STRENGTHENING TRUST IN THE FUTURE ICT INFRASTRUCTURE

Tai-Won Um[1], *Gyu Myoung Lee*[2], *Jun Kyun Choi*[3]

[1]Electronics and Telecommunications Research Institute (ETRI), Korea (Rep. of), twum@etri.re.kr
[2]Liverpool John Moores University (LJMU), United Kingdom, g.m.lee@ljmu.ac.uk
[3]Korea Advanced Institute of Science & Technology (KAIST), Korea (Rep. of), jkchoi59@kaist.edu

ABSTRACT

Moving towards a hyperconnected society in the forthcoming "zettabyte" era requires a trusted 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. In this paper, we introduce the concept of a social-cyber-physical infrastructure from the social Internet of Things paradigm and present different meanings from various perspectives for a clear understanding of trust. Then, the paper identifies key challenges for a trustworthy ICT infrastructure. Finally, we propose a generic architectural framework for trust provisioning and presents strategies to stimulate activities for future standardization on trust with related standardization bodies.

Keywords**—** Trust, social-cyber-physical infrastructure, Internet of Things, ICT

1. INTRODUCTION

The widespread availability of feature-rich communications is the result of end-user devices, advanced networks and new services that exploit the developments in Information and Communication Technology (ICT). Key technologies are the Internet of Things (IoT), web services, cloud computing (including distributed and embedded computing), big data analytics, smart objects and sensing technologies.

The IoT is one of the hottest and most promising topics in ICT today. As more heterogeneous objects get connected to the Internet, novel mechanisms to manage, describe, discover and use these connected resources and the data they produce become necessary. A number of initiatives are available borrowing from the fields of autonomous systems, intelligent systems and semantic technologies, etc.. One of the main challenges of the IoT is to develop solutions that are readable, recognizable, locatable, addressable and/or controllable via the Internet. The convergence of technologies like IoT and cloud computing will enable innovative services. These involve technologies such as bio-, nano- and content technologies going beyond traditional telecommunication services [1], [2].

From the perspective of connected devices, the introduction of sensors and devices in physical spaces poses particular challenges and increases the sensitivity of the data that are being collected. Connected devices are effectively allowing companies to digitally monitor our private activities. Moreover, the sheer volume of generated data allows those with access to the data to perform analyses and compile detailed profiles of consumer behaviour [3].

From the perspective of big data analytics, the processing and analysis of the large amount of data through cloud computing are becoming an important resource that can lead to increased knowledge, drive value creation, and foster new products, processes and markets. However, the large scale collection and analysis of data imposes 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 [4].

Although recent advances in ICT have brought changes to our everyday lives [5],[6], various problems exist due to the lack of trust. Therefore, it is important to process and handle data in compliance with user needs and rights in various application domains. Based on the significant efforts made to build converged ICT services and a reliable information infrastructure, ITU-T has recently started new work on future trusted ICT infrastructures.

These infrastructures will be able to accommodate emerging trends in ICT, while taking into account social and economic considerations. Thus, this paper discusses an effort to find a good solution to these problems while developing advanced technologies for intelligent autonomous networking and services. The aim is to create a trusted environment for an ICT infrastructure in order to share information and create knowledge.

Firstly, in Section 2 this paper introduces the concept of an emerging social-cyber-physical infrastructure from the social IoT paradigm. Secondly, Section 3 presents different meanings of trust from various perspectives. In Section 4, the paper identifies key challenges for trustworthy ICT infrastructures. The paper proposes a generic architectural framework for trust provisioning in Section 5 and presents strategies to stimulate activities for future standardization on trust with other standardization bodies.

2. FUTURE ICT INFRASTRUCTURE FOR A HYPERCONNECTED SOCIETY

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 hyperconnected 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 [7]. 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[1] [8] 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 [8]. The paradigm of Cyber-Physical-Social Systems (CPSS) [9],[10] 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.

Based on the CPSS, Figure 1 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.

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 [11]. This is mainly related to the data, information, knowledge, wisdom (DIKW)[2] process in the cyber world, see Figure 1.

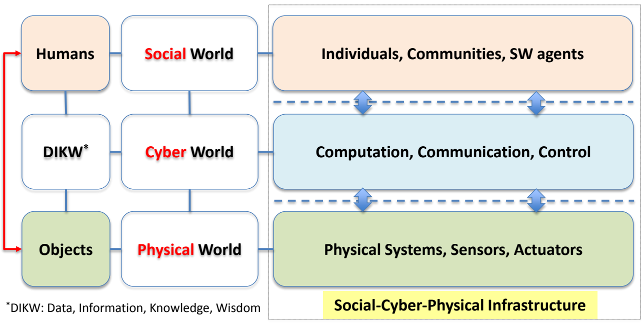
Humans
Social World
Individuals, Communities, SW agents
DIKW*
Cyber World
Computation, Communication, Control
Objects
Physical World
Physical Systems, Sensors, Actuators
*DIKW: Data, Information, Knowledge, Wisdom
Social-Cyber-Physical Infrastructure

Figure 1: The concept of a social-cyber-physical infrastructure

To strengthen trust while building a hyperconnected 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.

3. UNDERSTANDING OF TRUST

Because trust can be interpreted in different ways, we present its various meanings in the context of telecommunication systems and ICTs and highlight the relationship between knowledge and trust.

As a lexical-semantic, trust means reliance on the integrity, strength, ability, 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

[1] The Social Internet of Things is defined as an IoT where things are capable of establishing social relationships with other objects, autonomously with respect to humans [8].

[2] DIKW (Data, Information, Knowledge and Wisdom): This refers loosely to a class of models for representing purported structural and/or functional relationships between data, information, knowledge, and wisdom. "Typically information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge".
Source: https://en.wikipedia.org/wiki/DIKW_Pyramid

monitor or control the environment in which it operates [12].

In computer science, trust hast two aspects “user trust” and “system trust”. For a user, trust is based on psychological and sociological considerations because it is “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” [12].

For the IoT, trust relies on the integrity, ability or character of an entity [13]. Trust can be further explained in terms of confidence in the truth or worth of an entity. For example, the EU uTRUSTit project defines trust as a user’s confidence in an entity’s reliability, including a user's acceptance of vulnerability in a potentially risky situation [12].

From a technical perspective, trust could be classified along three dimensions; technical trust (like data security), business/trading/community trust (or credits), and human trust (perceived by an individual human or group of members).

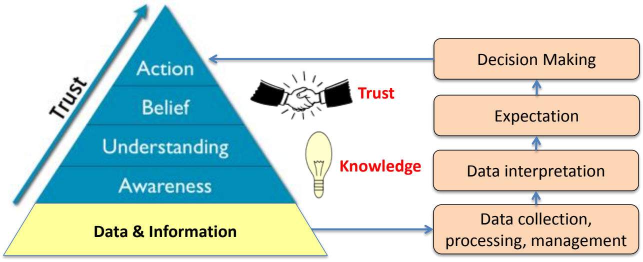

Figure 2: Knowledge and Trust (illustration compiled from trust pyramid [14])

The social and economic value of data is mainly reaped at two stages: firstly when data and information are transformed into knowledge (gaining insights) and secondly when they are used for decision making (taking action). The knowledge is accumulated over time by an individual or systems through data analytics. Data processing, management and interpretation for awareness and understanding have been considered as fundamental processes for obtaining knowledge. As shown in Figure 2, trust is strengthened from accumulated knowledge and it has a significant role as a link between knowledge (i.e., awareness and understanding) and action. It means that the expectation process for trust should be additionally considered before decision making.

4. CHALLENGES FOR THE TRUSTWORTHY ICT INFRASTRUCTURE

In a highly interconnected ICT world such as the SCP infrastructure, a number of independently developed, operated and managed systems network autonomously yielding a new kind of complex system that provides various services. Assuring continuous trustworthiness, taking into account such characteristics for future ICT infrastructures with highly interconnected systems, is becoming an essential issue. Therefore, this section identifies key challenges for the trustworthy ICT infrastructure.

4.1. 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 [15]. Thus, social trust[3] between humans and objects is quite important. As shown in Figure 3, 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 social-cyber-physical relationships, trust as a cross-domain relationship is needed, taking into consideration coexistence, connectivity, interactivity and spatio-temporal situations between vertical layers.

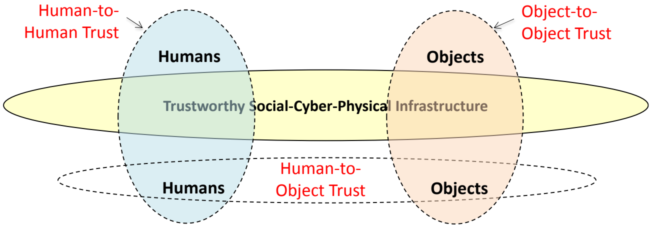

Figure 3: Trust relationships in a trustworthy social-cyber-physical infrastructure

4.2. Holistic Trust for Interconnected Systems

ICT services can be achieved through a chain of interconnected systems and components that share the responsibility for providing stable and robust services. Furthermore, many systems are based on open system architectures and their properties of interconnectivity and autonomics remove system boundaries. Such characteristics of interconnected systems lead to the introduction of security deficiencies that can be very hard to find and analyse. If this is not properly handled, the stability and safety of the overall system can be seriously threatened.

How can the stability and safety of such highly interconnected systems be achieved? Trust must be addressed and evaluated in all services and infrastructures, as well as in all system and component levels, in a holistic manner. Trust management is also required to apply between heterogeneous systems, service domains and

[3] Social trust implies that members of a community act according to the expectation that other members of the community are also trustworthy and expect trust from other community members.

stakeholders, while focusing on the relationships and dependencies between them [16].

4.3. Unified Approach to Trust-Security-Privacy

Scalability and complexity of the SCP infrastructure are due to the huge number of different links and interactions. Therefore, trust, security and privacy become tightly coupled because system features increasingly depend on networks, computation and processing. Trustworthiness requires cooperation and co-engineering of trust with security and privacy. It is not sufficient to address one of them in isolation, nor is it sufficient simply to combine components of trust, security and privacy. In order to address these issues, a unified approach is needed towards trust, security and privacy co-analysis, -design, -implementation and -verification [16].

4.4. Measurement and Formalization of Trust

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

Due to the diversity of applications and their inherent differences in nature, trust is hard to formalize in a general setting. However, it is important to quantify a level of trust in ICT. The level of trust can be measured and classified, similar to Quality of Service (QoS) used in an objective manner (e.g., measured quantitatively) or Quality of Experience (QoE) used in a subjective manner (e.g., counted qualitatively). A certain level of trust should be derived from the associated services and applications of trust. The level of trust should be well identified and measured objectively or subjectively. Depending on what levels of trust the users need to know, including those related to sensitivity of information and associated resources, there may be many Trust Level Agreements (TLA).

4.5. Trustworthy System Lifecycle

In order to achieve trustworthy systems, we need a systematic methodology to cover all relevant trust aspects of a design, development and operation life cycle. The trustworthy system lifecycle can be sub-divided into three stages: i) designing the definition and goal of trust, ii) developing trustworthy systems, and iii) maintaining trustworthy operations.

At the design phase, the definition, metrics and goals of trust for the target system should be determined and the system should be developed while trust measures are considered to meet the design goals in the development phase. Finally, the maintenance phase has to properly monitor the normal operation of the running of a trustworthy system and the dynamics of the execution environment to verify the trust provisions at runtime. Furthermore, certification and qualification are required to prove the system has been developed using a certification and testing process.

4.6. Dynamics of Trust

In the SCP infrastructure, the state of objects changes dynamically (e.g., sleeping and waking, connected/ disconnected, and node failure etc.), as does their context, including location and speed. Moreover, the number of entities also fluctuates. Basically, trust is situation-specific and changes over time. Due to the dynamics and complexity of trust, a single trust mechanism cannot perfectly solve all the issues; so it is necessary to combine different trust mechanisms.

4.7. Resource Constraints

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

5. ARCHITECTURAL FRAMEWORK FOR TRUST PROVISIONING

As mentioned in the introduction, ITU-T has recently started new work on future trusted ICT infrastructures to cope with emerging trends in ICT while also considering social and economic issues. As a result, ITU-T has established the Correspondence Group on Trust (CG-Trust). The CG-Trust is currently developing a technical report on trust provisioning of the ICT Infrastructure. Here we propose a generic ICT trust conceptual model and an architectural framework for trust provisioning which will be developed further in CG-Trust.

5.1. Generic ICT Trust Conceptual Model

From the concept of SCP infrastructure discussed in Section 2, the domain of ICT can be sub-divided into the physical, cyber and social spheres. The physical ICT sphere perceives the dynamic physical environment, collects and delivers data. The cyber ICT sphere analyses the data from the physical world and provides useful information or knowledge to users in the social world.

To clarify ICT capabilities for trust provisioning with social-cyber-physical relationships, a conceptual model is shown in Figure 4. The model comprises different horizontal layers (i.e., social, cyber and physical) and three different vertical layers (i.e., object, networking and DIKW). There are multiple service domains for supporting a multiplicity of applications. The SCP infrastructure is logically sliced so that individual service domains share the infrastructure.

In the proposed model, trust is associated with all vertical and horizontal layers. Thus similar to security, trust management technology is necessary as a separate common layer which covers all vertical and horizontal layers. Using this model, we intend to illustrate the complex relationships and roles required for trust provisioning between and across layers which are associated with an individual entity of SCP infrastructure and services.

5.1.1. Physical Layer Trust

A physical layer contains a huge number of objects (i.e., H/W, device) including sensors, actuators and mobile terminals, which generate data by using sensing technologies to sense physical objects and their behaviours within their environments (e.g., temperature, pressure, etc.). Collecting secure and reliable data from physical objects is the first step to providing trustworthy ICT services and applications because the propagation and process of false data will cause service degradation and waste system resources.

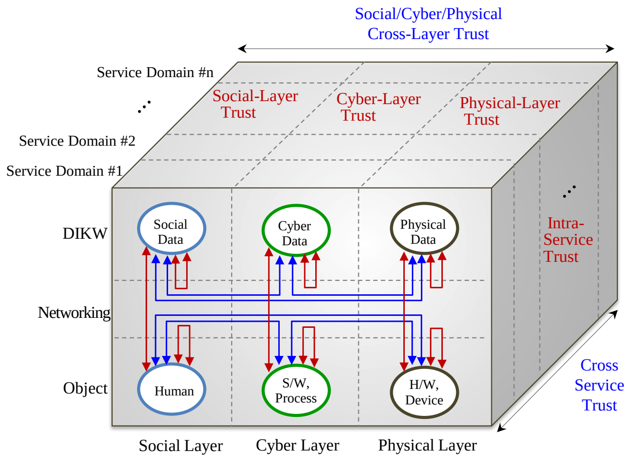

Figure 4: Generic ICT trust conceptual model

In order to detect trust problems in the physical layer such as injections of obstructive signals, malfunctions of systems, shutdowns or accidents, the operations of the physical objects and its data must be examined. Since many data are created from constrained devices, lightweight security and trust mechanisms are needed for data processing trust (e.g., efficiency, accuracy, reliability, etc.).

5.1.2. Cyber Layer Trust

A cyber layer includes virtual objects such as software agents, services and applications working over computing, storage and networking components. These virtual objects are seamlessly interconnected and cooperate for data coding, transmission, fusion, mining and analysing to provide information and knowledge to humans independent of location in fixed/mobile environments.

In order for virtual objects to safely cooperate, they have to distinguish malicious and non-malicious objects. One way to resolve this challenge is to evaluate the trust with their specific goal to decide which virtual objects to cooperate with. On the other hand, when huge amounts of data are collected in the cyber layer, they should be processed and analysed accurately and transparently.

Data, information and knowledge should be also transmitted and communicated in a reliable way via networking systems. Existing advances in networking and communications can be applied in order to achieve data transmission and communication trust. In particular, the trustworthy networking and communication protocols can support heterogeneous and specific networking contexts.

5.1.3. Social Layer Trust

Social networks are popular for sharing information and knowledge. Trust is an important feature in social networks because they rely on the level of trust that users have in each other, as well as in the service provider. Social layer trust actually depends on the behaviour and interactions of humans in the social networks. If trust is not gained by humans, they may not wish to share their experience and knowledge with others because of the fear that their knowledge and privacy will be misused.

5.1.4. Cross Layer Trust

In the SCP infrastructure, there are interactions between the social, virtual and physical objects, as well as data transmission between them. Actually, the objects in the physical and cyber world interoperate closely with each other and form a system organization around its (human) users in the social world. Human interactions with cyber/physical objects should be performed in a trustworthy way.

Furthermore, because most smart devices are human-related or human-carried devices, the social relationships between humans can spread between their devices. To define and manage trust between physical, cyber and social layers, appropriate trust models for the interactions between social, information and communication networks are required while taking into account the severe resource constraints and the dynamics. Trust evaluation and trust management are especially challenging issues in the social/cyber/physical cross layer trust.

5.1.5. Cross Service Trust

Trust management is service and domain specific, and it may be desirable to combine features from different trust management systems for developing a cross-service trust management that is able to cover social/cyber/physical trust relationships between different service domains.

Trust dissemination means to distribute or broadcast trust information. To disseminate trust information from one service domain to another, a trust service brokering mechanism can be used for efficient, effective and suitable trust dissemination.

5.2. Trust Architectural Framework

Based on the generic ICT trust conceptual model, this subsection describes a trust architectural framework consisting of three parts as shown in Figure 5: i) Trust Agent (TA) to gather trust-related data from social, virtual or physical objects; ii) Trust Analysis and Management Platform (TAMP) to model and analyse trust-related data and the trust relationship; iii) Trust Service Broker (TSB) to apply and disseminate trust-based knowledge to various services.

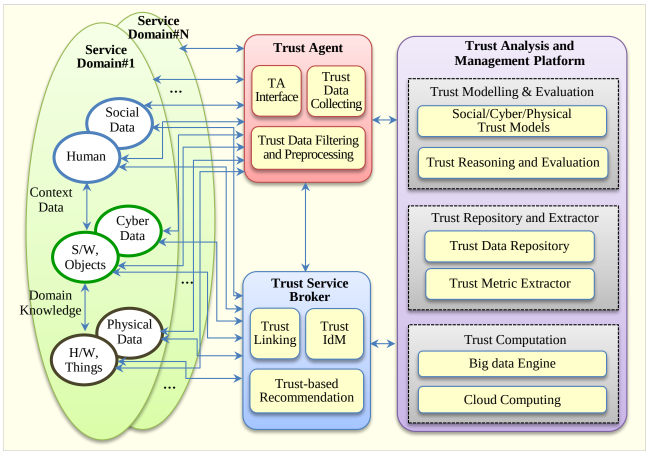

Figure 5: Trust architectural framework

5.2.1. Trust Agent (TA)

TA is used to collect trust-related data from the social, cyber and physical environments with the following modules.

- **TA Interface**: The TA provides lightweight interfaces to collect trust-related data from various types of objects in the social, cyber and physical layers. Furthermore, TA interfaces need to be easily connected to existing platforms and devices in order to extract the required data.
- **Trust Data Collection**: In order to evaluate a trust level of an object, the Trust Analysis and Management Platform (TAMP) identifies the required trust metrics for the object and informs TA's trust data collection module accordingly, as the trust data collection module is responsible for gathering the data required for the trust evaluation.
- **Trust Data Filtering and Preprocessing**: This module is used to refine trust data sets without including other data that can be repetitive, irrelevant or even sensitive for trust evaluation.

5.2.2. Trust Analysis and Management Platform (TAMP)

TAMP is used for modelling, reasoning and managing trust data collected from TAs to check whether the physical objects, virtual objects or humans satisfy certain trust criteria.

TAMP consists of several modules: trust modelling, trust reasoning and evaluation, trust data repository, trust metric extractor, trust computation, and so on.

- **Trust Modelling**: A trust model is used to specify, annotate and build trust relationships between objects for the purpose of reasoning trust data. Trust modelling is layer-specific and service domain-specific and there are social, cyber and physical trust models to define a trust model for each layer in the SCP infrastructure. According to its layer and a particular service domain, a suitable trust model is selected and applied for trust modelling. The trust-related data collected from trust agents can be transformed to structured and annotated formats by using semantic and ontology technologies through this trust modelling module.
- **Trust Reasoning and Evaluation**: Trust evaluation is used to analyse and assess trust levels based on the trust model. There are various types of reasoning methods which depend on the layer and service domain, and a proper reasoning method will be chosen for the specific object. For example, policy-based trust reasoning makes a binary decision according to which an object is trusted or not. Because trust status could change with time and circumstantial context, a trust reasoning method must handle such dynamics of trust.
- **Trust Data Repository**: The structured trust data including operations of objects and the history of interaction between objects can be maintained in the trust data repository. For trust evaluation, the necessary data will be loaded from this repository to the computation module.
- **Trust Metric Extractor**: A trust metric is used to judge or decide the trustworthiness of an object and it is separately defined in each service or each object. The trust metric extractor recognizes trust characteristics, accounts for factors influencing trust and determines proper trust metrics for the trust modelling and reasoning by analysing the metadata or semantic ontologies.
- **Trust Computation**: This module is used for data processing for trust evaluation. Trust computation happens when the state of an object has changed or an interaction occurs between objects. To process the large amount of data related to trust evaluation, it can adopt big data technologies, batch processing big data engines for calculation of the trust level of objects and real-time big data engines for examining the change of the trust state of objects based on direct observation.

5.2.3. Trust Service Broker (TSB)

TSB is used to provide trust knowledge of physical objects, virtual objects and humans for various types of services and applications in the ICT world. Furthermore, it can merge and disseminate trust knowledge across service domains or social/cyber/physical layers.

- **Trust Linking**: Trust linking is a module capable of creating a link between data/information/knowledge entities generated from a physical/cyber/social object based on trust criteria.
- **Trust IdM**: The identity management (IdM) can be used to manage digital identification/authentication of physical objects, virtual objects and humans. Trust IdM is able to involve trust knowledge to assure the identity of trustworthy objects and support trust-based services and applications.
- **Trust-based Recommendation**: This module provides recommendations to other objects. More specifically, a number of individual objects can be interconnected to construct a complex system for providing various services, and many objects with identical capabilities will exist on the Internet. This module aims at providing a recommendation for selecting a suitable object that meets the trust level.

6. CONCLUSION AND FUTURE STANDARDIZATION

This paper has looked at the future of converged ICT services and information infrastructures for a hyperconnected society and has provided the concept of an SCP infrastructure from emerging social IoT paradigms. From the understanding of trust, we have identified key challenges for trustworthy ICT infrastructures and proposed an architectural framework for trust provisioning as a key activity of the ITU-T CG-Trust. In conclusion, the future of ICT infrastructures is evolving towards a trustworthy SCP infrastructure with trust-enabled, knowledge-centric networking and services.

Until now, a number of standards focusing on network security and cybersecurity technologies have been developed in various standardization bodies including the 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 the Online Trust Alliance [17] and the Trusted Computing Group [18]. 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, we first need to 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 specified in relation to the relevant standards. In addition, global collaborations with related standardization bodies are required to further stimulate trust standardization activities.

Acknowledgement

This research was supported by the ICT R&D program of MSIP/IITP [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system].

REFERENCES

[1] Gyu Myoung Lee, et al., “Internet of Things,” in a book “Evolution of Telecommunication services,” *LNCS*, volume 7768, Springer, ISBN 978-3-642-41568-5, pp.257~282, 2013.

[2] Overview of Internet of Things, ITU-T Y.2060, June 2012.

[3] Edith Ramirez, Privacy and the IoT: Navigating Policy issues, Opening remarks of CES, Jan. 2015, https://www.ftc.gov/public-statements/2015/01/privacy-iot-navigating-policy-issues-opening-remarks-ftc-chairwoman-edith (visited on 2015-11-17).

[4] Data-driven Innovation for Growth and Well-being – Interim synthesis report, *OECD*, Oct. 2014, http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf (visited on 2015-11-17).

[5] Ovidiu Vermesan, Peter Friess, “Building the hyperconnected society – IoT research and innovation value chains, ecosystems and markets,” River Publishers, 2015.

[6] “The Zettabyte Era: Trends and Analysis,” *Cisco white paper*, May 2015.

[7] KCN (Knowledge Centric Networking), https://www.ee.ucl.ac.uk/kcn-project/ (visited on 2015-11-17).

[8] L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization,” *Computer networks*, vol. 56, no. 16, pp. 3594-3608, Nov. 2012.

[9] Fei-Yue Wang, “The Emergence of Intelligent Enterprises: From CPS to CPSS,” *IEEE Intelligent Systems*, July 2010.

[10] Jay Lee, et al., “A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems,” Elsevier Journal, Jan. 2015.

[11] George Vanecek, “The Internet of Things, ambient intelligent and the moving towards intelligent systems,” *IEEE Smart Tech 2012*, Sep. 2012.

[12] Wanita Sherchan, Surya Nepal, Cecile Paris “A survey of trust in social networks”, *ACM Computing Survey*, vol.45, issue 4, no. 47, August 2013.

[13] Zheng Yan, et al., “A survey on trust management for Internet of Things,” *Journal of Network and Computer Applications*, Mar. 2014.

[14] Trust pyramid, http://www.johnhaydon.com/how-make-people-trust-your-nonprofit/ (visited on 2015-11-17).

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

[16] “Trustworthy Systems of Systems,” *ERCIM News*, no.102, Jul. 2015.

[17] The Online Trust Alliance, https://otalliance.org/ (visited on 2015-11-17).

[18] The Trusted Computing Group, http://www.trustedcomputinggroup.org/ (visited on 2015-11-17).