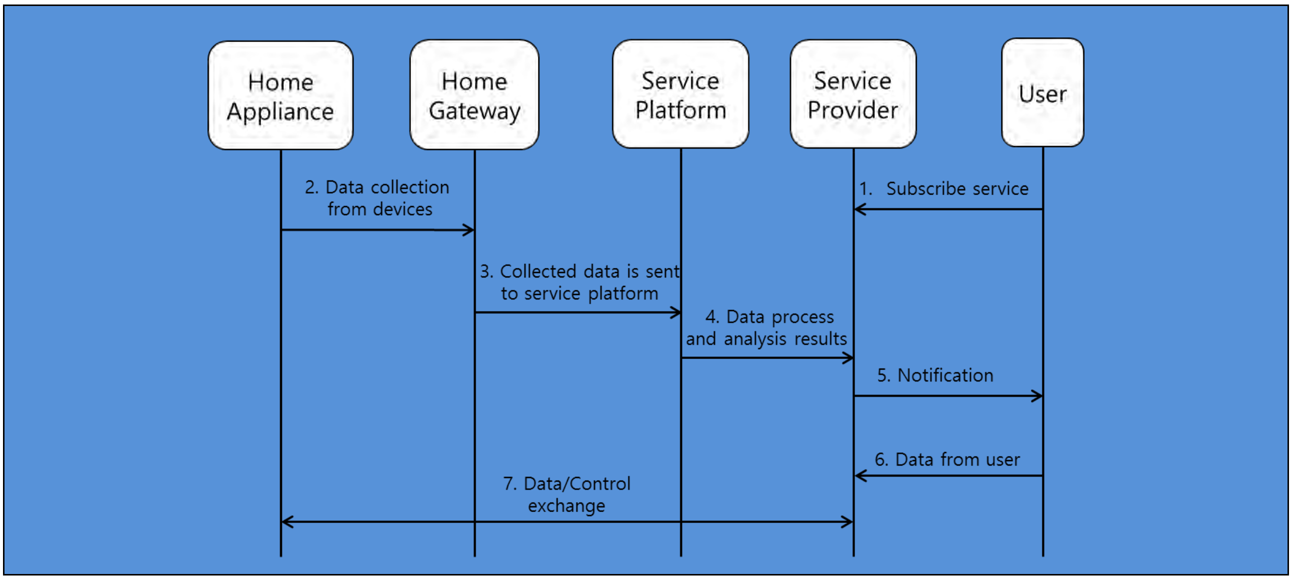


Figure IV.2: Smart home service flow

Detailed Flow Description

1) A user subscribes to a smart home service.

2) Data from multiple devices such as home appliances (smart meters, electric lightening, fridge, washing machine etc.) is collected. Data may include status of door lock, temperature, level of energy consumption and others.

3) Collected data is stored in the service platform and may be processed at home gateway. Based on polices, the home gateway sends control messages to devices.

4) Collected data may also be sent to service provider which contains the service platform for storage via communication network.

5) Notified information is available for processing. A service provider can process the information before sending to a user depending on subscription profile.

6) A user reacts to the shared /collected information and can send control message (e.g., to switch a home device such as light /appliance or washing machine).

7) Control is propagated back through different operator to appropriate home appliances(s).

1.4 Trust matrix

Trust matrix presents trust relationship among actors in this use case.

Table IV.1 – Trust matrix for smart home service

To From	Home Appliance	Home Gateway	Service Platform	Service Provider	User
Home Appliance	-	Trusted data collection and aggregation	-	-	-
Home Gateway	Trusted data collection and aggregation	-	Trusted data collection and aggregation Trusted data process and analysis	-	-
Service Platform	-	Trusted data process and analysis	-	Trustworthy application	-
Service Provider	-	-	Trustworthy application	-	Privacy
User	-	-	-	Privacy	-

1.5 Analysis

– Trusted data collection and aggregation

Transmitted data should be trustworthy from devices (home appliances) to home gateway and gateway to service platform. In flow #2, data from devices is collected in a gateway and service platform. When data is produced and transmitted to other entities, trustworthiness of data is required.

– Trusted data process and analysis

Information which is processed by home gateway and service platform should be trustworthy. In flow #3, collected data is processed and analysed in a gateway to decide extra actions depending on policies stored in the gateway. Also, the gateway can put additional data (e.g., location, time, etc.) to collected data in order for a service platform to get accurate conditions of each device at home. In flow #4, a service platform also can process and analyse data from the gateway to produce useful information to a user. Since the gateway and the service platform manipulate collected data, the trustworthiness of information (i.e., processed and analysed data) is required to be maintained in each process.

– Trustworthy application

In flow #5, application (service provider) notifies processed information to user depending on their subscription profile. The trustworthiness of application is recommended to be maintained in each process.

– Privacy

In flow #5, when smart home management system notifies some information to user, providing displayable event or control information to the end-user/consumer terminals (e.g., PC, mobile phone, TV screen, etc.) may be unintentionally exposed. Application (or service provider) utilizes user's data for big data process, and this may cause user privacy issue.

2 Smart office service

2.1 Description

In a trust-based smart office service, usage rights on various office facilities depend on each users' trust level. For example, it is assumed there are three kinds of user trust level - high, middle and low. For a user who has a high level of trust, he or she can read and write the cloud storage. However, a user who has middle level of trust can only read the documents in cloud storage. A user who has low level of trust has no right to access. Figure IV.3 shows an example of smart office service with different priority of users and different permission to office facilities. For the trust management, various properties like social/business relationship and membership can be considered to analyse user's trust level.

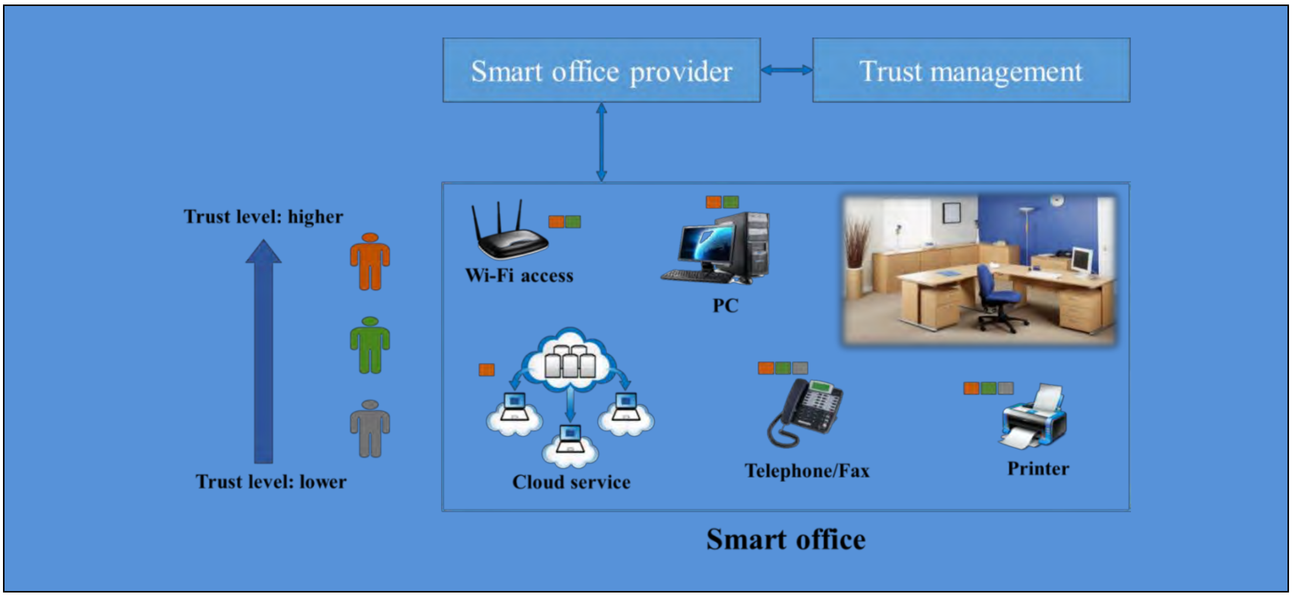


Figure IV.3 – Smart office service high level illustration

2.2 Actors

- User: users are able to control and access smart office devices and facilities by using their own devices or office devices (e.g., employer, employee, etc.).
- Smart office devices and facilities: connected devices and facilities in office (e.g., Wi-Fi access point, personal computer, telephone, printer, meeting room, canteen, etc.).
- Smart office provider: a smart office provider is in charge of providing common functionalities for smart office services. It is collecting the status of smart office devices and facilities. Based on user's trust level provided by trust management service, it permits appropriate usage right of them to users (e.g., building management service provider, service providers, etc.).
- Trust management service provider: a trust management service provider responses trust level and information request from smart office providers or service brokers.

2.3 Detailed service flow

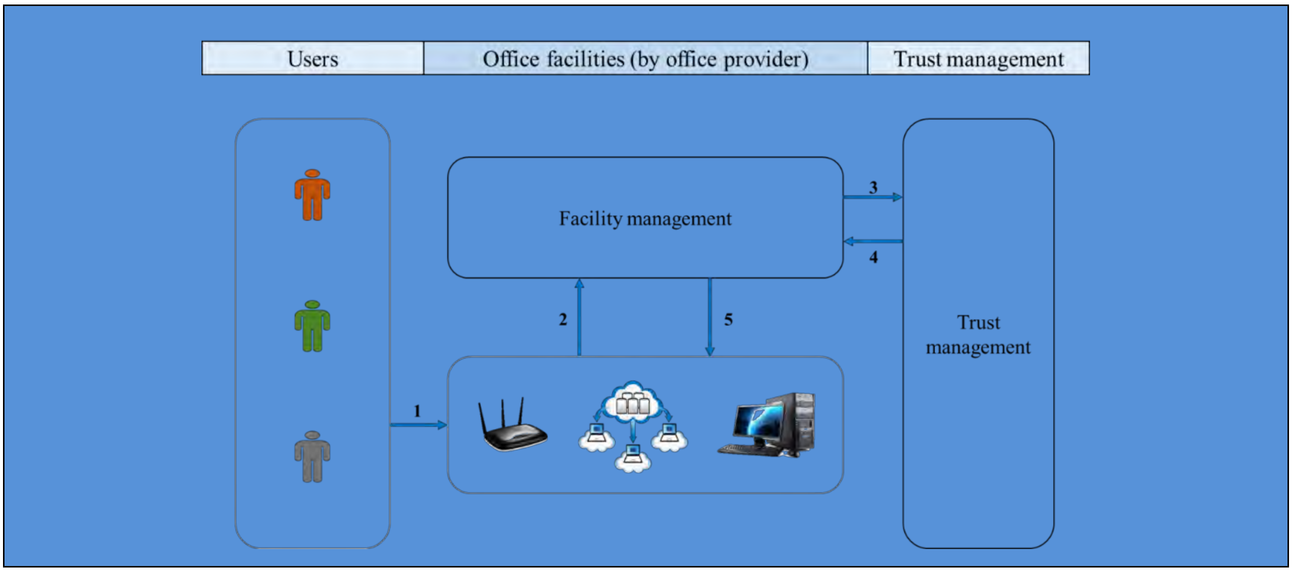


Figure IV.4 – Smart office service flow

Detailed Flow Description

1) Users request to use office facilities.

2) Office facilities request the validation of users and user's trust information.

3) Facility management requests user's information including trust level.

4) A trust management evaluates user's trust level after analysing user data gathered in physical and cyber ICT domain.

5) Based on the user's trust level, facility management decides the usage right on each facilities and functions for a user.

2.4 Trust matrix

Trust matrix presents trust relationship among actors of this use case based on flow of data.

Table IV.2 – Trust matrix for smart office service

To / From	Office Devices & Facilities	Smart Office Service Provider	Trust Management Service Provider	User
Office Devices & Facilities	-	Trusted data collection and aggregation	-	-
Smart Office Service Provider	Trustworthy application	-	Trustworthy application	-
Trust Management Service Provider	-	Trusted data process and analysis	-	Privacy
User	-	-	Privacy	-

2.5 Analysis

– Trusted data collection and aggregation

Data should be trustworthy from smart office devices and facilities to smart office service provider and from trust management service provider to smart office service provider. In flow #2, smart office devices and facilities produce data, and smart office provider collects data from devices and facilities. When data is produced and transmitted to other entities, trustworthiness of data is required to be maintained.

– Trusted data process and analysis

Information which is processed by trust management service provider should be trustworthy. In flow #4, collected data is processed and analysed in a trust management service provider to decide the trustworthiness of user, devices and facilities.

– Trustworthy application

In flow #3 and #5, an office service provider provides smart office application to not only devices and facilities but also trust management service provider. Smart office application should be trustworthy.

– Privacy

When a trust management service provider collects and analyses data and information for deciding trustworthiness of user, the trust management service provider may access user privacy information and it may cause user privacy issues.

3 Document sharing service

3.1 Description

This use case considers a social IoT [b-Atzori] environment with no centralized trusted authority. In the social IoT, each device has the subjective value based on the owner's social relationship as well as the Community of Interest (CoI) [b-Bao] of each device. This use case focuses on using the social trust when sharing the document between co-workers. Without the social IoT trust, a document owner takes the document from own storage, sends the document to receiver and notifies a guest account to receiver. However, the document owner does not need to do anything with the social IoT trust. A trust management platform calculates the trust value using the collected social data from intermediate entity (e.g., smartphone) of co-workers and then, these trust value will be used to judge whether a receiver has enough authorization to get the document or not.

3.2 Actors

– User: A user who takes the ownership of the things (e.g., wireless portable hard drive, smartphone, etc.) and wants to share the documents in the wireless portable hard drive.

– Smartphone: A device which is an intermediate entity and is available to send its owner’s social relationship information and its CoI information to wireless portable hard drive.

– Trust management platform: A trust management platform is mainly in charge of collecting the social relationship and calculating the subjective trust value.

– Wireless portable hard drive: A device, which is mainly in charge of judging authorization to share the document.

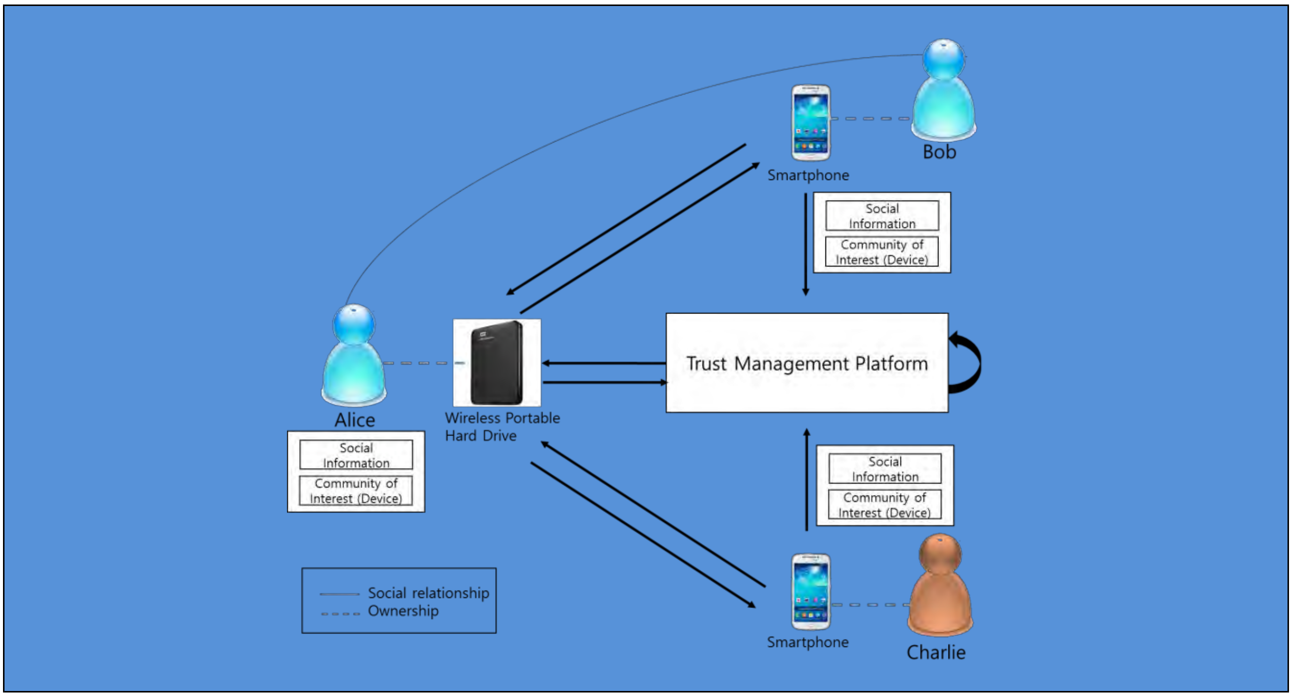

Bob
Smartphone
Social Information
Community of Interest (Device)
Trust Management Platform
Alice
Wireless Portable Hard Drive
Social Information
Community of Interest (Device)
Social Information
Community of Interest (Device)
Social relationship
Ownership
Smartphone
Charlie

Figure IV.5 – Document sharing service high level illustration

3.3 Detailed service flow

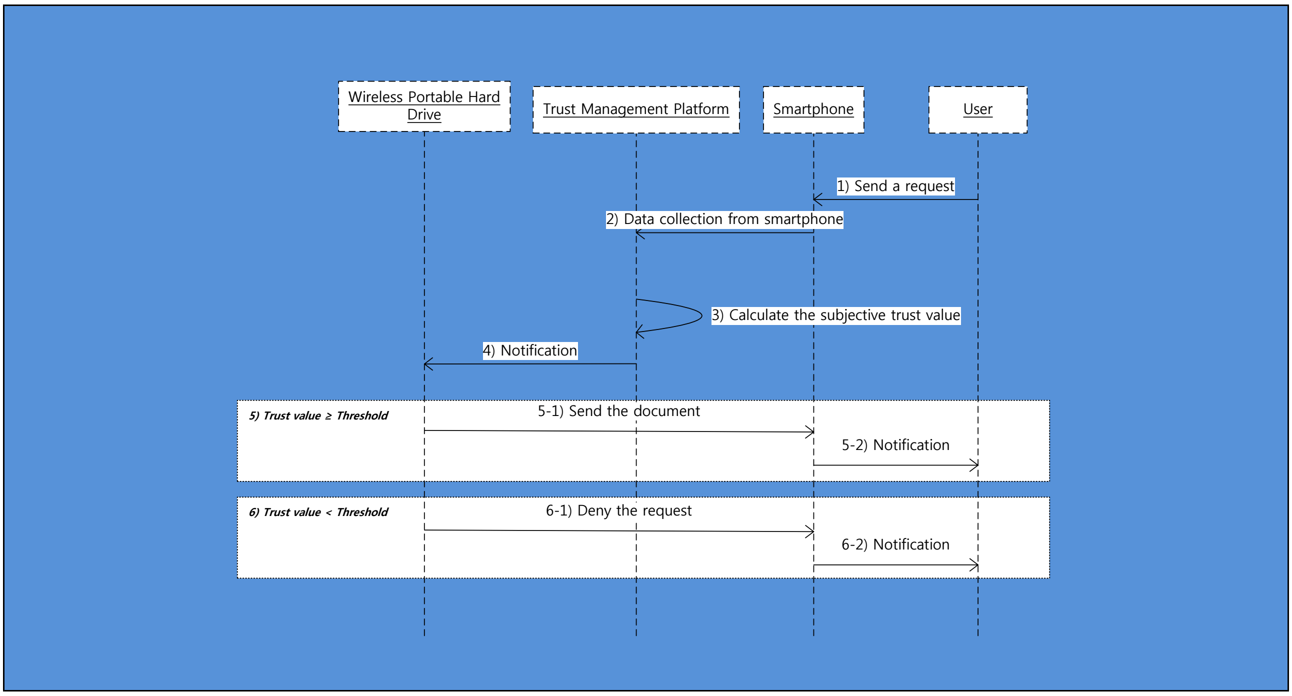

Wireless Portable Hard Drive
Trust Management Platform
Smartphone
User
1) Send a request
2) Data collection from smartphone
3) Calculate the subjective trust value
4) Notification
5) Trust value ≥ Threshold
5-1) Send the document
5-2) Notification
6) Trust value < Threshold
6-1) Deny the request
6-2) Notification

Figure IV.6 – Document sharing service flow

Detailed flow description

1) When User B requests the document to User A's wireless portable hard drive (WPH) by using B’s own smartphone.

2) User B's smartphone as a gateway sends User B’s social information CoI value to trust management platform.

3) From User A’s perspective, trust management platform calculates the subjective trust value (Ta,b) of User B toward User A by using given information of User A and B.

4) The trust management platform notifies the subjective trust value to WPH. After that, WPH judges whether User B has enough authorization to get the document.

5) If the subjective trust value exceeds the threshold value,

1-1) WPH sends the document to User B's smartphone.

1-2) Then, the smartphone notifies User B of results.

6) If the subjective trust value is lower than the threshold value,

1-3) WPH notifies that the request was denied.

1-4) Then, the smartphone notifies User B of results.

3.4 Trust matrix

Trust matrix presents trust relationship among actors in this use case.

Table IV.3 – Trust matrix for document sharing service

To From	Smartphone / Wireless portable hard drive	Trust Management Platform	User
Smartphone / Wireless portable hard drive	-	Trusted data collection and aggregation Trusted data process and analysis	Ownership
Trust Management Platform	Trusted data collection and aggregation Trusted data process and analysis	-	-
User	Ownership	-	-

3.5 Analysis

– Trusted data collection and aggregation

- Social relationship information: This trust property represents whether or not the trustee is socially cooperative with the trustor. We use the social friendship relationship among device owners to characterize the cooperativeness.
- CoI information: This trust property represents whether or not the trustor and trustee are in the same social communities of interest (e.g., co-location, co-work, or parental object relationship).

– Trusted data process and analysis

- A trust management platform processes and analyses data from other devices to produce useful information (e.g., subjective trust value) to a user.

– Ownership: This trust property represents whether or not the objects (smartphones) used by the device owner.

4 Device selection for data transmission

4.1 Description

This use case also focuses on using the social trust when selecting the device for data transmission in multi-hop D2D (Device-to-Device) environment. Reliable transmission is possible by using social information in the process of D2D communication. Trust management platform calculates the trust value by using the collected social data from intermediate entity (e.g., smartphone) of users and then, this trust value will be used to judge whether that device has enough authorization to send information or not. The social IoT trust also can be used in the device selection process for the reliable exchange of information. To complement the objective trust, the subjective trust is required in addition.

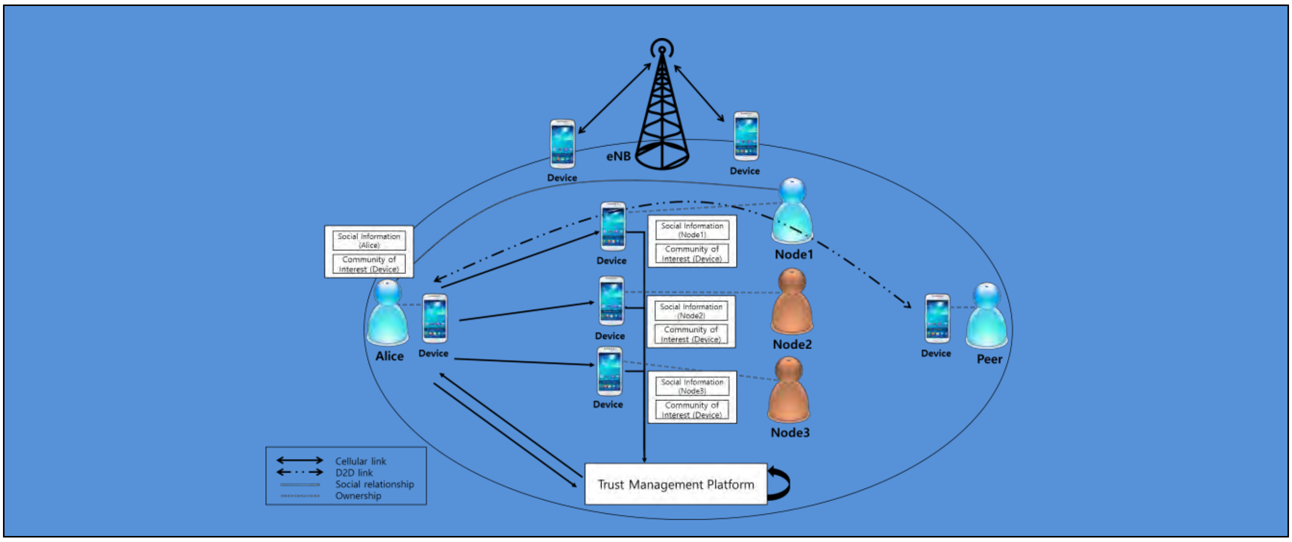

eNB
Device
Device
Social Information (Alice)
Community of Interest (Device)
Device
Social Information (Node1)
Community of Interest (Device)
Node1
Device
Social Information (Node2)
Community of Interest (Device)
Node2
Alice
Device
Device
Social Information (Node3)
Community of Interest (Device)
Node3
Device
Peer
Cellular link
D2D link
Social relationship
Ownership
Trust Management Platform

Figure IV.7 – Device selection for data transmission

4.2 Actors

– User: A user who takes the ownership of the things (e.g., smartphone, laptop, etc.) and wants to exchange information with another peer via other users.

– Device (Smartphone): A device, which is an intermediate entity, is available to send its owner's social relationship information and its CoI information to other devices. Also, it is in charge of judging authorization to send information.

– Trust management platform: A trust management platform is mainly in charge of collecting the social information and calculating the subjective trust value.

4.3 Detailed service flow

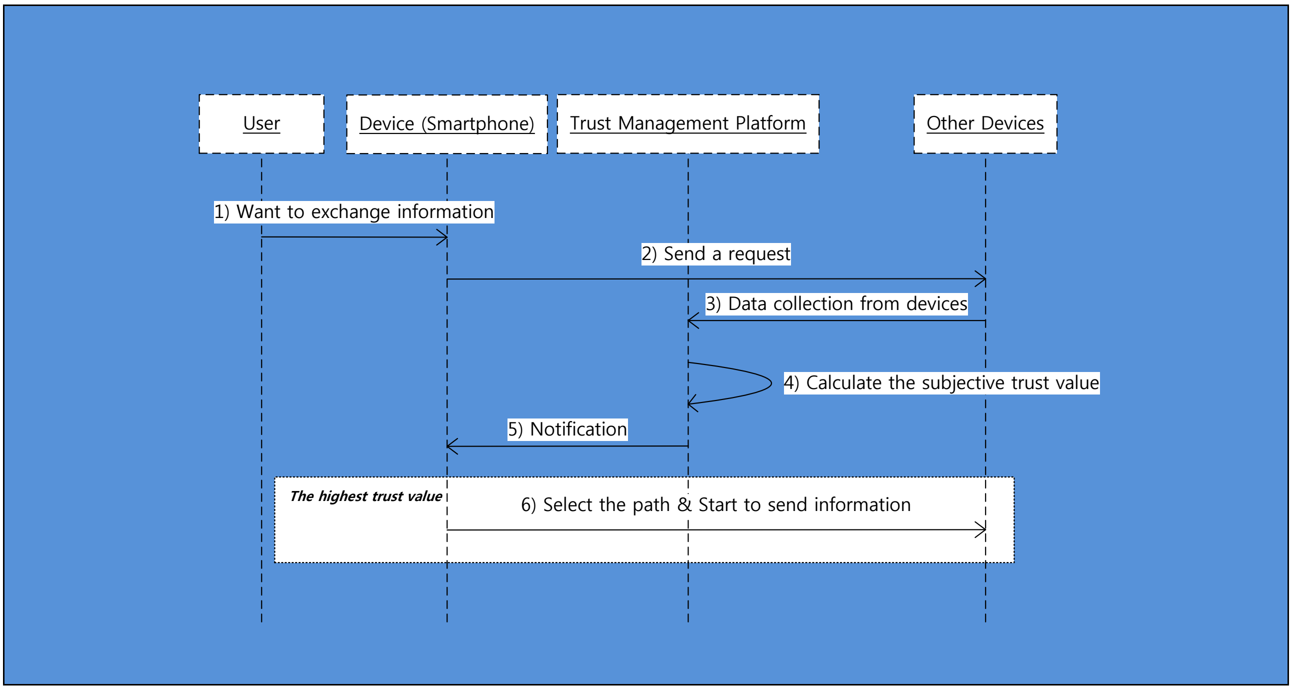

User
Device (Smartphone)
Trust Management Platform
Other Devices
1) Want to exchange information
2) Send a request
3) Data collection from devices
4) Calculate the subjective trust value
5) Notification
The highest trust value
6) Select the path & Start to send information

Figure IV.8 – Device selection for data transmission service flow

Detailed flow description

1) User A wants to exchange information with another peer in multi-hop D2D environment.

2) User A's smartphone requests the social information of other devices (e.g., Node 1, Node2, Node 3) and its CoI value.

3) The trust management platform collects relevant information from other devices.

4) Then, the trust management platform calculates subjective trust values (e.g., $T_{a,n1}$, $T_{a,n2}$, $T_{a,n3}$) of other devices from the perspective of User A.

5) The trust management platform notifies the subjective trust value to User A’s smartphone. After that, User A’s smartphone judges which Nodes have enough authorization to send information.

6) If Node 1’s subjective trust value ($T_{a,n1}$) is the highest value, User A's smartphone judges Node 1 has enough authorization to send information and select the transmission path with Node 1. Then, it starts to send information.

4.4 Trust matrix

Trust matrix presents trust relationship among actors of this use case.

Table IV.4 – Trust matrix for device selection as data transmission service

To From	Device (Smartphone)	Trust Management Platform	User
Device (Smartphone)	-	Trust data collection and aggregation Trusted data process and analysis	Ownership
Trust Management Platform	Trust data collection and aggregation Trusted data process and analysis	-	-
User	Ownership	-	-

4.5 Analysis

– Trusted data collection and aggregation

- Social relationship information: This trust property represents whether or not the trustee is socially cooperative with the trustor. We use the social friendship relationship among device owners to characterize the cooperativeness.
- CoI information: This trust property represents whether or not the trustor and trustee are in the same social communities of interest (e.g., co-location, co-work, or parental object relationship).

– Trusted data process and analysis

- A trust management platform process and analysis data from other devices to produce useful information (e.g., subjective trust value) to a user.

– Ownership: This trust property represents whether or not the objects (smartphones) used by the device owner.

5 Car sharing service

5.1 Description

Car Sharing aims at offering a new service for automobile transportation. Simply, car sharing is a self-service, on-demand alternative to car ownership; a service that is offered to urban residents (B2C) and businesses (B2B).

This service is particularly designed for two user groups – first of all, people who live in cities but do not drive a car every day and secondly tourists who live in cities but do not own a car. Thus, people who need a car at short period can take this alternative to car ownership.

The brief procedure of this service is 1) joining the membership, 2) unlocking the car door, 3) driving away, 4) parking to any reserved spot provided by the service provider and/or public, and 5) paying as you drive (including gas, insurance, and etc.).

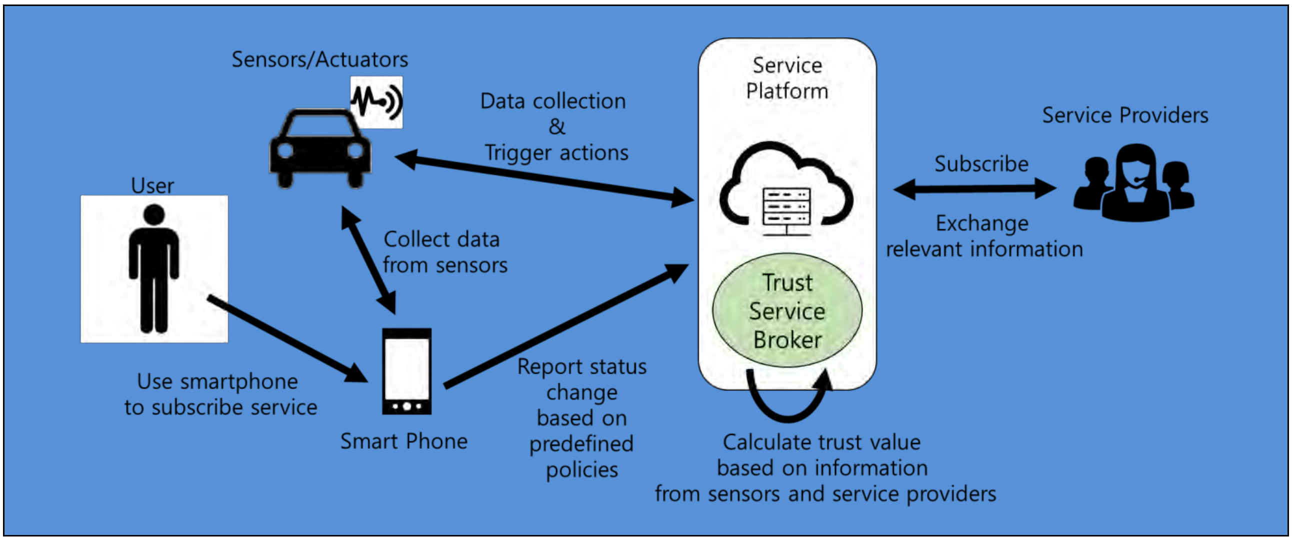


Figure IV.9 – Car sharing service high level illustration

5.2 Actors

- Users: A user who takes the ownership of the shared things which are car. Users would connect to the service with their smartphone which have not only capability of communicate with sensor devices, but also applications that used by car sharing services.
- Sensors (or Sensor Devices): Sensor Devices can be various based on its usage, and do not have any direct communication interfaces to the service platform.
- Service Platform: In charge of providing common functionalities for the services. It is mainly in charge of collecting the status and configuration information of sensors and controlling them via the smartphone and/or gateway.
- Service Providers: Companies which provide its own services for the user through the service platform. The service providers can be various according to the types of services.

5.3 Detailed service flow

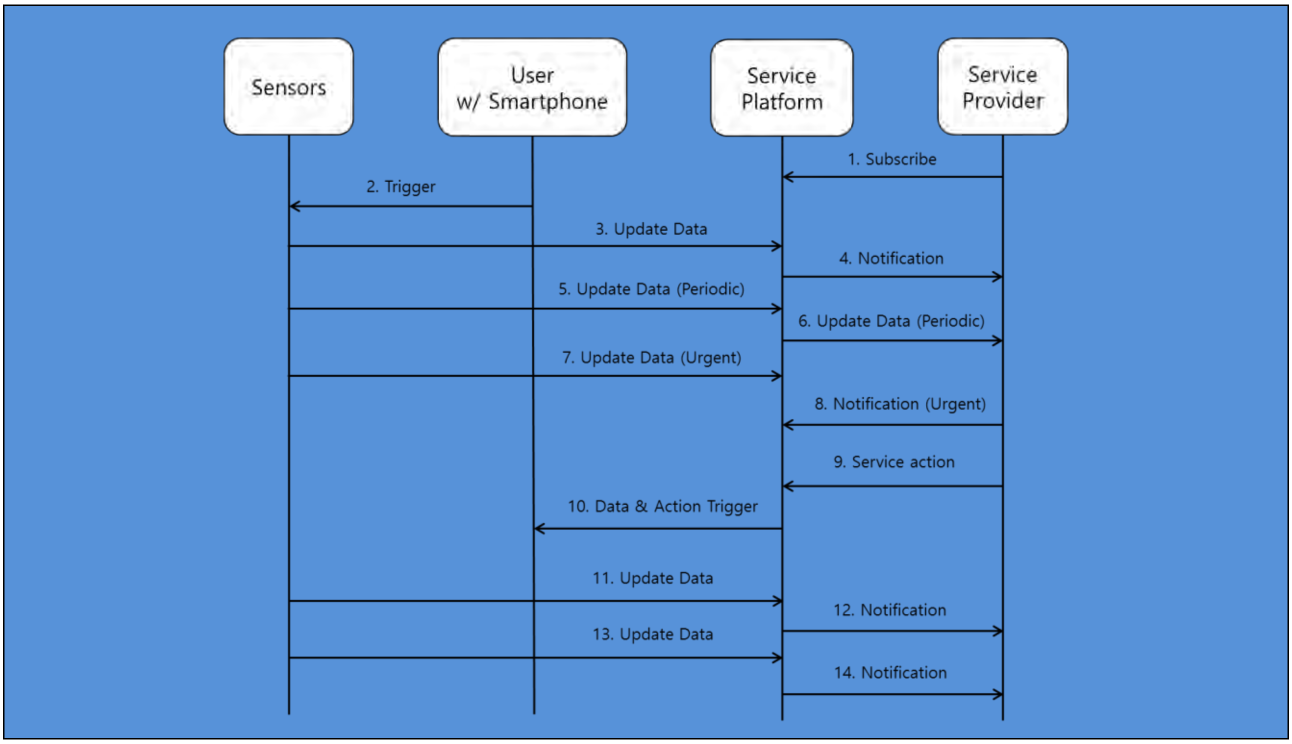


Figure IV.10 – Car sharing service flow

Detailed flow description

1) The applications of each service provider in the service domain register and subscribe to changes of resources (or information) about the car sharing service in the service platform.

2) As the user finds a shared car, opens the car door and turns on the ignition using interfaces of the Smartphone such as Bluetooth or Near Field Communication (NFC), if the user is authorized.

3) The sensors report the changed status to the service platform via the smartphone as a gateway when the specific condition of "Car is just got used" is triggered.

4) The service platform notifies the car sharing service provider of the changed status.

5) The sensors report the changed status to the service platform. It is occurred periodically that are location reporting and car health check for maintenance reasons.

6) The service platform notifies the car sharing service provider of the changed status.

7) The sensors report the changed status of "low fuel" to the service platform.

8) The service platform immediately notifies the car sharing service provider of the changed status.

9) The car sharing service provider finds out the nearest gas station according to the received location information and a service agreement between the car sharing service provider and the gas station, and the provider sends the route information to service platform.

10) The service platform notifies the smartphone of the route information.

11) After filling gas, the sensors report the changed status of "enough amount of fuel" to the service platform.

12) The service platform reports the change of car status.

13) As the user arrives at the destination, and turns off the ignition, the sensors report the accumulated information, normal event subscription information, to the service platform via smartphone.

14) The service platform notifies the car sharing provider of the usage of the shared car.

5.4 Trust matrix

Trust matrix presents trust relationship among actors of this use case based on flow of data.

Table IV.5 – Trust matrix for car sharing service

To / From	Sensors	Smart Phone (User)	Service Platform	Service Provider
Sensors	-	-	Trusted data collection and aggregation	-
Smart Phone (User)	Trusted data collection and aggregation	-	Privacy	Privacy
Service Platform	Trusted data collection and aggregation	Privacy	-	Trusted data process and analysis
Service Provider	-	Privacy	Trusted data process and analysis	Trustworthy application

5.5 Analysis

– Trusted data collection and aggregation

Data should be trustworthy from devices (sensors) to gateway (smartphone) service platform. In flow #3 and #5, devices produce data, and data is collected in a service platform. And, in flow #11, data is transmitted from service platform to devices. In flow #7 and #11, devices report their status to the service platform via gateway. When data is produced and transmitted to other entity, trustworthiness of data is required to be maintained.

– Trusted data process and analysis

Information which is processed by service platform and application should be trustworthy. In flow #1, applications send registration information with proper access right of the resources and grant that request to service platform. In flow #4, #6, #8 and #12, service platform detects changed status by processing collected data from devices and notifies to applications. Since the gateway and service platform manipulate collected data, the trustworthiness of information (i.e., processed and analysed data) is required to be maintained in each process.

– Trustworthy application

This use case can contain multiple service providers (applications), so trustworthy application and interactions between applications are important. In flow #7 and #13, two applications exchange data and information (e.g., location information, transaction information, etc.) to provide proper services. Since applications handle many data and information, the trustworthiness of application is required to be maintained in each process.

– Privacy

In flow #2, user profile information is used to figure out authorized user. User profile and payment information contains many user privacy data (e.g., location, amount of payment, credit card information etc.) Thus, privacy preserving is required to consider OS.

6 Used car transaction service

6.1 Description

While the used car market has been growing consistently in worldwide, there exists inevitable distrust in used car transactions. Comparing to purchasing a new car, buying a used car involves high level of uncertainty and risk. The market for used car is called as "the market for the lemons", which is produced by asymmetric information, in which a buyer can not accurately assess the exact condition of the car through examination before sale is made while a seller can more accurately assess the condition of the car prior to sale. Specifically, owners of good cars will not sell their cars while only owners of defective cars will sell their cars. When a seller is going to sell their used vehicle, he or she has a weak motivation of disclosing the problems in the car. As a result, consumers are hardly satisfied with the used cars because of unexpected car trouble. General transaction model and each entity's information level of a used car are depicted in Figure IV.11.

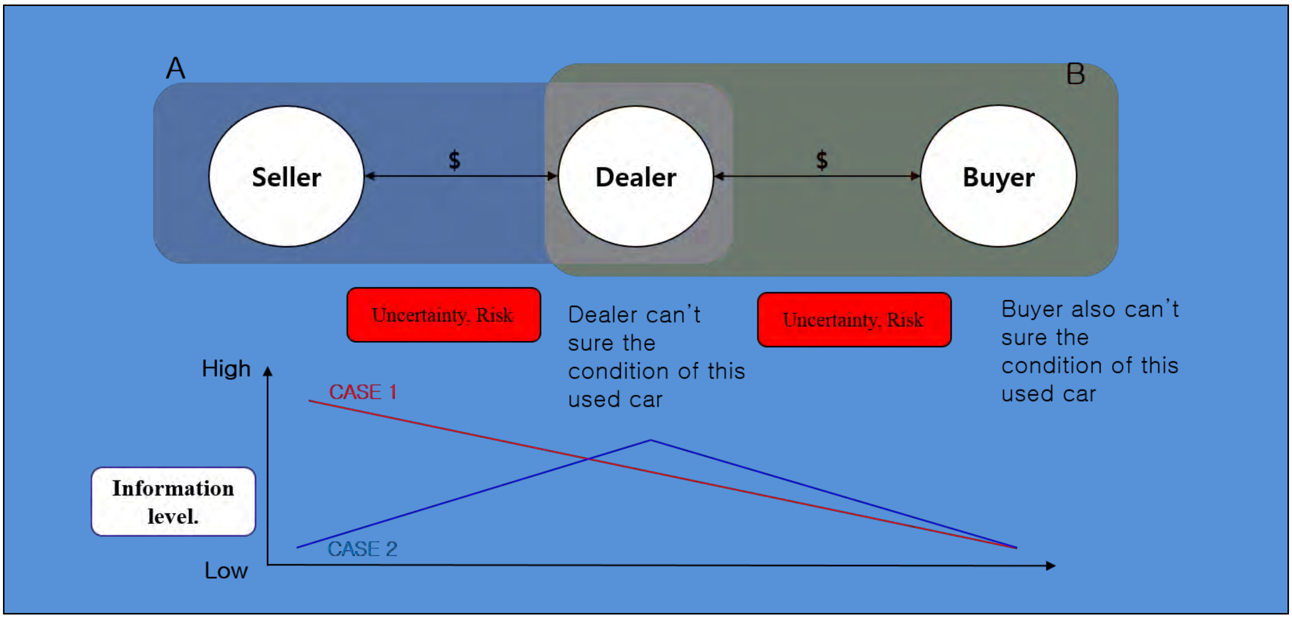

A
B
Seller
$
Dealer
$
Buyer
Uncertainty, Risk
Dealer can't sure the condition of this used car
Uncertainty, Risk
Buyer also can't sure the condition of this used car
High
CASE 1
Information level.
CASE 2
Low

Figure IV.11 – Risk, uncertainty and motivation in used car transactions

Transaction *A* describes a situation that a dealer purchases a used vehicle from a seller. In this transaction a dealer is a risk taker. A dealer should investigate the car carefully to assess the condition of the car and evaluate the price because a dealer cannot confirm a seller's explanation about the car. Specifically, a seller does not have a strong motivation of disclosing all information about the car because this information directly influences the price (Case 1). It is also plausible to assume that a seller is not aware of the exact condition of the car because symptoms of trouble has not yet clearly shown (Case 2). Thus, a deal should investigate the car. However, this cross-sectional investigation is not enough to understand the real condition of the car. Thus, intense disputes commonly occurs after a transaction.

Transaction *B* describes the situation of that a buyer purchases a dealer the used car. In this transaction, a buyer is a risk taker. Similar to transaction *A*, a buyer cannot trust in a dealer (seller) because a dealer has a strong motivation of hiding the exact information about current condition of the car (Case 1). Although a dealer detects the critical problems of the used vehicle after transaction *A* finished, a dealer will not intend to unveil the detected the problems (Case 2) because this transaction accounts for dealer's income. As a result, a dealer – a risk taker in transaction *A* – sells defective used cars deliberately partly with intention, partly by accident.

As a result, each entity participating in these transactions have conflicting motivations of unveiling information on the condition of a used vehicle, so motivations cannot be aligned without an external intervention. Because of this confliction, "trust" cannot be guaranteed in used vehicle transaction. Although a seller and buyer need a mediating entity – a dealer – to reduce transaction cost, the problem is that a dealer is a buyer in transaction *A* and also a seller in transaction *B*. Here, transaction cost refers to a cost incurred in making an economic exchange. In addition, a dealer always tries to make used car transactions for his or her revenue.

As a result, asymmetric information causes inevitable distrust in economic transaction for used car through conflicting motivation. A buyer cannot trust in sellers' word about the condition of the vehicle. While consumers need a careful investigation in order to avoid purchasing defective vehicle, they are not accustomed to investigate the car. Consequently, asymmetric information makes them fail to trust in sellers and used cars, so level of satisfaction is always threatened. A great number of articles have shown that trust is strongly related to satisfaction of various goods.

In summary, as seen in Figure IV.12, the current used car transaction involves following inevitable problems; (1) asymmetric information, (2) conflicting motivation of disclosing the condition of used car due to (1), and (3) distrust among entities due to (2). Thus, an appropriate intervention is needed for avoiding dispute among entities and activating the used car market.

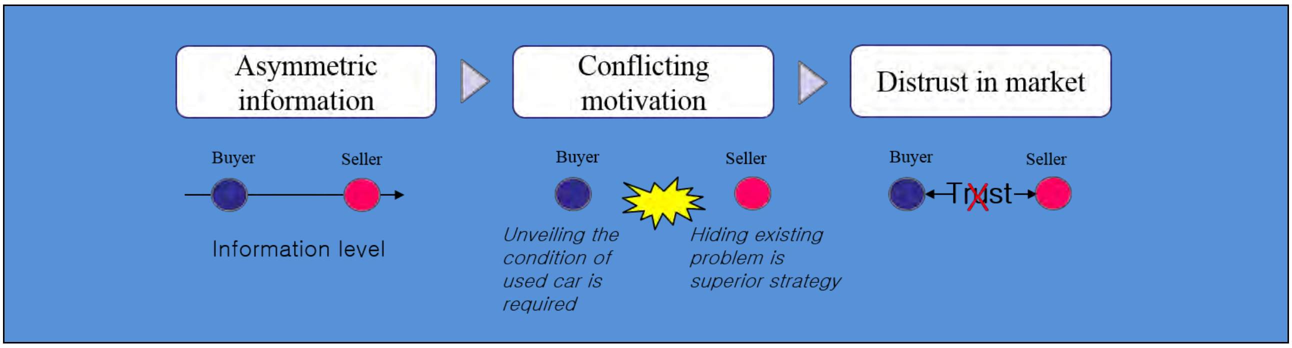


Figure IV.12 – Problems of the current used car transaction service

In order to overcome sequential problems discussed, it is direct remedy to make participants share information. Trust management platform can play an important role in mediating entities who participate in used vehicle market and sharing trustful data and information (Figure IV.13).

When a buyer request selling his/her car, a dealer registers that vehicle in an online market place liked to trust service broker. Then, trust management platform automatically collects data from various sources such as insurance company, public organization, social network services, and vehicle itself. If a vehicle owner attaches On-Board Diagnostics 2 (OBD2) scanner, this IoT device records and accumulates wide ranges of vehicle-oriented information such as driving distance, recorded fuel efficiency, accident, driving habits, and maintenance and repair history.

In the next step, by transforming these fragmented data into single information, trust management platform identifies and evaluate the level of trust of an owner of used car, a registered vehicle, and a dealer. Based on this refined and trustful information, a buyer can assure the condition of the used vehicle prior to purchasing and make a purchase decision with comparably low level of uncertainty and risk.

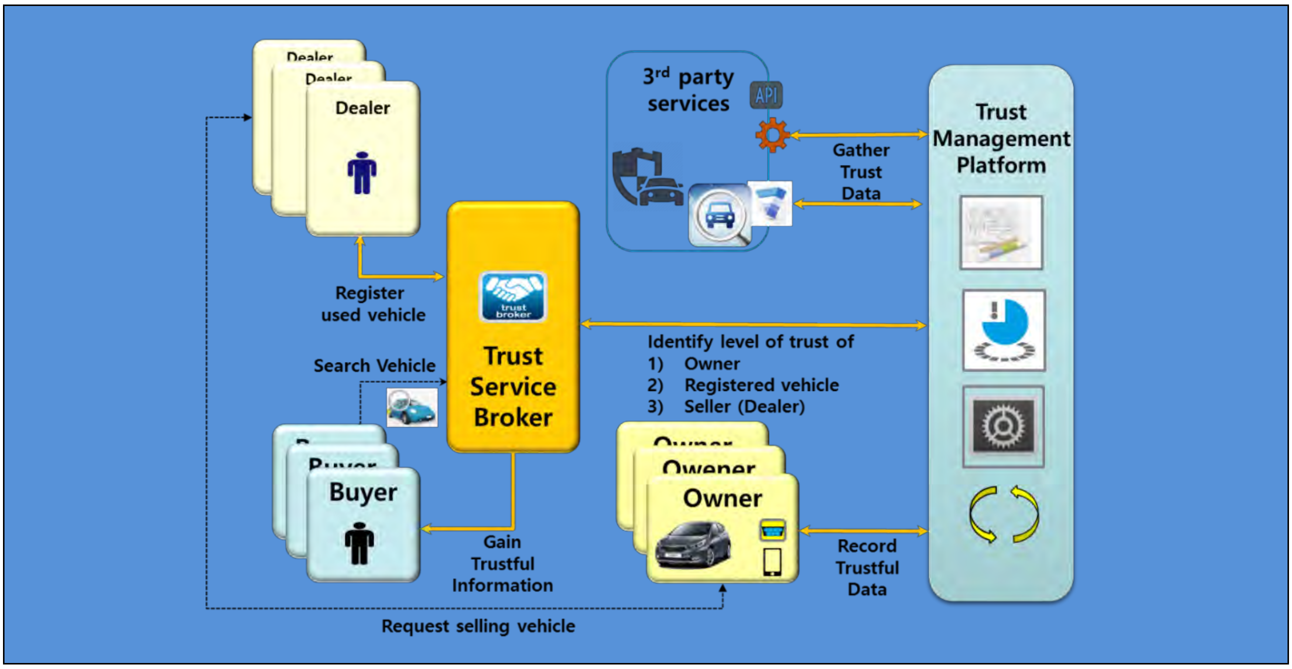


Figure IV.13 – Used car transaction service high level illustration

6.2 Actors

As the participants in the used car transaction process depicted in Figure IV-13 have different goals, each actor plays a distinctive role and conducts different function.

- Dealer
  - The major role of a dealer is mediating buyer and seller (owner) to gain economic profit.
  - A dealer can sell the possessed cars, which were already purchased, or can mediate the transaction between sellers and buyers.
- Buyer
  - A buyer is someone who wants to purchase a used car from a dealer or seller.
  - When a buyer wants to purchase a used car, a buyer can search the car in a market place or on the web provided by service broker.
  - When a buyer requests dealers and brokers for purchasing the car, he or she generally describe the specific constraints such as vehicle age, accumulated mileage, brand, model, budget, and so on.
  - Based on identified information about the condition of the car, he or she can make a purchase decision under relatively low uncertainty and risk.
  - The more provided information is trustful and abundant, the more they can reduce risk and uncertainty.
- Owner (Seller)
  - An owner (seller) is someone who wants to sell his or her car to others including a dealer and individual buyer.
  - When an owner tries to sell the car, he or she simply sell a dealer or an individual the car at a negotiated price. Otherwise, he or she can ask a dealer transaction brokering.
- (Trust) Service Broker
  - Trust service broker is a broker mediating an interaction among buyers, sellers, and dealers through the information transferred by trust management platform.
  - Based on the information, trust service broker can inform the identified level of trust of owner, registered vehicle, and seller.

- Trust Management Platform
  - Trust management platform responses various requests from a service broker and others.
  - Trust management platform analyses the level of trust by tracing the accumulated data from various sources including social network, insurance company, vehicle repair shop, public, and the car itself.

6.3 Detailed service flow

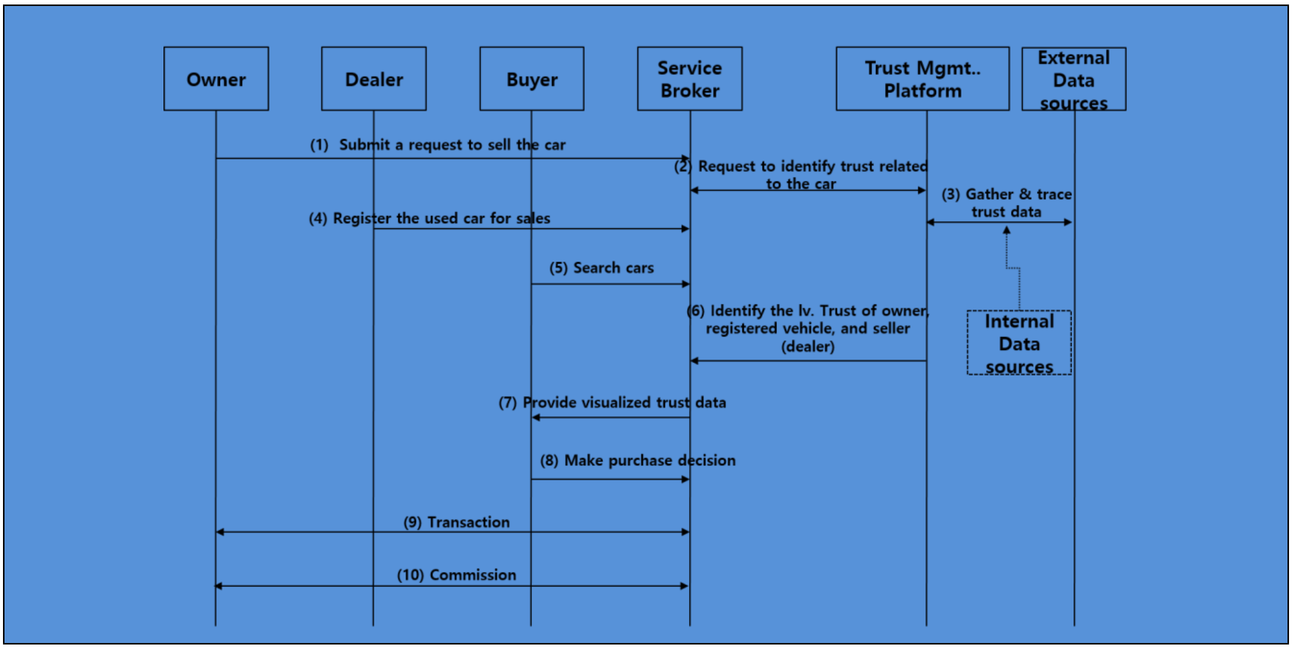

Owner
Dealer
Buyer
Service Broker
Trust Mgmt.. Platform
External Data sources
(1) Submit a request to sell the car
(2) Request to identify trust related to the car
(3) Gather & trace trust data
(4) Register the used car for sales
(5) Search cars
(6) Identify the lv. Trust of owner, registered vehicle, and seller (dealer)
Internal Data sources
(7) Provide visualized trust data
(8) Make purchase decision
(9) Transaction
(10) Commission

Figure IV.14 – Used car transaction service flow

Detailed flow description

1) A dealer registers the used car in trust service brokers as an owner makes a request to a dealer for selling the used car.

2) Trust management platform complies with a service broker's request of transferring trustworthy data related to the car.

3) Trust management platform gathers the relevant data from not only the external data sources such as insurance company, public organization, social network services, but also an internal data source such as OBD scanner, which transfers historical data from car to the platform. If car owner attaches OBD scanner in the car, he can confirm the condition of the car and identify problems via applications on a smartphone.

4) A dealer registers the car with explanatory data about the car in the marketplaces connecting with a number of service brokers. At this time, the car is ready for sales.

5) A buyer can search number of used cars in order to purchase the car.

6) When a buyer is interested in a specific car, he or she can ask the service brokers relevant data and information. Then, trust management platform replies service broker's requests by providing processed trustful data including the level of trust of owner, registered car, and seller (or dealer).

7) In order to help a buyer's purchase decision, a service broker visualizes the analysis results.

8) A buyer can make a purchase decision with relatively low risk and uncertainty.

9) The used car transaction occurs among parties.

10) After completing the transaction, transaction commission can be transferred. The commission rate and recipient depends on business model and pre-determined rules.

6.4 Trust matrix

In order to achieve valuable analysis results, the proposed system needs data from various sources. The data source includes social network service, insurance company, an organ of credit, car repair shop, bank, and OBD2 scanner attached in the car. An example for possible trust matrix structure is shown in Table IV.6.

Table IV.6 – Trust matrix for used car transaction

To From	Owner	Used car	Trust Management Platform	Buyer
Owner	-	Ownership	Trusted data collection and aggregation Trusted data process and analysis	-
Used car	Ownership	-	Trusted data collection and aggregation Trusted data process and analysis	Risk, uncertainty
Trust Management Platform	Trusted data collection and aggregation Trusted data process and analysis	Trusted data collection and aggregation Trusted data process and analysis	-	Trustworthy application
Buyer	-	Risk, uncertainty	Trustworthy application	-

6.5 Analysis

– Participants' advantage of adopting used car transaction through trust management platform.

This clause describes how trust can be achieved in used car transaction by trust management platform, which plays an important role in reducing the information gap among entities, refining data from various data sources, and mediating entities through trust service broker. By adopting this platform, each entity participating in used car ecosystem can take following advantage. Details are explained in following Table IV.7.

Table IV.7 – Advantages of actors from trust based used car transaction service

	Main advantages	Side advantages
Seller	- Providing trustful data which influence on selling price	- Reasonable vehicle maintenance based on trustful data transmitted by vehicle itself - Reducing insurance cost by a vehicle specific data
Dealer	- Reducing investigation effort - Decreasing dispute	- Restoring confidence in used car transaction
Buyer	- Reducing uncertainty and risk from purchasing used goods	- Succession to well-maintained vehicle - Purchasing relatively low retail price in P2P market
Insurance Corp.	- Realizing usage-based insurance by absorbing deadweight loss	
Government	- Reducing dispute - Revitalizing market - Promoting international vehicle transaction	- Improving road infrastructure and traffic flows
Vehicle Manufacturer	- Detecting defective vehicle model in early stage	- Gathering real data for improving vehicle performance
OBD2 Scanner manufacturer	- Creating new revenue stream	- Taking opportunity of analysing vehicles' historical data

– Cost structure of adopting used car transaction through trust management platform

In order to adopt the used car truncation based on trust, it is required to discuss who has a responsibility for deploying the trust platform, which is composed of trust service broker, trust management platform, and other entities. Although the adoption of this platform needs investment, the responsibility for deployment depends on business model and government policy.

For example, buyers can compensate for the investment since they are regarded as the one who takes the most advantage of adopting trust platform. Otherwise, the government can invest on building and operating trust management platform instead of consumers. Simply, government will invest on this platform if the platform can increase both consumer and producer surplus. If dealers can take the most advantage, dealers should be responsible for deploying trust platform. However, it needs further studies because a careful investigation is required to figure out who is taking the greatest advantage.

As we discussed, there exists other issues such as business models, ecosystem, and policies. Careful investigation about these issues can lead to figure out the cost structure and responsibilities. When each entity's motivations are clearly aligned, the problem of cost structure can be resolved. Thus, relevant studies on business models and ecosystem, and economic analysis for this platform are fundamentally required.

Bibliography

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*

[b-ITU-T Y.2060] Recommendation ITU-T Y.2060 (2012), *Overview of the Internet of things*

[b-Afuah] Afuah, Allan and Tucci, Christopher L. (2001), *Internet Business Models and Strategies, McGraw-Hill Irwin.*

[b-UN] Understanding Knowledge Societies: In twenty questions and answers with the Index of Knowledge societies, UN. 2005.

[b-UNESCO] Towards Knowledge Societies, UNESCO Publishing, ©UNESCO 2005, ISBN 92-3-204000-X

[b-Alcalde] Alcalde, B., Dubois, E., Mauw, S., Mayer, N. and Radomirović, S. (2009), Towards a Decision Model based on Trust and Security Risk Management, 7th Australasian Conference on Information Society, Vol. 98, pp. 61-70.

[b-Josang] Josang, A., Ismail, R. and Boyd, C. (2007), *A Survey of Trust and Reputation System for Online Service Provision*, Decision Support System, Vol. 43, No.2, March, pp. 681-644.

[b-McKnight] McKnight, D.H., Carter, M., Thatcher, J.B. and Clay, P.F. (2011), *Trust in a specific technology: An investigation of its components and measures*, ACM Transactions on Management Information Systems (TMIS), Vol. 2, No. 2, June, pp. 12-36

[b-uTRUSTit] Trust Definition White Paper (2012), *Defining, Understanding, Explaining TRUST within the uTRUSTit Project*, August.

[b-Chang-2005] Chang, E., Hussain, F.K. and Dillon T.S. (2005), *Fuzzy nature of trust and dynamic trust modelling in service oriented environments*, Proceedings of the 2005 workshop on Secure web services (SWS '05). ACM, New York, NY, USA, November, pp. 75-83.

[b-Chang-2006] Chang, E., Dillon, T. and Hussain, F.K. (2006), *Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence*. West Sussex, England: John Wiley & Sons Ltd.

[b-Bertino] Bertino, E. (2012), *Trusted Identities in Cyberspace*, IEEE Internet Computing, Vol. 16, No. 1, February, pp. 3-6.

[b-Wahab] Wahab, O.A., Bentahar, J., Otrok, H. and Mourad, A. (2015), *A survey on trust and reputation models for Web services: Single, composite, and communities*, Decision Support Systems, Vol. 74, June, pp. 121-134.

[b-Grandison] Grandison, T. and Sloman, M. (2000), *A Survey of Trust in Internet Applications*, Communications Surveys & Tutorials, IEEE, Vol. 3, No. 4, September, pp. 2-16.

[b-Blaze] Blaze, M., Kannan, S., Lee, I, Sokolsky, O., Smith, J.M., Keromytis, A.D. and Lee, W. (2009), *Dynamic Trust Management*, IEEE Computer, Vol. 42, No. 2, February, pp. 44-52.

[b-Yan] Yan, Z., Zhang, P. and Vasilakos, A.V. (2014), *A survey on trust management for Internet of Things*, Journal of Network and Computer Applications, Vol. 42, March, pp. 120-134.

[b-Govindan] Govindan, K. and Mohapatra, P. (2012), *Trust computations and trust dynamics in mobile adhoc networks: A survey*, Communications Surveys & Tutorials, IEEE, Vol. 14, No. 2, May, pp. 279-298.

[b-Yu] Yu, H., Shen, Z., Leung, C., Miao, C. and Lesser, V.R. (2013), "*A survey of Multi-Agent Trust Management systems*," IEEE Access, Vol. 1, May, pp. 35-50.

[b-Ahmed] Ahmed, A., Bakar, K.A., Channa, M.I., Haseeb, K. and Khan, A.W. (2015), *A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks*, Frontiers of Computer Science, Vol. 9, No. 2, April, pp. 280-296.

[b-Sherchan] Sherchan, W., Nepal, S. and Paris, C. (2013), *A Survey of trust in social networks*, ACM Computing Surveys, Vol. 45, No. 4, August, pp. 47-79.

[b-EU-Safeharbor] EU Safe Harbor, http://www.export.gov/safeharbor/eu/eg_main_018476.asp

[b-Yoo-2012] Yoo, Y., Boland, R.J., Lyytinen, K. and Majchrzak, A. (2012), *Organizing for Innovation in the Digitized World*, Organization Science, Vol.23, No.5, October, pp. 1398-1408.

[b-Yoo-2010] Yoo, Y., Henfridsson, O. and Lyytinen, K. (2010). *Research commentary: The new organizing logic of digital innovation: an agenda for information systems research*, Information Systems Research, Vol.21, No. 4, June, pp. 724-735.

[b-Eisenmann] Eisenmann, T., Parker, G., and Van Alstyne, M. W. (2006). *Strategies for two-sided markets*. Harvard business review, Vol.84, No.10, October, pp. 92-104.

[b-Gawer] Gawer, A. (Eds.) (2009). *Platforms, markets and innovation,* Cheltenham, UK: Edward Elgar Publishing.

[b-Sandberg] Sandberg, J., Holmstrom, J. and Lyytinen, K. (2013). *Platform change: theorizing the evolution of hybrid product platforms in process automation*, In Platform Strategy Research Symposium. Boston University, Boston, MA.

[b-Mayer] Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). *An integrative model of organizational trust*, Academy of management review, Vol.20, No. 3, July, pp. 709-734.

[b-Gilson] Internet of Things Lacks Safety Today, Opening Door to Major Threats Tomorrow, Warns OTA. Online Trust Alliance. Retrieved from https://otalliance.org/news-events/press-releases/internet-things-lacks-safety-today-opening-door-major-threats-tomorrow

[b-OTA] OTA IoT Trust Framework – Pre-Release Draft. Retrieved from https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_lastcall.pdf

[b-TCG 2013] TCG Published. (2013, October). Architect's Guide: Cybersecurity. TCG Published. Retrieved from http://www.trustedcomputinggroup.org/files/resource_files/CA36D107-1A4B-B294-D08829372D5796E1/Architects Guide Cybersecurity.pdf

[b-Leigh Ann Gilson] Leigh Ann Gilson. (2015). Internet of Things Lacks Safety Today, Opening Door to Major Threats Tomorrow, Warns OTA. Online Trust Alliance. Retrieved from https://otalliance.org/news-events/press-releases/internet-things-lacks-safety-today-opening-door-major-threats-tomorrow

[b-TCG 2015] TCG Published. (2015, September 14). Guidance for Securing IoT Using TCG Technology. 1.1. TCG Published. Retrieved from https://www.trustedcomputinggroup.org/files/resource_files/CD35B517-1A4B-B294-D0A08D30868AB3D1/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[b-Christensen] Christensen, Clayton M. (2014). Disruptive Innovation. In: Soegaard, Mads and Dam, Rikke Friis (eds.). The Encyclopedia of Human-Computer Interaction, 2nd Ed. Aarhus, Denmark: The Interaction Design Foundation.

[b-McKnight 2002] McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validatingt trust measures for e-commerce: An integrative typology. Information systems research, 13(3), 334-359.

[b-Tilson] Tilson, D., K. Lyytinen, et al. (2010). Research Commentary – Digital Infrastructures: The Missing IS Research Agenda. Information Systems Research.

[b-Atzori] L Atzori, et al., "The social internet of things (SIoT)–when social networks meet the internet of things: Concept, architecture and network characterization", Computer Networks 56 (16), 3594-3608, 2012

[b-Bao] F. Bao, I. R. Chen, and J. Guo, “Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems,” 11th International Symposium on Autonomous Decentralized System, Mexico City, Mexico, 2013.

4.

The basic principles of trusted environment in ICT infrastructure

Recommendation ITU-T Y.3051 (2017) – The basic principles of trusted environment in ICT infrastructure

Table of Contents

A
B
C
D
F
G
H
I
1
2
3
4
5
6
7
8
HERJ 590
WPT 234
WPEY 287
HGLW 557
WQST 107
AZDR 17
ACDU 557
QTYC 17
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350

1 Scope

This Recommendation is devoted to the issue of creating trusted environment in ICT infrastructure providing information and communication services. This issue becomes extremely important in modern knowledge society with such a significant growth rate of information technology. This Recommendation contains rationale for necessity of trusted environment in ICT infrastructure, common requirements and the basic principles of its creation. This Recommendation is relevant for services developers as well as for network designers and should be considered as a set of fundamental principles for creating convenient and secure environment. While basic principles outlined in this Recommendation aim at creating trusted environment for the provision of services using ICT, they may be applied in a broader interpretation of the concept of trusted environment.

2 References

The following ITU-T Recommendations and other references contain provisions, which through the references in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2701]	Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 trust [ITU-T Y.3052]: Trust is the measureable belief and/or confidence which represents accumulated value from history and the expecting value for future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of entities, value-chains among multiple stakeholders, and human behaviours including decision making.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 trusted environment (in ICT infrastructure): ICT enabled environment providing a set of technical and regulatory conditions sufficient for establishing trust between interacting entities.

NOTE – From a broader perspective, the trusted environment can be perceived as a multidimensional concept with technological and societal implications.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ICT	information and communication technologies

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Necessity of trusted environment in ICT infrastructure

Due to the development of information technology and future networks where the number of entities and their interactions (e.g., "human to human", "human to machine", "machine to machine", etc.) increases significantly. In any uncertain circumstance, people need to be able to predict the results of these interactions especially with the entities they cannot control remotely. To provide the desired level of confidence and protection it is necessary to conduct a complex of special technical and organizational measures. One of the possible ways is to create trusted environment in ICT infrastructure.

The globalization and the widespread of information technologies leads to the displacement of the context of trust by special technological means. Therefore, ICT infrastructure needs to play an important role for building up trusted environment with interoperability and information security. In addition, ICT infrastructure needs trust between interacting parties under a high level of responsibility in resource-limited environment (e.g., to save human lives for the case of emergencies).

Trusted environment in ICT infrastructure is necessary for social, critical and life-demand services (e.g., e-government, e-commerce, e-health, etc.). For such services establishing of trust between service provider and consumers may solve problems of fraud and increase availability of services.

In summary, creating trusted environment in ICT infrastructure allows interacting entities to predict the results of interactions and excludes risks caused by the growing number of interactions and the lack of its context while providing interoperability and information security.

7 Requirements of trusted environment in ICT infrastructure

Trusted environment in ICT infrastructure must meet the following requirements:

Predictability

- All participants interacting within trusted environment are required to be equipped with the capability to predict the outcome of the interactions in order to reduce the risks of negative consequences caused by the inappropriate behavior of any participants.
- For this, ICT infrastructure used for trusted environment is required to meet a certain level of quality.
- Handy user interfaces and systems of accesses to trusted environment are recommended to be provided for participants to improve predictability by using comfortable and familiar methods of interaction each time.

Information security

- It is required to provide confidentiality, integrity and the availability of information as well as the absence of misinformation (spam, etc.) for all participants interacting within trusted environment.
- Each participant is required to be verified for compliance with the common minimal security requirements.
- Minimal security requirements for trusted environment in ICT infrastructure are required to be developed for all security dimensions [b-ITU-T X.805] with the goal to provide electronic exchange of information in trusted environment with the same level of trust in a non-electronic interaction.

Interoperability

- It is required to provide for all participants interacting within trusted environment to be able to exchange information with any entity within trusted environment in ICT infrastructure.
- Trusted environment in ICT infrastructure is required to support internetwork connections to provide unified interaction capabilities to each participant independent of technical infrastructure (core networks) used.
- All predictability, information security and availability of administration services requirements are required to be supported for internetwork connections.

Availability of administration services

- Continuous customer support is required to be provided for all participants of interaction within trusted environment in ICT infrastructure as well as prompt compensation in the case of failure in the provision of services.
- Trusted environment in ICT and its technical infrastructures are required to maintain the capacity to enroll new participants enabling them to rapidly integrate and start operating within trusted environment in ICT.

8 The basic principles of trusted environment in ICT

The need to create trusted environment is associated with the increased convergence of ICT, general mobility and increasing the number of interactions between humans and machines. The task of creating trusted environment especially actual for ICT used in socially and economically significant interactions between machines, humans, organizations and other entities. Examples of such interactions are e-commerce, e-government and rescue guidance in emergency. The latter is related to a direct threat to human life and also represents high importance interaction within trusted environment.

The trusted environment in global scope is prevented by absence of ICT interoperability. The field of interoperability of ICT can be characterized by the following statements:

1) Presence of a large number of information systems operating within the governmental institutions and companies. These systems typically use their own hardware and software, and most of them can not exchange information directly in the "machine-to-machine" mode.

2) The presence of many competing standards that only hinder the exchange of information despite the excellent work carried out by numerous standardization bodies (at national, regional and international levels).

3) The majority of developed economies are not ready to abandon the already established and well-functioning information systems for the benefit of future non-prescribed systems.

Basic principles of creation of trusted environment in ICT are:

1) The principle of **non-discrimination** - the electronic interaction in trusted environment will not be exempted from legal consequences, validity or enforceability solely on the ground that it is provided in electronic form. This involves adoption of regulatory legal acts, but the first step is to provide related technological capabilities in ICT infrastructure to ensure the same level of security for electronic transactions as signature on the paper documents. E-signature and certification authorities can serve as examples of such technologies.

2) The principle of **technological neutrality** of ICT in trusted environment, which involves creating trusted environment in ICT neutral with regard to the given technology used. Given the rapid pace of technological progress neutral regulations are intended to allow the use of any future development without further action of the legislative procedure.

3) The principle of **functional equivalence**, which sets the criteria by which electronic interactions (for example, electronic document) may be recognized as the equivalent of live interactions (paper documents). This provision involves the adoption of regulatory legal acts, but the first step is to

provide related technological capabilities in ICT infrastructure to ensure the integrity of transported information (electronic documents).

4) The principle of **unification**. ICT used in trusted environment is required to have unified forms of information, while maintaining its unique content. Due to the possible wide range of entities involved in information interaction within the trusted environment, it is especially important to use unified interfaces of information interaction within the entire trusted environment.

5) The principle of **scalability**. Organizational and technical infrastructures of trusted environment in ICT are required to have the capacity to enroll new participants enabling them to start operating within trusted environment. These infrastructures are also required to enable their users to choose a set of services matching the user's needs.

6) The principle of **equal reliability** of infrastructure of trusted environment, which applies common minimal security requirements to all of the participants, regardless of their own parameters. This is important to prevent the occurrence of vulnerabilities in trusted environment in ICT, which can be used to attack the whole trusted environment.

7) The principle of **legalization** of electronic documents in trusted environment, ensuring that issued e-documents are equally recognized by respective jurisdictions (e-apostille). It is important to ensure safety and integrity of information flows during transportation through networks which combined numerous ICT and standards.

8) The principle of **client-oriented** architecture which includes simple, clear and handy user interfaces and unified system of accessors to the services in trusted environment in ICT. It also includes providing capabilities of trusted environment in ICT within the widely used general purpose networks, e.g. Internet.

9) The principle of **systematization**, which includes three main components:

– consistency of organizational, legal and technical arrangements;

– consistency in reliability structures and infrastructure systems;

– moving from bilateral interoperability arrangements towards multi-vectored ones, where appropriate.

This principle concerns not only technological area, but mainly legal and organizational field.

10) The principle of **finiteness** of trusted environment which suggests that trusted environment could be organized in the scope of a specific information interaction space and to be continuously maintained and improved within this space. In case where trusted environment in ICT covers the whole existing ICT infrastructure, the complexity of trusted environment maintenance (including administration) becomes extremely high. Therefore it is reasonable to establish trusted environment only within the specific part of the ICT infrastructure, where maintaining is possible.

It is important for ICT infrastructure to support implementation of all these principles to be compatible with trusted environment.

Appendix I

The first steps to create trusted environment for cross-border e-commerce

(This appendix does not form an integral part of this Recommendation.)

Cross-border e-commerce is an example of informational interaction of entities, which are residents of different economies, and therefore subjects to different regulatory and legal acts. Each economy has its own rules of information handling and this fact is a reason of an important issue with e-commerce. Cross-border e-commerce should support rules of each interacting economy to establish trust between interacting entities. Therefore, the system of cross-border e-commerce may be implemented within trusted environment with such properties as interoperability and information security.

The forthcoming first steps to implement the above mentioned principles:

1) To initiate a dialog at the global level on cross-border regulatory exchange of information and start collecting information on existing practices in this area.

2) To exchange national experiences on co-regulatory initiatives of private sector in consultations with regulators.

3) To establish a cross-sector group on cross-border e-commerce.

4) To initiate the development of Interoperability Legal Framework at the global level.

5) Providing not direct interoperability ICT but ensuring recognition of certificates of authenticity of transmitted information in cross-border transmission. This can be achieved through the following steps: creation of national systems of certification authorities and national regulators of these systems; conclusion of an international agreement on mutual recognition and the conditions of mutual recognition of certificates of authenticity transmitted to the cross-border transmission of information.

6) Ensuring cross-border, transparency and accessibility requirements. It is required to develop a standardized process to ensure the integration and exchange of data with the legal significance, both within economies and between economies.

7) Overcoming linguistic barriers. Search for solution of the problem of incompatibility of existing standards, standard classifications, reference books (national, international, industry, etc.) used in the Internet economy and the development of electronic transactions and linguistic algorithms for information systems of e-commerce.

Appendix II

Use case of creating trusted environment for rescue systems

(This appendix does not form an integral part of this Recommendation.)

This Appendix describes an example of forming trusted environment in the domain of ensuring the safety of people in emergency situations.

Nowadays it is not easy for a person to navigate in technological environment. This problem becomes extremely actual in the case of an emergency, when the wrong action or procrastination leads to human victims. The use of modern ICT to create a different kind of warning and safety systems to assist the evacuation process can improve the safety of people in the case of an emergency.

Moreover, services of safety systems (e.g. notification, evacuation management) should be provided in trusted environment. This is related to a direct threat to human life or his activity that occurs in the case of an unwanted effect from the interaction or security breach in the environment.

The basic properties of trusted environment can be implemented in safety systems as follows:

Predictability: it is required to inform users about the possible operation scenarios of the system, the types of information provided by this system (audio, video, text or tactile messages) and its mission. It is required to pre-define the alarm messages and introduce to the users the verity of possible alarm messages. In the process of evacuation the system is required to use only familiar to users evacuation plans to minimize the perception time of information and avoid any delay that could lead to human victims.

Information security: It is required for the integrity and availability of warning signals, information about the evacuation process and other vital information in an emergency to be guaranteed for all users of the system.

Interoperability: all users of the system is required to be able to receive alarm messages and other information via any of the established public communication channels (cellular, radio and television broadcasting, Internet, etc.) and with any of available devices (mobile phone, smart phone, TV, etc.). It is required for the alarm messages and other emergency information to be provided for both residents (employees) and non-residents (visitors) in the appropriate language.

Availability of administration services: continuous customer support is required to be provided for all users of the system (residents, workers, visitors, etc.) in terms of assistance in safety related issues. All actions and instructions of the system is required to be recorded in a special vault (black box) in order to allow further establish their eligibility.

The basic principles of safety systems in trusted environment can be described as follows:

The principle of **non-discrimination** – in security systems based on ICT electronic alerts and evacuation instructions in case of emergency is required to have the same legal force and the same level of responsibility as the direct commands of rescue services.

The principle of **technological neutrality** – the information from the security system is required to be provided using all available for users technologies (see Interoperability).

The principle of **functional equivalence** – in security systems based on ICT electronic alerts and evacuation instructions in case of emergency is required to be equivalent to the direct commands of rescue services.

The principle of **unification** – the substantial part of the information from security system is required to be independent on transmission technology used in the communication channel.

The principle of **scalability** – the security system is required to support the connection of new users and groups, and ensure their interaction with the system immediately after the connection. For example, a man entered the building, in which there was an emergency, should be immediately informed about the emergency situation and his further actions should be corrected by the security system.

The principle of **equal reliability** – individual user characteristics (limits of hearing, vision, motor functions, etc.) is required not to affect the timeliness of the information provision, the eligibility notification and control process in an emergency evacuation.

The principle of **legalization** – the information from one security system is required to have full legal force in another within trusted environment. For example, the alarms from external security systems (federal, regional, municipal) should be relevant in the object security system (in the buildings) in the case of natural disasters. The object system is required to organize the evacuation process and other actions of people in the building in accordance with the external instructions to minimize the risk for human lives.

The principle of **client-orientation** – messages and signals from the security system is recommended to be personalized for user. For example, the object security system may support individualized management of the evacuation process and provide personal messages to mobile users terminals.

The principle of **systematization** – it is required to develop the uniform standards for security systems in trusted environment as well as the uniform set of instructions in case of emergencies.

The principle of **finiteness** – the security system is recommended to be implemented within a limited space (of the object, state, federal), in which the system will be maintained and improved: updating manuals, instructions, the set of supporting events, types of emergencies, types of natural and man-made disasters, technical characteristics of sensors, etc.

Bibliography

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications.*

5.

Overview of Trust Provisioning in ICT Infrastructures and Services

ID# 546-2901-544

Recommendation ITU-T Y.3052 (2017) – Overview of Trust Provisioning in ICT Infrastructures and Services

Table of Contents

LOW
MID
HIGH
RISK

Summary

This Recommendation provides an overview of trust provisioning in ICT infrastructures and services. It introduces necessity of trust to cope with potential risks due to lack of trust. The concept of trust provisioning is explained on the trusted ICT infrastructures and services. From the general concept of trust, the key characteristics of trust are described. In addition, the trust relationship model and trust evaluation based on the conceptual model of trust provisioning are introduced. Finally, it describes trust provisioning processes in ICT infrastructures and services.

NOTE – Details of potential risks and trustworthiness attributes, and use cases of trust provisioning are also provided in the informative appendices.

Keywords

Trust, Trust provisioning, Trust index, Trusted ICT infrastructure

1 Scope

This Recommendation provides an overview of trust provisioning in ICT infrastructures and services. More specifically, this Recommendation covers the following:

- potential risks and necessity of trust;
- trusted ICT infrastructures and services;
- the concept of trust and characteristics of trust;
- trust relationship model and trust evaluation based on the conceptual model of trust provisioning;
- trust provisioning processes.

NOTE – Detailed potential risks are provided in Appendix I, trustworthiness attributes is described in Appendix II, and use cases of trust provisioning are provided in Appendix III.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Trust: Trust is the measureable belief and/or confidence which represents accumulated value from history and the expecting value for future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of entities, value-chains among multiple stakeholders, and human behaviours including decision making.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPS	Cyber-Physical System
DIKW	Data, Information, Knowledge and Wisdom
ICT	Information and Communication Technology
IoT	Internet of Things

5 Conventions

None.

6 Introduction

As evolution of digital technologies, information and communication technology (ICT) infrastructures and services are increasingly important toward future knowledge society. ICT infrastructure not just only improves the transmission speed at which users send and receive multimedia data, but also allows individual users to enjoy previously inconceivable tools that improve life and business.

The world can be divided into physical, cyber, and social worlds. The physical world is composed of the physical things which connect to other physical things, controlled by human and device. The physical things have sensing and actuating capabilities. They can gather the raw data for data analysis and actuates the corresponding physical things autonomously.

In the cyber world, the ICT infrastructures and services provide computing, communication, and control platforms between human-to-human and human-to-machine. Big data analytics and cloud computing technologies are becoming important to drive value creation, and foster new products, processes, and markets. Moreover, it may be possible to invent a new eco-system by extracting accumulated knowledge from the raw data gathered by things in the physical world.

The social world contains social entities such as individual human beings and social organization. The ICT infrastructures and services enable the social entities to connect the cyber world. With the advent of online social network services, people can share their opinions and experiences in the cyber world. On the other hands, human-centric computing technologies make for human to interact with physical and cyber worlds by using human interfaces (i.e., five senses of human). Moreover, the knowledge extracted by big data analytics can give wisdom to human beings [b-Chen-2014]. ICT technologies also provide convergence services for various industrial areas to offer a common service platform. The ICT infrastructures and services act as glue for integrating physical, cyber, and social worlds.

6.1 Potential risks and necessity of trust

While ICT infrastructures and service have grown in size and complexity, the ICT world has risks, threats and vulnerabilities at component, device, system, service, and human levels. There are many potential risks in the world as follows.

- **Risks in nature**: Any scientific progress and technology development may incur potential risks. The development of new technologies may be sometimes undesirable if the certain levels of controllability and credibility are not guaranteed. Furthermore, the adaptation of new technologies may cause instability and insecurity since new technologies always have uncertainty. New technological revolution may provide great advantages for utilizing networking resources, however, it confronts unidentified risk beforehand.

- **Risks at the physical world:** Devices and sensors have been more and more integrated to ICT infrastructures which are sometimes unrecognized by humans. The physical components are usually resource-constrained, computation-limited, and resulting in poor security mechanisms implemented. Thus, they are vulnerable to both external and internal attacks.
- **Risks at the cyber world:** The number of vulnerabilities, threats, and cyber-attacks is increased in cyberspace. Cyber security and privacy mechanisms should protect both networks and services from unauthorized access. However, the large-scale data collection and data analytics can pose critical privacy, security, and trust issues. The risks of unanticipated uses of consumer data (such as human life and business behaviours) may be outstanding.
- **Risks at the social world:** Social networking services have given rise to numerous online communities and people use them as a communication medium. Also, social networking services try to connect as many people as possible. Since many people share their private activities on the social networks, their private information is propagated to others outside community. On the other hand, artificial intelligence or social internet of things, which try to mimic human, also have unexpected risks.
- **Risks from the integration of the physical, cyber, and social worlds:** In ICT infrastructures and services, entities in the physical, cyber, and social worlds are integrated. Cyber-physical system (CPS) cannot be fully operable if a physical world and a cyber world have some mismatch. If the malfunction of a physical system does not notify at the responsible entities in the cyber world, there are some risks to prevent safety in the physical world. Moreover, without recognizing a set of rules and external conditions of CPS, both humans and devices may understand or perceive CPS operations incorrectly, which may result on risks or failures of the integrated environment. Unintentional or intentional errors as well as mismatch of the integrated environment may be a primary cause or a contributing factor in risks and accidents.
- **Risks at data, information, knowledge, and wisdom process:** ICT infrastructures and services provide data, information, knowledge, and wisdom (DIKW)[1] process. As numerous data is generated, the number of erroneous data is also increasing. Malfunction of DIKW process, which may be caused by malicious inputs, misbehaviour of process itself, or unintended/intended manipulation, etc., creates false or biased results. There are also unidentified risks about entities, which produce and utilize DIKW.

NOTE – Detailed potential risks are explained in Appendix I.

ICT has an important role for the increasing interconnectivity in physical, cyber, and social worlds. However, the lack of trust have been invoked various problems as aforementioned. The large-scale data acquisition from sensors and devices in the physical world impose many issues, ranging from risks of unanticipated uses of consumer data offered by stakeholders to undesirable discrimination enabled by data analytics. If all the entities in ICT infrastructures and services are exploited for malicious intentions, it irreparable damage and uncertain dangers may be happened. Therefore, it is important to build the trusted ICT infrastructure to minimize the unexpected risks and maximize the survivability of physical, cyber, and social worlds.

The concept of trust infers belief and confidence, which the functional entities in ICT infrastructures and services will behave in expected ways. As ICT-based applications and services will scale over other industrial domains and involves multiple stakeholders, trust evaluation for corresponding value chains of business, as well as for system and component levels in a holistic manner may enable the users to have confidence on their services and applications. Consequently, the trust provisioning is one of the most important functional capabilities in the ICT infrastructures and services.

[1] DIKW (Data, Information, Knowledge and Wisdom) [b-Rowley]: This refers loosely to a class of models for representing purported structural and/or functional relationships between data, information, knowledge, and wisdom. "Typically information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge."

6.2 Trust provisioning in ICT infrastructures and services

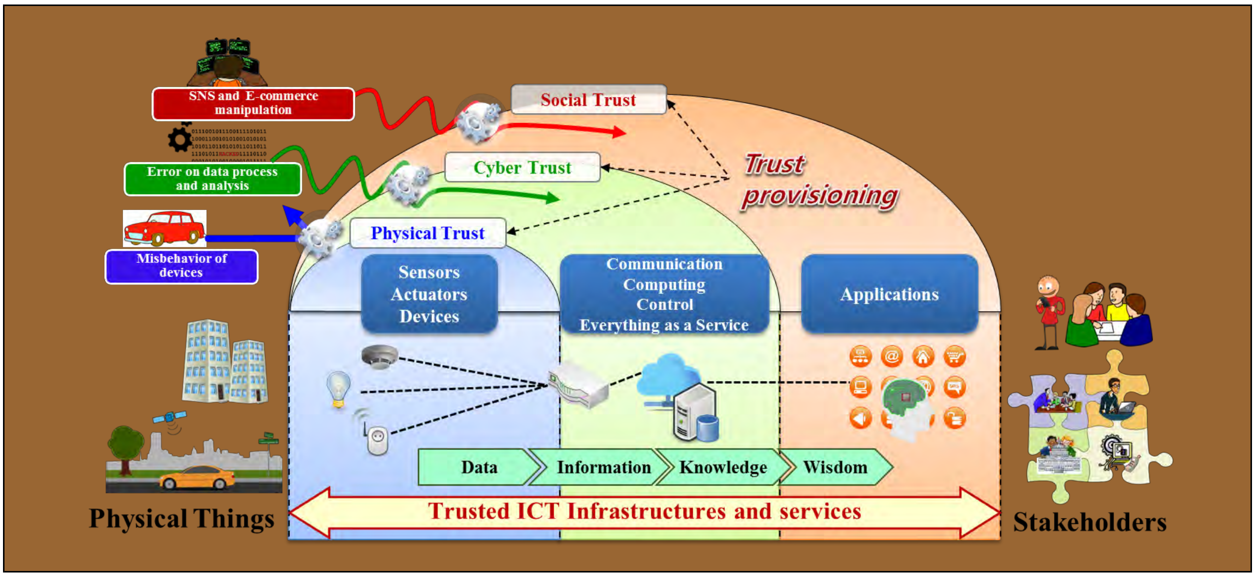


Figure 1 – The concept of trusted ICT infrastructures and services

Trust provisioning is an integral function for the physical, cyber, and social trust which provides a valuable method to minimize the risks through identifying trust characteristics of entities. Using trust provisioning, it is able to develop trusted ICT infrastructures and services that cooperate with ICT applications in order to support these applications and services for better quality of services and experience by mitigating inherent and extraneous risks.

Figure 1 shows the concept of trusted ICT infrastructures and services. Three types of trust provisioning are classified into physical trust for physical things (including sensors, actuators, and devices), cyber trust for communication, computing, and control, and social trust for stakeholders, which are mapped with trust in physical, cyber, and social worlds, respectively. In the trusted ICT world, trust entities may assume to take DIKW processes to minimize potential risks and maximize value of assets.

NOTE – Detailed explanations of physical, cyber, and social trust are described in clause 7.3

7 Overview of trust and trust provisioning

7.1 Concept of Trust

Trust concept itself is a complicated notion with different meanings depending on both participators (i.e., a trustor is an entity that trusts the other entity, who is a trustee in reverse direction) and situations, and influenced by both measurable and non-measurable factors. From a sociological point of view, trust is defined as the trusting behaviour that one person suspect another person in a situation where an ambiguous path exists. In such situation, trust is used to mitigate risks of business dealings with others. Trust is also interpreted as the capacity and belief of an entity that the other entity would meet its expectations.

The term trust in the contexts of the physical and cyber worlds differs from that of the social world. Trust in the social world can be viewed as a subjective expectation that a social entity predicts about other social entity’s future behaviour. On the other hand, trust in physical and cyber worlds can be viewed as the expecting performances that a physical thing or a cyber object will accomplish a given task in an expected manner to fulfil its intended purpose.

In the ICT environments, trust affects the preference of an entity to consume a particular service offered by another entity. It also affects the decision making of an entity to transact with other entity. The trust evaluation is especially significant in the ICT environments where a huge number of entities mutually interact with each other to provide and consume the information and/or resources.

From the perspectives of standardization, trust should be quantitatively and/or qualitatively calculated and measured, which is used to evaluate values of physical components, value-chains among multiple stakeholders, and human behaviours including decision making. Trust is an important factor on the decision-making process not only used by humans but also by application and service transactions in ICT environments. Therefore, trust has been highlighted to evaluate the functional capabilities of ICT resources, as well as the ICT services and applications.

When a trustor and a trustee make trust relationships, both the trustor and the trustee have their own characteristics so-called trust propensity and trustworthiness, respectively [b-Mayer]. Trust propensity (i.e., characteristic of the trustor) is a trait that leads to a generalized expectation about the trustworthiness of others. Trustworthiness (i.e., characteristic of the trustee) refers to a property that can be trusted and relied upon the trustee.

In general, a trustor considers three main sources of information when seeking for trust as own understanding about a trustee (as knowledge), personal expertise about the situation and the context (as experience), and public evidences on the trustee (as reputation). Knowledge can be characterized as direct trustworthiness attributes. It is measured from the primary data which are available to the trustor at first hand even before any meaningful communication would happened. On the other hand, experience and reputation information can be reflected as indirect trustworthiness attributes which are estimated basically from secondary data, often available after at least one interaction with each other.

7.1.1 Direct trust

Figure 2 shows various trustworthiness attributes that are categorized into three major factors: ability, integrity, and benevolence [b-Mayer, b-Colquitt]. Many attributes can represent trustworthiness, which can be applied to ICT infrastructures and services.

– **Ability (or capability)**: Ability means characteristics that enable an entity to have influence within some specific contexts. The ability is specific because the trustee may be highly competent in some technical area, affording that person is trusted on tasks related to that specific area. The attributes related to ability include robustness, safety, stability, scalability, and reliability, etc.

– **Integrity (or honesty)**: Integrity means the quality of being honest and fair in the social world or means the state of being complete in cyber and physical worlds. In terms of information, integrity means that information of an object is prevented from being modified; in other words, information consistency by assuring that information will not be accidentally or maliciously altered or destroyed. The attributes related to integrity include completeness, consistency, accuracy, certainty, and recency, etc.

– **Benevolence (or cooperation)**: Benevolence means the desire to do well to others, in other words, working or acting together willingly for a common purpose or benefit when trustor has an interaction with trustee. Benevolence is also the extent to which a trustee is believed to do good to the trustor, aside from an egocentric profit motive. The attributes related to benevolence include availability, assurance, relevance, and credibility, etc.

NOTE – Appendix II provides detailed information about trustworthiness attributes.

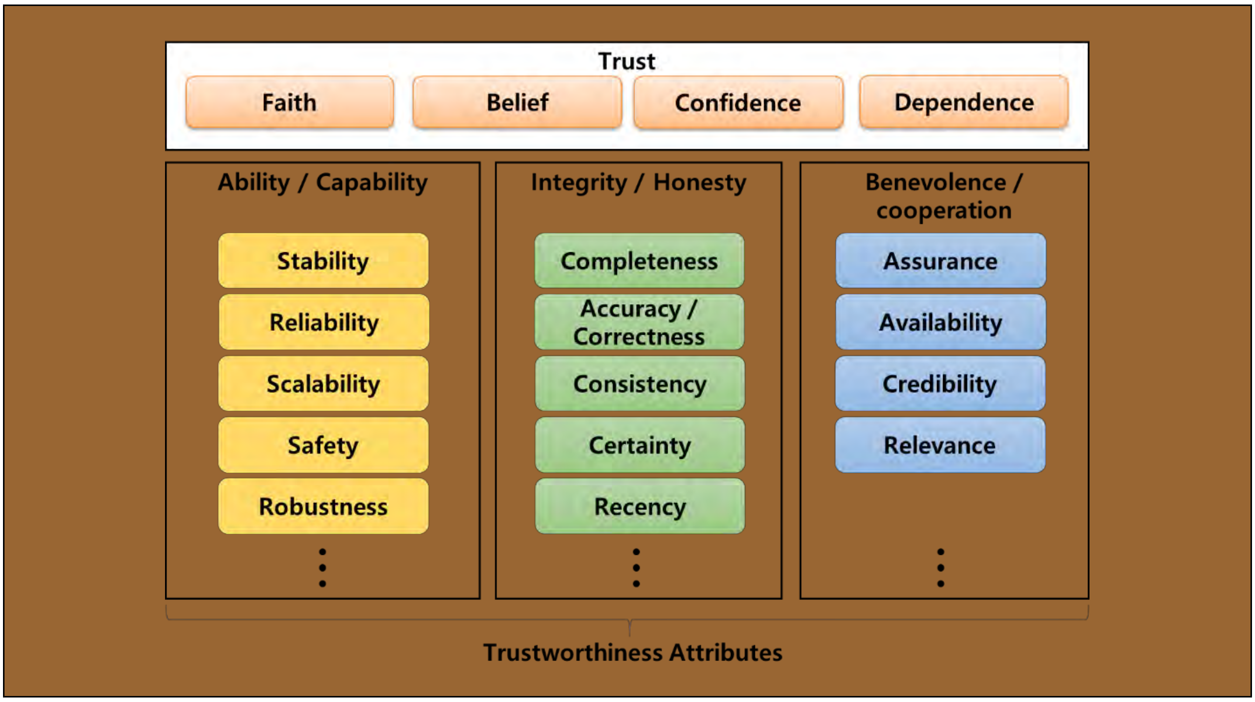


Figure 2 – Attributes related to trustworthiness

7.1.2 Indirect trust

Indirect trust is formed from the self-judgment about the situation and third party reputations. Unlike direct trust, indirect trust is derived via the experience gained through previous conversations with the trustee and the reputation gained through the global views on the trustee, respectively. This is particularly important in a circumstance where information to estimate trustworthiness attributes are not available at first-hand.

– **Experience**

The experience represents a personal observation considering only interactions from a trustor to a trustee. Experience is achieved by accumulating state of the interactions among entities over time. The left hand side of Figure 3 illustrates how the trust based on experience is formed between the trustor and the trustee using the previous interactions between the two.

– **Reputation**

Reputation is a public assessment of the trustor regarding the trustee's prior behaviour and performance. Reputation can be evaluated based on accumulated experiences of trustors about the trustee as shown in the right hand side of Figure 3. To acquire trust information based on the reputation of a trustee, two kinds of information are necessary to examine: (i) the previous trust transactions from all entities to the trustee; and (ii) the relationship between a trustor to the trustee.

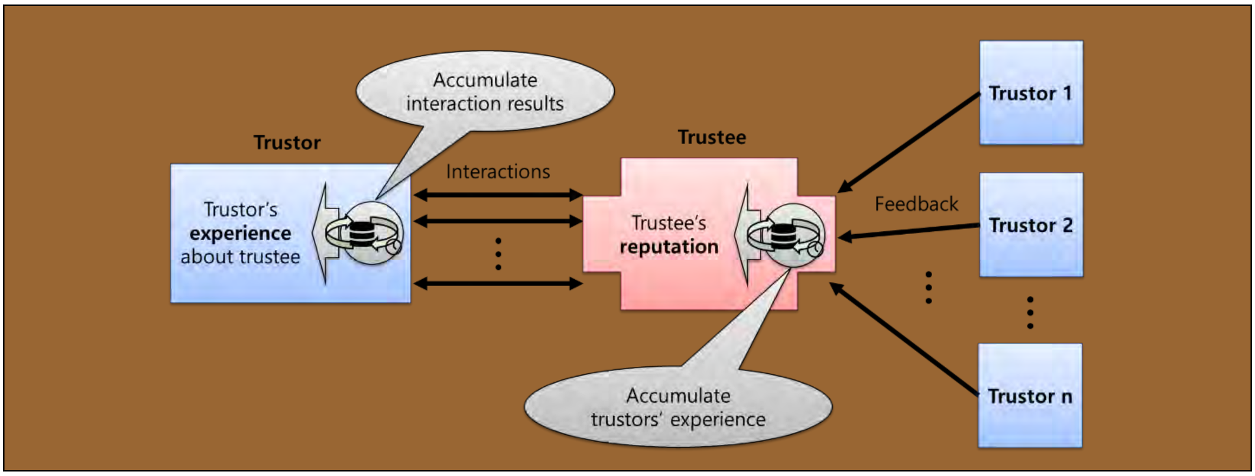

Accumulate interaction results
Trustor
Trustor's experience about trustee
Interactions
Trustee
Trustee's reputation
Feedback
Trustor 1
Trustor 2
Trustor n
Accumulate trustors' experience

Figure 3 – Indirect trust (experience and reputation)

7.2 Fundamental characteristics of trust

There are several important characteristics of trust that further enhance our understanding of trust.

– **Trust is dynamic**: trust applies only in a given time period and maybe change as time goes by.

NOTE – For the past one year Alice highly trusts Bob. However, today Alice found that Bob lied to her; consequently, Alice no longer trusts Bob.

– **Trust is context-dependent**: trust applies only in a given context. The degree of trust on different contexts is significantly different.

NOTE – Alice may trust Bob to provide financial advice but not for medical advice. Also, the articulation of trust context in two entities may differ based on the opposing perspective. For example, Alice trusts Bob in the context of "buying" book; however, the context from Bob to Alice is "selling" book.

– **Trust is not transitive in nature but maybe transitive within a given context**: when entity A trusts entity B and entity B trusts entity C, entity A may or may not trust entity C. Entity A may trust any entity and entity B trusts entity C in a given context although this derived trust may be explicit and hard to be quantified. Also, the time period of trusting relationship may be defined differently between the entities.

NOTE – Alice trusts Bob for three years, however, Bob may think that the trust relationship only lasts for one year.

– **Trust is an asymmetric relationship**: trust is a non-mutual reciprocal in nature. That means if entity A trusts entity B, then the statement "entity B trusts entity A" is not always true.

– **Trust is subjective**: trust is influenced by or based on personal feelings. Also, the degree of seriousness in trust relationships may differ between the entities.

NOTE – Bob gives an opinion about music. If Alice thinks that Bob's music recommendation was good, she will trust Bob's review. However, John may think differently about Bob's opinions and may not trust his review.

7.3 Model for trust provisioning

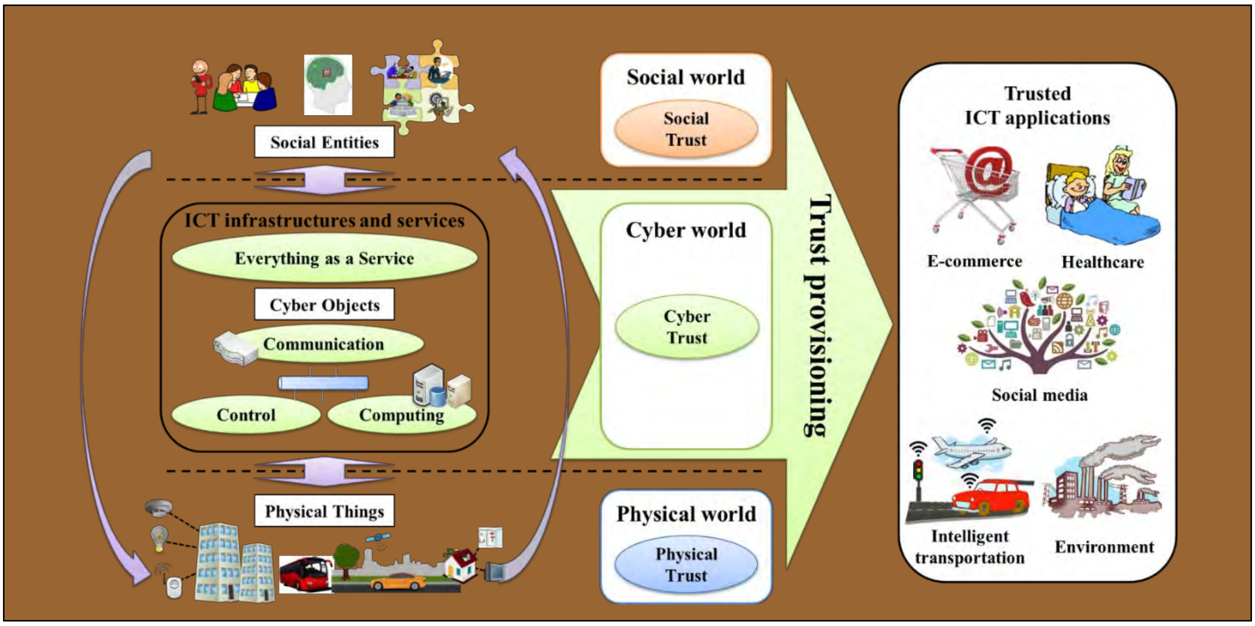


Figure 4 – Trust provisioning in the ICT world for trusted ICT applications

With the perspectives of trust provisioning, there are physical, cyber, and social worlds. To build ICT ecosystem, the raw data from physical things in the physical world are produced by physical interfaces like sensors and actuators. In the cyber world, there are physical objects and logical objects. Physical objects are the objects mapping to hardware devices and equipment which have capabilities of data processing, data storage, and communication, etc. Logical objects are algorithms, functions, and software which are working over computing, storage, and networking components. In the social world, social entities like human, stakeholders, and software agents, which are a computer program that acts for a user, produce and consume various data and applications through user interfaces. Physical things, cyber objects, and social entities make interactions to perform trusted ICT applications with considering physical, cyber, and social trust, respectively. Figure 4 shows trust provisioning in the ICT world to realize various trusted ICT applications.

– **Physical trust**: The physical trust reflects various trust aspects of physical things, which can be measured by counting on its trustworthiness in terms of capability, integrity, and cooperation. Its capability means the ability of the physical thing to perform its task with correct functionality. Its integrity means the state of the physical thing being stable without trouble or breakdown. Its cooperation means that the physical thing is working together with other physical things for their common purposes. The physical trust reflects trust propensity which is affected by risks related to the physical world.

– **Cyber trust**: The cyber trust reflects various trust aspects of cyber objects, which can be measured by counting on its trustworthiness in terms of capability, integrity, and cooperation. Its capability means that the ability of a cyber object is correct and assured to execute control, computing, and communication. Its integrity means that data handled or provided by cyber objects are not accidentally or maliciously altered or destroyed during control, computing, and communication. Its cooperation means how much the cyber object is well working together with other objects. The cyber trust reflects trust propensity which is affected by risks at the cyber world.

– **Social trust**: The social trust reflects various trust aspects of social entities. A social trust can be measured by considering its trustworthiness in terms of ability, honesty, and benevolence. Its ability means human competence in his/her activity. Its honesty implies that the social entity treats others honestly. Its benevolence means how much the social entity behaves nicely to other social entities or how much the social entity has interactions with other entities for their kindness. The social trust reflects trust propensity which is affected by risks at the social world.

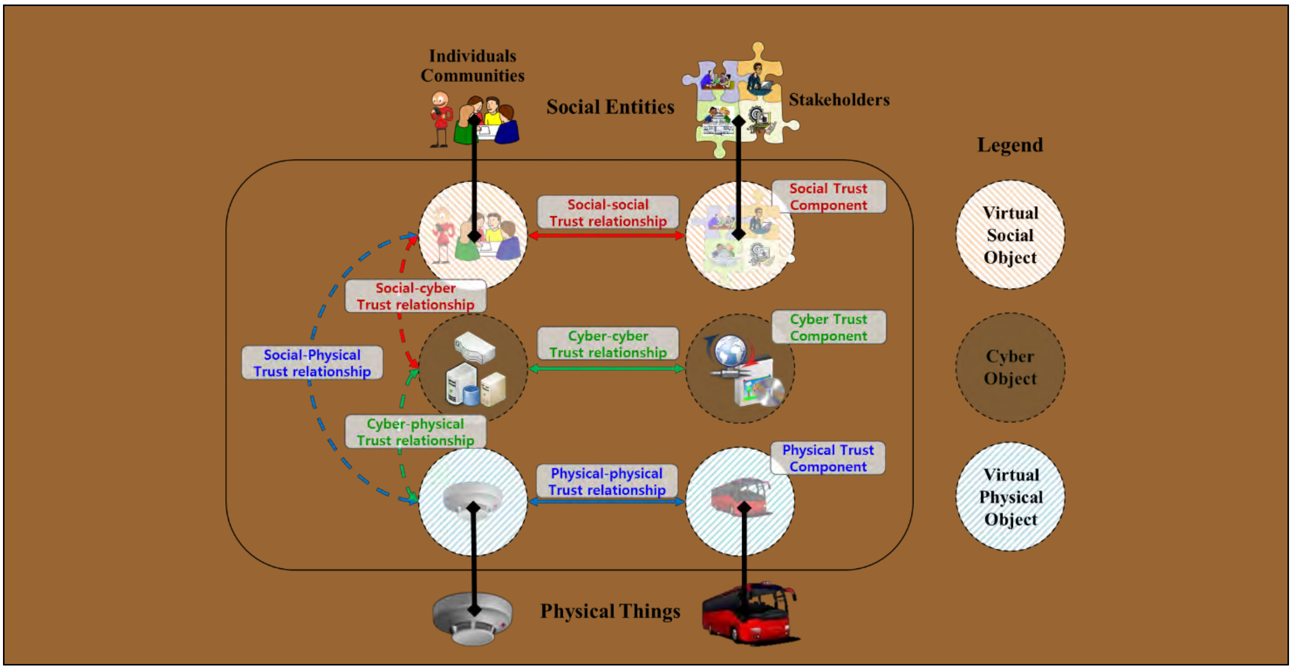

Individuals
Communities
Social Entities
Stakeholders
Legend
Social-social Trust relationship
Social Trust Component
Virtual Social Object
Social-cyber Trust relationship
Social-Physical Trust relationship
Cyber-cyber Trust relationship
Cyber Trust Component
Cyber Object
Cyber-physical Trust relationship
Physical-physical Trust relationship
Physical Trust Component
Virtual Physical Object
Physical Things

Figure 5 – Trust relationship model

In trust relationship model, cyber objects and virtual objects are linked with physical things and social entities as shown in Figure 5. A virtual physical object is the virtualized model of physical thing through physical interfaces such as sensors and actuators. The cyber objects are modelled as physical objects and logical objects. The physical object is modelled of hardware device and equipment and the logical object is modelled by the corresponding software. A virtual social object is the virtual model of social entity through applications and user interfaces. Virtual physical objects, cyber objects, and virtual social objects can be seen as the trust components for physical trust, cyber trust, and social trust, respectively.

Based on the model of physical, cyber, and social trust components, there are various trust relationships in ICT infrastructures and services horizontally: social-social trust relationship, cyber-cyber trust relationship, and physical-physical trust relationship. Also, trust relationships of trust components are established vertically among different types of trust components: social-cyber trust relationship, cyber-physical trust relationship, and social-physical trust relationship. When a trust component establishes trust relationships with others, the component gets trust information from others.

7.4 Trust evaluation for trust provisioning

To compare the degree of trust of different entities, a method is needed to measure, quantify, and assess trust. Trust evaluation is the way from input data of various sources to calculate trust for the target services or objects. Three types of trust information are defined as follows.

- **Trust attribute**: Trust attributes represent characteristics of an entity (include direct and indirect trust), which consists of qualitative and quantitative attributes. Trust attributes refer to properties and features of an entity that can be trusted upon. Qualitative attributes need the quantization process to accumulate with quantitative attributes.
- **Trust indicator**: Trust indicators are used to calculate a trust index by combining qualitative and quantitative attributes of trust. Objective trust indicators stand for features that represent trustworthiness of an entity quantitatively. Subjective trust indicators reflect subjective or personal attributes of trust entities. The trust indicators are calculated at the measurement instance of their trustworthiness since their values are changing as time goes.
- **Trust index**: A trust index is a composite and relative value that combines multiple trust indicators into one benchmark measure for representing trustworthiness of an entity, which is similar to ICT development index or stock market index. A trust index is a comprehensive accumulation of the

objective trust indicators and the objectified subjective trust indicators which are objectified for calculation. A trust index evaluates and quantifies trustworthiness of trustee.

For trust evaluation as shown in Figure 6, it is needed to collect data from various sources. Collected data are categorized into two trust attributes, i.e., qualitative and quantitative attributes. Trust attributes are self-accumulated from the inputs of various sources. Trust attributes are used to calculate trust indicators. Trust indicators also have the self-accumulated properties from subjective and/or objectives attributes. It notes that the time-varying behaviours of trust indicators also appeared by accumulation of every new instance. A trust index is calculated by the self-accumulated manner with combination of objective trust indicators and subjective trust indicators. The trustor finally makes a decision with a certain a trust value. A trust value represents a numerical quantity decide an entity's trust in a trustor's perspective. Based on trust indicators and trust index about the entity, the trustor obtains a trust value of the entity to make a decision.

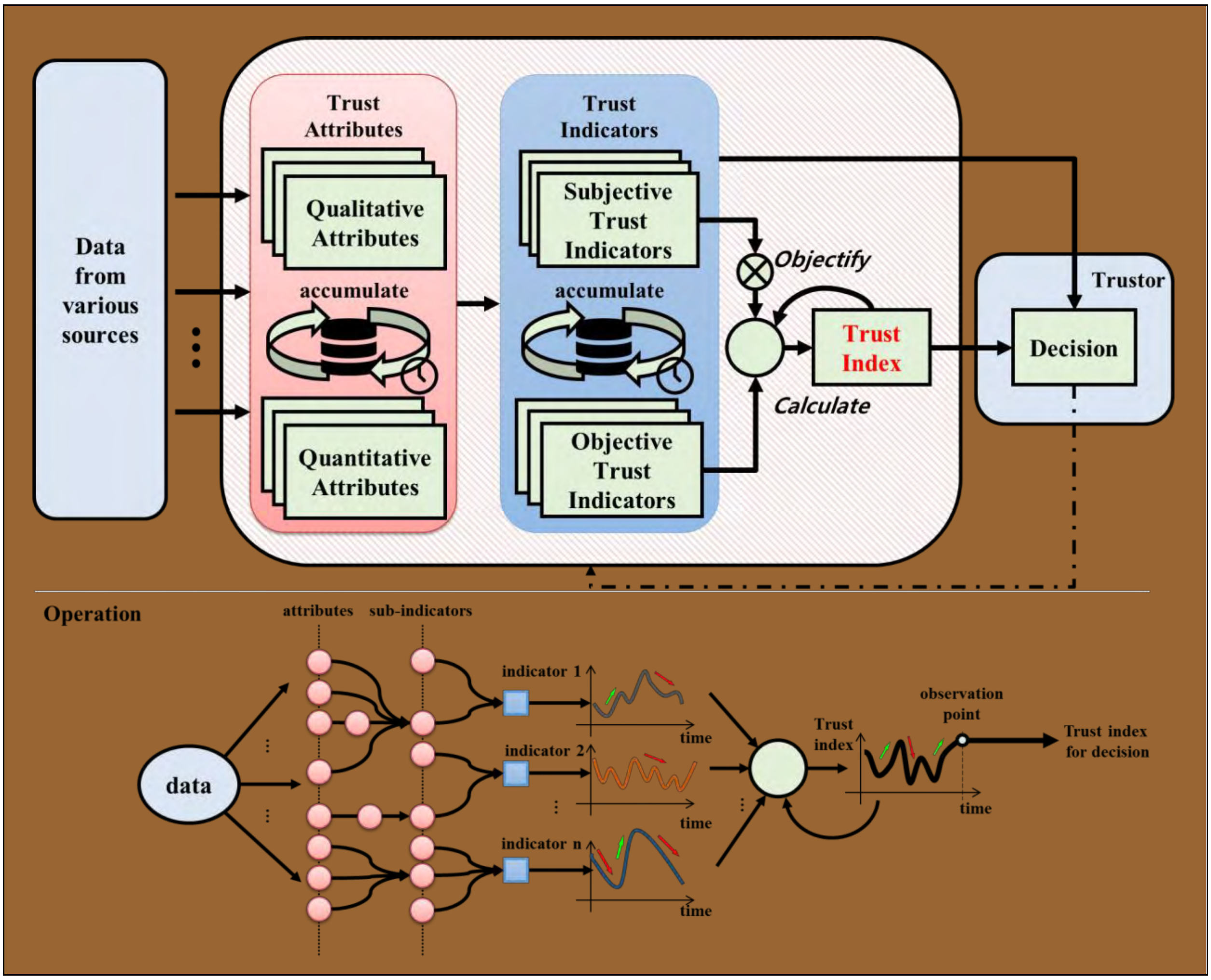


Figure 6 – Trust evaluation for trust provisioning

8 Trust provisioning processes

Trust provisioning in ICT infrastructures and services consists of a set of processes, which include gathering data from entities, producing and distributing trust information by evaluating all aspects of trust, to support entities' decision making for establishing trust relationship with other entities. This clause describes trust provisioning processes as follow: i) data collection, ii) data management, iii) trust information analysis, iv) dissemination of trust information, and v) trust information lifecycle management.

8.1 Data collection

Data collection process conducts to collect raw data for trust information. Data collection should be deliberated on what and how many data should be collected. Collection of data are tightly related to the purpose of trust provisioning. Data should be collected with acceptable expense to extract relevant trust information because excessive collection of data may cause privacy problems.

8.2 Data management

In this process, the collected data is used to generate trust information. Data are carefully handled with the regard of trustworthiness. As the number of data sources and types are dramatically increased, the trustworthiness of data itself is significant. Because false data will lead to degrade the accuracy of trust information and increase waste of resources, it is important to detect corrupt or polluted data. In the perspective of data management, the data should be protected to extract the correct trust information.

8.3 Trust information analysis

Trust information analysis process extracts the meaningful trust information from data. Because trust can be measured by considerations of the complicate relationship between the trustor and the trustee, trust information explicitly reflects the trust relationship in the objective and subjective manners.

As much as the ICT environments are emerging, building trust is much more challenging. Since trust is difficult to be quantified, the exact trustworthiness value of an entity may have different interpretation. The trust attributes should be defined as mutually independent characteristics of entities. They may reflect the dynamic characteristics of trust.

A trust model is a method to specify, build, evaluate and ensure trust relationships among entities. The trust model is used to obtain the trust information. The trust model is designed to understand trust characteristics and account trust factors. Since a trust model is domain-specific, there exist numerous ways to define a trust model according to application domains. In order to calculate a trust index for specific applications, the common indicators should be developed to identify trust characteristics of an entity and compare with trust indices of different entities.

8.4 Dissemination of trust information

Dissemination of trust information means a way to distribute trust information to others. There are various ways of disseminating trust information in different domains (e.g., binary data transmission in the physical world, service/product recommendations in the cyber world, and information visualization considering human perceptions in the social world). The efficient, effective, and suitable dissemination methods should be developed so that a trustor can determine trust of the trustee with the subjective criteria of trust information.

8.5 Trust information lifecycle management

Because of the dynamic characteristic of trust, trust information is created, updated and abolished as time goes. The trust information is replaced due to the change of a trust component. The feedback from the trustor who receives trust information of the trustee also could be used to recalculate trust values during the update phase. At the update phase, the trust index is updated and trust value is re-evaluated.

NOTE – Appendix III provides trust provisioning use cases.

9 Security considerations

Trust is the concept that can cover security and privacy. Security is considered as technological aspects, and privacy is considered as user aspects. By utilizing security and privacy mechanisms, trust can be realized in ICT infrastructures and services.

Appendix I

Detailed potential risks in ICT infrastructures and services

(This appendix does not form an integral part of this Recommendation.)

This appendix provides detailed potential risks in ICT infrastructures and services with respect to physical, cyber, and social worlds.

I.1 Risks at the physical world

– **Natural threats [b-Brauch]**

Natural threats such as earthquakes, hurricanes, floods, and fire could cause severe damages to physical components and computer systems. It is hard to predict and prevent natural disasters in advance, and few safeguards can be implemented against them.

– **Physical threats**

Outbreaks caused by physical threats tamper with hardware components and device protocols such as insertion of positive reputation and recommendation values into a untrustworthy device, inserting and booting with fraudulent or modified software, and environmental/side-channel manipulation, both before and after of the device's deployment.

Trust and privacy are also issues in the physical world due to the broadcast nature of the communication media. Confidential information communication is vulnerable over a network in the presence of eavesdroppers that may intercept the information exchange between legitimate terminals and interrupt the desired behaviour of the legitimate users and devices.

On the other hand, inadequate and unreliable information or physically unstable devices themselves can make potential risks to the proper behaviour of the system. Furthermore, due to interdependencies, the system structure (e.g., cascade or parallel) and compatibility issues among systems can do more harm than expected.

I.2 Risks at the cyber world

a) **Cyber/Information security threats** [b-Wilson]

1) Threats on the core network such as delivery of fake trust information, impersonation of devices, traffic tunnelling between impersonated devices, and mis-configuration of the firewall in the network equipment could be the target of several kinds of hazards.
2) Configuration vulnerabilities such as fraudulent software update/configuration changes, mis-configuration by the software agents, subscribers, users, or the owner, and mis-configuration or compromise of the access control lists.
3) Compromise of credentials comprising brute force attacks on authentication tokens and algorithms, physical intrusion, or side-channel attacks, and malicious cloning of authentication tokens.
4) User data and identity privacy attacks including eavesdropping for other users or devices data sent over the systems; masquerading as other user/subscribers device; user's network identifier or other confidential data revealed to unauthorized third parties.
5) Access vulnerabilities is that unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access vulnerabilities; the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to Internet-connected devices.

b) **Privacy threats** [b-Weber]

Privacy protection, especially in Internet of Things (IoT) environments, has become increasingly challenging due to large volumes of information easily available through remote access mechanisms.

1) **Lack of control and information asymmetry:** interaction between objects that communicate automatically and by default, between objects and individuals´ devices, between individuals and other objects, and between objects and back-end systems, will result in the generation of data flows that can hardly be managed with the traditional tools that have been used to ensure the adequate protection of the data subjects' interests and rights.

2) **Quality of the user´s consent:** the possibility of rejecting certain services is not a real alternative in IoT environments and classic mechanisms used to obtain consent are hardly applicable. Therefore, new ways of obtaining the user´s valid consent should be considered, including implementing consent mechanisms through the devices themselves as privacy proxies and "sticky" policies (conditions and constraints attached to data that describe how it should be treated).

3) **Inferences derived from data and repurposing of original processing:** secondary uses of data, inferences from raw information, sensor fusion, make important that at each level IoT stakeholders make sure that the data is used for purposes that are compatible with the original purpose of the processing and that those purposes are known by the user.

4) **Intrusive identification of behaviour patterns and profiling:** generating knowledge from trivial or even anonymous data will be made easy by the proliferation of sensors and that might enable very detailed and comprehensive life and behaviour patterns.

5) **Security risks:** weak points can occur not only at device level but also in the communication links, storage infrastructure and other inputs of this ecosystem.

c) **Cyber-crimes**

The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, a violation of patent, trade secret, copyright laws, identity theft, brand theft, and fraud. In addition, cybercrime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data.

Botnets are becoming a major tool for cybercrime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal.

Malicious codes, such as computer viruses, are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer when the user opens an email attachment, or clicks an innocent-looking link on a website.

I.3 Risks at the social world

a) **Risk of lacking trust in interactions**

1) **Human-to-human interactions:** If there is no trust among peoples, their interactions (e.g., exchanging data and information) have meaningless due to lack of confidence with each other. If the people are not trustworthy, personal interactions do not invoke any response. The unclear decision making or unrealistic situation may be happening from low or broken trust in human relationships.

2) **Human-to-machine interactions:** When a human cannot trust a machine (e.g., delivering imprecise data from a machine to a human), human-to-machine interactions cannot be established and potential benefits on system performance will be lost. The human-machine systems have always proved unpredictable and fallible, whereas the nature of the system is to function normally. It relies on technological dependency which accentuates risks.

b) **Threats in the social world** [b-Chen-2015]

A malicious entity is dishonest and socially uncooperative in nature and can break the basic functionality of the ICT infrastructures and services. The entity can perform the following attacks.

1) **Self-promoting attacks:** a malicious user can intentionally promote its importance (by providing good recommendations for itself) in order to be selected as the service provider, but then it provides malfunctioned service.

2) **Whitewashing attacks:** a malicious entity can disappear and re-join the application to wash away its bad reputation.

3) **Discriminatory attacks:** a malicious entity can discriminatively attack non-friends or entities without strong social ties (without many common friends) because of human nature or propensity towards friends in social networks.

4) **Bad-mouthing attacks:** a malicious entity can ruin the reputation of another well-behaved entity by providing bad recommendations so as to decrease the chance of this good entity being selected as a service provider. This is a form of collusion attacks, i.e., it can collaborate with other bad entities to ruin the reputation of the good entity.

5) **Ballot-stuffing attacks:** a malicious entity can boost the reputation of another bad entity by providing good recommendations for it so as to increase the chance of this bad entity being selected as a service provider. This is also a form of collusion attacks, i.e., it can collaborate with other bad entities to boost the reputation of each other.

c) Threats in social networks

Social networking tools have changed the way people interact in their personal life and business. Increasingly, these tools play a significant role in how business gets done; however, they also have risks as follows [b-PANet].

1) **Phishing bait**: Many users of the social networking services had their accounts compromised. Although this was only a tiny fraction of a percent, it is still a significant number considering that famous social networking services have over several million users. To their credit, the social networking services acted quickly, working to blacklist that domain, but many copycat efforts ensued.

2) **Data leaks**: Social networks are all about sharing. Unfortunately, many users may share too much sensitive information about their organizations such as projects, products, financial, organizational changes, and/or scandals, etc.

3) **Botnets**: Recently, the accounts of a social networking service are used as the command and control channel for a few botnets. It is shutting these accounts down given the ease of access of infected machines via the social networking service.

4) **Advanced persistent threats**: One of the key elements of advanced persistent threats is the gathering of intelligences of persons of interest, for which social networks are a data source. Perpetrators use this information to further their threats by placing more intelligence gathering (e.g., malware, Trojans), and then gaining access to sensitive systems.

5) **Cross-site request forgery**: This attacks exploit the trust that a social networking application has in a logged-in user's browser. Consequently, as long as the social network application is not checking the referrer header, it is easy for an attack to share an image in a user's event stream that other users might click on to catch and spread the attacks.

6) **Impersonation**: The social network accounts of several prominent individuals with thousands of followers have been hacked. Furthermore, several impersonators have gathered hundreds and thousands of followers.

I.4 Risks from the integration of the physical, cyber, and social worlds

a) A numerous number of ICT resources

Risks threaten ICT infrastructures and services to cope with complexity of interactions and mechanisms of the entities. The access of a large number of ICT resources causes irreparable damages and creates unpredictable dangers. It is essential to make ICT resources accessible to all the people with promises but with unknown dangers.

b) **Complexity of network operation**

There are many algorithms for network resource optimization including efficient routing, congestion avoidance, and guaranteeing quality of service and quality of experience. When the unpredictable situations are happened in a network, the out-of-service possibility is increasing. Intentional attacks from outside (e.g., distributed denial-of-service attacks) are also a part of risks. While network control functions can arrange the by-pass or de-tour route to cope with overflowed traffic, the unexpected side effects like traffic fluctuation and domino effect may bring additional risks. To increase network survivability during network operation, networking protocols and operations, administrations, maintenance, and provisioning functions should be re-designed to be trustworthy. Moreover, when a network infrastructure includes a cloud platform with large volume of storage and processing capabilities, network instability is not coming only from traffic congestion. The operation of the cloud platform and high level applications are additional harmful sources to increase network risks. The existing security functions including firewall and deep packet inspection may be replaced to provide the certain level of trust, through the implementation by a trust gateway system and trust-guaranteed network operations, administrations, and maintenance functions.

Appendix II

Trustworthiness attributes

(This appendix does not form an integral part of this Recommendation.)

This appendix provides some descriptions about trustworthiness attributes. Table II.1 shows general description of trustworthiness attributes which are introduced in clause 7.1.1.

Table II.1 – Trustworthiness attributes

Trust-worthiness	Attributes	Description
Ability / Capability	Stability	The quality or state of something that is not easily changed or likely to change at any time.
		Stability means that a physical things perform its own operation consistently. That is, with a given input, the physical thing always gives the same output. Users may consider cyber objects to be stable if they performs communication, control, and computing functions work continuously. In other words, stability might imply that a stakeholder continuously performs his/her role.
	Reliability	The ability of an entity to perform a required function sufficiently under any conditions.
		Reliability means that a physical thing works properly by following user's requests at any condition. The reliability of a cyber object might imply that the cyber object fulfils the required quality of service. The reliability can be measured as probability that an entity correctly performs a required job in a specified period of time under stated conditions.
	Scalability	The ability of something to adapt to increased demands. The capability of a system or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.
		Cyber-physical systems which can afford to handle numerous sensors and their measured data might be judged scalable. Cyber objects that can process huge amount of queries and requests also might be considered as scalable.
	Safety	The ability to protect the entity from existing risk and danger; the ability to take care of oneself not to be in danger of oneself. The ability to operate without risk of injury or harm to users and the system's environment.
		A service that adopts the cyber security system might be thought safe from existing internal and external cyber-attack. On the other hands, the device itself might be safe when the device satisfies safety certification of each country.
	Robustness	Strong and effective in all or most situations and conditions. The ability of a system to cope with errors during execution and erroneous input. The capability of the service to behave in an acceptable way in anomalous or unexpected situations or when the context changes.
		Users might consider the system with backup process and fault tolerant robust. For example, the communication system might be established with robustness by installing duplicate paths to each

Trust-worthiness	Attributes	Description
		destination. The robustness might also consider the financial status of stakeholder because it explains whether the stakeholder can have an ability to endure the financial crisis or not.
Integrity / Honesty	Accuracy / Correctness	The condition or quality of being true, correct, or exact. Freedom from error or defect. Set or make true, accurate, or right. Remove the errors or faults.
		Accuracy means the degree of difference between the truth and the present. This trust attribute does not imply the ability to measure the environment correctly or the ability to correct the error, but implies the willingness to measure the truth. A physical thing with appropriate sensors and a cyber object not infected by any viruses might have accuracy and they give the correct data to other.
	Consistency	Steadfast adherence to the same principles, course, form, etc.
		Data consistency refers to the usability of data; Data must be consistent within the confines of many different transaction streams from one or more applications. Once a person makes a decision, takes a stand, or performs an action, he or she strives to make all future behaviour match this past behaviour.
	Certainty	Free from doubt or reservation or satisfaction of someone’s expectation.
		Certainty means that the entity works exactly following someone’s expectation. It is possible to consider the entity has certainty when a physical thing and a cyber object perform their own function without any exception.
	Recency	Reducing the duration left from the revision of the data.
		Trust is dynamic, so the measurement of data needs to be conducted as soon as possible for the accuracy of the data.
Benevolence / Cooperation	Assurance	A positive declaration intended to give confidence. It also means promise, pledge; guaranty, or surety.
		The degree of confidence that the process or deliverable meets defined characteristics or objectives. That is, assurance implies the guaranteed value how much the trustee can cooperate with the trustor.
	Credibility	The quality of being believable or worthy of trust.
		Credibility indicates the degree to which the trustor believes that trustee will participate in the collaboration. Trustee might provide the assurance to the trustor to notify the degree to guarantee the degree to participate in the cooperation; however, the trustor might determine the trust of trustee by analysing not only the assurance but also the credibility. Credibility in information might be measured based on the level of uncertainty, which is observed with conflicting, incomplete, etc. Credibility in social media might be measured by statistical methods.
	Relevance	The degree connected with the matter in hand; the relation between the trustor and the trustee.
		Relevance of entities might be measured by similarity, for example, the number of interactions among entities, and etc. Similarity represents how many common criteria, attributes or behaviour patterns exist between entities.

Trust-worthiness	Attributes	Description
	Availability	The ability of the system to be in a state to perform adequately at a given instant of time within a given time interval.
		Availability might be measured with the amount of capacity of the trustee to cooperate or help the trustor. The limit of the cooperation or benevolence might be restricted by the availability of the trustee.
	Cooperation	Working or acting together willingly for a common purpose or benefit.
		The number of interactions between entities that have been held in positive manner. For example, in communication networks, packet dropping or forwarding behaviour is used to estimate cooperative behaviour of a node. In information networks, whether sharing information or not would reflect an aspect of cooperative behaviours. In social networks, prompt and/or frequent email replies can be regarded as cooperative behaviour.

Appendix III

Trust provisioning use cases

(This appendix does not form an integral part of this Recommendation.)

This appendix provides trust provisioning use cases in ICT infrastructures and services. In this appendix, five use cases are introduced: peer-to-peer accommodation, smart office sharing, document sharing service, intermediate device selection for device-to-device environment, and used car sharing service. Each use case describes following items:

– Description: describes its background including high level description and illustration;

– Actors: play a role in each use case;

– Service flow: describes a detailed service flow for each use case.

III.1 Trustworthy Peer-to-Peer Accommodation service

III.1.1 Description

This use case shows a peer-to-peer accommodation service scenario when a peer-to-peer accommodation service provider connects hosts (vendors of rooms/accommodations) and travellers. Hosts provide their available rooms through the service provider, and travellers choose rooms based on price, grade of facilities, review scores, etc. When a traveller chooses the room a host will make decision whether accept the traveller or not. During this transaction, there are three trust of entities: i) trust of the accommodation, ii) trust of the host, and iii) trust of the traveller. Trust information provider collects data, which can be utilized for calculating trust index, and provides trust index to all entities. Figure III.1 shows high level illustration of a peer-to-peer accommodation scenario. This use case example illustrates how trust information (including trust index) is applied to of service provider, users (host and traveller), and accommodation facility by showing how trust index of each actor is accumulated and managed during transaction.

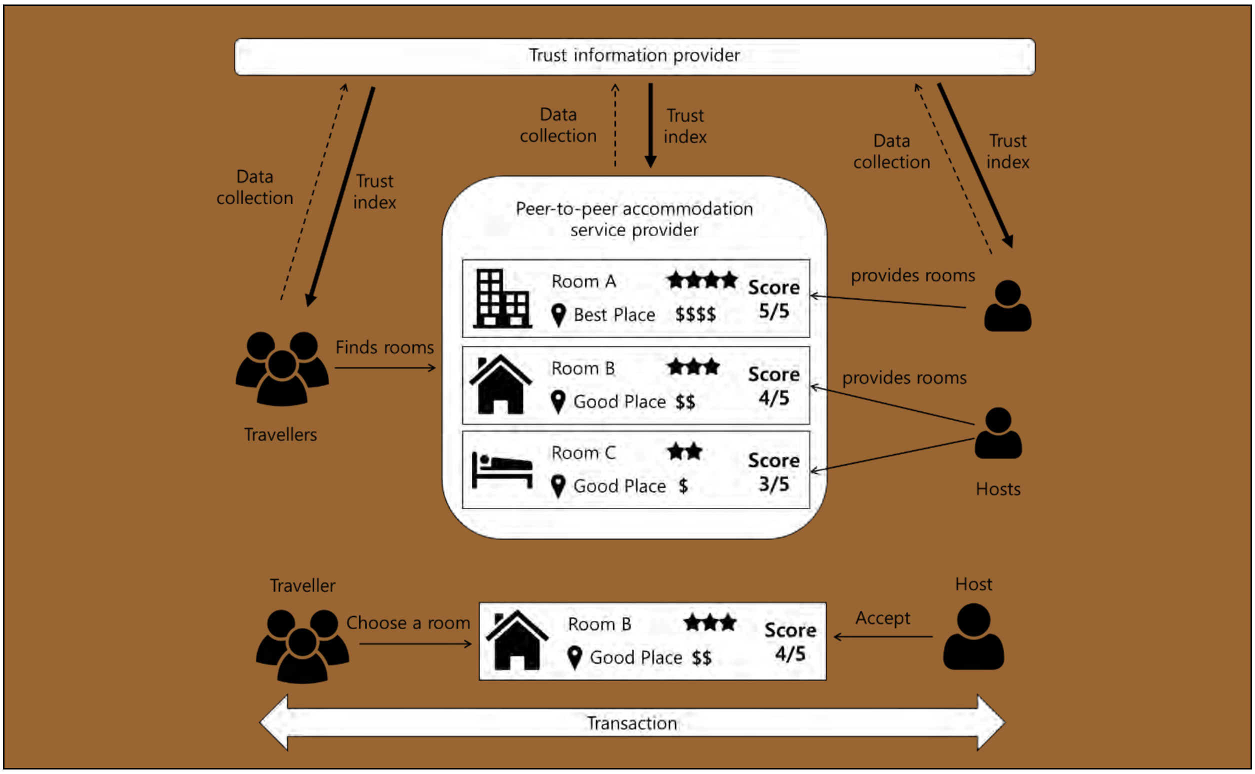


Figure III.1 – High level illustration for peer-to-peer accommodation scenario

III.1.2 Actors

This use case involves interactions among the following entities:

– Host: provides available accommodations

– Traveller: uses accommodations from host

– Accommodation: facilities provided by host

– Peer-to-peer accommodation service provider: provide services that connects hosts and travellers for their transactions

– Trust information provider: provide trust index of each entity based on collected information.

III.1.3 Service flow

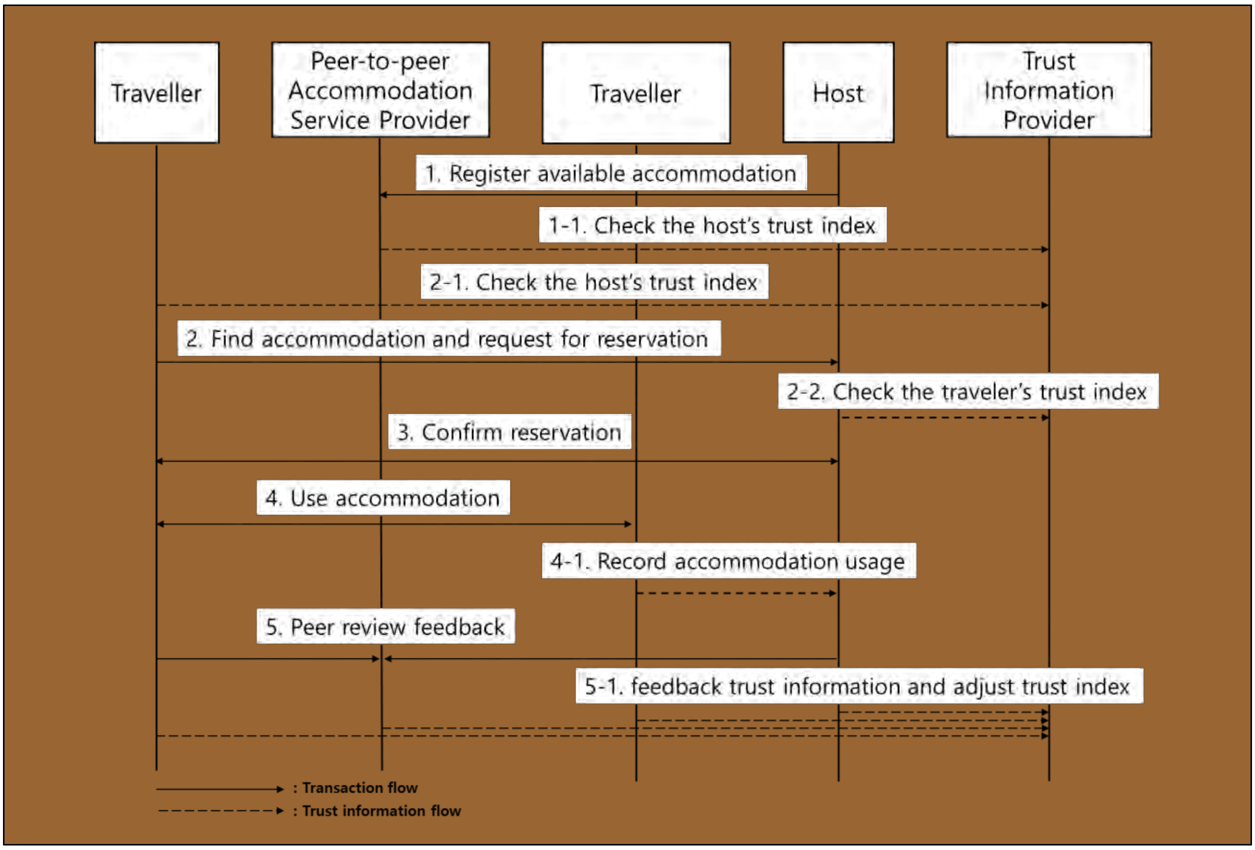

Traveller
Peer-to-peer Accommodation Service Provider
Traveller
Host
Trust Information Provider
1. Register available accommodation
1-1. Check the host's trust index
2-1. Check the host's trust index
2. Find accommodation and request for reservation
2-2. Check the traveler's trust index
3. Confirm reservation
4. Use accommodation
4-1. Record accommodation usage
5. Peer review feedback
5-1. feedback trust information and adjust trust index
: Transaction flow
: Trust information flow

Figure III.2 – Peer-to-peer accommodation service flow

– Detailed flow description (Figure III.2)

1) A host registers his/her available accommodation to the service provider (The service provider checks the host's trust index).

2) A traveller finds accommodation through the service provider and chooses one for reservation based on trust index of accommodation (The traveller checks trust index of the accommodation, and the host checks trust index of the traveller).

3) The host receives the traveller's reservation request and accepts it based on traveller's trust index.

4) The traveller stays in the accommodation during reservation duration. During this period, resource usage is recorded by the host for further evaluation.

5) After the traveller checks out, then both the host and the traveller reviews about these review results are transferred to trust information provider for adjusting actors' trust index.

III.2 Smart office sharing

III.2.1 Description

In a trust-based smart office service, usage rights on various office facilities depend on each users' trust level which is derived from trust index of each users. For example, it is assumed there are two kinds of user trust level (high and low) with certain trust index threshold. For a user who has a high level of trust, he or she can read and write the cloud storage. However, a user who has middle level of trust can only read the documents in cloud storage. A user who has low level of trust has no right to access. Figure III.3 shows high level illustration for smart office service with different priority of users and different permission to office facilities. For the trust information provider, various properties like social/business relationship and membership can be considered to analyse user's trust level.

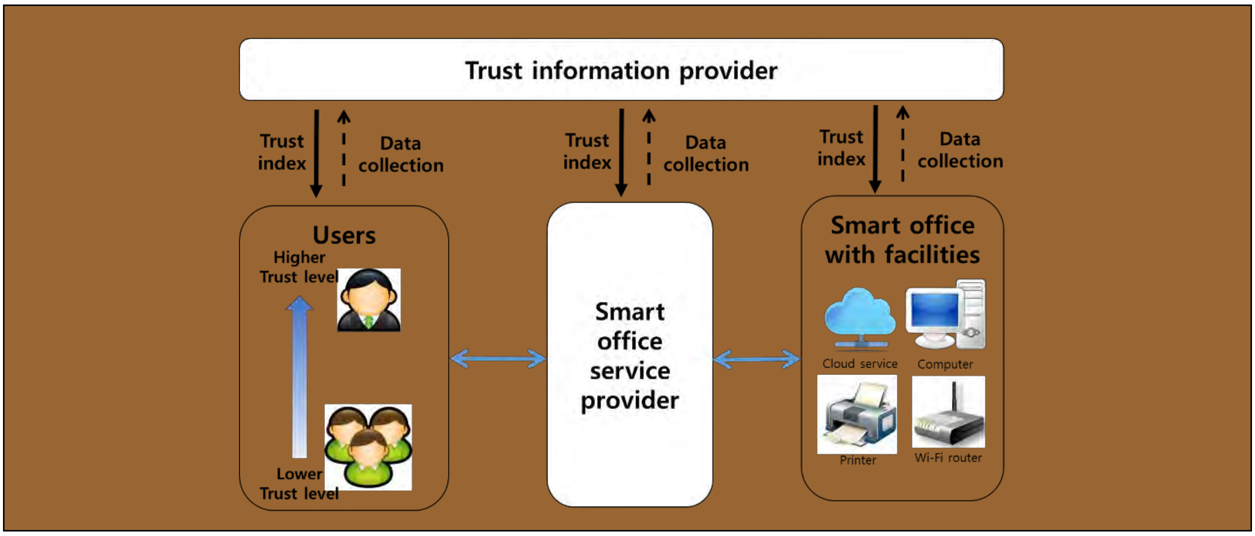


Figure III.3 – High level illustration for smart office service

III.2.2 Actors

– User: users are able to control and access smart office devices and facilities by using their own devices or office devices (e.g., employer or employee, etc.)

– Smart office devices and facilities: connected devices and facilities in office (e.g., Wi-Fi access point, personal computer, telephone, printer, meeting room, and canteen, etc.)

– Smart office provider: a smart office provider is in charge of providing common functionalities for smart office services. It is collecting the status of smart office devices and facilities. Based on user's trust level provided by trust management service, it permits appropriate usage right of them to users (e.g., building management service provider and service providers, etc.)

– Trust information provider: a trust information provider responses trust index and information request from smart office providers or service brokers.

III.2.3 Service flow

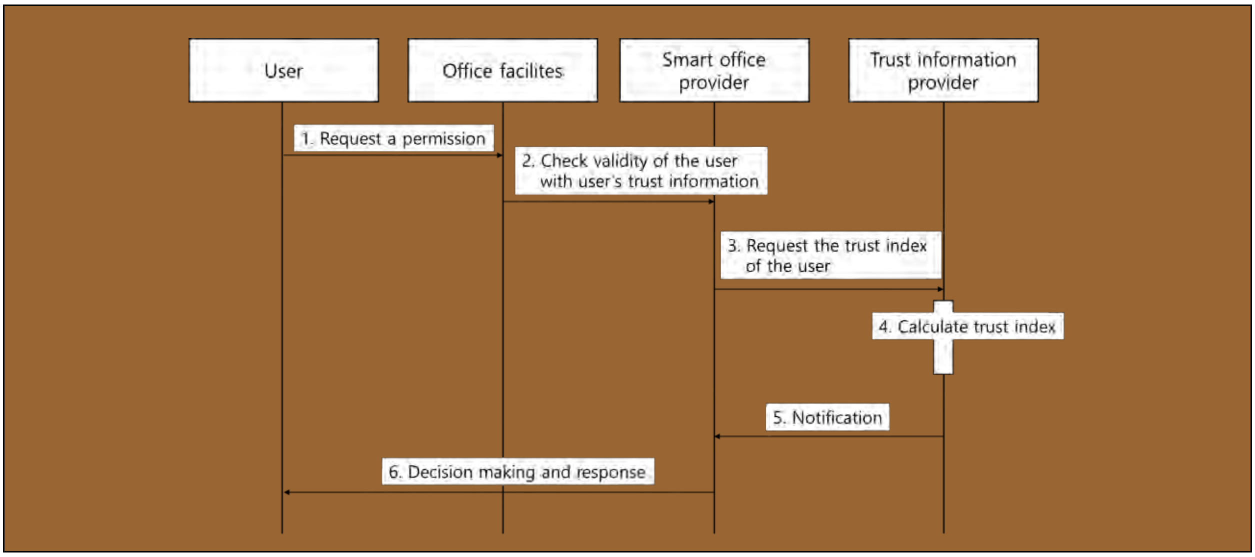

User
Office facilites
Smart office provider
Trust information provider
1. Request a permission
2. Check validity of the user with user's trust information
3. Request the trust index of the user
4. Calculate trust index
5. Notification
6. Decision making and response

Figure III.4 – Smart office service flow

– Detailed flow description (Figure III.4)

1) Users request to use office facilities.

2) Office facilities request the validation of users and user's trust information.

3) Facility management requests user's information including trust index.

4) A trust information provider evaluates user's trust index after analysing user data gathered.

5) Based on the user's trust index, facility management decides the user's trust level and the usage right on each facilities and functions for a user.

III.3 Document sharing service

III.3.1 Description

This use case considers a social internet of things (IoT) environment with no centralized trusted authority. In the social IoT, each device has the subjective value based on the owner's social relationship as well as the community of interest [b-Bao] of each device. This use case focuses on using the social trust when sharing the document between co-workers. Without the social IoT trust, a document owner takes the document from own storage, sends the document to receiver and notifies a guest account to receiver. However, the document owner does not need to do anything with the social IoT trust. A trust management platform calculates the trust value using the collected social data from intermediate entity (e.g., smartphone) of co-workers and then, these trust value will be used to judge whether a receiver has enough authorization to get the document or not. Figure III.5 shows high level illustration for document sharing service.

III.3.2 Actors

- User: a user who takes the ownership of the things (e.g., wireless portable hard drive and smartphone, etc.) and wants to share the documents in the wireless portable hard drive.
- Smartphone: a device which is an intermediate entity and is available to send its owner's social relationship information and its community of interest information to wireless portable hard drive.
- Trust information provider: this is mainly in charge of collecting the social relationship and calculating the trust index.
- Wireless portable hard drive: a device, which is mainly in charge of judging authorization to share the document.

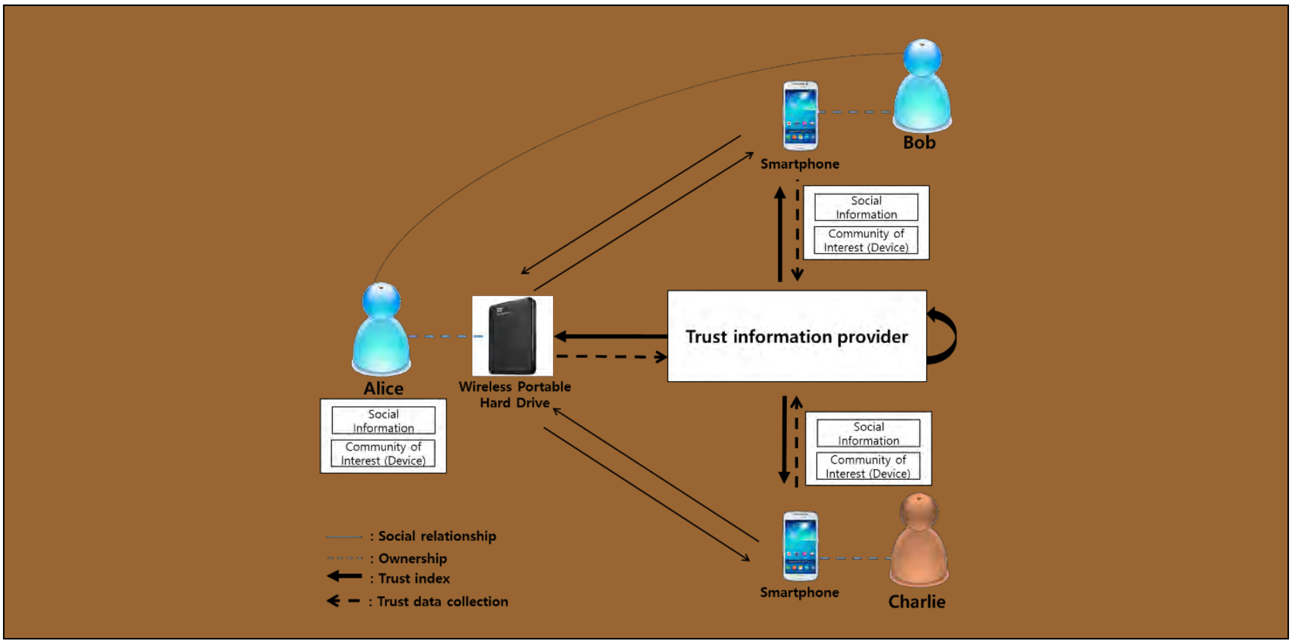


Figure III.5 – High level illustration for document sharing service

III.3.3 Service flow

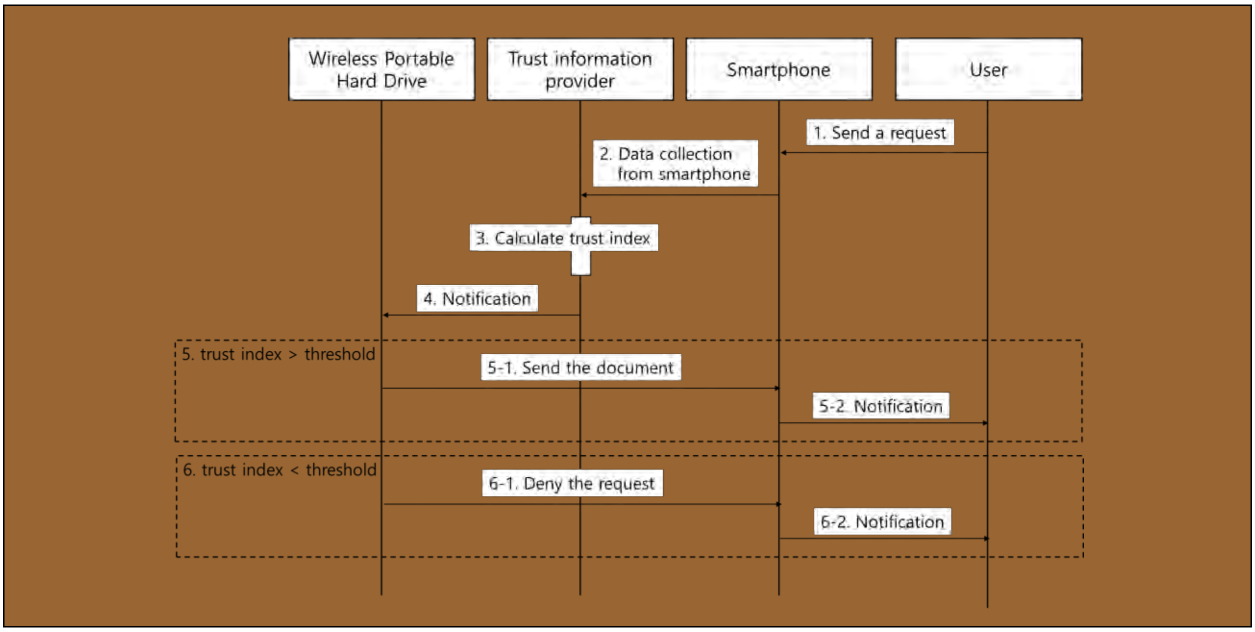


Figure III.6 – Document sharing service flow

– Detailed flow description (Figure III.6)

2) When User B requests a document to User A's wireless portable hard drive by using B's own smartphone.

3) User B's smartphone as a gateway sends User B's social information community of interest value to trust information provider.

4) From User A's perspective, trust information provider calculates a trust index of User B by using given information of User A and B.

5) The trust information provider notifies the trust index to the wireless portable hard drive. After that, it judges whether User B has enough authorization to get the document.

6) If the trust index exceeds the threshold value,

   6.1) The hard drive sends the document to User B's smartphone.

   6.2) The smartphone notifies result to User B.

7) If the trust index is lower than the threshold value,

   7.1) The hard drive notifies that the request was denied.

   7.2) The smartphone notifies result to User B.

III.4 Intermediate device selection in device-to-device environment

III.4.1 Description

This use case focuses on using the social trust when selecting the device for data transmission in multi-hop device-to-device environment. Reliable transmission is possible by using social information in the process of device-to-device communication. Trust information provider calculates the trust index by using the collected social data from intermediate entities (e.g., smartphone) of users and then, this trust index will be used to judge whether that device has enough authorization to send information or not. The social IoT trust also can be used in the device selection process for the reliable exchange of information. Figure III.4 shows high level illustration for intermediate device selection scenario in device-to-device environment.

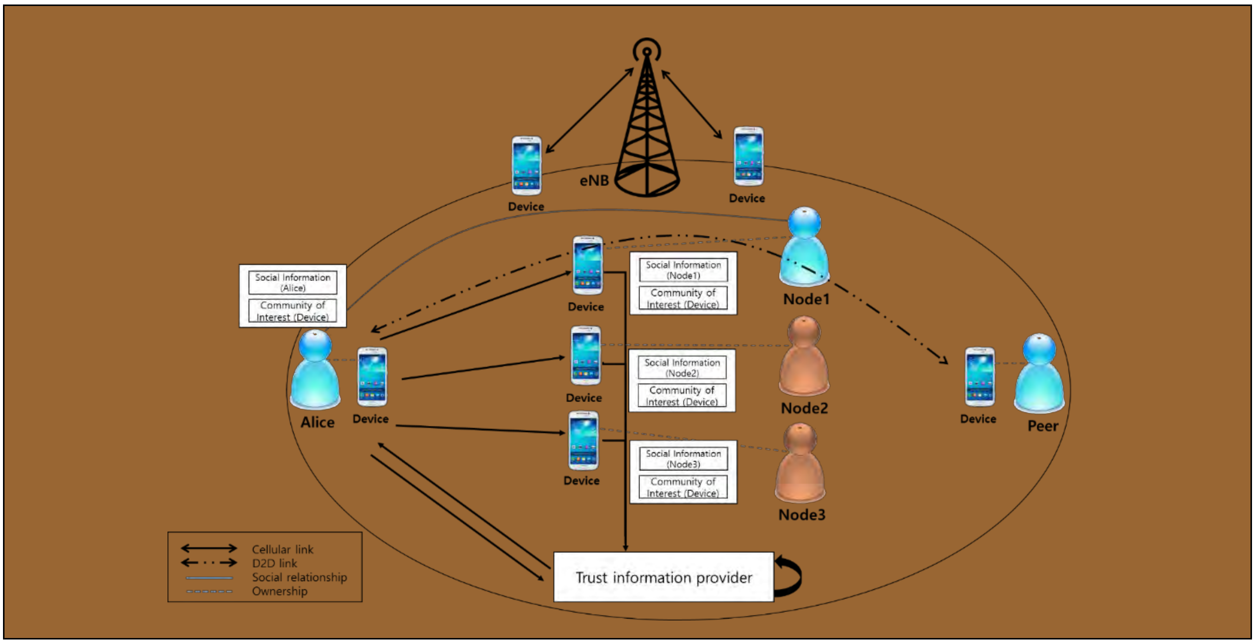

eNB
Device
Device
Social Information (Alice)
Community of Interest (Device)
Device
Social Information (Node1)
Community of Interest (Device)
Node1
Device
Social Information (Node2)
Community of Interest (Device)
Node2
Device
Social Information (Node3)
Community of Interest (Device)
Node3
Alice
Device
Device
Peer
Cellular link
D2D link
Social relationship
Ownership
Trust information provider

Figure III.7 – High level illustration for intermediate device selection

III.4.2 Actors

- User: A user who takes the ownership of the things (e.g., smartphone and laptop, etc.) and wants to exchange information with another peer via other users.
- Device (Smartphone): A device, which is an intermediate entity, is available to send its owner's social relationship information and its community of interest information to other devices. Also, it is in charge of judging authorization to send information.
- Trust information provider: this is mainly in charge of collecting the social information and calculating the trust index.

III.4.3 Service flow

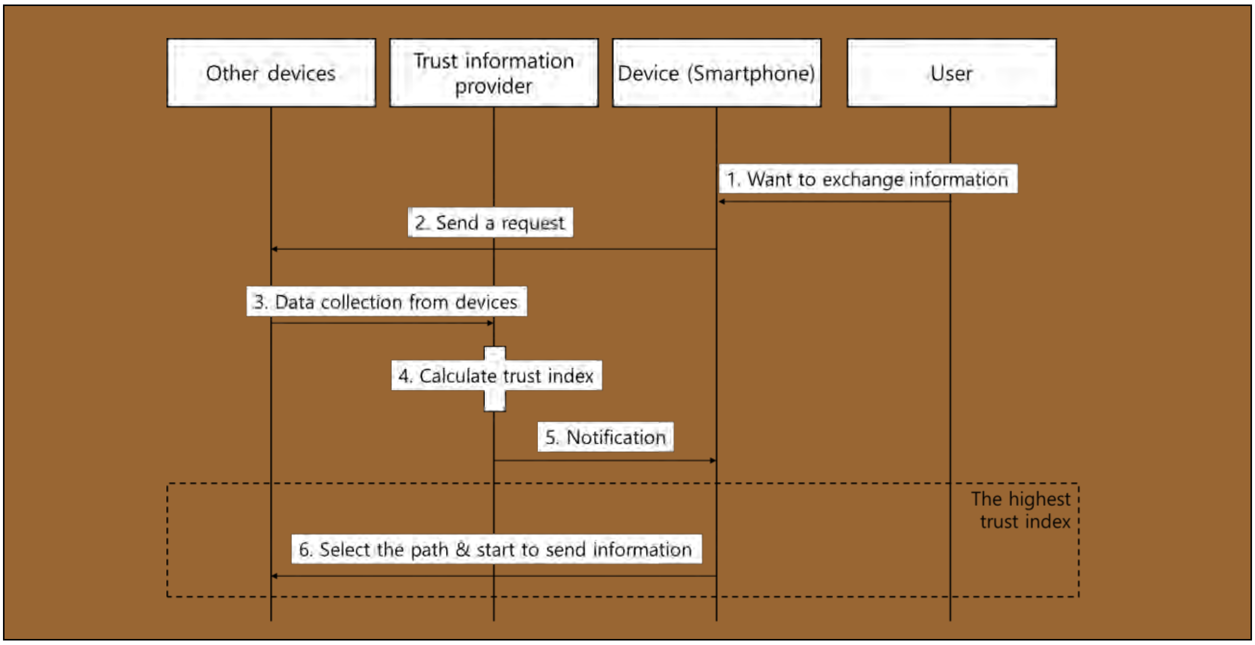

Other devices
Trust information provider
Device (Smartphone)
User
1. Want to exchange information
2. Send a request
3. Data collection from devices
4. Calculate trust index
5. Notification
The highest trust index
6. Select the path & start to send information

Figure III.8 – Intermediate device selection service flow

– Detailed flow description (Figure III.8)

1) A user wants to exchange information with another peer in multi-hop device-to-device environment.

2) The user's smartphone requests the social information of other devices (e.g., node 1 and node 2) and its community of interest value.

3) The trust information provider collects relevant information from other devices.

4) Then, the trust information provider calculates trust indices of devices.

5) The trust information provider notifies the trust index to the user’s smartphone. After that, it judges which nodes have enough authorization to send information.

6) If node 1’s trust index is the highest value, the user's smartphone makes decision that node 1 has enough authorization to send information and select the transmission path with node 1. Then, it starts to send information.

III.5 Used car transaction service

III.5.1 Description

While the used car market has been growing consistently in worldwide, there exists inevitable distrust in used car transactions. Comparing to purchasing a new car, buying a used car involves high level of uncertainty and risk. The market for used car is called as “the market for the lemons”, which is produced by asymmetric information, in which a buyer can not accurately assess the exact condition of the car through examination before sale is made while a seller can more accurately assess the condition of the car prior to sale. Specifically, owners of good cars will not sell their cars while only owners of defective cars will sell their cars. When a seller is going to sell their used vehicle, he or she has a weak motivation of disclosing the problems in the car. As a result, consumers are hardly satisfied with the used cars because of unexpected car trouble. General transaction model and each entity’s information level of a used car are depicted in Figure III.9.

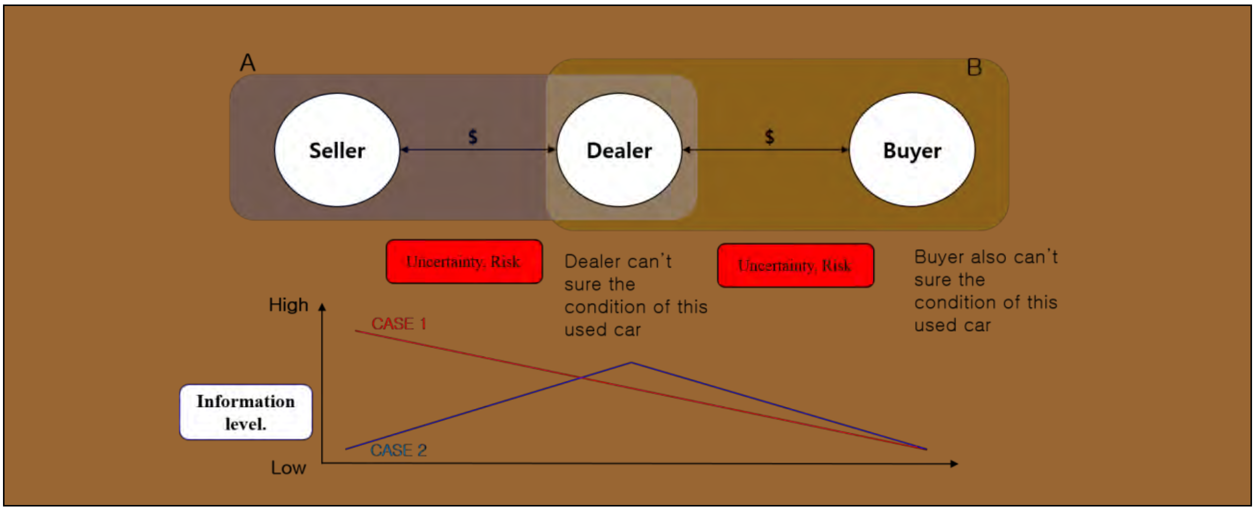

A
B
Seller
$
Dealer
$
Buyer
Uncertainty, Risk
Dealer can't sure the condition of this used car
Uncertainty, Risk
Buyer also can't sure the condition of this used car
High
CASE 1
Information level.
CASE 2
Low

Figure III.9 – Risk, uncertainty and motivation in used car transactions

Transaction *A* describes a situation that a dealer purchases a used vehicle from a seller. In this transaction a dealer is a risk taker. A dealer should investigate the car carefully to assess the condition of the car and evaluate the price because a dealer cannot confirm a seller's explanation about the car. Specifically, a seller does not have a strong motivation of disclosing all information about the car because this information directly influences the price (Case 1). It is also plausible to assume that a seller is not aware of the exact condition of the car because symptoms of trouble has not yet clearly shown (Case 2). Thus, a deal should investigate the car. However, this cross-sectional investigation is not enough to understand the real condition of the car. Thus, intense disputes commonly occurs after a transaction.

Transaction *B* describes the situation of that a buyer purchases a dealer the used car. In this transaction, a buyer is a risk taker. Similar to transaction *A*, a buyer cannot trust in a dealer (seller) because a dealer has a strong motivation of hiding the exact information about current condition of the car (Case 1). Although a dealer detects the critical problems of the used vehicle after transaction *A* finished, a dealer will not intend to unveil the detected the problems (Case 2) because this transaction accounts for dealer's income. As a result, a dealer – a risk taker in transaction *A* – sells defective used cars deliberately partly with intention, partly by accident.

As a result, each entity participating in these transactions have conflicting motivations of unveiling information on the condition of a used vehicle, so motivations cannot be aligned without an external intervention. Because of this confliction, "trust" cannot be guaranteed in used vehicle transaction. Although a seller and buyer need a mediating entity – a dealer – to reduce transaction cost, the problem is that a dealer is a buyer in transaction *A* and also a seller in transaction *B*. Here, transaction cost refers to a cost incurred in making an economic exchange. In addition, a dealer always tries to make used car transactions for his or her revenue.

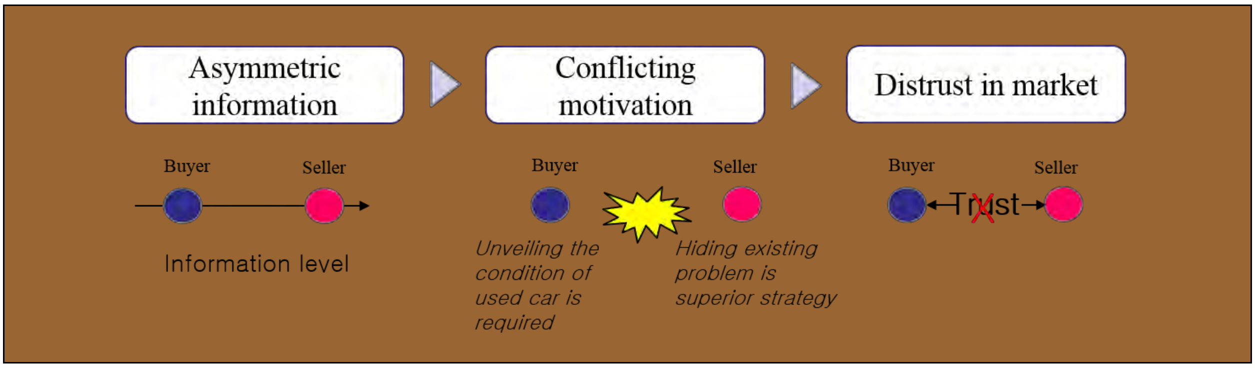


Figure III.10 – Problems of the current used car transaction service

As a result, asymmetric information causes inevitable distrust in economic transaction for used car through conflicting motivation. A buyer cannot trust in sellers' word about the condition of the vehicle. While consumers need a careful investigation in order to avoid purchasing defective vehicle, they are not accustomed to investigate the car. Consequently, asymmetric information makes them fail to trust in sellers and used cars, so level of satisfaction is always threatened. A great number of articles have shown that trust is strongly related to satisfaction of various goods.

In summary, as seen in Figure III.10, the current used car transaction involves following inevitable problems; (1) asymmetric information, (2) conflicting motivation of disclosing the condition of used car due to (1), and (3) distrust among entities due to (2). Thus, an appropriate intervention is needed for avoiding dispute among entities and activating the used car market.

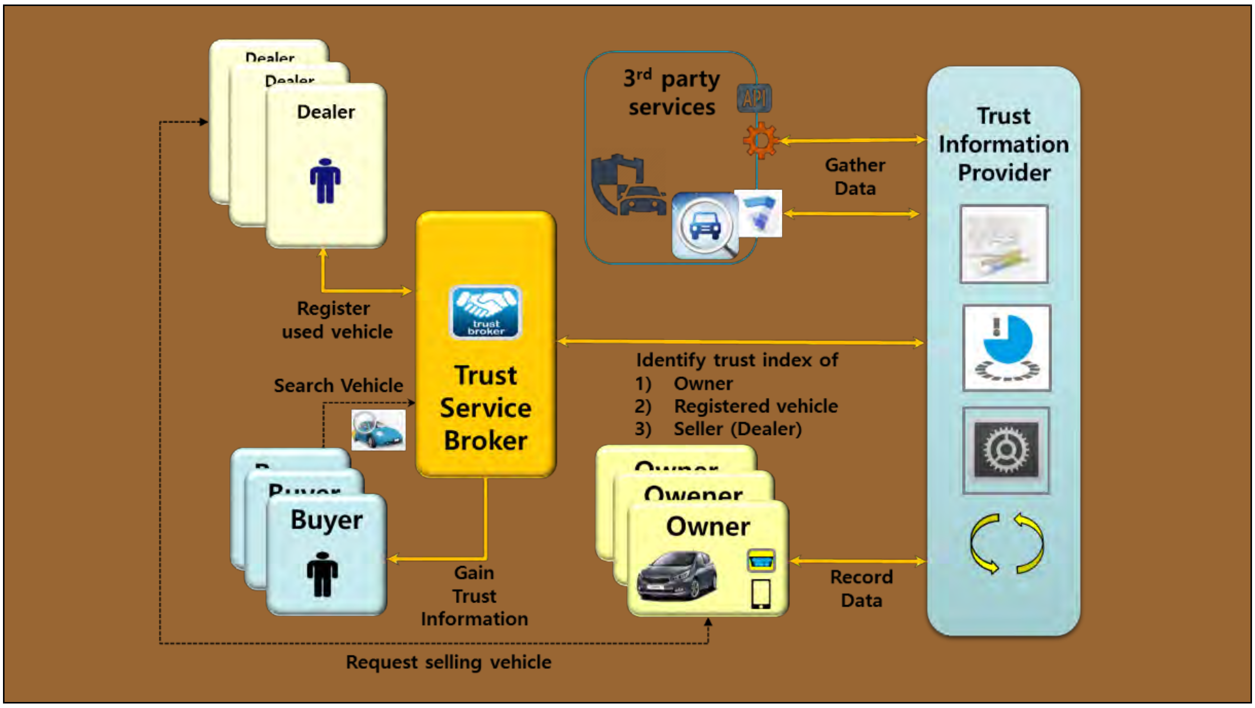


Figure III.11 – High level illustration for used car transaction service

In order to overcome sequential problems discussed, it is direct remedy to make participants share information. Trust information provider can play an important role in mediating entities who participate in used vehicle market and sharing trustful data and information as shown in Figure III.11.

When a buyer request selling his/her car, a dealer registers that vehicle in an online market place liked to trust service broker. Then, trust management platform automatically collects data from various sources such as insurance company, public organization, social network services, and vehicle itself. If a vehicle owner attaches an on-board diagnostics scanner, this device records and accumulates wide ranges of vehicle-oriented information such as driving distance, recorded fuel efficiency, accident, driving habits, and maintenance and repair history.

In the next step, by transforming these fragmented data into single information, trust management platform identifies and evaluate the level of trust of an owner of used car, a registered vehicle, and a dealer. Based on this refined and trustful information, a buyer can assure the condition of the used vehicle prior to purchasing and make a purchase decision with comparably low level of uncertainty and risk.

III.5.2 Actors

As the participants in the used car transaction process depicted in Figure III.11 have different goals, each actor plays a distinctive role and conducts different function.

– Dealer: The major role of a dealer is mediating buyer and seller (owner) to gain economic profit. A dealer can sell the possessed cars, which were already purchased, or can mediate the transaction between sellers and buyers.

– Buyer: A buyer is someone who wants to purchase a used car from a dealer or seller. When a buyer wants to purchase a used car, a buyer can search the car in a market place or on the web provided by service broker. When a buyer requests dealers and brokers for purchasing the car, he or she generally describe the specific constraints such as vehicle age, accumulated mileage, brand, model, budget, and so on. Based on identified information about the condition of the car, he or she can make a purchase decision under relatively low uncertainty and risk. The more provided information is trustful and abundant, the more they can reduce risk and uncertainty.

– Owner (Seller): An owner (seller) is someone who wants to sell his or her car to others including a dealer and individual buyer. When an owner tries to sell the car, he or she simply sell a dealer or an individual the car at a negotiated price. Otherwise, he or she can ask a dealer transaction brokering.

– Service Broker: Service broker mediates an interaction among buyers, sellers, and dealers through the information transferred by trust information provider. Based on the information, trust service broker can inform the identified level of trust of owner, registered vehicle, and seller.

– Trust information provider: Trust information provider responses various requests from a service broker and others. Trust information provider analyses the level of trust by tracing the accumulated data from various sources including social network, insurance company, vehicle repair shop, public, and the car itself.

III.5.3 Service flow

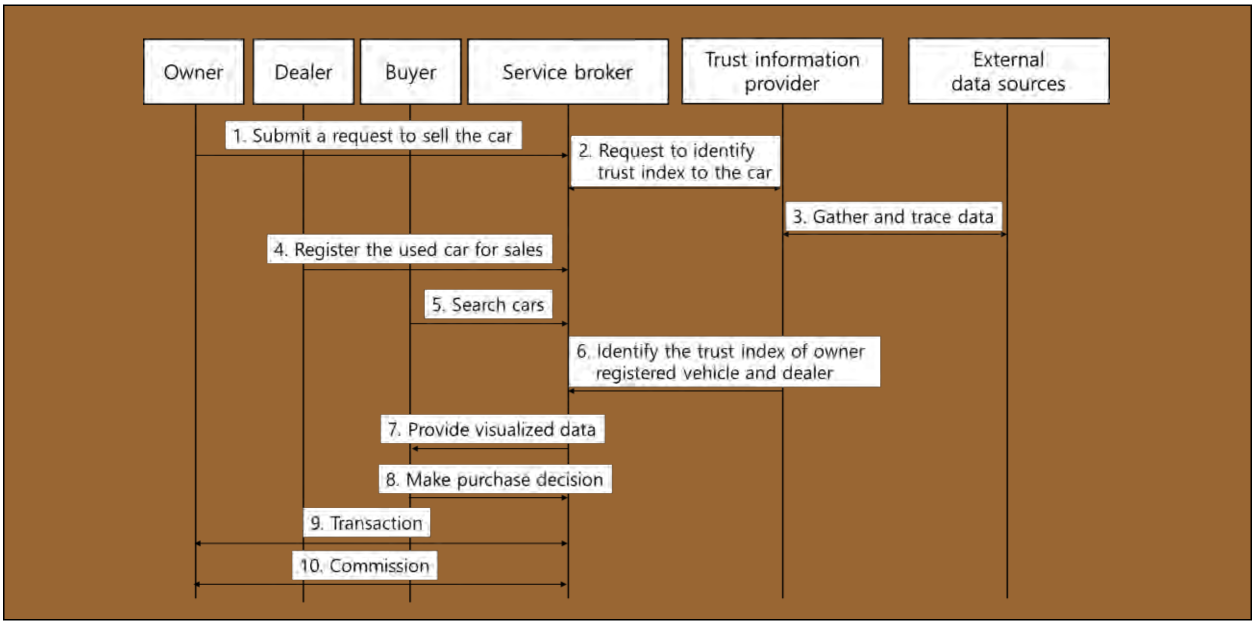

Owner
Dealer
Buyer
Service broker
Trust information provider
External data sources
1. Submit a request to sell the car
2. Request to identify trust index to the car
3. Gather and trace data
4. Register the used car for sales
5. Search cars
6. Identify the trust index of owner registered vehicle and dealer
7. Provide visualized data
8. Make purchase decision
9. Transaction
10. Commission

Figure III.12 – Used car transaction service flow

– Detailed flow description (Figure III.12)

1) A dealer registers the used car in trust service brokers as an owner makes a request to a dealer for selling the used car.

2) Trust information provider complies with a service broker's request of transferring trustworthy data related to the car.

3) Trust information provider gathers the relevant data from not only the external data sources such as insurance company, public organization, social network services, but also an internal data source such as on-board diagnostic scanner, which transfers historical data from car to the platform. If car

owner attaches on-board diagnostic scanner in the car, he can confirm the condition of the car and identify problems via applications on a smartphone.

4) A dealer registers the car with explanatory data about the car in the marketplaces connecting with a number of service brokers. At this time, the car is ready for sales.

5) A buyer can search number of used cars in order to purchase the car.

6) When a buyer is interested in a specific car, he or she can ask the service brokers relevant data and information. Then, trust information provider replies service broker's requests by providing processed trustful data including the trust index of owner, registered car, and seller (or dealer).

7) In order to help a buyer's purchase decision, a service broker visualizes the analysis results.

8) A buyer can make a purchase decision with relatively low risk and uncertainty.

9) The used car transaction occurs among parties.

10) After completing the transaction, transaction commission can be transferred. The commission rate and recipient depends on business model and pre-determined rules.

Bibliography

[b-Chen-2014] J. Chen, et al., "Waas: Wisdom as a Service," IEEE Intelligent Systems, vol. 29, no. 6, pp. 40-47, 2014.

[b-Rowley] J. Rowley, "The wisdom hierarchy: representations of the DIKW hierarchy," Journal of Information Science, vol. 33, no. 2, pp. 163-180, April 2007.

[b-Mayer] R.Mayer, J. Davis, and F. Schoorman, An Integrated Model of Organizational Trust, Academy of Management Review, 1995, vol.20, N0. 3, pp. 709-734

[b-Colquitt] J. A. Colquitt, B. A. Scott, and J. A. LePine, "Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance," Journal of Applied Psychology, vol. 92, no. 4, pp. 909-927, 2007.

[b-Brauch] H. G. Brauch, "Concepts of Security Threats, Challenges, Vulnerabilities and Risks," Copying with Global Environmental Change, Disasters and Security, vol. 5, pp. 61-106, 2011.

[b-Wilson] C.Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress," CRS Report for Congress DTIC Document, Washington DC, 2008.

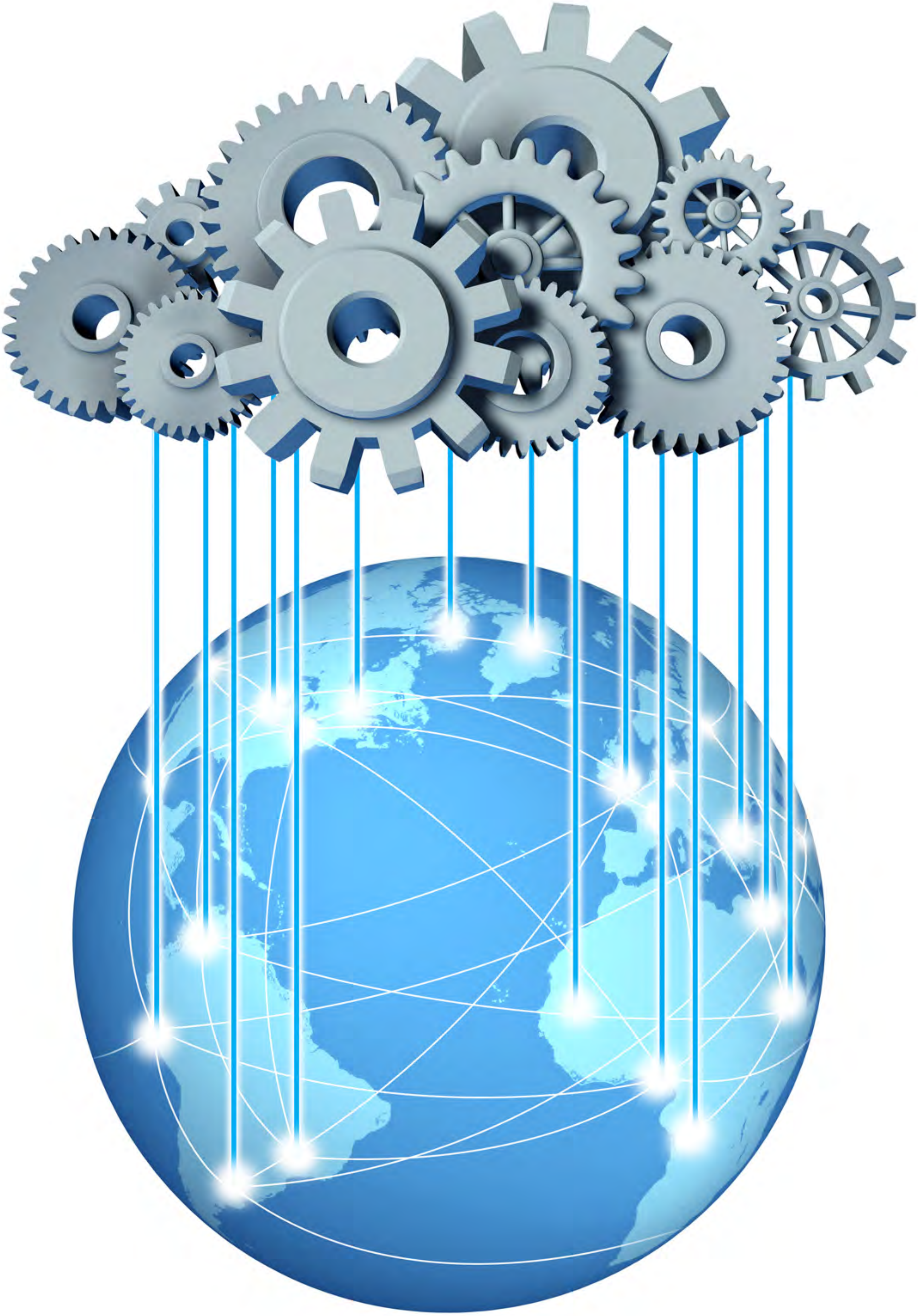
[b-Weber] R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, 2010.

[b-Chen-2015] F. B. J. G. Ing-Ray Chen, "Trust-based Service Management for Social Internet of Things Systems," IEEE Transactions on Dependable and Secure Computing, 2015.

[b-Bao] F. Bao, I. R. Chen, and J. Guo, "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems," 11th International Symposium on Autonomous Decentralized System, Mexico City, Mexico, 2013.

6.

ITU Workshop on “Future Trust and Knowledge Infrastructure” – Phase 1



Presentation slides: ITU Workshop on "Future Trust and Knowledge Infrastructure" - Phase 1 (Geneva, Switzerland, 24 April 2015)

Geneva, Switzerland, 24 April 2015

Presentations

Future Information Society and their Infrastructures, Chaesub Lee, Director of TSB
Opening_P3-Chaesub-Lee.pdf

What is the Knowledge Society?: Alexander Lutokhin, (NIIR, Russian Federation)
S1P1-Aleksander-Lutokhin.pptx

Data Types and Formats for Cyber Physical Space Toward Future Knowledge Society: Jun Kyun Choi, (KAIST, Korea)
S1P2-Jun-Kyun-Choi.pptx

Tussles for Edge Network Caching: Patrick Gwydion Poullie, (University of Zurich, Switzerland)
S2P1-Patrick-Poullie-V4.pptx

Impacts of Software Capability and Convergences (Including Energy, Transportation, and Health, etc.): Subin Shen, (Nanjing University of Posts and Telecommunications (NUPT, China))
S2P2-Subin-Shen-R1.pptx

Challenges for Trustworthy Social-Cyber-Physical Infrastructure: Gyu Myoung Lee, (LJMU, UK/KAIST, Korea)
S2P3-Gyu Myoung Lee.pdf

Trusted Environment in Future ICT Infrastructure and the Role of the Context: Viliam Saryan, (NIIR, Russia)
S2P4-Viliam-Saryan.pptx

Beyond Data Security: How to Build Trust Through Transparency: Mark Jeffrey, (Microsoft, USA)
S3P1-Mark-Jeffrey.pptx

Open and Secure, Paradox or Property: Olaf Kolkman, (Internet Society)
S3P2-Olaf-Kolkman.pptx

The Policies for a Balanced Cyber-Security and Privacy Posture: Giampiero Nanni, (Symantec Corporation, UK)
S3P3-Giampiero-Nanni-V2.pptx

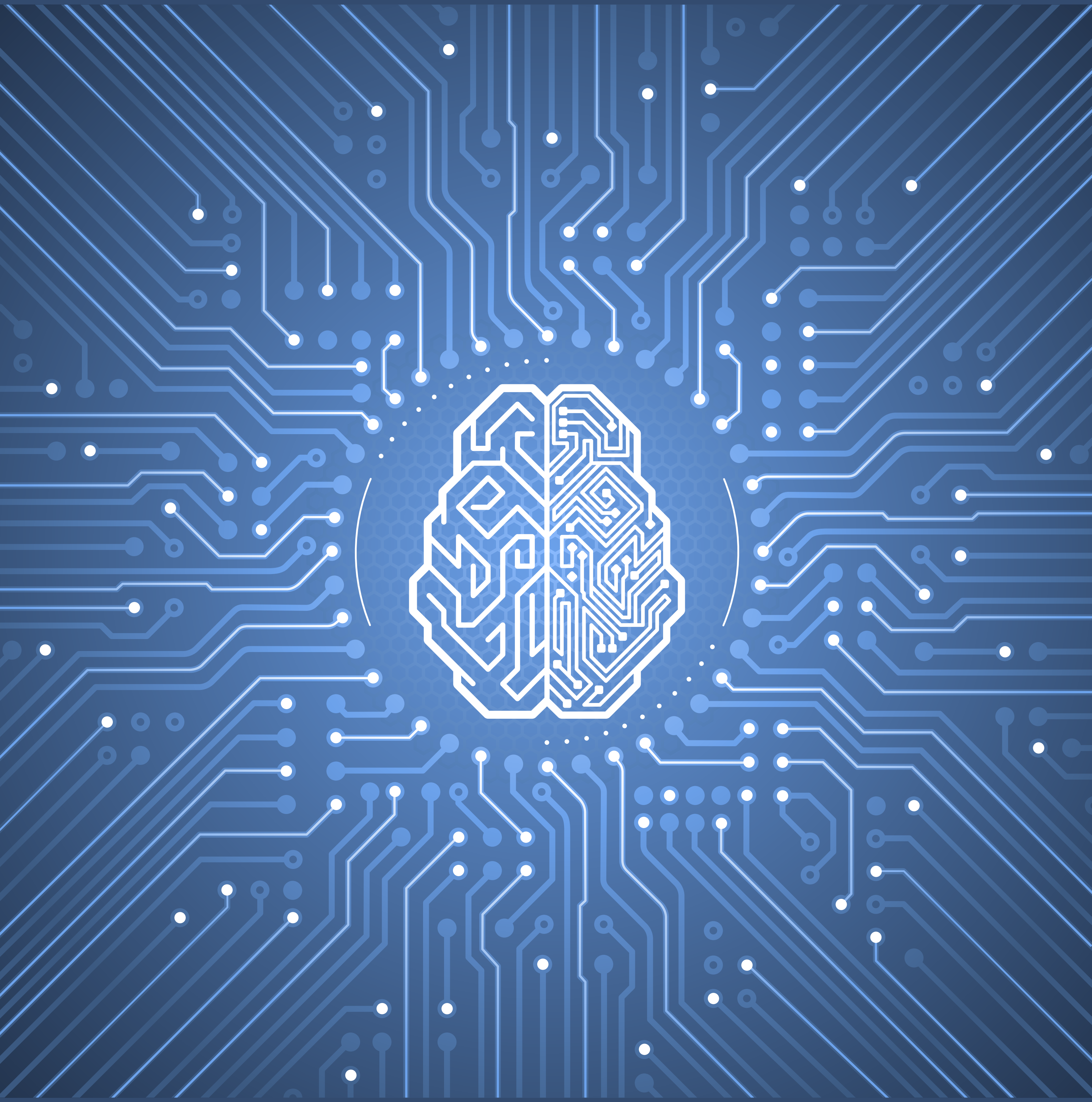
IoT Data Platform Based on OneM2M: Omar Elloumi, (OneM2M)
S4P1-Omar-Elloum-V2.pptx

Platform Cloud for Future Platforms to Carry and Share: Olivier Le Grand, (Orange, France)
S4P2-Olivier-LeGrand.pdf

Trust Computing and The Need for Ensuring Platform Integrity: Alec Brusilovsky, (InterDigital, USA)
S4P3-Alec-Brusilovsky.pptx

7.

ITU Workshop on “Future Trust and Knowledge Infrastructure” – Phase 2



Presentation slides: ITU Workshop on "Future Trust and Knowledge Infrastructure" Phase 2 (Geneva, Switzerland, 1 July 2016)

Geneva, Switzerland, 1 July 2016

Presentations

Introduction to the Workshop's Objectives, Agenda, and Participants' Expectations, Rim Belhassine-Cherif, Convener of the Workshop's Steering Committee, Tunisie Telecom, Tunisia
Opening_P3_Rim_Belhassine_Cherif.pdf

New Value Chains and Technical Issues for Future Trusted Information Infrastructure, Jun Kyun Choi, KAIST, Korea
S1P1_Jun_Kyun_Choi.pdf

The Quest for Privacy, Corinna Schmitt, UZH
S1P3_Corinna_Schmitt_v3.pdf

The Foundation of Trust: Technological Integrity, Zoltán Précsényi, Symantec
S1P3_Zoltan_Precsenyi_v2.pdf

Overview - Trust in ICT Infrastructure and Services, Gyu Myoung Lee, LJMU, UK/KAIST, Korea
S2P1_Gyu_Myoung_Lee.pdf

Key Trust Issues Related to NNAI and Services, Sherif Guinena, SG2 Chairman
S3P1_Sherif_Guinena.pdf

Trusted Inter-Cloud Challenges, Emil Kowalczyk, Orange Polska
S3P2_Emil_Kowalczyk.pdf

Trustworthy Communication Infrastructure: Principles and Framework, Woojik Chun, KAIST, Korea
S3P3_Woojik_Chun_v2.pdf

Trust Embedded Business Model of Online Service Network (OSN), Minzheong Song, Hansei University, Korea
S3P5_Minzheong_Song.pdf

From Weak Online Reputation Metrics to Standardized Attack-Resistant Trust Metrics, Jean-Marc Seigneur, Geneva University, Switzerland
S4P1_Jean-Marc_SeigneurV2.pdf

Introduction to X.cogent by Q4/SG17, A Design Consideration for Trustworthiness Indicators, Daisuke Miyamoto, University of Tokyo, Japan
S4P2_Daisuke_Miyamoto-v3.pdf

Trust Elevation Frameworks, Abbie Barbir, Rapporteur of Question 10/17 Trust Elevation Protocol (Presented by Martin Euchner, TSB/ITU)
S4P3_Abbie_Barbie_Martin_Euchner-v2.pdf

The SC40 Perspective on Trust, Frank van Outvorst, ISO/IEC JTC1/ SC40 / ASL BiSL Foundation
S4P4_Frank_van_Outvorst_v2.pdf

International
Telecommunication
Union

Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN 978-92-61-25391-2

9 789261 253912

Published in Switzerland
Geneva, 2017
Photo credits: Shutterstock