International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(December 2015)

Standardization of Trust Provisioning Study

Forward

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

CONTENTS

List of Figures

List of Tables

ITU-T Technical Paper

Standardization of Trust Provisioning Study

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.

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

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.

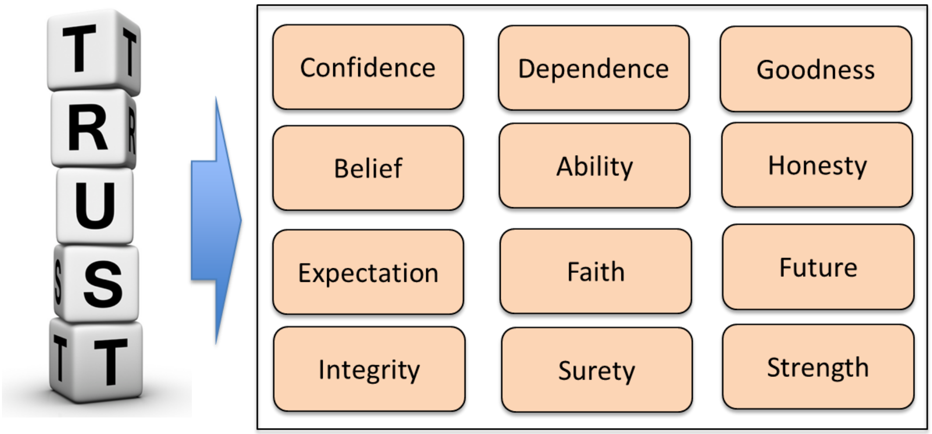

Figure 1 – Keywords for trust

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.

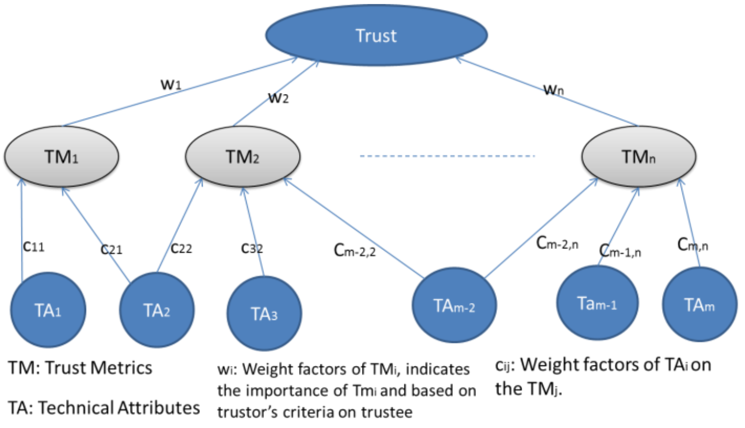

Figure 2 – General Trust Model with Trust Metrics and Technical Attributes

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.

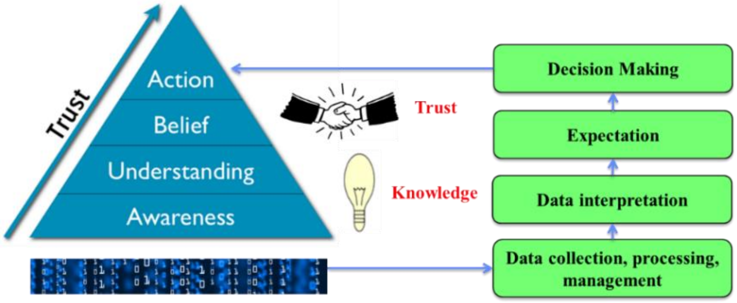

Figure 3 – Knowledge and Trust[1]

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 3, 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/

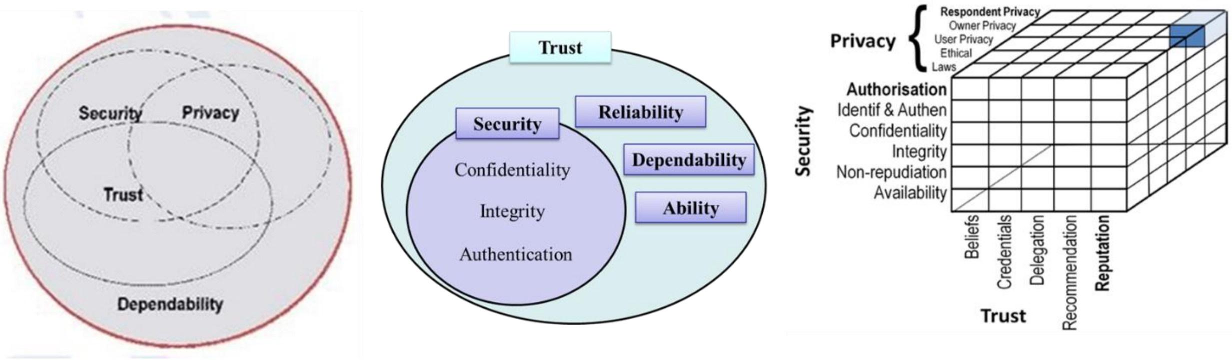

Figure 4 – Different views on trust

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

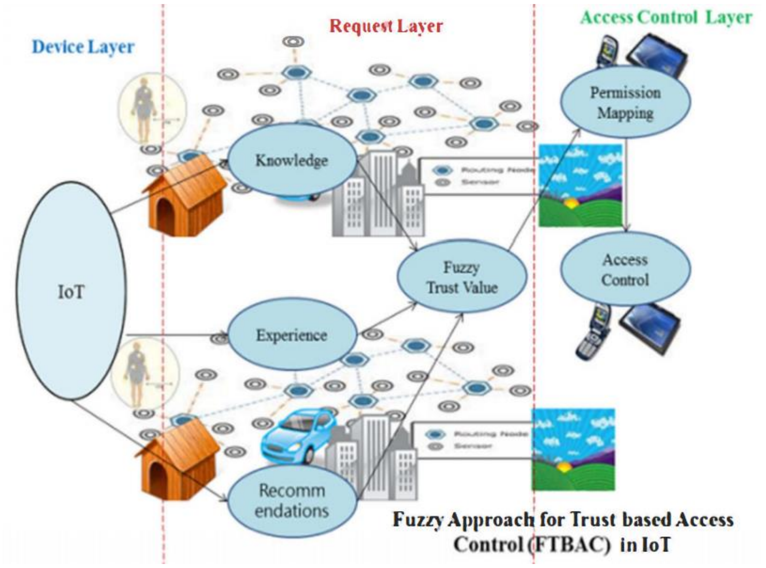

Figure 5 – High level illustration of trust based access control [112]

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.

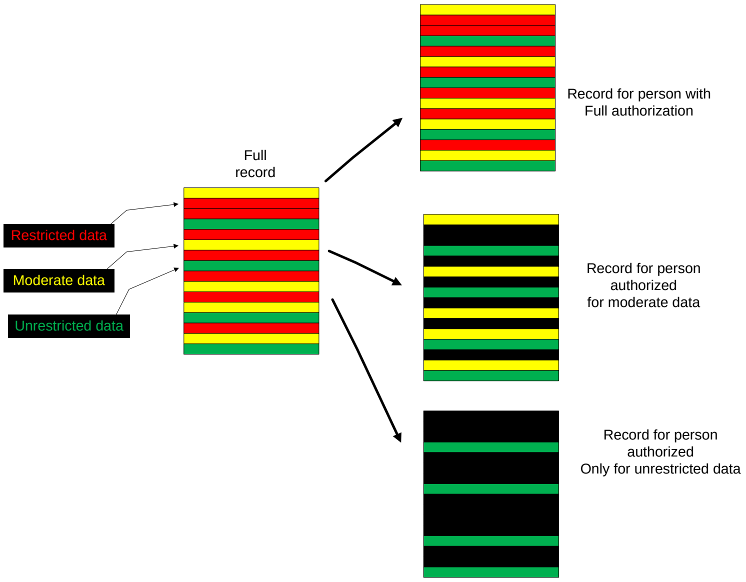
Restricted data
Moderate data
Unrestricted data
Full record
Record for person with Full authorization
Record for person authorized for moderate data
Record for person authorized Only for unrestricted data

Figure 6 – An illustration of a process with 2 levels of redaction [113]

The redaction 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.

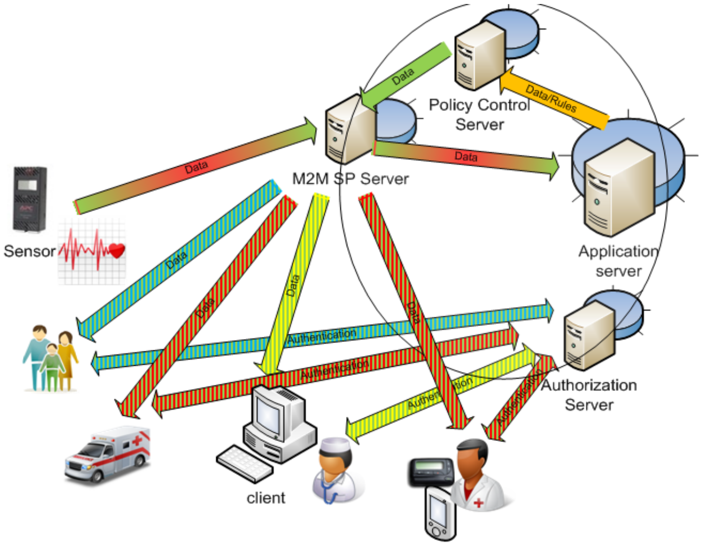

Figure 7 – An e-Health application service model [113]

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.).

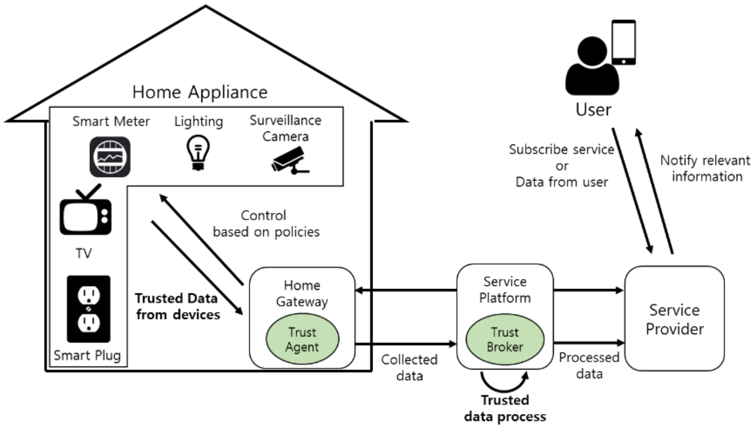

Figure 8 – Home energy management system high level illustration

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

5.2.4.3 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.

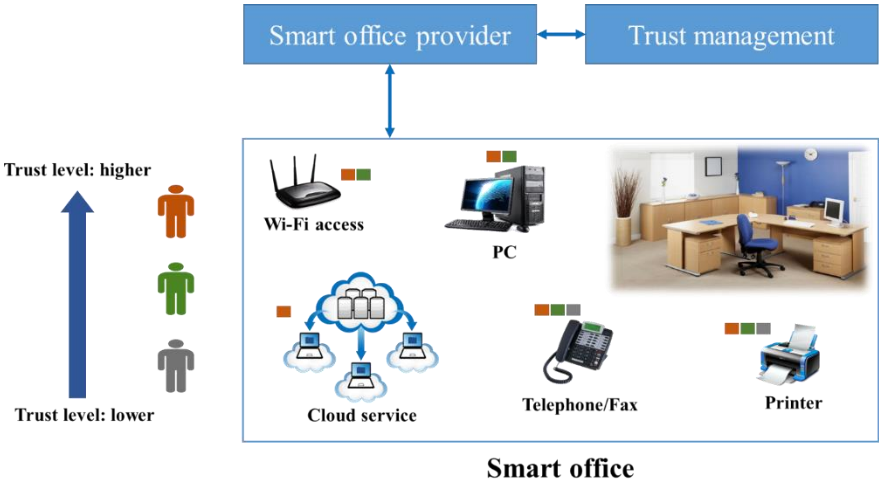

Figure 9 – Example of smart office service using trust information

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.

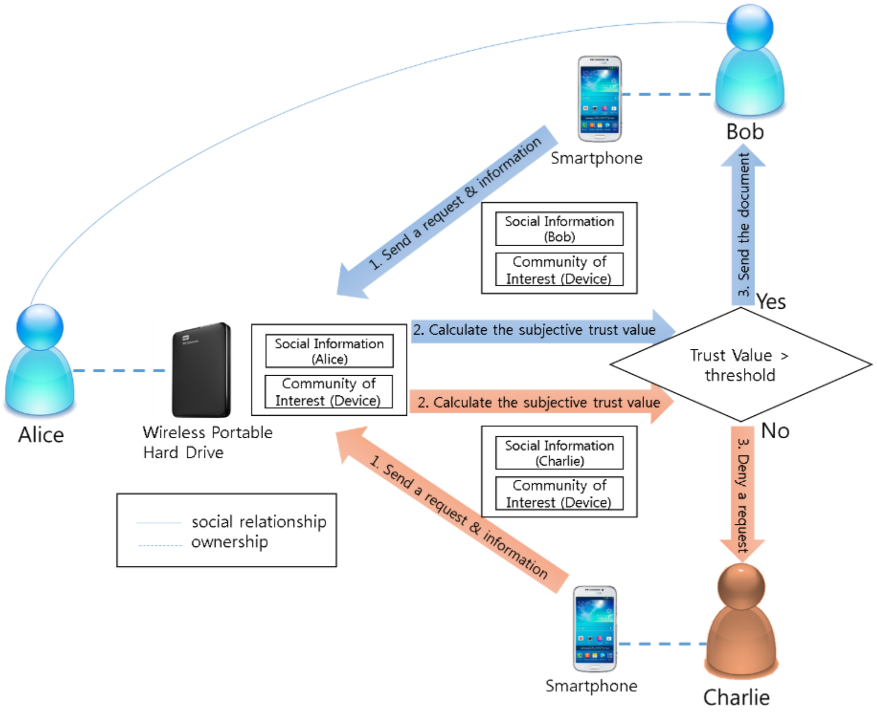
Bob
Smartphone
1. Send a request & information
Social Information (Bob)
Community of Interest (Device)
3. Send the document
Yes
Alice
Wireless Portable Hard Drive
Social Information (Alice)
Community of Interest (Device)
2. Calculate the subjective trust value
Trust Value > threshold
2. Calculate the subjective trust value
No
Social Information (Charlie)
Community of Interest (Device)
3. Deny a request
1. Send a request & information
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 11, 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.

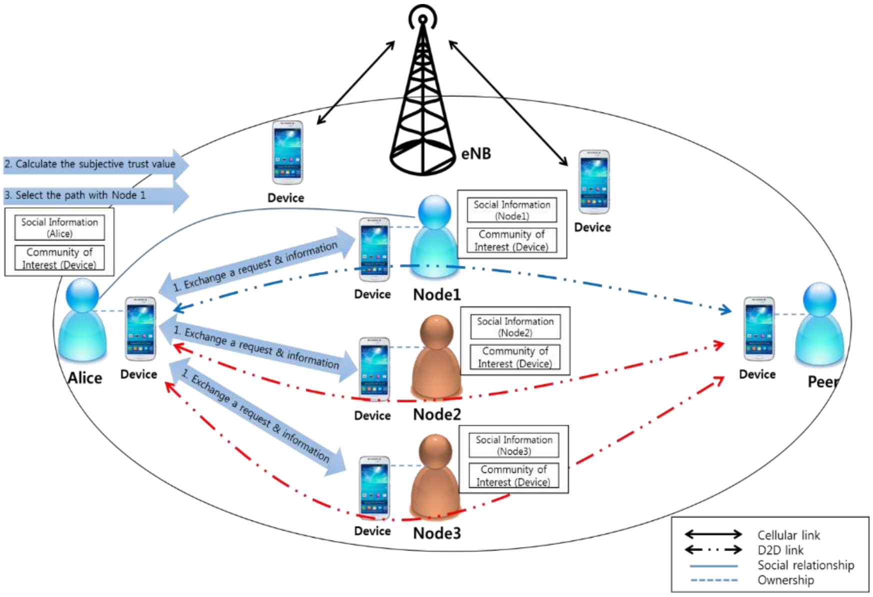
eNB
Device
Device
2. Calculate the subjective trust value
3. Select the path with Node 1
Social Information (Alice)
Community of Interest (Device)
Social Information (Node1)
Community of Interest (Device)
1. Exchange a request & information
Device
Node1
Alice
Device
1. Exchange a request & information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

Figure 11 – 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 12.

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 13.

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.

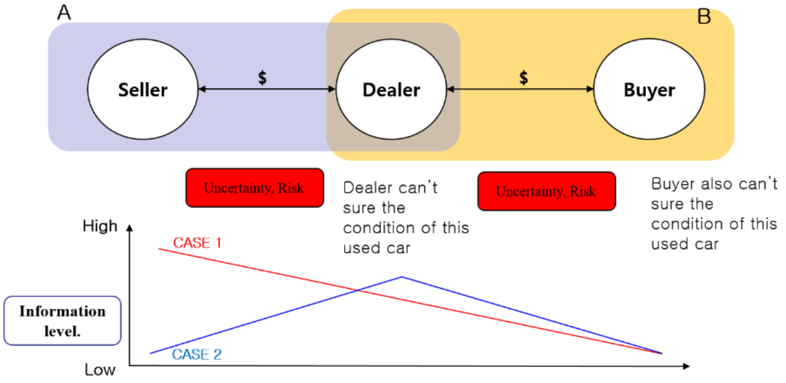
A
B
Seller
$
Dealer
$
Buyer
Uncertainty, Risk
Dealer can't sure the condition of this used car
Uncertainty, Risk
Buyer also can't sure the condition of this used car
High
CASE 1
Information level.
CASE 2
Low

Figure 12 – Used car transaction model and each entities' information level

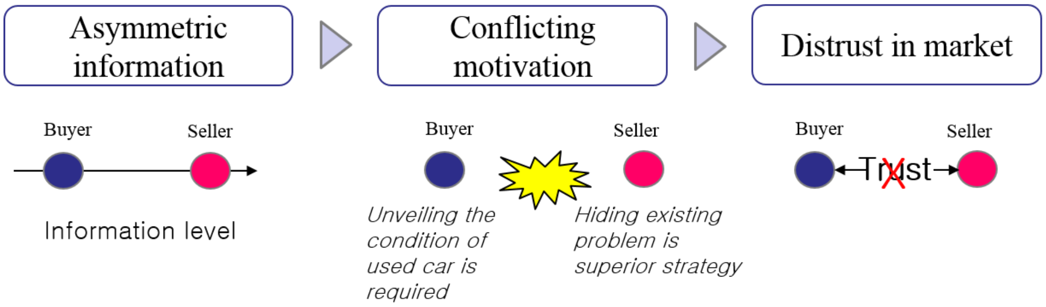

Figure 13 – Asymmetric information, conflicting motivation, and distrust in used car transaction

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 14: 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.).

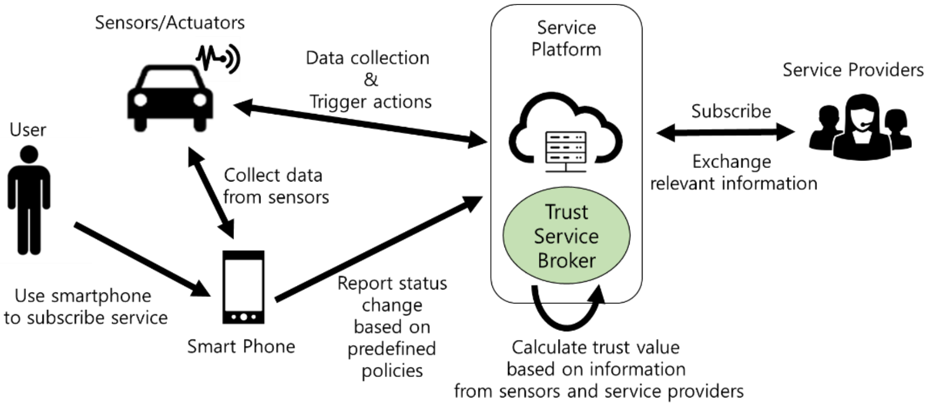
Sensors/Actuators
Data collection & Trigger actions
Service Platform
Service Providers
Subscribe
Exchange relevant information
User
Collect data from sensors
Trust Service Broker
Use smartphone to subscribe service
Smart Phone
Report status change based on predefined policies
Calculate trust value based on information from sensors and service providers

Figure 14 – 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 15 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.

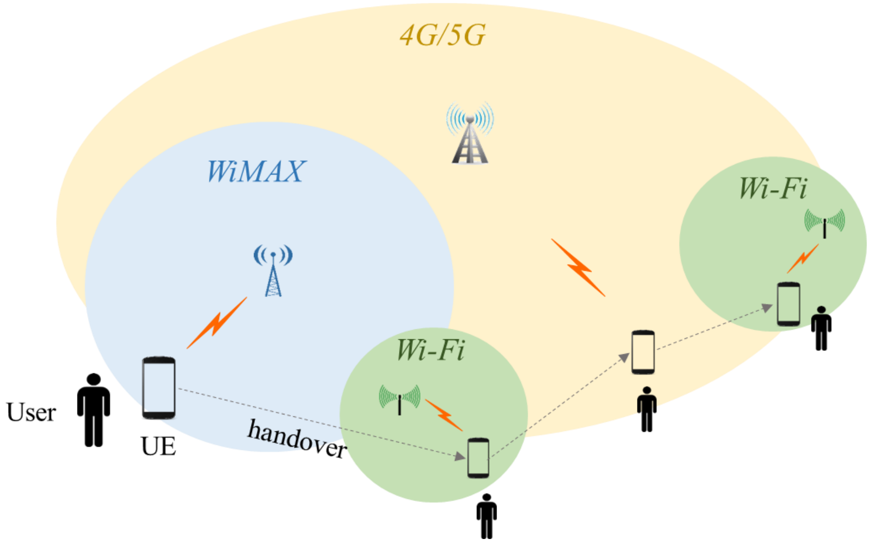

Figure 15 – A handover scenario among heterogeneous mobile networks

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.

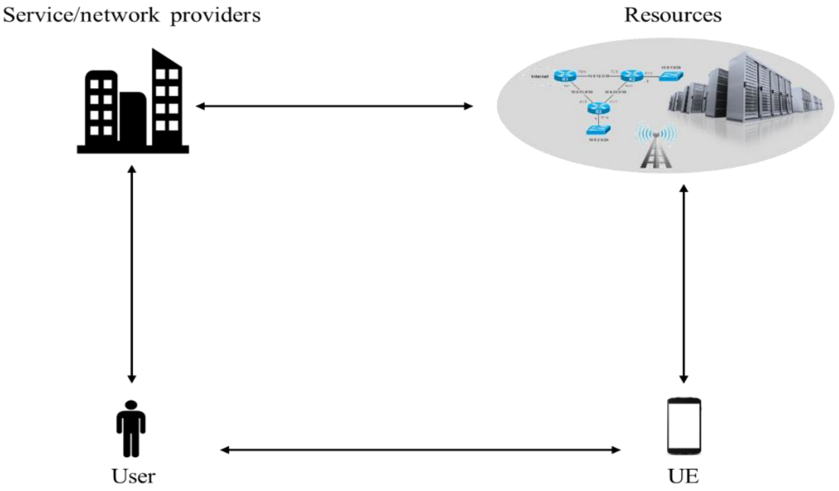

Figure 16 – Trust entities and their relations in mobility scenario

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)

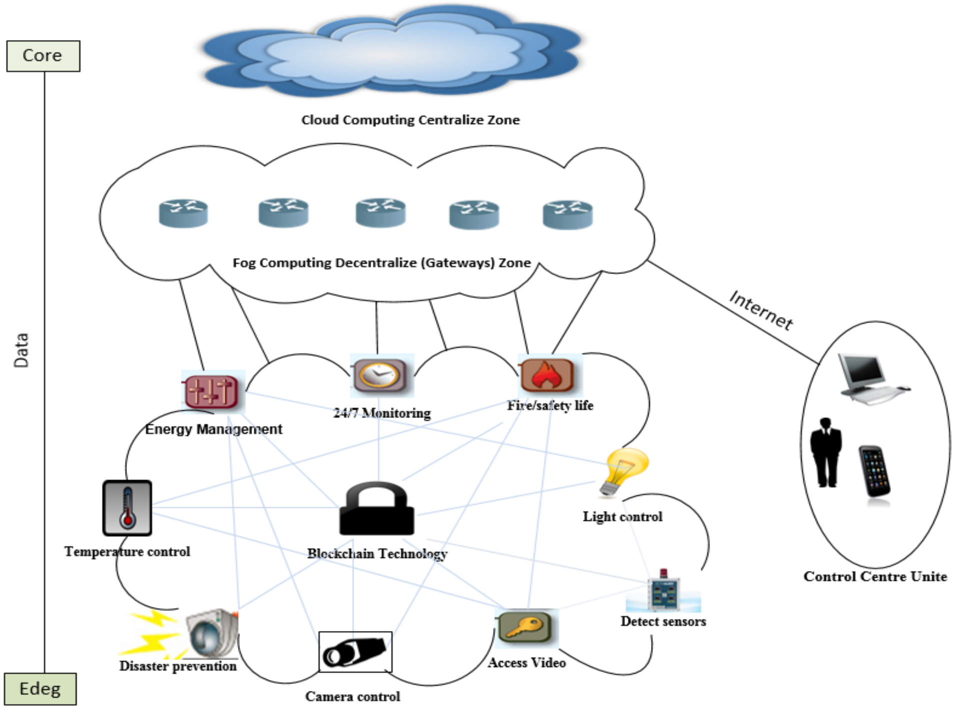

Figure 17 – Smart building with M2M connections

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					
5.1.1	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
5.1.2	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
5.1.3	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
5.2.7	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
5.2.10	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					

ID	Use case	Purpose	Method	Actors	Considerations for measuring trust
5.2.4	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.
5.2.5	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
5.2.1	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**
5.2.6	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

ID	Use case	Purpose	Method	Actors	Considerations for measuring trust
5.2.2	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
5.2.3	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
5.2.8	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.

ID	Use case	Purpose	Method	Actors	Considerations for measuring trust
5.2.9	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**
5.2.9	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 18 is the taxonomy providing initial insights into the ways trust benefits can be felt.

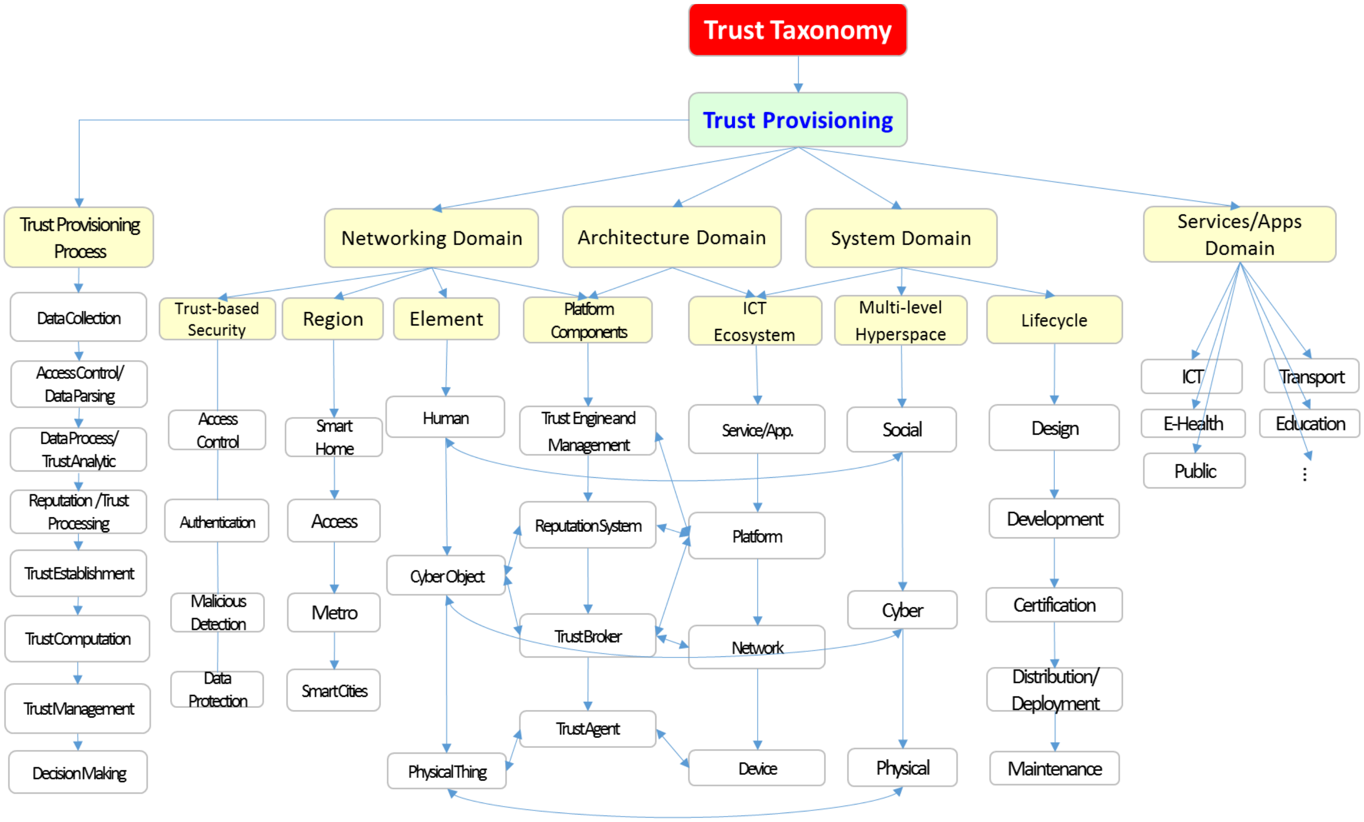

Figure 18 – Overall Trust Taxonomy in different domains

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 18 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 19 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.

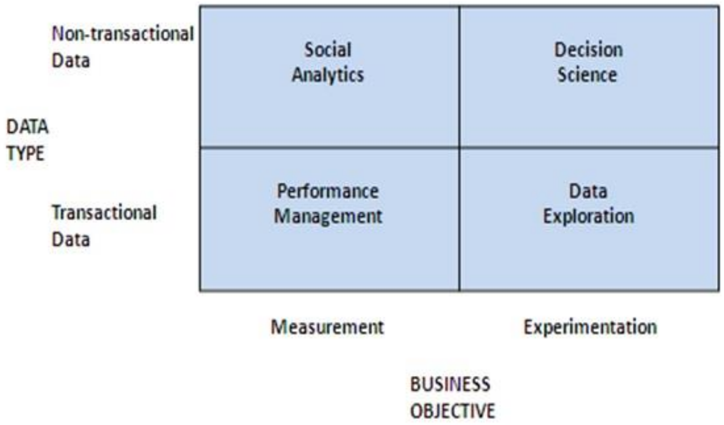

Figure 19 – Data collection dimensions and strategies

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 20).

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.

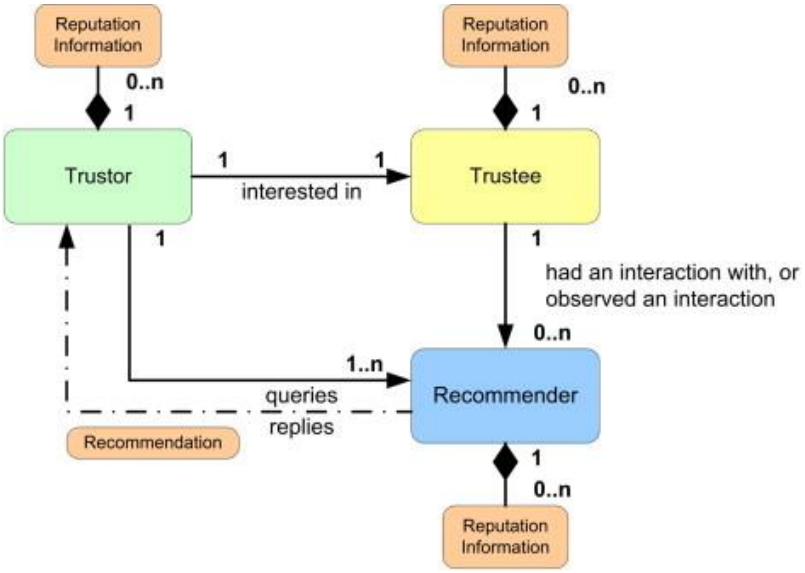

Figure 20 – A reference model for reputation systems

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.

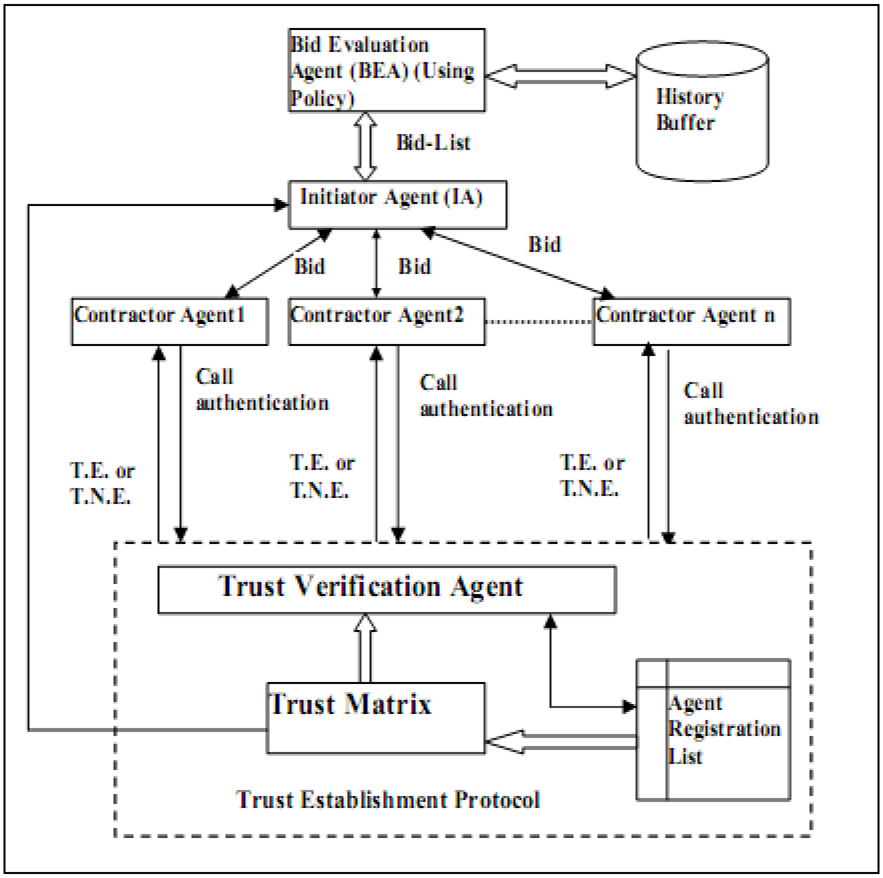

Figure 21 – Trust Establishment Contract Net Protocol Architecture [19]

The high level view of Trust Establishment Protocol (TEP) is shown in the Figure 21. 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 22.

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.

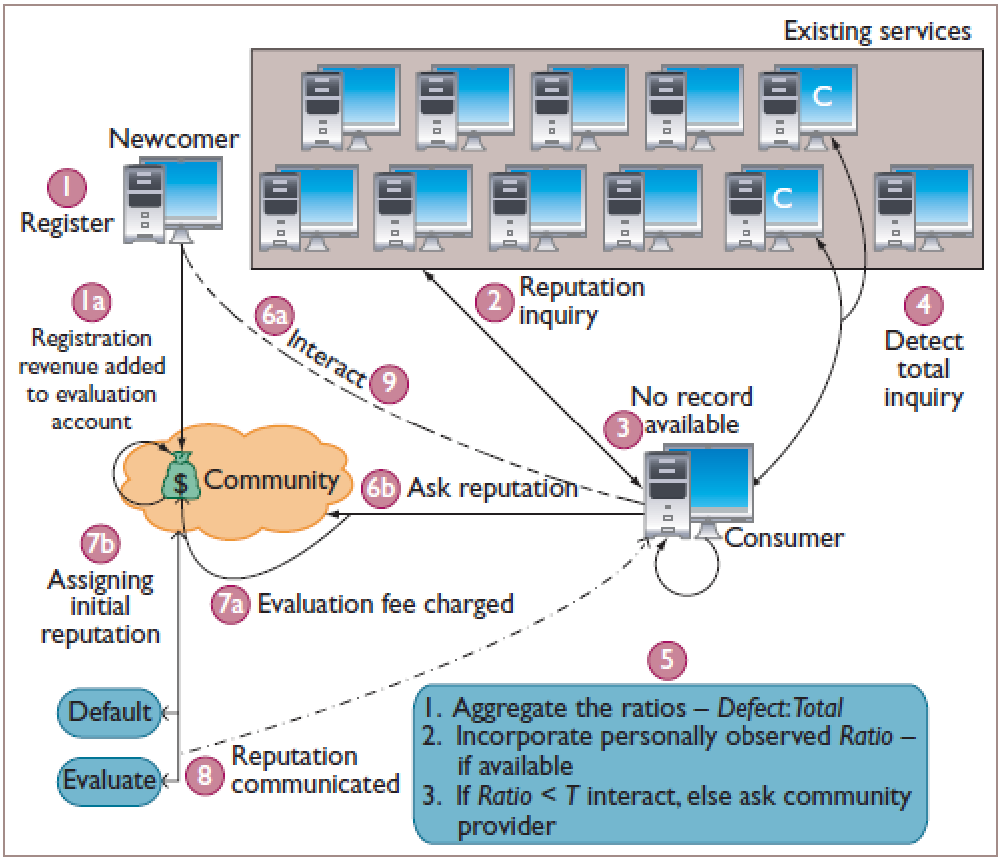
Existing services
C
C
Newcomer
1 Register
1a Registration revenue added to evaluation account
2 Reputation inquiry
6a Interact 9
4 Detect total inquiry
No record 3 available
$ Community
6b Ask reputation
Consumer
7b Assigning initial reputation
7a Evaluation fee charged
5
Default
Evaluate
8 Reputation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

Figure 22 – 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 trustworthy, 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 23, 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].

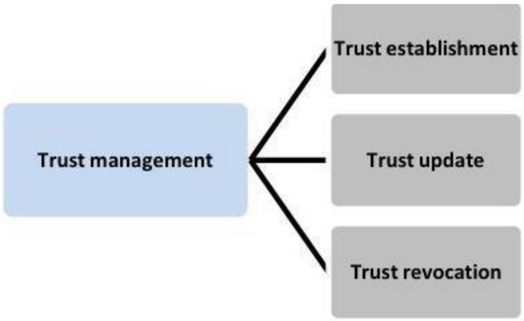

Figure 23 – Trust Management Tasks break down

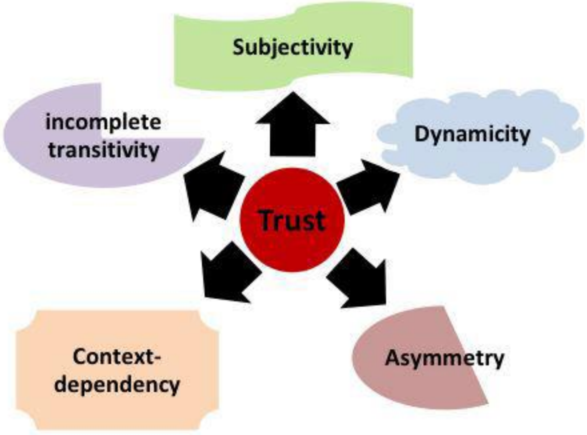

Figure 24 – General Trust Model with Trust Metrics and Technical Attributes

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 ICT 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.

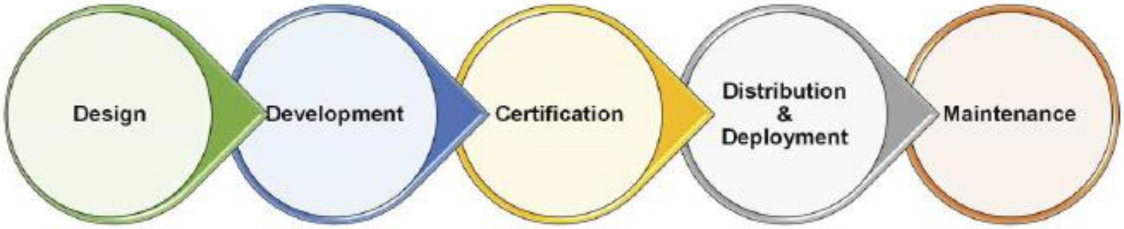

Figure 25 – The OPTET Lifecycle[2]

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.

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.

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

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 26 [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).

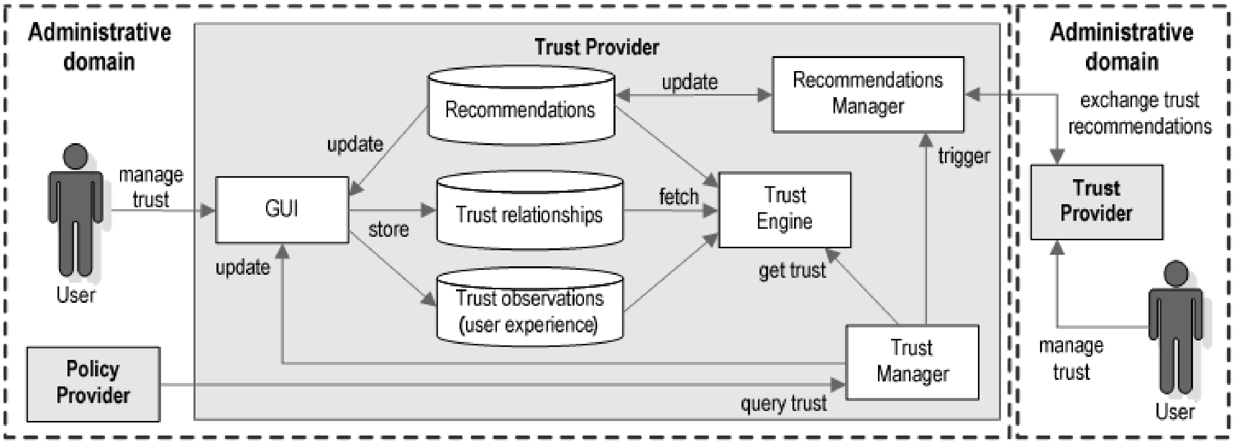

Figure 26 – Distributed trust management architecture [42]

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 28 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.

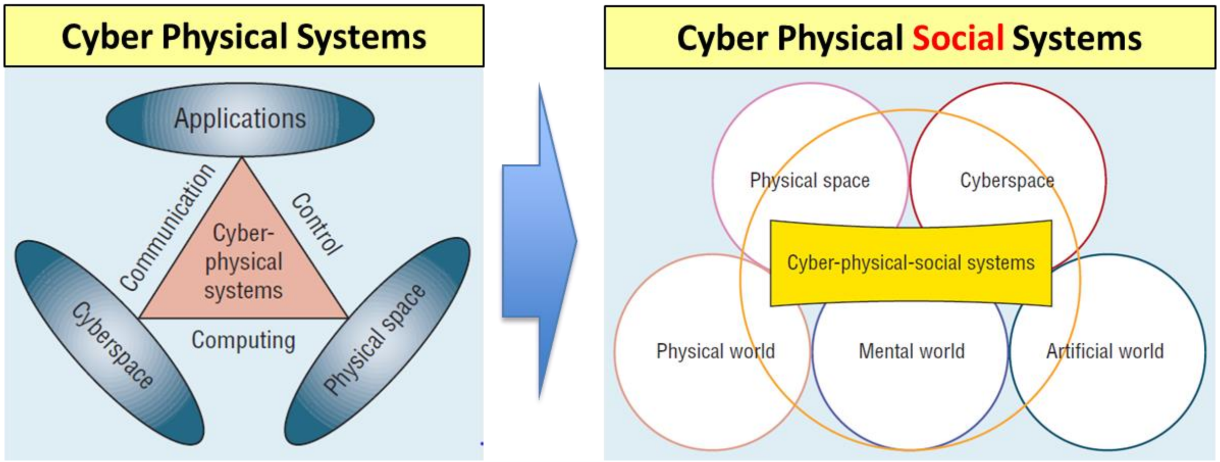

Figure 27 – From cyber physical systems to cyber physical social system

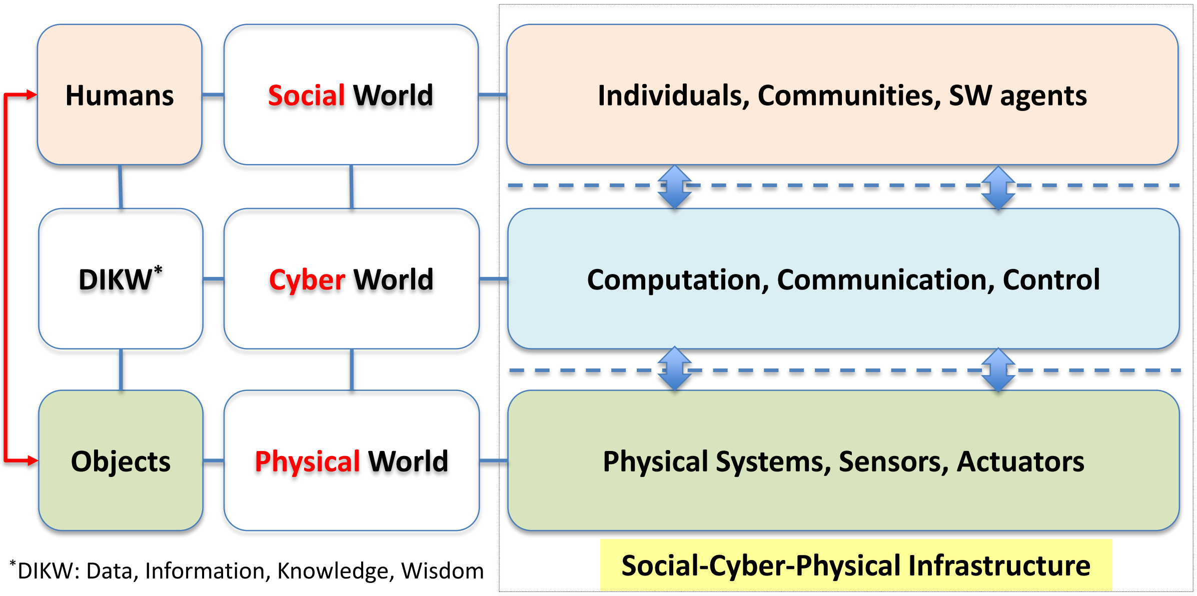
Humans
Social World
Individuals, Communities, SW agents
DIKW*
Cyber World
Computation, Communication, Control
Objects
Physical World
Physical Systems, Sensors, Actuators
*DIKW: Data, Information, Knowledge, Wisdom
Social-Cyber-Physical Infrastructure

Figure 28 – 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 28).

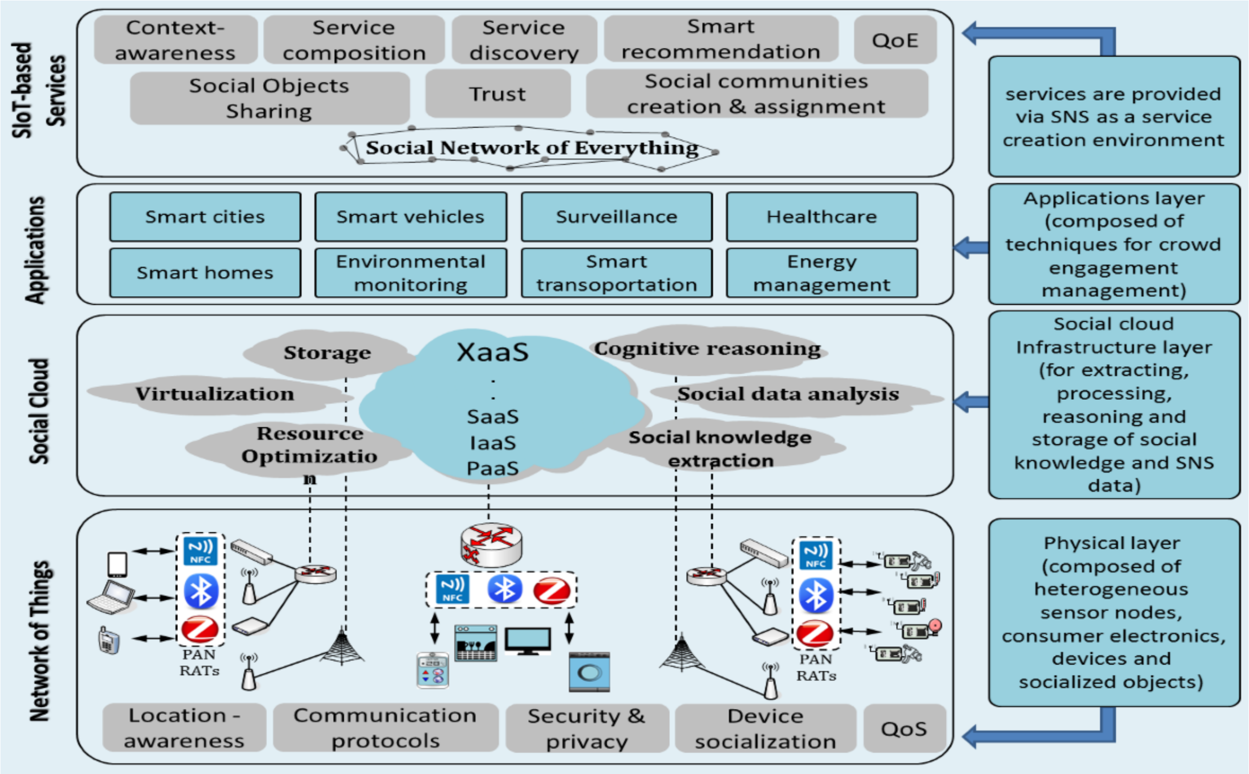

Figure 29 – A conceptual framework for the integration between the SIoT and the SoC

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 30, 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.

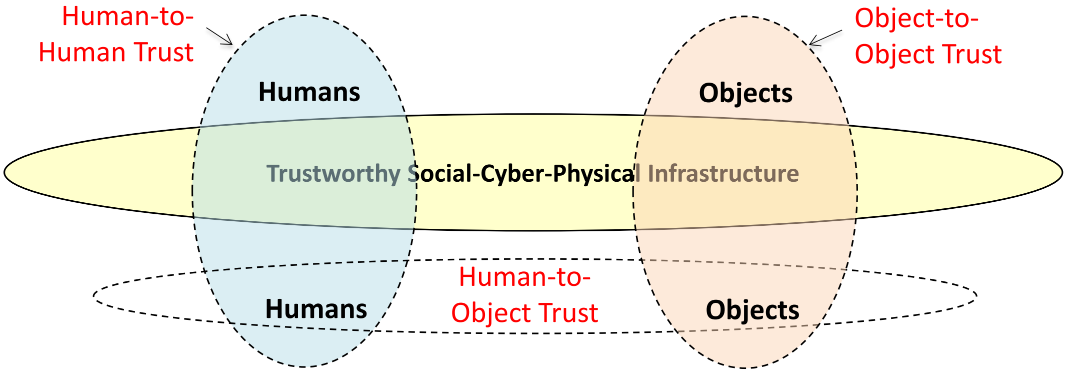

Figure 30 – Trust relationships in a trustworthy social-cyber-physical infrastructure

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 31).

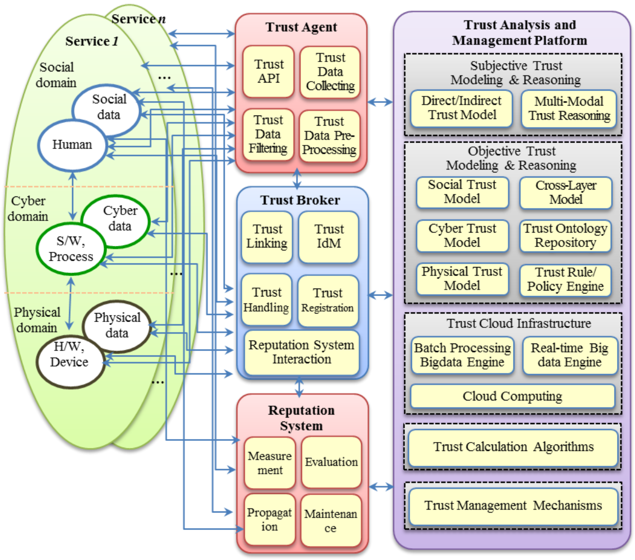
Service n
Service 1
Social domain
Social data
Human
Cyber domain
Cyber data
S/W, Process
Physical domain
Physical data
H/W, Device
...
Trust Agent
Trust API
Trust Data Collecting
Trust Data Filtering
Trust Data Pre-Processing
Trust Broker
Trust Linking
Trust IdM
Trust Handling
Trust Registration
Reputation System Interaction
Reputation System
Measurement
Evaluation
Propagation
Maintenance
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 31 – 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].

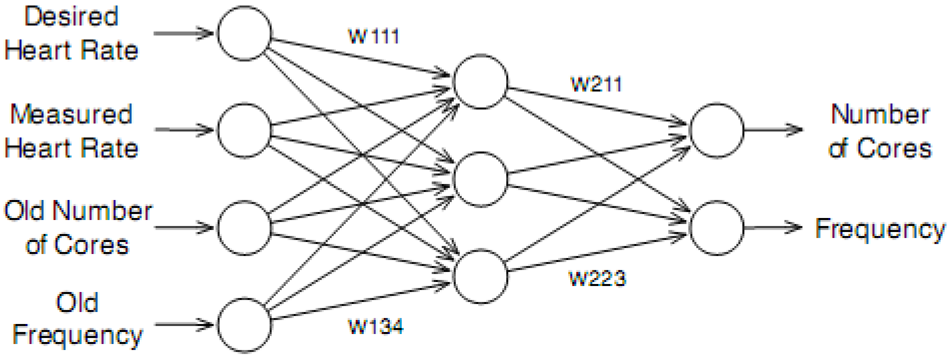

Figure 32 – Neural network topology [52].

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 32, 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.

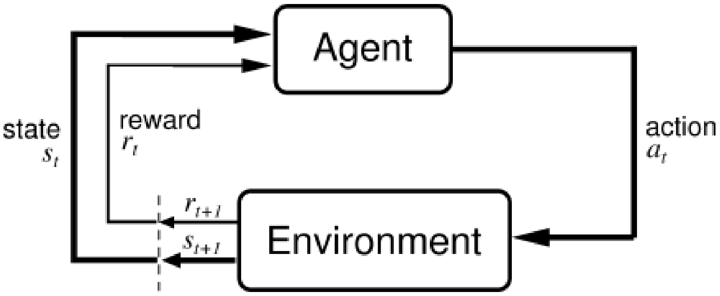

Figure 33 – The agent-environment interaction [53]. .

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.

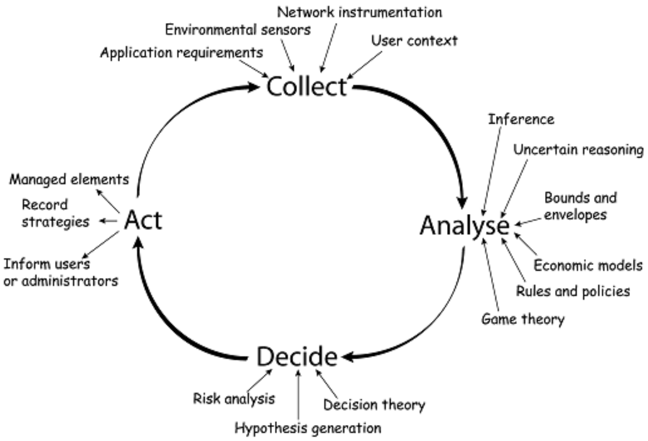

Figure 34 – Autonomic control loop [57].

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 35 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.

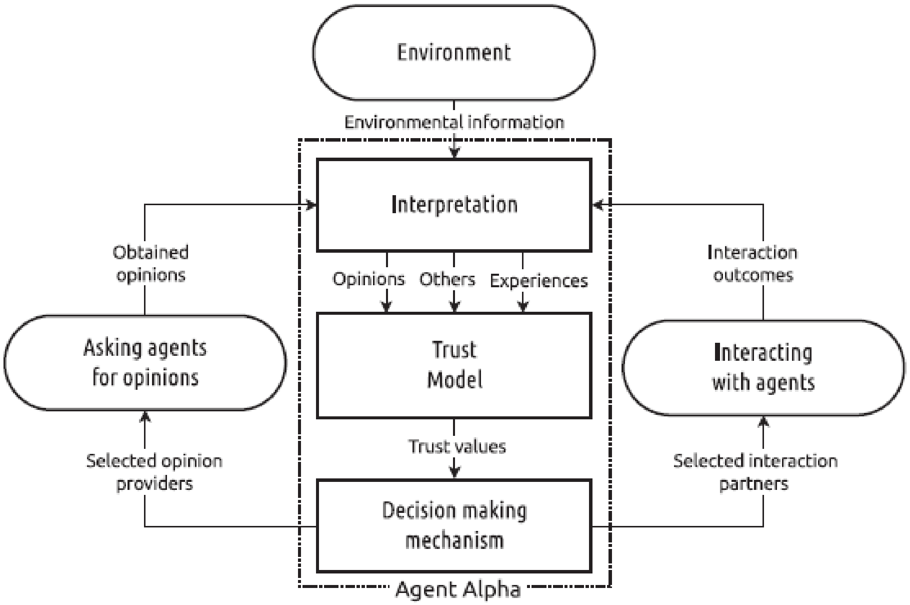

Figure 35 – Information context of a trust model

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.

8.2.1.5 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 36).

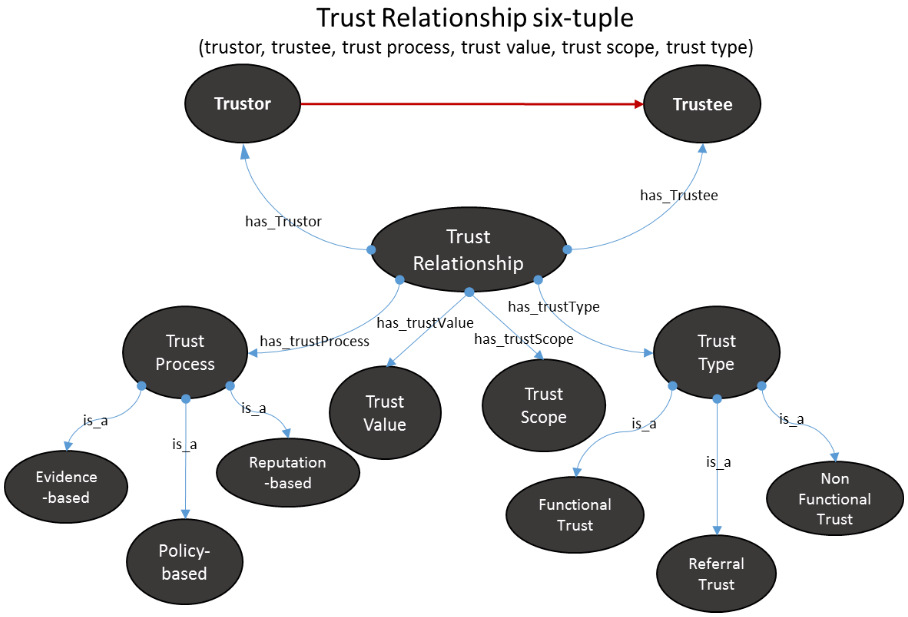

Figure 36 – Trust Model illustrating all the concepts and relationships between the concepts

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 37) 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.

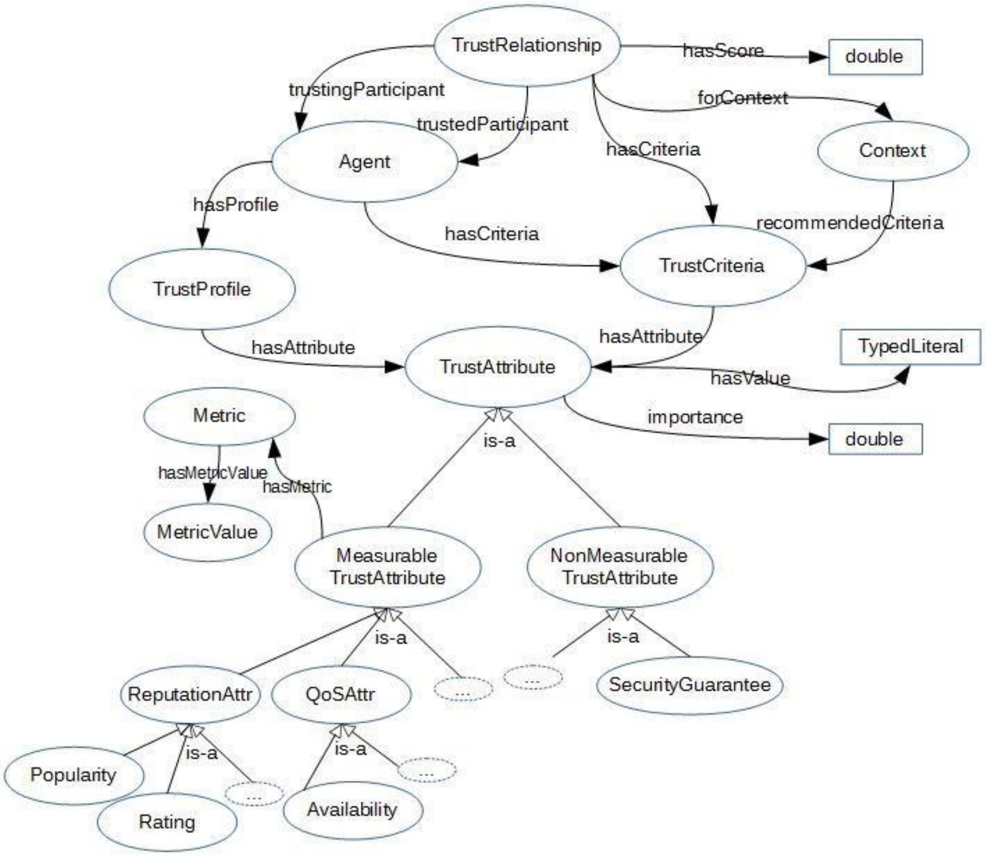

Figure 37 – Trust ontology [77]

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

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.

8.2.3.2 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 38:

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.

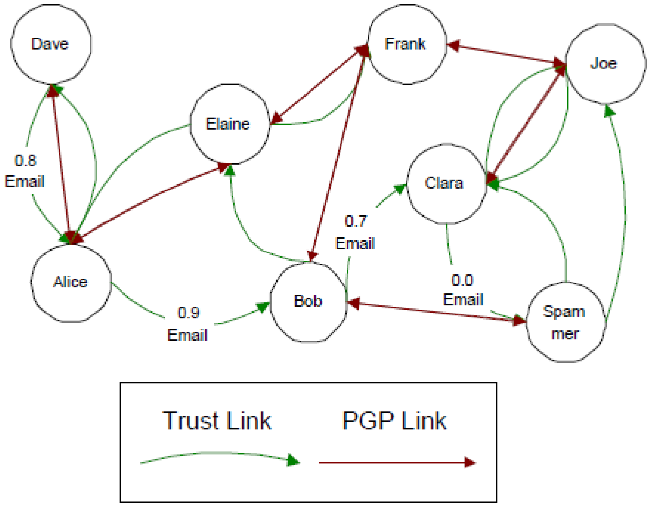

Figure 38 – Combined Trust Network Ontology in Konfidi

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 39, 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.

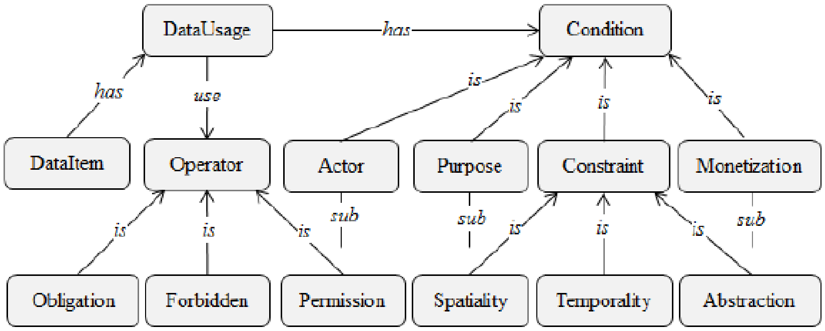

Figure 39. A Trust Data Usage Ontology

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 40.

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.

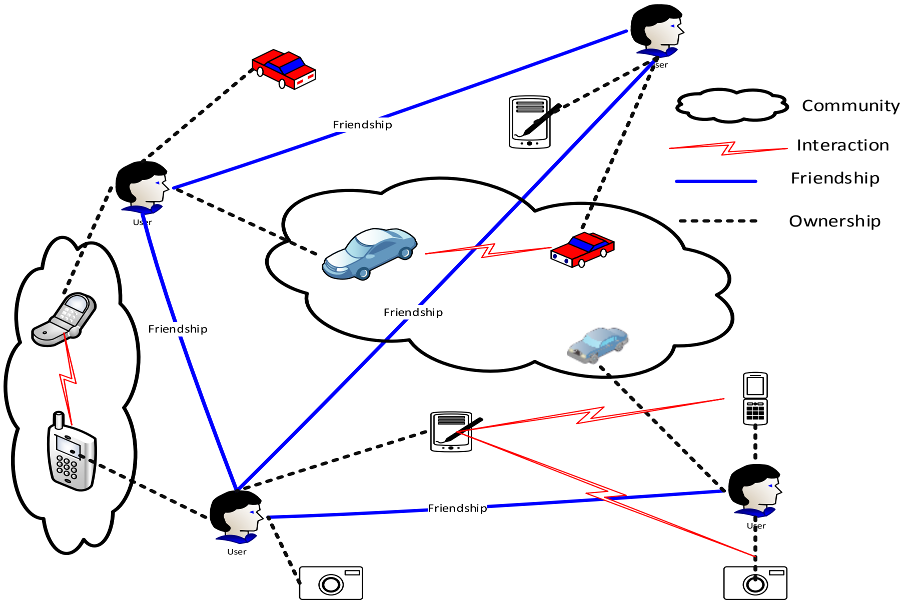

Figure 40 – Social structures of the IoT

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 41).

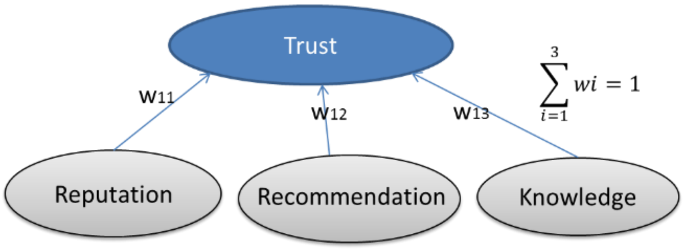

Figure 41 – A Trust Model with three Trust Metrics

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 42.

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

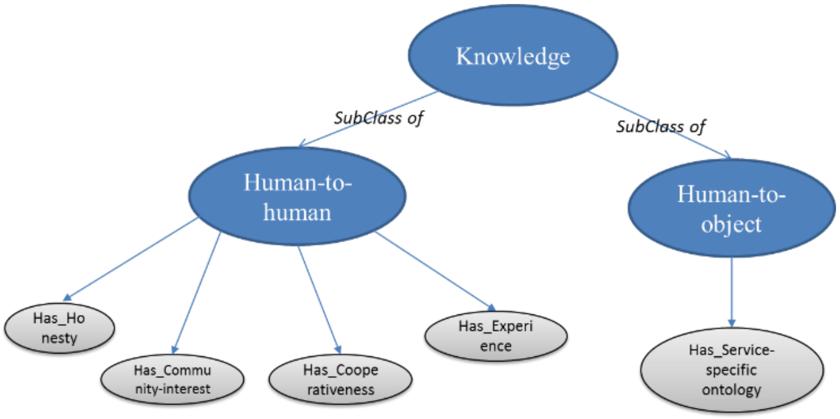

Figure 42 – The Knowledge TM is divided into two sub-ontologies

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.

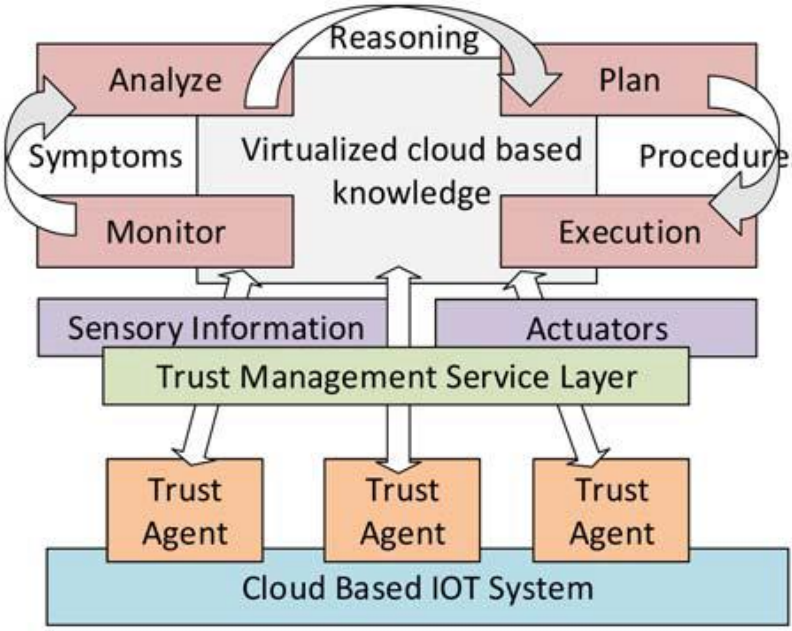

Figure 43 – MAPE-K feedback loops for adaptive trust agents.

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 43 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.

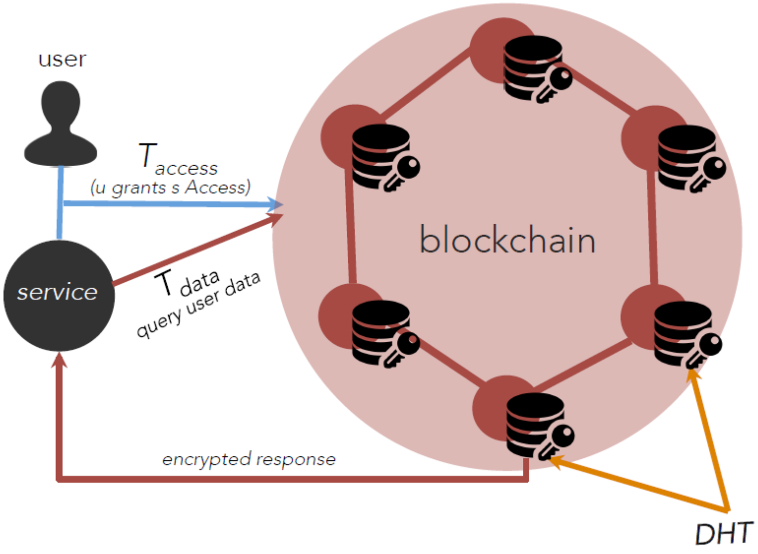

Figure 44 – Overview of the decentralized platform [114]

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.

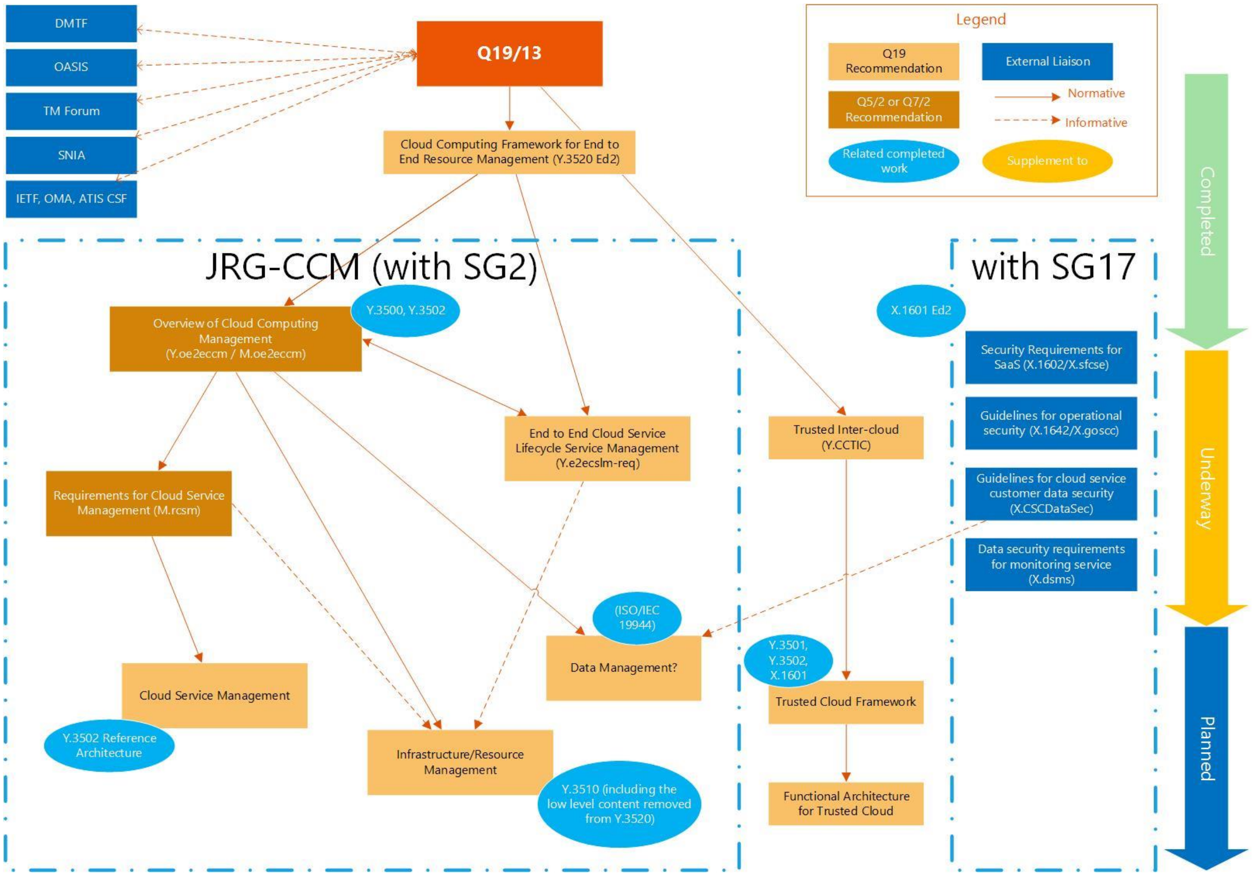
DMTF
OASIS
TM Forum
SNIA
IETF, OMA, ATIS CSF
Q19/13
Cloud Computing Framework for End to End Resource Management (Y.3520 Ed2)
Legend
Q19 Recommendation
External Liaison
Q5/2 or Q7/2 Recommendation
Normative
Informative
Related completed work
Supplement to
Completed
Underway
Planned
JRG-CCM (with SG2)
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 45 – 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.

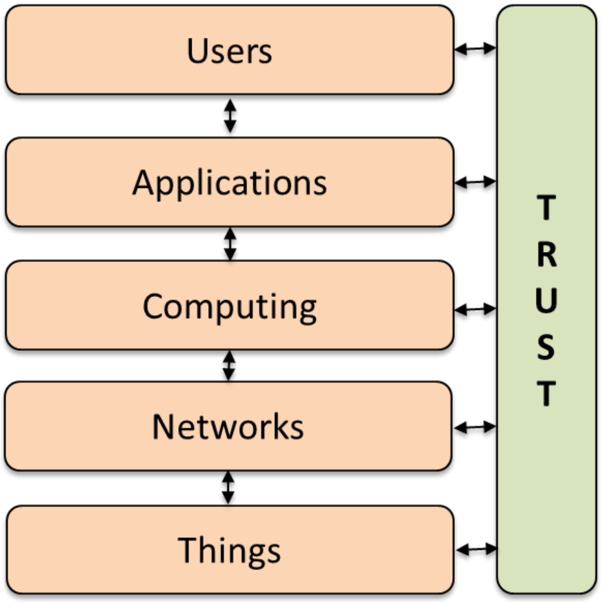

Figure 46 – Trust management (Trust as a cross domain relationship)

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).

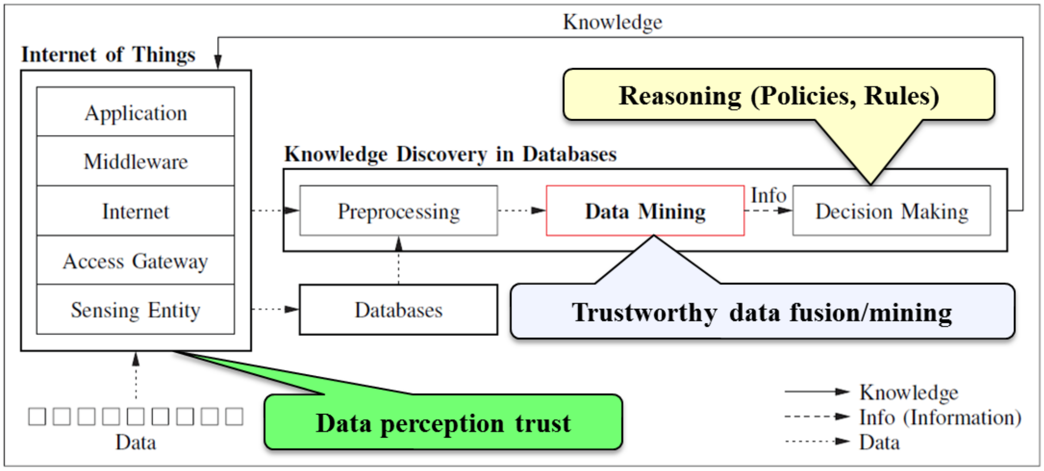

Figure 47 – Trust-based decision making

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.