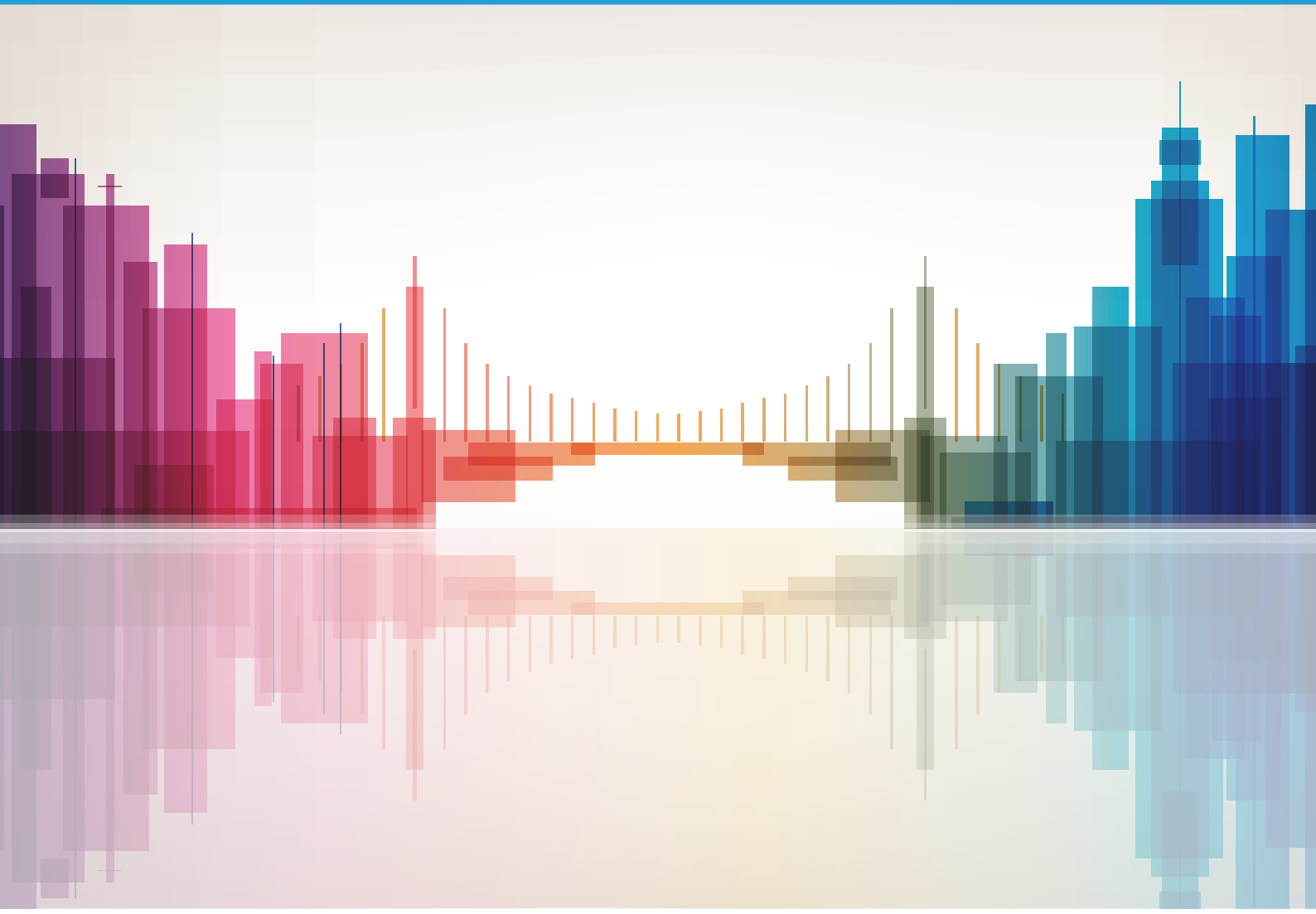
United 4 Smart Sustainable Cities

Unlocking the potential of trust-based AI for city science and smarter cities

Case study of the U4SSC City Science Application Framework



UNECE

UN HABITAT
FOR A BETTER URBAN FUTURE

ITU

11 SUSTAINABLE CITIES AND COMMUNITIES

Case study: Unlocking the potential of trust-based AI for city science and smarter cities

October 2019

Foreword

This publication has been developed within the framework of the United for Smart Sustainable Cities (U4SSC) initiative.

Acknowledgements

The development of the Case study: Unlocking the potential of trust based AI for city science and smarter cities has been researched and written by Gyu Myoung Lee (SMIEEE), John Moores University, Department of Computer Science, Faculty of Engineering and Technology, Adjunct Professor, KAIST, Korea, ITU-T Chair of FG-DPM, SG13 WP3 Chair, Q16/13, Q4/20 Rapporteur and has been edited and revised by Okan Geray (Smart Dubai Office).

The authors wish to thank the U4SSC management team, Nasser Al Marzouqi (U4SSC Chairman) and Victoria Sukenik, Paolo Gemma, Abdurahman M. Al Hassan and Albert Medrán (U4SSC Vice-chairmen) for their respective assistance and contributions. The authors also wish to extend their gratitude to the contributing organizations along with their representatives: Cristina Bueti, Chris Ip and Reyna Ubeda from the International Telecommunication Union (ITU), Paola Deda, Amie Figueiredo and Agata Krause from the United Nations Economic Commission for Europe (UNECE) and Robert Lewis-Lettington from the United Nations Human Settlements Programme (UN-Habitat).

CONTENTS

Foreword ii

Acknowledgements ii

1. Introduction 1

2. Trust-based AI Data Management Solution 4

3. Conclusions 9

A. References 10

B. List of discussion partners/interviews 11

1. Introduction

1.1 Background

With the rising economy and social opportunities that urban areas have to offer, people have been moving from countryside to cities, resulting in the largest wave of urbanization throughout the world in our history. By 2030, the urban population is estimated to reach 5 billion (about 60 percent of the world population), which produces massive opportunities for the economic and social development of cities [1]. Due to the ever-growing demands of local residents, the development of fundamental infrastructure and policies are lacking behind. Moreover, this unplanned and overly fast urban growth is amplifying some of the greatest urban challenges that cities are already facing, including climate change, growing energy demands and consumption, environment degradation, and human health.

To mitigate the challenges of rapid urbanization, it is imperative to improve governance and service delivery, offer swift and seamless mobility, facilitate easily assessible urban public facilities, access to affordable housing, quality healthcare, education etc [2]. A special spotlight is needed, covering urbanization trends in innovative management of urban operations and delivering a variety of “smart” services to local residents, visitors, and the government to satisfy the ever increasing and diverse demands [3].

As an emerging paradigm, the smart city leverages a variety of promising technologies, such as the Internet of Things (IoT), cyber-physical systems, big data analysis, and real-time control, to enable intelligent services and provide comfortable life for local residents [4]. It integrates ubiquitous sensing components, heterogeneous network infrastructure, and powerful computing systems to sense the physical changes from cities and feed back to the physical world. Specifically, RFID devices, sensors, and versatile wearable devices are promoted to offer real-time monitoring and ubiquitous sensing, from energy to environments, from road traffic to healthcare, from home area to public venues, and so on. Then this sensing information is transmitted to a control center via heterogeneous networks. This control center takes comparative advantage of powerful computing systems, such as cloud servers, to process and analyze the collected data.

Fueled by human intelligence, the control center makes optimal decisions and manipulates the urban operations via feedback components, such as actuators [3]. Having the advanced information, communication, and control technologies as backbones, a smart city can offer various applications, including intelligent transportation, smart energy, intelligent healthcare, and smart homes. Not only can this up-and-coming connected city quickly identify the demands of people and a city, but it can also manipulate urban operations to improve urban living quality in an intelligent and sustainable way. It is expected that the global smart city market will exceed US$1200 billion by 2020, which is almost triple that in 2014 [1].

When cities become smarter, people may suffer from a series of security and privacy threats due to the vulnerabilities of smart city applications [5]. For example, malicious attackers may generate false data to manipulate sensing results such that services, decisions, and control in a smart city are influenced and not “intelligent” enough. Moreover, these malicious attackers could also launch

denial-of-service attacks, disrupting the sensing, transmission, and control to degrade the quality of intelligent services in a smart city. In addition, the pervasive video surveillance in a smart city captures a tremendous number of images and video clips, which may be utilized to infer local residents' trajectories and inherently endanger their privacy.

The home area information collected and managed by smart home applications may pave the way to disclosing residences' highly privacy sensitive lifestyle and even cause economic loss. Although some off-the-shelf techniques (encryption, authentication, anonymity, etc.) and policies might be directly applied to avert these problems [5], the emerging "smart" attackers could still infer and violate privacy in many other ways, such as side channel attack and cold boot attack [6]. Without sufficient security and privacy protections, users may refrain from accepting the smart city, which would remain as a far-off futuristic idea.

Figure 1. Smart city applications [7].

1.2 Challenge and response

Smart cities provide services that benefit from the city-scale deployment of sensors, actuators, and smart objects. Such services are mainly driven by data and can be broadly classified as producers of data, consumers of data, or a combination of both. For example, a parking service that deploys a message queue telemetry transport (MQTT) broker to publish parking lots' availability data is considered a producer, while cars which subscribe to that broker are considered consumers. Cars can produce other data for use by other smart city components. For instance, cars use device-to-device (D2D) communications to alert nearby vehicles and pedestrians of their presence and potential traffic hazards. In a city scale deployment of smart services, data is generated at high rates, which presents new challenges for smart city designers and developers.

Unfortunately, most of the generated data is wasted without extracting potentially useful information and knowledge because of the lack of established mechanisms and standards that benefit from the availability of such data. The main culprit is the lack of a large amount of labeled

data. Moreover, the highly dynamic nature of smart cities calls for a new generation of approaches that are flexible and adaptable to cope with the dynamicity of data to perform analytics and learn from real-time data. Development of smart city applications supported by big data analytics is subject to several challenges that need to be addressed to achieve a reliable and accurate system. Some of the major challenges include the following.

Integrating Big and Fast/Streaming Data Analytics:

In a smart city context, there are many time-sensitive applications (e.g., smart and connected vehicles) that need real-time or near-real-time analytics of the stream of data. Such applications call for new analytic frameworks that support big data analytics in conjunction with fast/streaming data analytics.

Preserving Trust, Security and Privacy:

Data-driven approaches (e.g., deep learning) can be attacked by false data injection (FDI), which compromises the validity and trustworthiness of the system. Resilience against such attacks is a must for such inference algorithms. 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. Privacy preservation is another important factor since a large part of smart city data comes from individuals who may not prefer their data to be publicly available. Data modelling algorithms should address these concerns to enable the wide acceptance of smart city systems by organizations and citizens.

On-Device Intelligence:

Smart city applications also call for lightweight AI algorithms deployable on resource constrained devices for hard real-time intelligence. This is also in line with the trust, security and privacy preservation requirement since data is not transferred to the fog or cloud.

Big Dataset Shortage:

Development and evaluation of smart city applications need real-world datasets, which are not readily available for many application domains. It is necessary to confirm results based on simulated big data.

Context Awareness:

Integrating contextual information with raw data is crucial to get more value from the data, and perform faster and more accurate reasoning and actuation. For example, detecting a sleepy face in a human pose detection system could lead to totally different actions in the contexts of driving a car and relaxing at home.

In addition, there are other challenges that affect the design of a smart city ecosystem such as integration of different analytic frameworks, distribution of analytic operations, and lack of comprehensive testbeds.

The ever-growing volume of data and devices in a smart city poses open problems for intelligent services, trust and privacy. Inside-attackers exploit human intelligence and have access to big data such that the privacy of data owners may be inferred and violated; even the traditional cryptographic schemes have been applied to big data.

An alternative to detect these inside attackers is to enhance the traceability and allow a trusted third party to monitor and audit. Meanwhile, collaborative efforts among municipalities, regulation departments, industry, academia, and business companies are necessary to set up privacy policies and regulations.

In addition, to improve the data privacy, availability, and management of the city network, a distributed computing architecture which delegates AI based processing of data towards the edge of the network must be considered. Further a smart city is vulnerable to false data injection in both sensing and control phases. Digital signature techniques cannot prevent the data from being tampered from the origination. An insight into detecting false data injection is to leverage machine learning and data mining along with trust-based concepts to come up with a boundary of reasonable sensing data.

The proposed approach intends to instill a trusted environment for various City Science applications in the smart city context. It proposes a distributed computing architecture which is conducive to enhancing trust while enabling innovation for City Science applications.

Important Note: This case study is an example of an R&D project related to city science, rather than an actual city example. City Science is a relatively novel field and will require substantial R&D (Research & Development) for developing future urban solutions. The proposed approach is an actual research project currently being conducted by the author.

2. Trust-based AI Data Management Solution

2.1 Vision and content

The proliferation of computing, networked systems and end-node processing power, has made Internet a highly dynamic system. Maintaining trust across a large-scale heterogenous distributed system is a formidable task. It requires preservation of data processing security policies in a distributed system which can be substantially challenging. Existing security mechanisms (e.g. authentication, authorization) are not sufficiently scalable for today's large-scale networks. Hence, the trust-based approach to distributed systems is developed to address the inadequacy of traditional mechanisms.

In a smart city, user-related information works as oil to fuel the state of art applications and services. Consumers, who use these services, provide personal information to service providers, intentionally or unintentionally and often without considering their trustworthiness. However, this personal information often reveals one's identity and may lead users to face unexpected outcomes, ranging from uninvited advertisements to identity theft. To regulate such issues, this approach investigates state of the art data governance techniques that are built on trust, blockchain, and the distributed AI concepts.

As the aim of a smart city is to make decisions about its data in a more trustworthy manner and meeting the essential KPIs, the proposed trust-based data management solutions has enormous potential to securely process and handle data of any service providers or customer.

Further combination of blockchain and IoT will facilitate the sharing of AI services and resources leading to the creation of a marketplace of services between devices.

For cross-border applications, it can serve as an intermediate broker to handle the negotiations for particular interaction without any ambiguity or human intervention which outsmart current techniques based on third party regularity bodies.

With great interest in artificial intelligence around the world today, the approach has the potential to open up a new chapter in human-machine interaction by giving interoperability to existing AI technology and combining it with the trust-based data governance concepts.

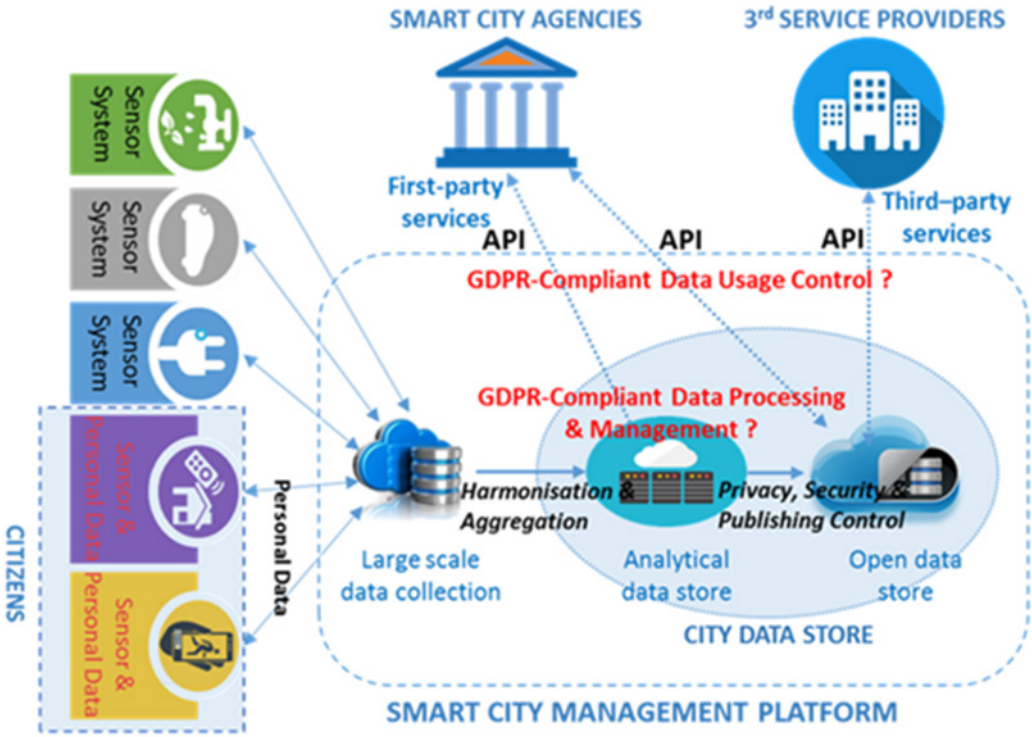
The proposed Trust-based AI cross-domain microservices across Roof, Fog and Cloud continuum will not only support the development of real-time applications that address latency and bandwidth related problems of the current systems but also privacy leakages and security attacks. It will also support plug and play AI reusable and dynamically composable components that are deployed as microservices for the development of value-added cross-border use case applications.

2.2 Implementation

Figure 2 illustrates a conceptual system model for data collection, processing and sharing in Smart Cities from various data sources, including personal data. In a Smart City big data architecture, collected data are processed and stored in a structured format that can be queried using analytical tools in an analytical data-store for supporting querying from Smart City agencies. Also, data is shared with third-party service providers through an open data-store after conducting publishing control mechanisms.

According to the GDPR [8] legislation in Smart City contexts, citizens (i.e., Data Subjects) authorize Smart City operators (i.e., Data Controllers) to control their personal data. Data Controllers determine the purposes for which, and the method in which, personal data is processed by Data Processors (i.e., Smart City agencies and third-party service providers)- who will be responsible for processing the data on behalf of the controllers. Therefore, Data Controllers are subject to comply with requirements and obligations imposed by GDPR when determining personal data usage policies for Data Processors.

Figure 2. Data Management and Sharing in Smart Cities.



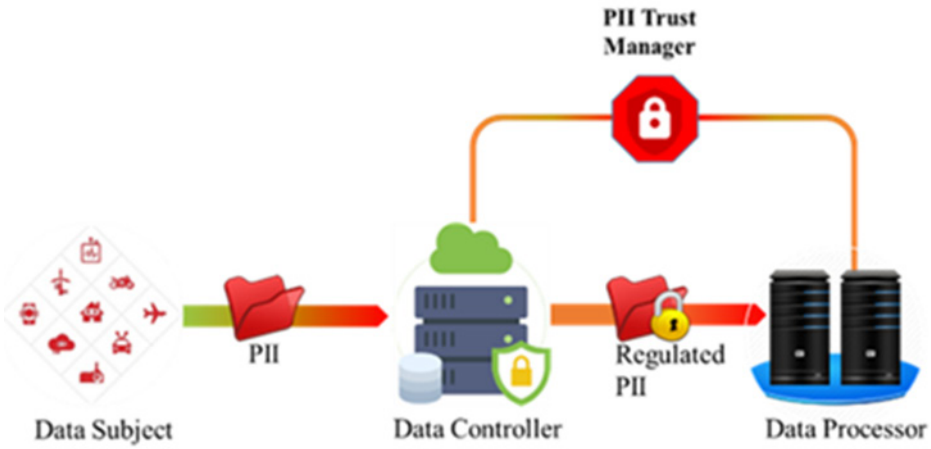
GDPR also specifies the rights of Data Subjects including Right of Access and Right of granting citizens the rights to monitor their personal data and information about how the personal data is being processed; and the right to control the related personal information. Therefore, a Smart City management platform, which take on the role of a Data Controller, should take appropriate measures not only to provide citizens information related to how their personal data is being processed and managed but also the ability to control their data usage ensuring security and privacy.

Moreover, in the absence of proper safety mechanisms, data can be compromised at various points or even via the interfaces of different smart city devices. Nevertheless, objects in large-scale networks like in smart city possibly lack the knowledge to evaluate services' reliably as both untrustworthy and trustworthy objects can interact with each other in the absence of a trusted intermediary which governs each transaction.

To fill this gap, the suggested approach proposes an intermediary authority named the Trust Manager to evaluate each interaction in a trustworthy manner as shown in Figure 3.

In a large heterogeneous distributed system (e.g. smart city), there is a large number of requests to access and process data. In Figure 3, data subject refers to any individual that can be identified, directly or indirectly, through an identifier and whose personal data is being collected (refereed to as PII – personally identifiable information). The data controller determines the purposes for which and the means by which personal data is processed. On the other hand, the data processor processes personal data on behalf of the controller.

Figure 3. High level architecture of the Trust based Data Governance.



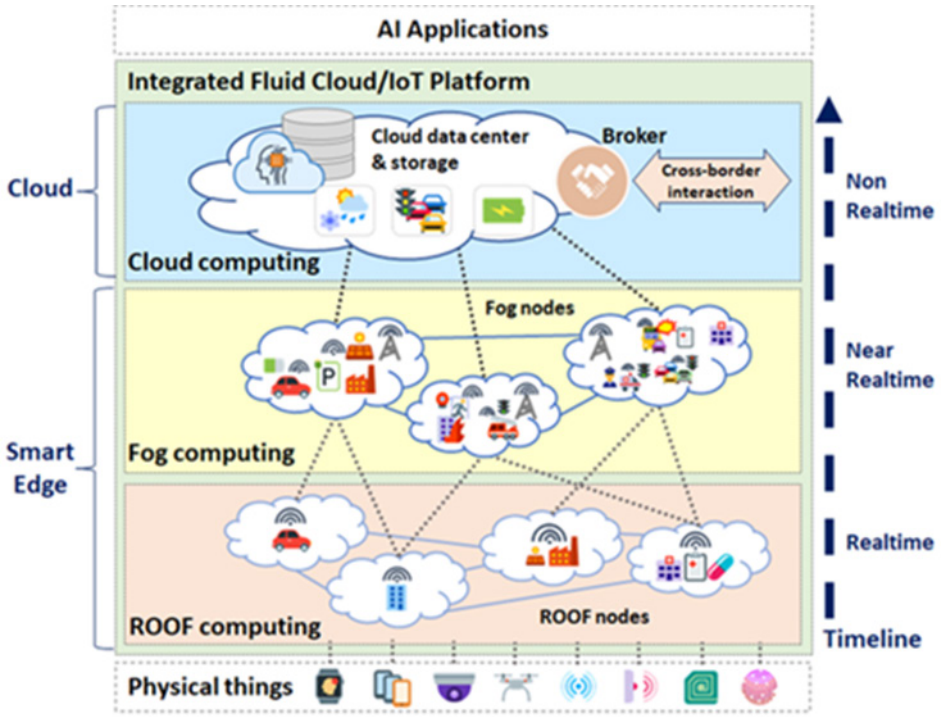
The interactions related to several distributed data subjects, data controllers and data processors in a smart city context can be handled by a Trust Manager from a security perspective. Different systems in a smart city may have different local policies for security. In general, there is a staggering number of resources and services to be accessed in a smart city. Trust manager receives these access requests together with a set of credentials and determines if the provided credentials for access request comply with the local security policy to access the intended resource or service (in this case it can be data that entails personally identifiable information). Hence, it uses a general-purpose application-independent algorithm and supports features like delegation, policy specification, refinement at the different layers of a policy hierarchy. So, the Trust Manager solves the consistency and scalability problems present in traditional mechanisms.

Recent technological innovations of smart edge devices and services which heavily rely on real-time data processing and localized intelligent decision-making, have created a vacuum for a novel approach that extends the traditional means of research in cloud computing towards edge computing. The idea of edge computing refers to fluid data management and decision-making towards physical things, working as a middle layer between cloud and the users.

Major advantages of doing so include but not limited to (a) minimizing response delay by addressing the bottom level request at the network edge instead of servicing it at far located cloud data centers, (b) minimize downward and upward traffic volumes in the network core and (c) maximizing the support for cross-border applications due to effective resource and security management at cloud. Complying with edge computing requirements, the proposed approach further breaks down the so-called middle layer by introducing two layers ROOF computing and Fog Computing which places just below the cloud as shown in Figure 4 in order to make the system architecture more feasible and deployable in real-time environment with an ambitious vision for seamless fluid control and decision-making through harmonize resource management among different layers.

Fog computing layer is implemented with the idea of achieving the second objective of the edge computing scenario which is improving application performance and resource efficiency by removing the need for processing all the information in the cloud, thus also reducing bandwidth consumption in the network. A Fog node can be defined in several ways. It can be regarded as an

Figure 4. Vision towards Integrated Fluid Cloud/IoT Platform.



entry point into enterprise or service provider core networks. Examples include routers, switches, integrated access devices (IADs), multiplexers, and a variety of metropolitan area network (MAN) and wide area network (WAN) access devices.

Unlike the Fog and the Cloud, the primary goal of the ROOF computing layer is to provide real-time computing needs for building the contexts and required actions along with efficient and flexible connectivity to the Fog and Cloud providers. As the ROOF will be the first contact points for heterogeneous physical things, it must be equipped with technologies that can handle interoperability, mobility and importantly smart decision-making abilities to fulfil the goals of three-layer architecture presented here.

The distributed AI based architecture will not only improve the fluidness of traffic flow and promptness of decision-making but also will save ample amount of resources at the Cloud layer, which can be used by future applications like cross-border interactions. This will open a new paradigm for new business models, like inter-regional collaboration for law and order, international travelling and global research activities. However, ensuring business uptake and regulatory compliance in such an environment is critical and manual intervention is almost impossible without an autonomous and more secure intermediate agent called, trust manager. The trust manager essentially ensures trust across different domains. It allows free flow of data or services while maintaining trust as it passes across different domains (each domain might have different governance, regulations, administration, etc.). In this context, the main responsibilities of the trust manager will be to regulate federated AI platform and ensure reliable and trustworthy data aggregation and decision-making.

2.3 Results

Approximately 70% of the world's population will live in urban areas by 2050 according to a recent United Nations report. This will exacerbate the existing pressures on resources and infrastructures in cities and communities. If appropriate steps are not taken this will significantly and adversely affect the quality of life of all citizens.

From a technical perspective, the Trust paradigm, coupled with the power of AI to unlock insights from big data, offers significant opportunities to make our cities and communities "smarter", "more responsive", and "trustworthy". Potential benefits include more efficient transportation, optimization of the use of natural resources and enhanced safety for citizens.

On the other hand, association of trust and AI microservices will foster and enhance the capability of SMEs and other small-scale technology companies to exploit proposed federated Cloud-Edge platform to deliver cutting edge AI-based applications in a more trustworthy manner.

SMEs can take advantage of the new technologies provided to break the current barrier regarding transmitting of huge volume of IoT data to the cloud for analytics to provide real-time intelligence at the edge. SMEs providing smart living services, smart city applications, smart cars, smart transportation such as emergency support, crowd congestion control, etc. will benefit from the provided technologies.

3. Conclusions

The processing and analyzing big data by leveraging 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 pose 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. Therefore, it is important to process and handle data in compliance with user needs and rights in various application domains without human intervention.

To cope with the development of a large number of complex and intelligent applications and services like in smart cities, it is needed to create a trusted environment for ICT infrastructure in order to share information and create knowledge. Consequently, there is a critical need to develop a trusted infrastructure as one of the most important parts in the future ICT environment.

A. References

[1] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in Smart City initiatives: Some stylised facts," *Cities,* vol. 38, pp. 25-36, 2014.

[2] R. G. Hollands, "Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?," *City,* vol. 12, no. 3, pp. 303-320, 2008.

[3] J. Liu, Y. Li, M. Chen, W. Dong, and D. Jin, "Software-defined internet of things for smart urban sensing," *IEEE communications magazine,* vol. 53, no. 9, pp. 55-63, 2015.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal,* vol. 1, no. 1, pp. 22-32, 2014.

[5] A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *IEEE Communications Magazine,* vol. 51, no. 6, pp. 136-141, 2013.

[6] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine,* vol. 49, no. 11, 2011.

[7] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Communications Magazine,* vol. 55, no. 1, pp. 122-129, 2017.

[8] European Union, "General Data Protection Regulation (GDPR)," *Official Journal of the European Union,* vol. L119, pp. 1-88, 2016.

B. List of discussion partners/interviews

This case study has been prepared by:

- Gyu Myoung Lee, PhD SMIEEE
- Reader, Liverpool John Moores University
- Department of Computer Science, Faculty of Engineering and Technology
- Adjunct Professor, KAIST, Korea
- ITU-T Chair of FG-DPM, SG13 WP3 Chair, Q16/13, Q4/20 Rapporteur

This case study has been edited and revised for U4SSC compliance by:

- Okan Geray
- Strategic Planning Advisor, Smart Dubai Office

For more information, please contact:
u4ssc@itu.int
Website: http://itu.int/go/u4SSC