Um, TW, Lee, E, Lee, GM and Yoon, Y

Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments

http://researchonline.ljmu.ac.uk/id/eprint/11647/

Article

Citation (please note it is advisable to refer to the publisher's version if you intend to cite from this work)

Um, TW, Lee, E, Lee, GM and Yoon, Y Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments. Sensors. ISSN 1424-8220 (Accepted)

Article

Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments

Tai-Won Um [1], Eunhee Lee [2], Gyu Myoung Lee [3] and Yongik Yoon [4,*]

[1] Dept. of Information and Communication Engineering, Chosun University, Gwangju, 61452, Korea (Rep. of); twum@chosun.ac.kr
[2] School of IT Engineering, Sookmyung Women's University, Cheongpa-ro 47-gil 100, 140-742, Korea (Rep. of); eunhee@iitp.kr
[3] Dept. of Computer Science, Liverpool John Moores University, Liverpool, L3 3AF, UK; g.m.lee@ljmu.ac.uk
[4] School of IT Engineering, Sookmyung Women's University, Cheongpa-ro 47-gil 100, 140-742, Korea (Rep. of); yiyoon@sm.ac.kr
* Correspondence: yiyoon@sm.ac.kr; Tel.: +82-02-710-9771

Received: date; Accepted: date; Published: date

Abstract: As the vast amount of data in social Internet of Things (IoT) environments considering interactions between IoT and people is accumulated and processed through cloud and big data technologies, the services that utilize them are used in various application fields. The trust between the IoT devices and their data is recognized as the core of IoT ecosystem creation and growth. Connection with suspicious IoT devices may pose a risk to services and system operation. Therefore, it is very essential to analyze and manage trust information for devices, services, and people as well as to provide the trust information to the other devices or users that need them. This paper presents a trust information management framework which contains a generic IoT reference model with trust capabilities to achieve the goal of converged trust information management. Then, a Trust Information Management Platform (TIMP) consisting of trust agents, trust information brokers and trust information management systems is proposed, which aims to provide trustworthy and safe interactions among people, virtual objects, and physical things. Implementing and deploying TIMP enable to build a trustworthy ecosystem while activating social IoT businesses by reducing the transaction costs as well as by eliminating the uncertainties in the use of social IoT services and data transactions.

Keywords: Trust, trust information management platform, trust index, internet of things, cyber physical system

1. Introduction

At the beginning stage of Internet of Things (IoT) technologies, physical sensors and devices were considered as main targets to be managed and controlled by IoT service operators for the purpose of providing sensing services to users. However, as IoT is evolving as a common service infrastructure, various applications and services of IoT have been emerging into markets in broad areas, e.g., smart home/building, health care, security, transportation, and so on. Recently, IoT is stimulated by the advent of Cyber Physical Systems (CPS) [1], where physical things are connected to each other and connected to cyber objects to provide intelligent services [2]. In CPS, the physical domain and the cyber domain are substantially the same, in which both functional capabilities are connected and affect each other.

In more recent years, studies on interactions between IoT and people such as Cyber Physical Social Systems (CPSS) [3] and Social IoT (SIoT) [4],[5] are actively being carried out. The paradigm of CPSS and SIoT has been expanded to encompass not only the physical and the cyber domain but also the social domain. The physical IoT domain perceives the dynamic physical environment, collects and delivers data by using physical things, while the cyber IoT domain computes and analyzes the data through one or more cyber objects, and useful information or knowledge for context awareness and decision making can be used by users in the social IoT domain through interactions among individuals and communities as well as physical things.

However, the introduction of newly developed technologies is always subject to uncertainty, which is likely to cause problems in terms of stability and security [6]. In particular, there is no guarantee of a certain level of control and reliability. If there is no trust between humans, the exchange of data and information between them is also meaningless because there is no confidence in each other [7]. Human-to-machine interactions have also proven to be unpredictable and unreliable, regardless of the normal functioning of the human and machine systems [8].

The direct connection between IoT devices occurs in variable manners, increasing the complexity of IoT services and applications, and there is a high likelihood of potentially unknown risks due to this complex interaction. In addition, as the IoT application services spread to the real world and the interactions between IoT devices and users become frequent, increased suspicion about whether IoT devices and services operate without any problems for their original purposes and whether they are harmful to users is recognized as a major obstacle [9].

A matter of trust on collecting data is also a critical issue in the physical IoT domain. Because of the hacked or damaged devices, IoT service quality will be significantly degraded even though trust in the cyber IoT domain can be fully supported. Next, data processing trust should be guaranteed in the cyber IoT domain. Therefore, trust in IoT needs to be managed through the physical and the cyber IoT domains in a holistic manner.

The expanded paradigm of IoT including CPSS and SIoT makes it difficult for users to grasp whether or not the neighboring things and services are reliable and credible. That is, collecting data from trustworthy physical things is the first step to provide trustworthy information and communication technology (ICT) services and applications and proper virtual objects have to be chosen to get a trustworthy knowledge or meaningful information by analyzing and calculating the data. However, current IoT infrastructures cannot fundamentally block both economic and financial losses from various malicious attacks, thus increasing user mistrust. In other words, the present security technology is a perimeter-based security solution, and it can cope with a malicious attack on a contact point, so there is a limit to the fundamental solution.

In this background, there are technical demands for verifying and confirming the trust of the SIoT based on the interactions between IoT devices, services, and people in the physical, the cyber, and the social IoT domains. Trust of IoT devices and data is a prerequisite for the spread and activation of SIoT-based industries and services such as smart home, connected cars and telemedicine. By analyzing and managing trust information for devices, services, and people as well as by providing the trust information to the other devices or users that need them, IoT devices and services will be more trustworthy and reliably used. However, the existing papers on trust have mainly focused on the theoretical aspects of users' trust analysis algorithms[10]. Thus, this paper aims to present a practical system design and implementation based on the service model to analyse and provide trust information for service realization in align with the international standard – ITU-T Y.3052 (see Clause 2.1) [11].

In this paper, we design a trust information management framework which contains a generic IoT reference model with trust capabilities to achieve the goal of converged trust information management. Then, we propose a Trust Information Management Platform (TIMP) consisting of trust agents, trust information brokers and trust information management systems in SIoT environments. The design and implementation of TIMP enables trust-based reliable and stable services by verifying and providing trust information for data, devices, services and users in emerging SIoT environments where people, objects and services interact frequently.

As a typical example of TIMP-based services, this paper considers various sharing services (e.g., Airbnb and Uber) that temporarily connect offices, accommodations, automobiles, owned by a particular person, to other people. These services have recently emerged and showed a high utilization rate. Unlike that individuals use well-known hotels and car rental companies, because strangers have short-term lease of each other's house and automobile in the sharing economy world, a tenant must confront uncertainty and risk in using such a lease service. Therefore, it becomes a big obstacle in using and spreading such a service. From the point of view of owners of resources, since a lender lends its resource to a complete stranger, the lender has a concern about whether the complete stranger will use the resource cleanly and carefully according to the contracted terms. From the illustration of a use case, the paper demonstrates a key operation and procedure of essential components to analyze and use trust information in emerging IoT services and applications to cope with sharing economy.

The remainder of this paper is organized as follows. Background information on trust is provided in Section 2. A trust information management framework is described in Section 3. Section 4 proposes detailed components of TIMP and presents a trust data analytics procedure including the trust data processing and analytics to derive trust indexes of physical things, virtual objects, users and services. In Section 5, we show the implementation of the proposed solutions and demonstrates a use case for TIMP-based resource sharing services . Finally, we summarize our work in Section 6.

2. Background

2.1. Definition and attribute of trust

In a lexical sense, trust is a concept that implies the integrity, power, ability, and assurance of a person or thing. Generally, trust is used as a measure of confidence that it will behave as expected, even though it lacks the ability to observe or control the environment in which it operates [6]. The concept of trust itself is very complex with different meanings depending on who/what the subject, situation, etc. and is influenced by various measurable factors and unmeasurable factors. There are also a number of trust attributes, but they frequently vary over a specific time period within a particular context. Thus, it's very difficult to make them be generalized, regardless of personal preferences and situation.

According to the previous research, trust is described by objective factors such as competence and reputation, along with some subjective factors such as the status in social relations and physical attributes. Here, competence is a measure of the ability of a person to perform a given task based on his/her degree, qualifications and experience, and reputation is formed based on the opinions of people who have previously interacted with the subject [4].

The term trust is a terminology originated from humanities and social sciences. Trust is thus a broad concept used in many fields and subject areas, but until now there has been no generally agreed definition. In the ICT domain, confusion arises in the use of terminology because it is mixed with various interpretations and definitions such as information security, privacy and reliability.

To build converged ICT services and a reliable information infrastructure, ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Study Group 13 on future networks and cloud has been working on future trusted ICT infrastructures and recently published the Recommendation Y.3052 "Overview of trust provisioning in ICT infrastructures and services"[11] regarding the concept of trust, a trust relationship model and trust evaluation with trust indicators and trust index. According to the Y.3052, trust is defined as "the measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future". Trust indicators represent fundamental criteria for evaluating trust of entities in ICT environments. Trust indicators can be categorized into two major parts: objective trust indicators and subjective trust indicators. Trust index is a comprehensive accumulation of trust indicators, which can evaluate and quantify trust of entities.

2.2. Previous researches on trust in SIoT

At the beginning stage of IoT technologies, sensors and devices were considered as passive objects to be managed and controlled. As people interact more and more closely with the circumambient physical things, IoT industries and academia have been paying much attention to

SIoT which is defined as an IoT where things are capable of establishing social relationships with other objects, autonomously with respect to people [4]. In the SIoT, a physical thing is capable of discovering and selecting other things in imitation of social relationships with people [5].

From the cognitive and subjective aspect of human's mind, the trust of things is recognized as a key challenge for invigorating IoT services. [5] proposes the subjective model and the objective model for trust management of SIoT. The former is used to compute the trust of things on the basis of its own experience and the reputation on the thing. In the latter, the trust of things is determined by using distributed and stored information based on peer-to-peer structure [12]. Ontology-based semantic models have also used to analyze the trust of things. However, existing trust models have mainly focused on limited IoT capabilities for the physical domain and reasoning for the trust of IoT devices.

On the other hand, social networks and social media are growing rapidly and users can share their thoughts (e.g., Twitter), multimedia (e.g., YouTube), personal activities, information (e.g., Facebook) and documents or calendars (e.g., Google+) through a variety of services [13],[14]. The social network based on the technology of Web 2.0 has greatly enhanced the participation of users on the web by providing an environment where users can easily communicate with each other and easily share interesting contents such as photographs and video clips [15]. Such social networks typically represent various attributes of user profiles and user relationships, that is, between a person and a person, and between a person and content. Many people spend more time on social networking sites than ever before and prefer to communicate and interact with friends through social media [16]. A social network is a social structure made up of a set of people and a set of links between people. The social network perspective provides a set of methods for analyzing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures [17]. There are some advantages by applying the social networking technologies to the IoT [4]: 1) Trust can be defined and examined for leveraging the degree of interactions among things, 2) Discovery of objects and services can be executed scalably and effectively like in the human social networks, and 3) Social network modeling and analysis can be re-used to address IoT related issues.

In the SIoT, trust of things is recognized as a key challenge to grasp whether or not the neighboring things and services are reliable and credible. For example, in crowd sourcing applications such as swarm intelligence, each object will be used as the bearer of its specific service to the community [4]. To realize this scenario, objects need to make social relationships including the policy, activities, object profile, etc. According to [5], relationships between objects in SIoT can be classified as follows [18]:

- 'co-location' relationship to be established among objects used always in the same place;
- 'co-work relationship to be established whenever objects collaborate to provide a common IoT application;
- 'parental' relationship to be related to objects belonging to the same production batch (e.g., same manufacturer, same model);
- 'co-ownership' relationship to be established among heterogeneous objects which belong to the same user.

The main advantage by using these social relationships between objects is that objects can offer services to their owners by autonomously cooperating with other objects, irrespective of whether or not there are social connections between the owners of such objects.

Especially, this SIoT concept may play an important role in the deployment of services that depend on loosely coupled interactions among objects and whose value is in their capability of dynamically discovering key information and services from unknown communities of objects. To realize this service based on SIoT, each object should be equipped with social functionalities to discover other social objects and to search for information and services by collecting the object social network.

It is evident that the openness of social behavior introduces many weaknesses from the security point of view that have to be addressed appropriately before deploying relevant applications. However, the evaluation of an object's trust can take advantage of the social network itself and be performed with appropriate models for managing the trust of the other social objects which may behave maliciously.

Our previous work [19] presented a trust evaluation model called REK, comprised of the triad of trust indicators: Reputation (public evidence on a trustee), Experience (personal expertise about the situation and the context) and Knowledge (understandings on a trustee). The REK model covers multi-dimensional aspects of trust by incorporating heterogeneous information from personal experiences to global opinions [20]. By extending the REK model, [21] proposed a quantifiable trust assessment model based on machine learning and [22] proposed a novel trust model called experience–reputation (E-R) for evaluating trust relationships between any two mobile device users.

Based on our previous theoretical trust model, this paper presents a framework for designing all required components to comprehensively cover the overall operations and procedure for trust information collecting, processing and management including analytics. It also focuses on implementation and demonstration of a service platform with trust solutions (i.e., TIMP) required for various services and applications in SIoT environments.

3. Trust Information Management Framework

In this section, we present a trust information management framework which contains a reference model and related capabilities with three IoT domains in order to achieve the design goal of converged trust information management.

3.1. Converged trust information management

Trust information services can be used to verify trust in people, objects, and applications in various SIoT services. Many SIoT service providers need the trust information service for the purpose of maintaining quality and providing reliable and stable transactions for their services. In addition, individual users also require the trust information service for the purpose of prevention of leakage of personal data, prevention of fraudulent telephone calls, prevention of housing invasion, and security check of user devices including IoT [23].

In order to provide the trust information services, it is necessary to collect trust-related data first for users, devices, applications including social, cyber, and physical areas of public, corporate, individual sectors according to the demand of SIoT service providers and users. After that, it is required to measure and analyze the trust of users, devices and applications through modeling and reasoning for suitable trust analysis according to the demand of the SIoT services. In addition, a convenient trust service interface based on a Web Application Programming Interface (API) must be provided so that various services and users can easily access the trust information service.

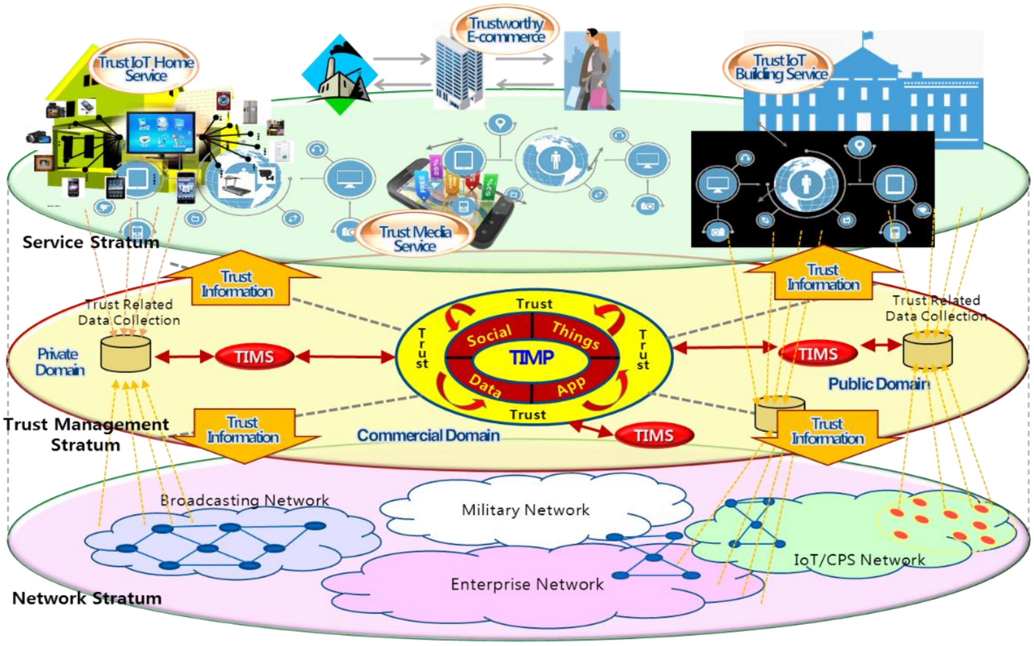


Figure 1. Converged trust information management.

Such a solution should not be limited to a specific service or application, but should be widely used for verifying reliability of users and devices in various IoT services and applications. To this end, the trust information management solution should minimize the dependency on services and applications, and the functions such as trust information analysis and management should be as common as possible so that they can be reused in various services.

Figure 1 shows a conceptual diagram of the converged trust information management, which consists of network stratum containing of physical devices connected to each other through a network, service stratum transferring, storing and processing data and information in various services, and trust management stratum that is responsible for analyzing and providing trust information services to SIoT service providers and users. There is a Trust Information Management Platform (TIMP) that commonly analyzes and manages trust information on the Cloud. The home and building services can analyze and manage trust information within their service domains using the Trust Information Management System (TIMS) which is dynamically allocated from the TIMP according to the Software-as-a-Service (SaaS) method.

A trust domain is a collection of trustworthy objects and data including users, networks, data storages and applications. To provide end-to-end trustworthy services, multiple trust domains need to be associated and the trust information maintained and managed for objects, users, and services in each trust domain should be shared with each other.

3.2. Generic IoT trust reference model

Trust information management has been highlighted as a key issue in the mediation and handling of commercial services, as well as the decision making in business processes. Trust information management plays an important role in the IoT to detect, monitor and collect data from various kinds of devices such as sensor nodes, sensor gateways, user equipment, home gateways and network gateways in the physical IoT domain as well as cyber objects and services/applications in the cyber IoT domain as shown in Figure 2. Moreover, in the social IoT domain, trust information serves as a basis for decision-making, even as people select IoT services or connect to nearby IoT devices.

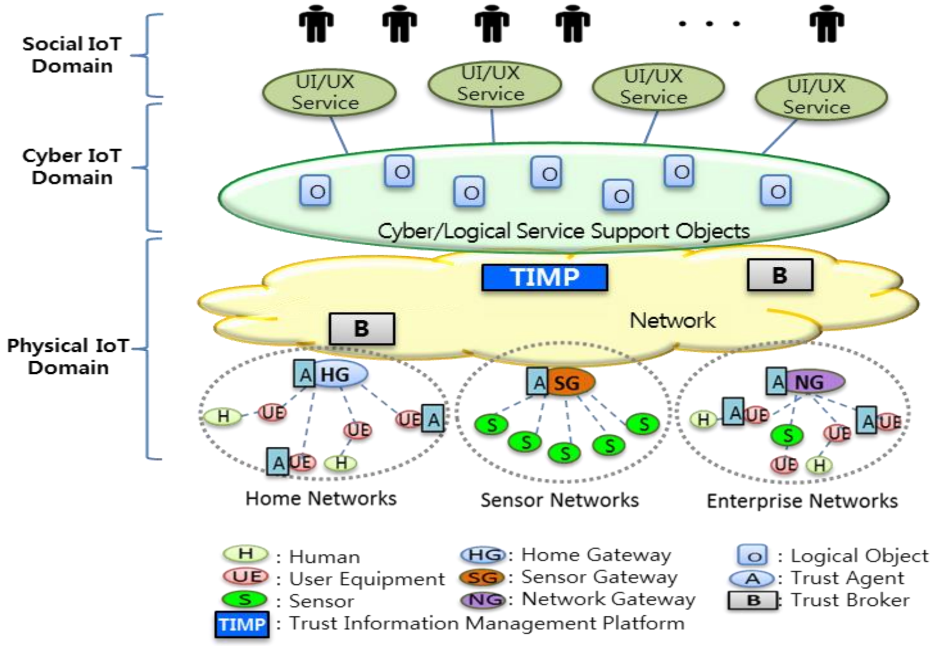


Figure 2. Trust in the physical, cyber and social IoT domains.

Through trust information management, the collected trust data can be further aggregated, classified and analyzed to determine an appropriate level of trust of physical things, cyber objects as well as people. Moreover, it helps people to overcome perceptions of uncertainty and risk, and engages in user acceptance and consumption on IoT services and applications. To provide trustworthy IoT services, all IoT entities including applications, platforms, networks and devices have to properly work together through the service goal.

In general, there are three IoT domains: (1) the physical IoT domain that perceives the dynamic physical environment, collects and delivers data; (2) the cyber IoT domain that analyzes and process the data from the physical IoT domain, and provides services to users; and (3) the social IoT domain that makes decisions based on IoT data analysis or uses physical IoT devices and cyber IoT services. The physical IoT domain and the cyber IoT domain are substantially different, but both capabilities are connected and affect each other in many aspects of data, control and management. In addition, the users generate social data, information and knowledge by themselves or through interactions among people, and the cyber data and knowledge are generated through the operation of the software and processes of the cyber IoT domain. Likewise, physical data is generated from a terminal at the physical IoT domain. Trust issues such as confidentiality, integrity and availability are important problems of the physical, cyber and social IoT domains that need to be considered [1].

As new services closely interact with each other in SIoT, it is necessary to analyze and manage the trust in each domain, and to analyze and manage the cross-domain trust between the other physical, cyber or social domains. In the case of convergence among heterogeneous services in SIoT environment, the trust information in each service must be able to be used in objects and data in other services beyond the service area. In this way, cross-service interactions require structural trust analysis and management for the service domain itself, and methods and procedures for supporting cooperation between trust-based service domains should be provided.

The growing use of IoT expects the generation of large volumes of data. Collecting trustworthy data from physical things or cyber objects is the first step to provide trustworthy IoT services and applications. There are a number of different types of algorithms and systems available to extract the information or knowledge from the aggregated data.

A trustworthy IoT service depends on reliable cooperation between the different IoT domains as well as each capability in the physical, the cyber and the social IoT domains. In order to develop a trust analysis algorithm, the specification of trust objects and attributes must precede the trust modeling. Here, trust modeling involves designing a trust domain by structuring and shaping trust data in a form that enables trust inference and interpretation of behavior and state data of users, devices and services. Furthermore, corresponding trust technologies at each domain should also be described to collaborate with the IoT capabilities.

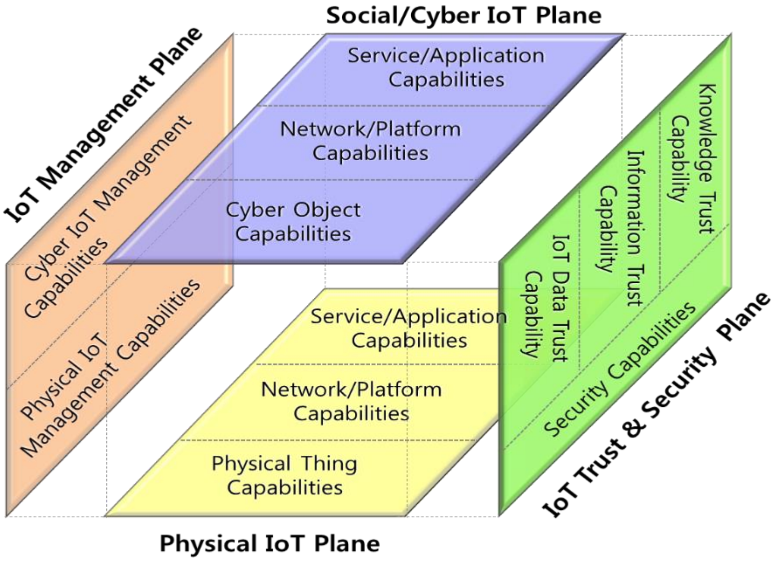


Figure 3. Generic IoT trust reference model and related capabilities.

Reflecting these considerations, a reference model needs to be defined to clarify the relationship between IoT capabilities and trust capabilities as shown in Figure 3, where IoT trust and security plane consists of IoT data trust capabilities, information trust capabilities, knowledge trust capabilities as well as security capabilities. The physical IoT plane consists of physical IoT device, network and platform capabilities, and the social/cyber IoT plane consists of software capabilities embedded in devices, networks and platforms. On the other hand, the IoT management plane is responsible for the operation and management of the capabilities on the physical IoT plane and the social/cyber IoT plane.

3.3. Constraints on data acquisition

In order to analyze and provide trust information for people, objects and applications, it is essential to collect data from public, private, corporate, and commercial areas. In the design of the trust information management framework, data related to trust should be designed in a way that reflects the practical constraints such as data silos and personal data protection laws. Service providers, individuals, corporations, and government agencies maintain and manage data from economic, social, cultural, and public activities, but these data are not generally allowed to share and sell because a data collection may involve privacy issues for service users or device owners in most cases.

For example, user data related to media services are very useful to provide customized services and target advertisements. However, a data collection in the media services imposes serious constraints and requires trust-enabled mechanisms such as trustworthy data crawling and reasoning with policies, and some of the data collected by smartphones may contain sensitive information such as the location data of the owners. Because of these constraints of data collection including user's privacy and regulations, a data analysis based service basically needs a data usage and protection agreement.

In accordance with these privacy considerations, enterprises and individuals who basically want to use the trust service should purchase a TIMP using their own trust data, or lease the trust service in the form of a software-as-a-service (SaaS) cloud to use as a business model. Otherwise, trust information can also be obtained through the Trust Information Broker (TIB) when trust information about any persons, objects, or application services held by other providers and public institutions is needed.

Trust information is required in many areas, including the commercial domain as well as the enterprise domain, the private domain, and the public domain. The targets of trust include not only people but also various objects of social, cyber, and physical fields such as physical objects to be traded, services on the Internet, and household appliances.

However, most of the data from users, devices, and services needed for trust analysis contain private data of individuals and are linked with sensitive service policies, so it is very difficult to share these data in each service domain with other services or users. In order to develop and apply a realistic TIMP to data silos, it is necessary to provide trust information in compliance with such data silos and privacy restrictions.

4. Trust Information Management Platform

4.1. TIMP Architecture

Considering the trust information management framework described in Section 3, this section describes the architecture of the proposed TIMP. Basically, it is designed to have a non-dependent structure for services and applications to be used in various fields. As shown in Figure 4, TIMP consists of seven subsystems: Trust Service Enabler (TSE), Trust Agent (TA), Trust Information and Management System (TIMS), Trust Information Broker (TIB), Trust System-Operations, Administration and Management (TS-OAM), Trust System-User Interface/User Experience (TS-UI/UX) and Bigdata Processing Cluster.

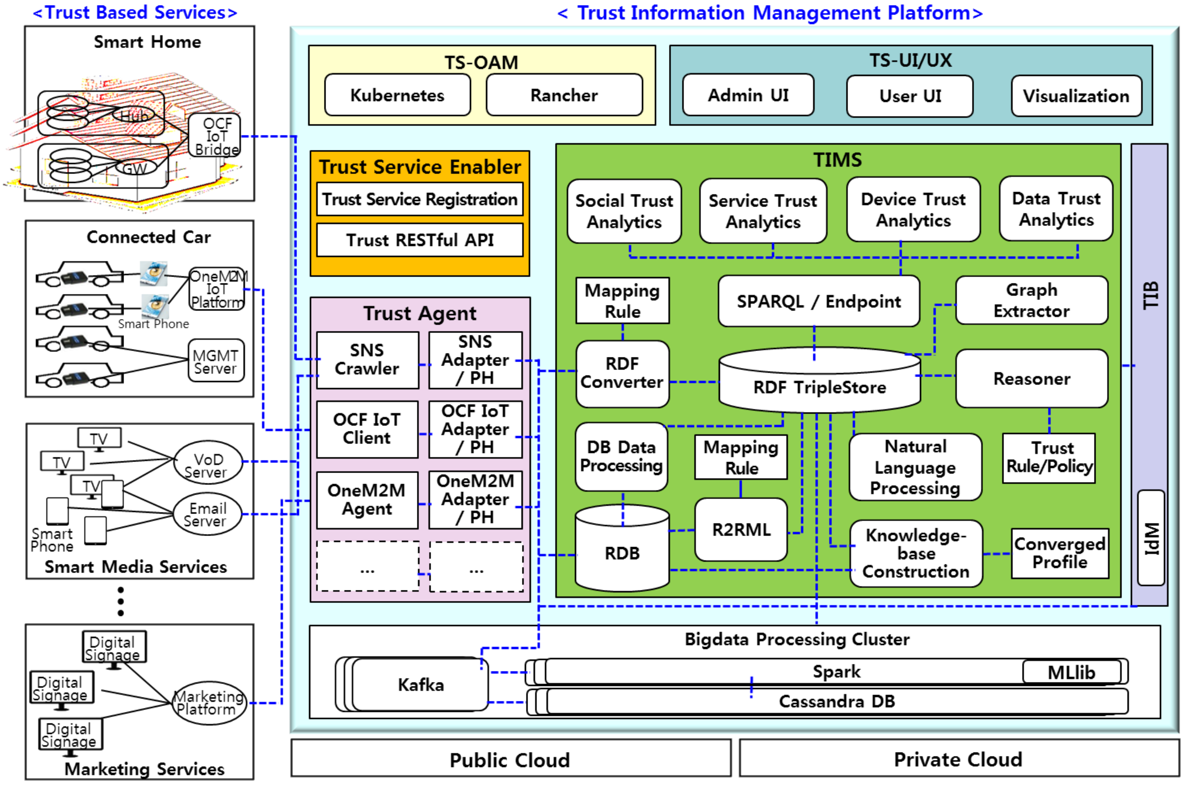


Figure 4. Architecture of trust information management platform

(1) Trust Service Enabler (TSE)

TSE performs the trust service registration from service providers and users requiring trust information, and it is responsible for dynamically generating and providing TIMS with the following modules:

- Trust RESTful API is an interface that enables various trust system modules such as TA, TIMS, TIB, databases to be registered and managed in TSE. Trust system module providers such as TA, TIMS, TIB, and databases can receive usage fees based on their usage when their modules registered with TSE are used for trust services.
- Trust Service Registration performs the function of dynamically configuring and allocating virtual TIMS to the service provider by receiving the registration of the trust information service from the service users and orchestrating the registered trust system modules using the Trust RESTful API.

(2) Trust Agent (TA)

TA provides a number of interfaces for data collection that can collect IoT and service data from various types of IoT services such as smart home, connected cars, and smart media with the following modules:

- SNS Crawler periodically acquires user data from various social network services such as Facebook, Twitter, Gmail and so on.
- SNS Adapter & Privacy Handler (PH) performs the function of anonymizing the user data received from the SNS crawler and transmitting it to the database of TIMS. Because TIMS stores, analyzes and manages trust information based on anonymized personal information, it can cope with the leakage of personal information due to hacking and the like.
- OCF/OneM2M IoT Clients are IoT data collection interfaces according to the OCF (Open Connectivity Foundation) standards and OneM2M standards, respectively.
- OCF/OneM2M IoT Adapter & PH modules anonymize and transfer data collected from the OCF/OneM2M IoT Client to TIMS similar to the one described in SNS Adapter & PH.

(3) Trust Information and Management System (TIMS)

TIMS analyzes the data of users, services and IoT devices delivered through TA by using social network analysis techniques, machine learning-based analysis techniques, natural language processing techniques, ontology-based analysis techniques, and it performs functions to infer and manage trust indexes of devices and so on with the following major modules:

- Social Network Analysis module serves to deduce the trust index among users by analyzing patterns of communication between users through social network services and e-mails. It uses ontology methods to share and deliver social network data in a systematic representation format. Several ontologies such as Friend-of-a-Friend (FOAF) [24] are used to represent social networks. FOAF ontologies which provide information extracted from user profiles and lists are widely used to provide portability between social networking sites and to model user-generated information and content in a machine-readable manner, since they can describe their relationships and online activities. In addition, Resource Description Framework (RDF)-based social data descriptions provide a much more effective way of representing online social networks than existing social network models. In addition, Semantic Web technology is also very useful for improving information retrieval performance and increasing flexibility in data access.
- Natural Language Processing module finds information such as stakeholder trust, IoT trust, service trust and data trust based on text data collected from Facebook, Twitter, and Gmail, and builds a knowledge base.
- Service Trust Analysis module analyzes service utilization data in smart home, connected car, and smart media services, which are generated by the service itself.

TIMS uses standard technologies related to Semantic Web for common representation of heterogeneous IoT data collected in the physical IoT domain and applies linked data technologies for common representation of trust information in the cyber and the social IoT domains. However, data in the social/cyber/physical domains can all be converted to RDF format, stored and looked up and used for trust analysis. IoT and social data collected from services such as smart home, connected cars, etc. are stored in the NoSQL-based Cassandra database and SQL-based MySQL database, and are converted and delivered to RDF-based TripleStore. By utilizing this Semantic Web technology, data on social networks can be integrated with data from other sources to develop more valuable data and information. Furthermore, Semantic Web technology is very effective in knowledge management processes that extract, maintain and develop knowledge.

(4) Trust Information Broker (TIB)

TIB arbitrates trust information for users, services, and IoT devices in other service domains to be received and transmitted through user consent and anonymization processing. Trust identity management (IdM) plays a role to identify whether trust objects of different service domains are the same user because each TIMS deduces and manages trust information based on anonymization of user information.

(5) Trust System-Operations, Administration and Management (TS-OAM)

TS-OAM module is responsible for the operation and management of trust system modules using Kubernetes [25] and Rancher [26], which are open source projects that bring cluster management capabilities to the world of virtual machines.

In order for TIMP to be effectively applied to various services, it is necessary for the user to easily identify user-friendly trust information for nearby IoT devices and services. For administrators, it is important to be able to easily monitor the use of TIMP services and respond quickly to problems. Trust System-User Interface/User Experience (TS-UI/UX) provides a user-friendly visualization interface that can effectively provide information about the trust system to administrators and users.

Storing and managing trust information in the IoT data and social network data collected and received in real time in order to extract and analyze the trust information is very disadvantageous from a cost point of view. TIMP adopts distributed big data processing clusters using real-time big data processing engines such as Apache Spark, thereby enabling cheap and fast trust analysis.

4.2. Trust Data Analytics Procedure

As described in Section 4.1., a trust index is quantitatively or qualitatively calculated and measured based on a trust evaluation model, and then used for the decision-making process not only by value-chains among multiple media stakeholders, but also by applications and service transactions.

The SIoT environment generally consists of IoT devices installed in homes and buildings, network functions for data transmission, IoT platform functions for analyzing data, services/applications using the analyzed information, and people using them. In this environment, TIMS should be used to analyze the trust information of users, services, and IoT devices themselves and the trust relationship between them. As mentioned in Section 4.1., TIMS has various trust analysis functions such as social network trust analysis function, natural language processing trust analysis function, machine learning based trust analysis function, and semantic ontology-based trust analysis function. Depending on whether the trustee is a person, a service, or an IoT device, a suitable trust analysis function is selected and used in TIMS.

For example, a trust analysis of a natural language processing method using text data on a social network service can be used for the trust analysis for the user, and a social network analysis function can be used for the trust relationship analysis between the users. Also, in order to confirm the trust index of the IoT device itself, a machine learning based trust analysis method will be used to determine whether the generated data is in a normal range. The trust relationship analysis of the semantic ontology can be used to identify the trust relationship based on the ownership and usage information between the user and the IoT device.

Thus, in order to analyze trust information between users and devices in a general IoT service such as smart home, various trust analysis techniques in TIMS are applied in combination. Here, the trust index between users, the trust index between devices, and the trust index between the device and the user are collected and combined after being individually analyzed. Figure 5 shows a procedural concept in which trust information such as users, devices, and services are collected and combined through subsequent stages to derive a trust index. In most cases, IoT services are a mixture of IoT devices, software and user-related functions. Therefore, in analyzing trust for these IoT services, it is necessary to derive individual trust indicators and indices for devices, software, and people, as well as cross-layer trust indexes resulting from their interactions.

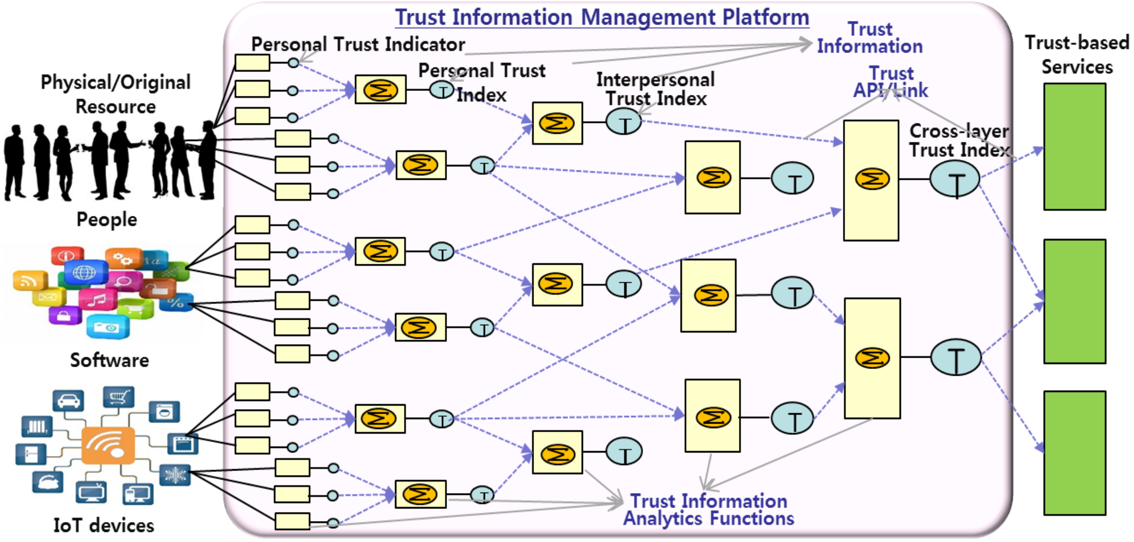


Figure 5. The procedure of trust data analytics

In TIMS, trust information of a user, a service, a device itself derived through individual trust analysis functions such as the natural language processing trust analysis function are structured in RDF format and linked data is stored and managed in the central TripleStore. According to the service requirement, the individual trust information stored and managed in the TripleStore is reconfigured based on the service value chain and transaction relationship, and the trust information is comprehensively calculated.

In this way, a direct and indirect trust relationship can be formed between people, services, and IoT devices. In order to intuitively inform the users of the trust relationship in a variable service environment, a graphic user interface (GUI)-based visualization is effective. Figure 6 shows the trust relationship between the users and the IoT devices owned by the user in the service named TrustBnB. By selecting each path, the trust index between users, services, and IoT devices can be confirmed.

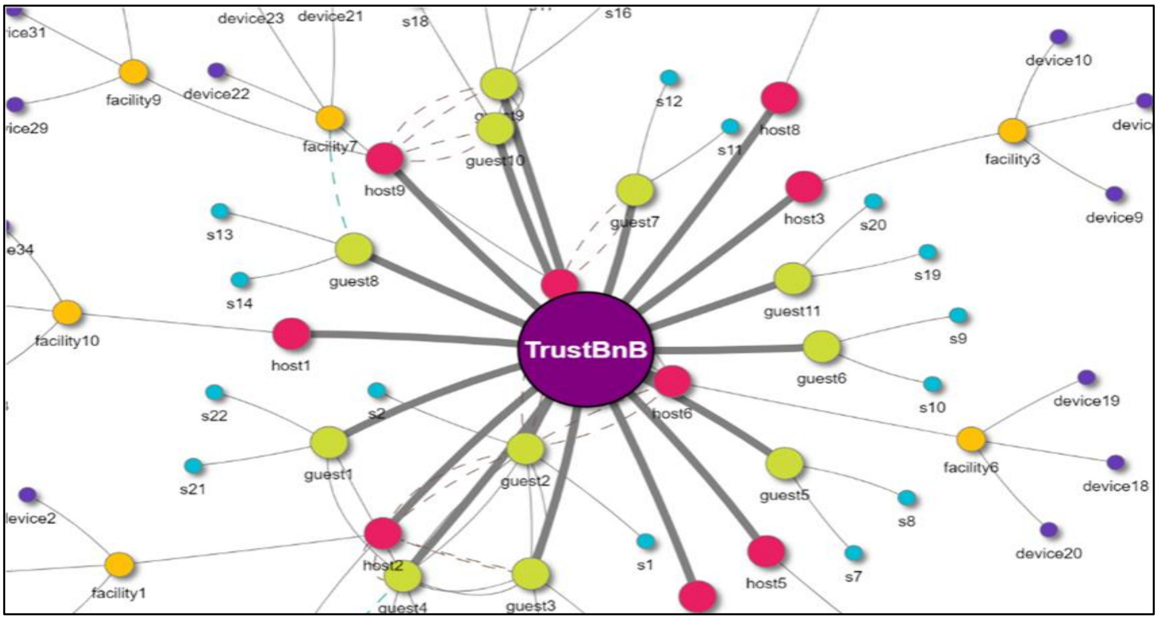


Figure 6. Trust visualization for trust relationship analysis

5. Implementation and Use-case

In this section, a specific illustration to implement TIMP will be described in detail along with a use case for TIMP-based services.

5.1. TIMP Implementation

Figure 7 shows an example of how TIMS and TIB are configured and applied to analyze and share trust information in services within each domain of the commercial domain, the enterprise domain, the private domain, and the public domain.

The services of each domain should be able to select and configure TIMS's functional elements appropriately to the types and attributes of the data they hold and the types and attributes of the trust information they want to receive. TIMS should be separately available from other service domains and be able to input and analyze users, devices and services related data held by each service.

In designing and implementing TIMS for satisfying the needs of each service while reflecting the latest trends in cloud and big data technology, it is a cost-effective way that TIMS uses a common service platform based on cloud computing rather than a proprietary system installed in a separate service domain. By adopting a SaaS approach to cloud computing, service providers will be able to access and use trust information services faster and at lower cost by selecting and configuring TAs, TIMS, and TIB capabilities that are appropriate for itself.

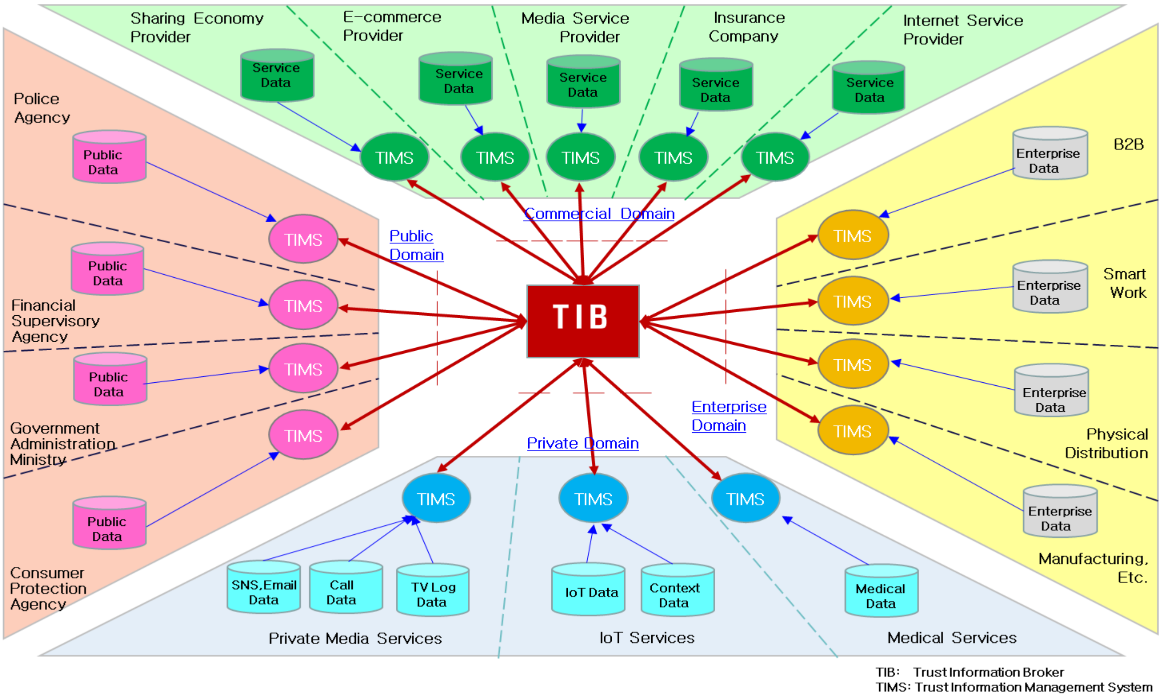
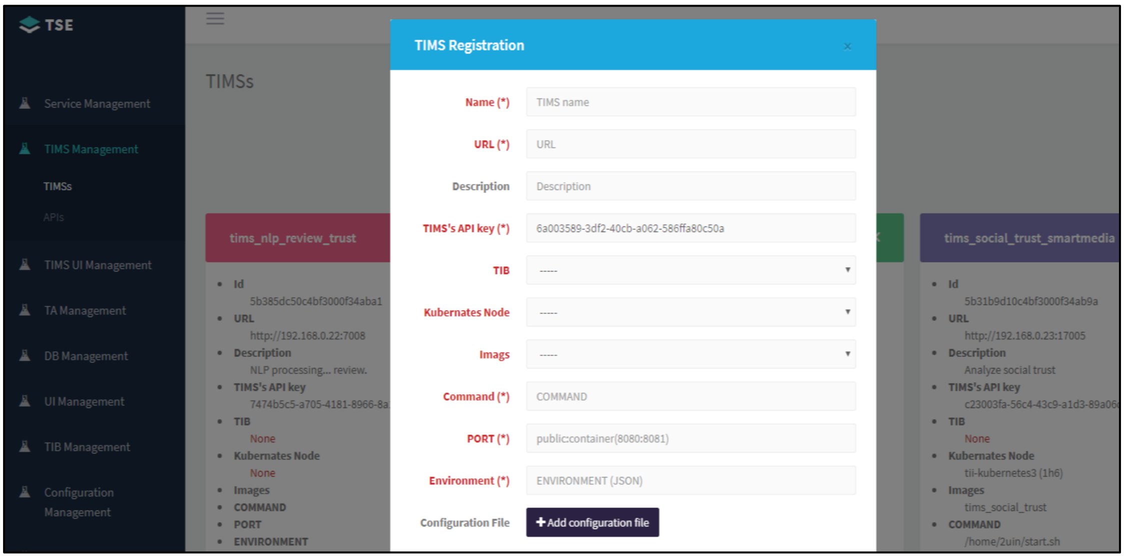


Figure 7. An Example of trust information broker implementation

Figure 8 shows the snapshot of real system implementation for TSE. On the left side, menus for registering TA, database (DB), TIB, and TIMS constituting TIMP, as well as menus for orchestrating and connecting them are shown. The right screen shows the examples of the configured trust service using the modules registered in TSE according to the trust service request, and detailed parameters information such as Id, URL, and TIMS's API key for the trust service.



TIMS Registration

Name (*)	TIMS name
URL (*)	URL
Description	Description
TIMS's API key (*)	6a003589-3df2-40cb-a062-586ffa80c50a
TIB	-----
Kubernates Node	-----
Imags	-----
Command (*)	COMMAND
PORT (*)	public:container(8080:8081)
Environment (*)	ENVIRONMENT (JSON)
Configuration File	+Add configuration file

tims_nlp_review_trust

- Id
  5b385dc50c4bf3000f34aba1
- URL
  http://192.168.0.22:7008
- Description
  NLP processing... review.
- TIMS's API key
  7474b5c5-a705-4181-8966-8a
- TIB
  None
- Kubernates Node
  None
- Images
- COMMAND
- PORT
- ENVIRONMENT

tims_social_trust_smartmedia

- Id
  5b31b9d10c4bf3000f34ab9a
- URL
  http://192.168.0.23:17005
- Description
  Analyze social trust
- TIMS's API key
  c23003fa-56c4-43c9-a1d3-89a06
- TIB
  None
- Kubernates Node
  tii-kubernetes3 (1h6)
- Images
  tims_social_trust
- COMMAND
  /home/2uin/start.sh

Figure 8. TSE implementation for registering trust systems

5.2. TIMP based Service Use-case

As a specific use case with TIMP, we illustrate a TIMS based services with accommodations/offices and automobiles among the "resources" to which the proposed TIMP is applied.

A resource sharing service intermediary or broker exists for each field (i.e., accommodations, automobiles, bicycle, facilities, etc.) of a trust-based resource sharing service. This may be implemented in the form of web sites or mobile apps such as Airbnb, Uber, and so on. The resource provider communicates with the web site or mobile application of the service intermediary in order to register a shared resource target (accommodations, automobiles, etc.) to provide renting (or sharing), charges, and other required items, then exchanging information related to the resource sharing service transaction.

Instead of a lender (or resource provider) or a tenant (or resource user), a service intermediary is responsible for management such as use permission limitation of resources such as accommodations/office, automobiles, etc. according to a user's trust index.

The TIMP can be used for trust-based resource sharing services during the lease period, using IoT technologies. The TIMP, unlike the existing sharing economy approach (e.g., Airbnb, Uber, and the like) that simply links the owner (or lender) of the resource with the user (or tenant), enables a trustworthy service transaction between a resource provider and a tenant, on the basis of the trust information analyzed through accumulated data collected through IoT sensors. The service intermediary may access the user trust information and the resource trust information through the TIMP.

The TIMP based resource sharing systems can perform resource sharing transaction including procedures of creating and managing a trust index of a user who uses resources, creating and managing a trust index of resources, and controlling the use of resources based on the user trust index and the resource trust index.

To achieve the trust-based service transaction, the method of utilizing trust information of a user and trust information of a resource itself is applied based on various technologies, such as IoT, smart home, etc., which is done between a resource provider (e.g., owner, manager, lender, and the like) and a resource user (e.g., tenant, and the like) through a resource sharing service intermediary that operates a sharing service web page or application system.

The procedure to provide TIMP-based resource sharing services is as follows:

- Based on the past offer history and the reputation on its use or the trust information at the time of resource registration, the resource provider undergoes a verification process for the service target (or shared resource) and the charge.

- Setting a minimum user trust index necessary for use permission of the user when the provider provides a resource; and comparing a user trust index set by the provider with a trust index of a user to use the resource to control the use of the resource in response to the comparison result.
- TIMP collects resource use status information from the resource and analyzes IoT data from the collected resource to determine whether contract violation, resource failure, or safety problem occurs; and a procedure of, when it is determined that contract violation, resource failure, or safety problem occurs while the user uses the resource, notifying this to the provider or the user.
- The resource user exchanges information with the service system of the service intermediary; inputs a target resource, a location, a number of users, and the like; searches for an available resource; and exchanges various service transaction information. At this time, the user inputs the required trust level of the resource to be used.
- After the user selects one of the listed resources and makes a reservation, when visiting the accommodations or taking over the automobiles at the scheduled time, the user uses the resource according to the contract details.
- TIMP generates and manages a trust index of a user using the resource by checking IoT data on resource management status (e.g., energy usage, whether a door is locked or not, smoking, etc.) during a resource use period. It can examine whether the service contract is actually observed through an IoT function (e.g., smoking, whether the number of contracted person is exceeded, safety observance, etc.).
- TIMP analyzes the trust information as follows:
    - . Setup of functional goals of analysis algorithms;
    - . Type of analysis: System Trust, Personal Trust, Interpersonal Trust (Social Interaction);
    - . Filtering and priority decision on trust information;
    - . Selection of trust analysis algorithm appropriate for each entity's type of trust information: Example 1) Rule-based, Machine-Learning-based algorithms in the case of users and resources themselves; Example 2) In the case of user relationship, Graph-based, Interaction-based algorithm; Example 3) Summing for heterogeneous trust analysis algorithm.
- TIMS calculates a user trust index by adding objective use status data collected from IoT sensors and subjective data from a resource provider and by reflecting past history between the user-resource provider entities.
- TIMP controls the use of the resource based on the user trust index and the resource trust index. It can limit the use of the resource of the user when the comparison result indicates that the trust index of the user to use the resource is lower than the trust index for the resource permission set by the provider.
- TIMP updates the trust information based on the feedback from the user and the resource provider, such as re-adjusting the trust index of the corresponding user and the trust index of the corresponding resource.

Figure 9 shows an accommodations service system depending on a trust-based resource sharing service. It should be understood that the system structure of Figure 8 organically combines the service intermediary and TIMP to provide trust-based accommodations renting services between an accommodations provider and a tenant.

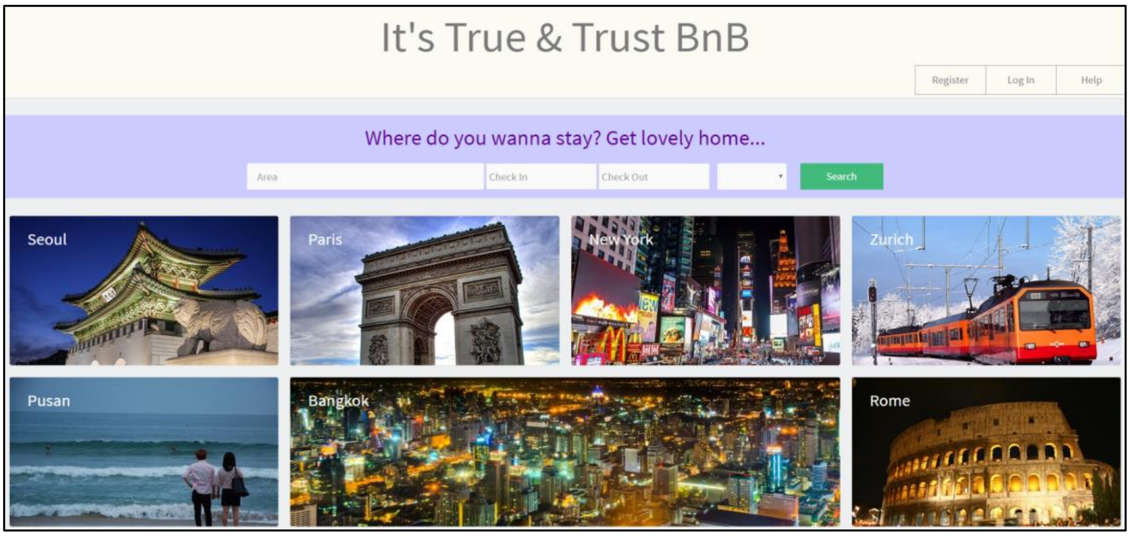
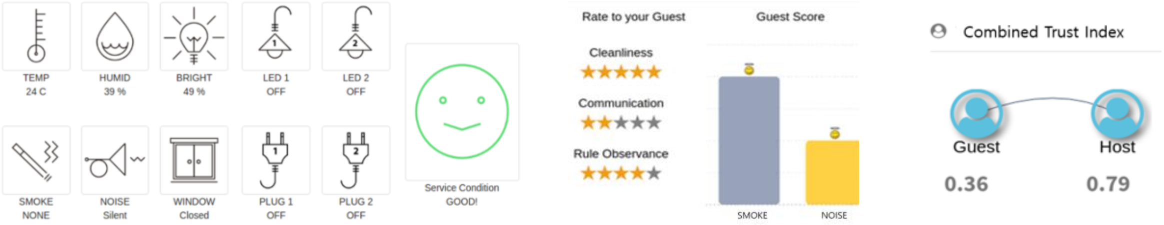


Figure 9. An example of TIMP based resource sharing services (an accommodation service)

We conducted trust analysis and evaluation of a Trust BnB service in a sharing guest house as shown in Figure 10. Figure 10 (a) below shows the status of IoT devices in a Trust BnB service. Through IoT devices, it is possible to objectively check the trustworthiness of the guest, such as whether the guest has complied with the accommodation contract. Figure 10 (b) represents the host's subjective evaluation of the guest, and Figure 10 (c) shows the guest's and host's trust index, which combine objective trust analysis and subjective evaluation.



(a) Objective trust analysis with IoT devices (b) Subjective trust evaluation (c) Trust index

Figure 10. Trust analysis and evaluation at Trust BnB

Although this section has been described with reference to the illustrations of accommodations/office resources, the technical scope of TIMP may be applied to other resources such as bicycles, various facilities, instruments, furniture, and so on.

Trust information in a resource sharing service can be utilized in terms of each entity as shown in Table 1:

Table 1. Usage of user or resource trust information

From the viewpoint	**Usage of user or resource trust information**
Resource provider	- Set the minimum user trust index of a user who is allowed to use provider's resource (e.g., select from 1 to 5 stars). - Resource use permission only for a user to be trusted. - Suggest differentiated charges and resource use options according to a user trust index (e.g., For five-star graded user, free internet and free parking with 50 dollars accommodations rental fee; For three-star graded user, 60 dollars accommodations rental fee and another extra fee for convenient facilities.).

Resource user	- Trust index of a resource is able to be checked through a trust-based resource sharing service. - Only the desirable resource of a trust index is selected by filtering a trust index in a resource use reservation search window. - Resource use is possible with better conditions in the future through observing the resource use rule (or contract) and enhancing the user trust.
Resource sharing service intermediary	- Provisions of differentiated resource use fees and options according to trust index when in the service system operation. - Trust-based resource use service system is configured with a trust index matching method between both sides (e.g., resource provider and user). - In order to increase a user trust index, a user is encouraged to comply with contract during resource use. - For a provider, a resource trust index is recognized as the factor of increased revenue to raise efforts to manage users and resources.

Rewards such as rate discounts and option changes are provided for future service provision and use, through trust information accumulated and updated for users and resources. This allows resource users to use resources cleanly and safely and provide motivation on user and resource management efforts to resource providers, so that it is possible to enable trust-based virtuous circle ecosystem. In addition, if necessary, by sharing the trust information of the user, accumulated through the trust-based resource sharing service, with other services and the third party through the TIB, trust services may be linked and spread.

Note that our implementation and demonstration results based on the international standard ITU-T Y.3052 [11] have been tested and certified from the Telecommunications Technology Association (TTA), Korea, as part of results from the previously conducted Trust Information Infrastructure (TII) project.

6. Conclusion

In this paper, we have targeted emerging SIoT environments that will activate the entirety of the production and distribution of goods and services throughout the ICT industries and the economy by combining the hyper-connectivity provided by IoT and the technologies assuring trust of the physical things and the cyber objects. After designing a trust information management framework, we have proposed TIMP which enables trust-based reliable and stable services by verifying and providing trust information for data, devices, services and users in SIoT environments where people, objects and services interact frequently. We have implemented core components, including trust data processing and analytics in TIMP and demonstrated a use case for TIMP-based services.

Implementing and deploying TIMP enable to build a trustworthy ecosystem while activating SIoT businesses by reducing the transaction costs as well as by eliminating the uncertainties in the use of IoT services and data transactions. In the future, it is necessary to timely implement and spread TIMP technologies to all ICT applications and services so that economic ecosystem formation and transaction structures can be dramatically improved.

Funding: This work was supported by research fund from Chosun University and Institute for Information communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) [2018-0-00691, Development of Autonomous Collaborative Swarm Intelligence Technologies for Disposable IoT Devices].

Acknowledgement: The authors are grateful to Hyunwoo Lee, Jun Kyun Choi for the collaboration and their contributions to develop and demonstrate our trust platform.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. Jay Lee, BehradBagheri, Hung-AnKao, A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, *Manufacturing Letters*, 2015; Volume 3, pp 18-23.
2. Zheng Yan, PengZhang, Athanasios V. Vasilakosd, A survey on trust management for Internet of Things, *Journal of Network and Computer Applications*, 2014; Volume 42, pp. 120-134.
3. F. Y. Wang, The Emergence of Intelligent Enterprises: From CPS to CPSS, *IEEE Intelligent Systems*, 2010; Volume 25, pp. 85-88.
4. Social Internet of Things, Available online: http://www.social-iot.org./
5. 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*, 2012; Volume 56, pp. 3594-3608.
6. G. Möllering, The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension, *Sociology*, 2001; Volume 35, pp. 403-420.
7. F. Huang, Building social trust: A human-capital approach, *Journal of Institutional and Theoretical Economics*, 2007; Volume 163, pp. 552-573.
8. S. P. Marsh, Formalising trust as a computational concept, Ph.D. dissertation, Dept. Computing Science and Mathematics, *University of Stirling*, Stirling, Scotland, UK., 1994.
9. Technical Report, Trust Provisioning for future ICT Infrastructures and Services, *ITU-T*, 2016.
10. Svetlana Kim, YongIk Yoon, Recommendation system for sharing economy based on multidimensional trust model, *Multimedia Tools and Applications*, 2016; Volume 75, pp. 15297–15310.
11. Recommendation Y.3052, Overview of trust provisioning in ICT infrastructures and services, *ITU-T*, 2017.
12. M. A. Azer, S. M. El-Kassas, A. W. F. Hassan, and M. S. El-Soudani, A survey on trust and reputation schemes in ad hoc networks, *in Third International Conference on Availability, Reliability and Security ARES*, 2008; pp. 881-886.
13. Samad Paydar, Mohsen Kahani, Fattane Zarrinkalam, PAD: A semantic social network, *ICCKE*, 2013; pp. 102~107.
14. Kee-Sung Lee, Myung-duk Hong, Jin-guk Jung, Geun-sik Jo, Building a Semantic Social Network Based on Interpersonal Relationships, *Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing*, 2012; pp. 90~95.
15. Peter A. Gloor, Jonas Krauss, Stefan Nann, Kai Fischbach, Detlef Schoder, Web Science 2.0: Identifying Trends through Semantic Social Network Analysis, *International Conference on Computational Science and Engineering*, 2009; Volume 4, pp.215-222.
16. Nichakorn Pankong, Somchai Prakancharoen, Marut Buranarach, A combined semantic social network analysis framework to integrate social media data, *Knowledge and Smart Technology*, 2012; pp.37~42.
17. Michele Ruta, Floriano Scioscia, Giuseppe Loseto, Eugenio Di Sciascio, A Semantic-Enabled Social Network of Devices for Building Automation, *IEEE Transactions on Industrial Informatics*, 2017; Volume 13, pp. 3379~3388.
18. Tai-Won Um, Gyu Myoung Lee, Hyun-Woo Lee, Trustworthiness management in sharing CDN infrastructure, *ICOIN*, 2018; pp73-75.
19. U. Jayasinghe, N. B. Truong, Gyu Myoung Lee, and Tai-Won Um, RpR: A Trust Computation Model for Social Internet of Things, *in Smart World Congress, Intl IEEE Conferences on Ubiquitous Intelligence & Computing*, 2016; pp. 930-937.
20. Nguyen Binh Truong, Hyunwoo Lee, Bob Askwith, Gyu Myoung Lee, Toward a Trust Evaluation Mechanism in the Social Internet of Things, *Sensors*, 2017; Volume. 17, pp. 1-24.

21. U. Jayasinghe, Gyu Myoung Lee, Tai-Won Um, Q. Shi, Machine Learning based Trust Computational Model for IoT Services, *IEEE Transactions on Sustainable Computing*, 2019;Volume 4, pp. 39-52.
22. Nguyen Binh Truong, Gyu Myoung Lee, Tai-Won Um, Michael Mackay, Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things, *IEEE Transactions on Information Forensics and Security*, 2019; Volume 14, pp 2705-2719.
23. Tai-Won Um, Gyu Myoung Lee and Jun Kyun Choi, Strengthening trust in the Future Social-Cyber-Physical infrastructure: an ITU-T Perspective, *IEEE Communications Magazine*, 2016; Volume 64, pp. 36-42.
24. Friend of a Friend (FOAF) Project, Available online: http://www.foaf-project.org/
25. Kubernetes, Available online: https://kubernetes.io/
26. Rancher Labs, Available online: https://rancher.com/