Security Requirements Analysis for the IoT

Se-Ra Oh
Security Engineering Laboratory
Dept. of Computer and Information Security
Sejong University
Seoul, South Korea
terious551@sju.ac.kr

*Young-Gab Kim
Security Engineering Laboratory
Dept. of Computer and Information Security
Sejong University
Seoul, South Korea
alwaysgabi@sejong.ac.kr

***Abstract*—Due to the rapid growth of network infrastructure and sensor, the age of the IoT (internet of things) that can be implemented into the smart car, smart home, smart building, and smart city is coming. IoT is a very useful ecosystem that provides various services (e.g., amazon echo); however, at the same time, risk can be huge too. Collecting information to help people could lead serious information leakage, and if IoT is combined with critical control system (e.g., train control system), security attack would cause loss of lives. Furthermore, research on IoT security requirements is insufficient now. Therefore, this paper focuses on IoT security, and its requirements. First, we propose basic security requirements of IoT by analyzing three basic characteristics (i.e., heterogeneity, resource constraint, dynamic environment). Then, we suggest six key elements of IoT (i.e., IoT network, cloud, user, attacker, service, platform) and analyze their security issues for overall security requirements. In addition, we evaluate several IoT security requirement researches.**

Keywords—Internet of Things; Security Requirements

I. INTRODUCTION

The era of IoT is opening with rapid growth of network infrastructure and sensor. There is no strict definition of IoT yet; however, usually IoT is described as collaborative ecosystem of context-aware, intelligent and automated device connected network for specific purpose.

Gartner, Cisco, and IDC (International Data Corporation) evaluate IoT as a promising technology of the future, and most of the corporation also think that IoT will become a key of their next-generation growth power. According to IDC, the IoT market scale is expected to grow from $655.8 billion in 2014 to $1.7 trillion in 2020 with a CAGR (compound annual growth rate) of 16.9% [1].

Accordingly, a lot of corporations in the world are developing IoT-related devices, services, and technologies to dominate the market in advance. However, they do not consider security as a functional requirement so that security concerns have come down in priority list. Therefore, corporations are reluctant to apply security sufficiently to the devices and services. For example, when TCP/IP was invented, the importance of security was not widely known, and most people did not know what attackers can do with security vulnerability. Because of these reasons, TCP/IP was not designed to secure enough. As a result of the insecure design, attackers are able to use a lot of vulnerability which causes security attack and huge monetary damage.

However, we currently know why security is critical, and what attackers can exactly do with security vulnerability. Thus, when IoT-related standards are being developed, we must discuss IoT security to avoid repeating the mistakes of the past. In order to overcome the problems, this paper proposes security requirements based on three characteristics of IoT and six key elements in IoT. In addition, evaluation is conducted with several researches.

This paper is organized as follows. Section 2 presents the related works on security requirements of IoT. Section 3 analyzes important features to understand IoT and common security requirements to apply to the whole IoT domain. In Section 4, we propose six key elements of IoT, and analyze each element to obtain security requirements respectively. In Section 5, we evaluate several security requirement researches compared to this research. Finally, in Section 6, we provide conclusions of this research.

II. RELATED WORK

There are some framework-related IoT security researches [21, 24, 28]. Alqassem [21] proposes requirements engineering framework ensuring privacy and security. He/She mention that information protection, and integration of heterogeneous technologies is required for security. Huang et al. [24] develop robust security framework, and investigate security requirements by analyzing each scenario (e.g., body IoT, home IoT, and hotel IoT). Furthermore, an interesting survey is conducted by 30 adults to determine the ranking of each security requirements (i.e., confidentiality, integrity, availability, access control). Rahman et al. [28] propose four-layered IoT security framework, and discusses security threats. In addition, the authors analyze security requirements regarding each component (i.e., IoT sensor node, base station, network, cloud) of their cloud scenario. The other papers [22, 23, 25, 26, 27] deal with security requirements, however, they do not handle overall security requirements the same as [21, 24, 28]. Lee et al. [21] present security threats, and security requirements according to IoT open platform, and interconnected environment. They highlight importance of security protocol meeting legacy network stack, and interoperability in heterogeneous network. Abomhara et al. [23] discuss IoT vision, security threats and challenges. They

* Corresponding Author

978-1-5090-5140-3/17/$31.00 ©2017 IEEE

select authentication, confidentiality, and data integrity as a primary security requirement. Alqassem et al. [25] categorize security requirement as access control, data integrity, contextual integrity, intrusion detection, and non-repudiation. Kim et al. [26] classify the type of IoT devices, and analyze security threats of each type. Key security requirements in Kim's research include the development of lightweight protocols and encryption algorithms, communications security, data protection, physical security, device identification and permission, and device monitoring and control. Li et al. [27] analyze security problems based on sensing, network, service, and application layered architecture.

However, there are no researches specialized in security requirements in the IoT environment. Therefore, for the rest of this paper, we analyze security-related issues to study overall security requirements.

III. ANALYSIS OF CHARACTERISTICS IN INTERNET OF THINGS

This section analyzes security requirements based on 3 typical IoT characteristics that have been researched in other researches. These security requirements are commonly applied in IoT security. Therefore, it is important to understand and take advantage of it to design security mechanisms in IoT environment.

A. Heterogeneity

In IoT, heterogeneity means diversity of hardware performances (e.g. CPU computation, memory footprint), protocols, platforms, policies, etc. The biggest problem of heterogeneity is absence of common security service [13]. heterogeneity weakens interoperability and causes extra fees about performance and money to interpret each other [10]. Besides, making security-related policies and updates are more complex. In order to solve these problems, we can use some technologies (e.g., meta data registry (MDR), middleware); however, it is not a fundamental solution. For providing common security service, unified IoT security standard has to be established. Then, developer who are related to IoT development should follow standards strictly. Recently, standards organizations (e.g., ITU-T, ETSI, ISO/IEC JTC 1) develop some standards for the security in the IoT.

B. Resource Constraint

Most IoT devices are lacking performance and battery capacity. Therefore, legacy security services, such as TLS (transport layer security), AES (advanced encryption standard), cannot be applied to IoT devices directly [8]. Therefore, these services or algorithms should be designed to be lightweight and straightforward to increase efficiency of CPU, memory and battery. In addition, scalability has to be considered.

Apart from lack of performance of device and network bandwidth also low, so that multicast is more effective than unicast [2]. Note that, CoAP (constrained application protocol) supports multicast in RFC 7252 officially, but MQTT (message queue telemetry transport) does not.

C. Dynamic Environment

Due to mobility and bad connections, IoT has a dynamic network topology. In very demanding cases (e.g., smart city), numerous devices may send a large number of requests. Hence, not only flexibility [7], but also scalability [6] is required in IoT communication protocols. Cisco forecasts that 50 billion devices will be created by 2020 [3], and after that, more and more devices will be made. Consequently, flexibility and scalability will be key security requirements of IoT.

IV. SECURITY ISSUES AND REQUIREMENTS FOR IOT ENVIRONMENTS

Fig. 1 shows six key elements of IoT (i.e., IoT network, cloud, user, attacker, service, and platform). We consider reviewing security requirements from the elements to be the most effective way. A more detailed description is in the following subsections.

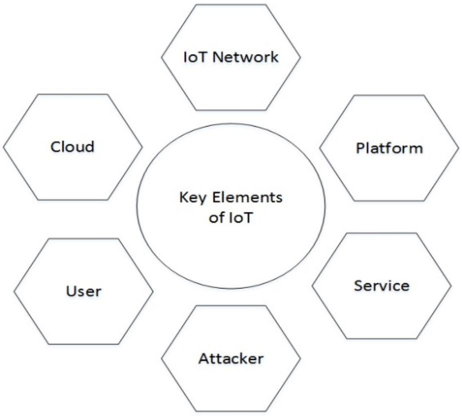

Fig. 1. Six Key Elements of IoT

A. IoT Network

IoT network is a specialized form of conventional network. It has three features as described in Section 3. In IoT network, there are many Things (e.g., gateways, sensors), and they may communicate using lightweight communication protocols, such as MQTT and CoAP based on IEEE 802.15.4.

The most important fact is that IoT network is basically not different from conventional networks. Therefore, most existing problems (e.g., fragmentation, security attacks) could happen in IoT network. In this subsection, we focus on the following issues: privacy, security in multicasting and bootstrapping.

Privacy. IoT is becoming more and more closer to human life like ubiquitous. It can be used anywhere, anytime with anything. People will be monitored by CCTV in everywhere, and sensors will send any sensed information to the network. Additionally, types of information will be diversified and amount of information will be gradually increased because of big data. In this situation, ensuring privacy is critical. Thus, from now on, we need to research security for privacy under understanding of characteristics and security requirements of IoT. Particularly, encryption and authentication is necessary to be made use of bitwise operation [17] rather than mathematical algorithm like ECC (elliptic curve cryptography) in order to make lightweight security service. Finally, privacy does not always have to be protected. If user is in emergency situation (e.g., car accident), privacy information is required to provide to doctor or close people [29].

Security in multicasting. IoT environment which is resource-constrained can be used multicasting more effective than conventional network. When using multicasting, multicast group should be created with authenticated users, and secret key that is shared with group members is required to keep securely [2].

Security in bootstrapping. Bootstrapping is a process that sends data (e.g., configuration information, key material) to participate secure IoT network. After that, authentication and authorization are performed. D. Garcia-Carrillo et al. [6] proposes a flexible, scalable and lightweight bootstrapping for demanding environment like smart city using AAA (authentication, authorization, accounting), EAP (extensible authentication protocol) and CoAP. Likewise, bootstrapping is required to designed in a flexible, scalable and lightweight manner. These are essential characteristics in the IoT environment.

Finally, it cannot be guaranteed to prevent security attack with only network security. So, devices should provide built-in security. Embedded security can support dynamic prevention, detection, diagnosis and isolation [7].

B. Cloud

Usually, IoT devices use cloud because they cannot save the data in their low memory capacity. In some cases, sensitive data (e.g., home CCTV video, personal location, health information) can be used for rescue people. However, if cloud out of order for some reasons, IoT devices cannot save the data. Then critical data that will be used for rescue can be missing. As a result, rescue service that require the data may be stopped. Therefore, in this case, availability is highly necessary, so that device should have back-up cloud to be replaced with original cloud.

There are a lot of data sent from many devices in cloud. To protect the data from unauthorized user, cloud should use proper access control (i.e., authentication, authorization), encryption, data anonymity, etc. In addition, the data may not be fully needed to be encrypted based on the importance of data. In this case, security-level based encryption is required for efficiency. It is the similar concept with contextual integrity in [25].

C. User

User is the most vulnerable element in IoT security. Even if information system is implemented securely, if a user, especially system engineer, is careless to manage, any security system will be useless. For example, in ID-password authentication model, if a user makes the password with a simple and guessable passphrase, attackers could crack the password easily using brute force attack or dictionary attack which is well known security attack. That is, the user has to follow strictly the security rules, and the user needs to be educated about social engineering.

D. Attacker

Security service can be compromised by attacker Although a user follows security rule. Due to IoT devices are connected to network, it can be victim anytime. most of IoT devices cannot apply strong security service because of its constrained resources. Besides, current IoT security services have not been fully validated. For these reasons, IoT is easy target to attack so that security attack will be increased and diversified. Thus, in this subsection, we analyze security requirements against security threats.

In IoT environment, security threats can be categorized into non-physical threats and physical threats. Non-physical threat can be described as threats which uses network, and physical threats also can be described as all threat except for non-physical threat. In contrast to conventional PC environment, IoT devices may not be placed on secure environment. Consequently, IoT devices could be easily destructed by nature and people who has malicious intention. If an attacker is able to access the device in insecure environment, the attacker can do side channel attack, or can analyze vulnerability of firmware or platform. Therefore, security mechanisms for the IoT device in harsh environment is required to be considered when device manufacturer implement the device.

Most of non-physical threats (e.g., buffer overflow, sniffing, man in the middle attack, spoofing) are attacks on confidentiality, integrity and availability. Due to heterogeneity, IoT security is too complex to prevent the types of attacks. Additionally, IoT device has constrained resource to adopt the strong security services (e.g., intrusion detection system, anti-virus [5]) for protecting system from security threats. For these reasons, IoT device is more vulnerable to security attacks (e.g., DDoS [15]) than conventional PC environment. Even simple DoS (Denial of Service) can stop operation of device if its performance is not enough. Gateway that performance is relatively sufficient compared to IoT device could adopt IDS or anti-virus on behalf of the device.

Attackers can attack on IoT system using the vulnerability of firmware, platform or communication protocol, etc. The security vulnerability is made by system designers and developers' inexperience or mistake. Each vulnerability has different impacts on system. Some of vulnerability is sufficient to break security system, or can steal root permission. Therefore, vulnerability must be minimized by using secure coding, static analysis, dynamic analysis, reverse engineering, etc.

In critical control field, control permission never be lost and changed by attacker, and operation should be supported continuously. Therefore, control system must need a fault tolerance [20] and back-up devices [13]. Back-up device can be replaced when main device is compromised or stopped.

E. Service

In this subsection, we analyze security issues (i.e., trust, access control, middleware, storage) as illustrated in Fig. 2. Before we describe the security requirements based on security issues, each element of the scenario in Fig. 2 will be explained. To take advantage of a service, the user needs to trust the server, and the server needs to provide privacy to the user. If the user decides the server is trustworthy, the user will use service provided by the server or group of devices with smart phone, smart watch, or some kind of network devices. After that, the devices have to progress bootstrapping and access control (i.e., authentication and authorization). Thereby, devices obtain trust from server. Especially, automated, intelligent and context-aware devices in real IoT environment might be operated by itself without human intervention. Finally, the attacker can compromise the server for malicious intentions (e.g., collecting personal information).

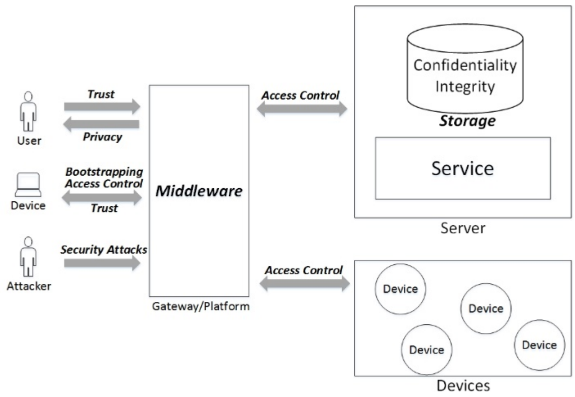

Fig. 2. Security Requirements among User, Device, Attacker, and Service

Trust is complex concept. In spite of its importance, there is no clear definition. Due to unclear definition of trust, it is hard to estimate and evaluate [7]. Therefore, we have to define trust clearly, and need to make the method for estimate and evaluate of trust in order to the IoT security. In fact, 'Trust' was used with two different meaning in Fig. 2. In case of the user, trust means belief. However, in other case of the device, trust means not only belief but also interoperability that any kinds of devices can be communicated with each device.

In IoT environment, middleware can be used for platform that support interoperability, and it can provide security for devices and data. Therefore, when we design middleware architecture, security, privacy, and use of multi communication medium should be considered [7].

As mentioned previously, access control is security service including authentication and authorization for ensuring security and privacy. Due to dynamic environment and resource constraint of IoT, access control should be flexible and scalable [16]. Furthermore, access control needs to handle various types of access control policies. In addition, identification method to authorize needs to be strict, and the process for managing authority should be easy and simple [7, 9]. As a result of the access control, certificate will be issued. There is a problem in the number of certificates. It could be created too many owing to scale of IoT (e.g., smart city). So, in this case, delegation of authentication and authorization will be necessary [8].

The last is storage issue. Confidentiality and integrity of data in storage should be supported as the cloud environment [18].

F. *Platform*

AllSeen, oneM2M, OIC (open interconnect consortium) and other standards organizations have been established IoT platform standards. Open IoT platform (e.g., Mobius, OneM2M, AllJoyn, COMUS) provides multiple functions (e.g., distributed cooperation, execution control, interoperability between heterogeneous devices to share data) [19]. They are focusing on the functionality of platform mainly, however, security is considered only in common services (e.g., encryption, access control through authentication and authorization, signature). At this time, as mentioned earlier, because it is necessary to consider the performance of various IoT devices, all of security services should be lightweight. In addition, according to the security level of device, security service should be supported optionally in order to overcome heterogeneity of device performance. Furthermore, for authentication and authorization, method for understanding many different security policies used in diverse devices and domain is required.

Finally, as mentioned in Subsection 4.4, attackers can seize device, and analyze vulnerability of the platform. Therefore, platform needs to minimize its vulnerability, and should be verified itself using the trusted platform module (TPM).

V. EVALUATION

We evaluate IoT security requirements researches compared to our research. As depicted in Table 1, most of the researches deal with only the security requirements about privacy, access control (i.e., authentication and authorization), and security threats. That is, the existing researches do not cover overall security requirement for IoT environment. In this paper, we first analyzed the basic security requirements based on the three characteristics (i.e., heterogeneity, resource constraint, dynamic environment). Second, privacy, multicasting and bootstrapping in IoT network, availability, data protection, etc. were analyzed based on six elements (i.e., IoT network, cloud, user, attacker, service, platform) in IoT environment.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we analyzed three key characteristics of IoT, such as heterogeneity, resource constraint, and dynamic environment to find out basic IoT security requirements. In addition, we analyzed overall IoT security requirements (e.g., privacy, trust, control system security) based on security issues of six key elements in IoT environment. And security requirements evaluation is performed with several researches. We hope this paper can be a guide to design IoT system securely, and improve general understanding of IoT security issues and requirements. In the future, we need to analyze international standards related to IoT security for interoperability among a lot of diverse security platforms, devices, policies, etc.

ACKNOWLEDGMENT

TABLE I. COMPARISON RESULTS BETWEEN EXISTING AND PROPOSED

Research	Characteristics	IoT Network	Cloud	User	Attacker	Service	Platform
	Heterogeneity, Resource Constraint, Dynamic Environment	***Privacy, Multicasting, Bootstrapping***	***Availability, Data Protection***	***Social Engineering***	***Threat, Control System Security***	***Trust, Access Control (Authentication, Authorization), Middleware***	***Security Service based on Security Level, Self-verification***
Alqassem [21]	Heterogeneity	Privacy	-	-	-	-	-
Lee et al. [22]	Heterogeneity	Privacy	-	-	Threat, Control System Security	Access Control	-
Aomhara et al. [23]	Resource Constraint	Privacy	-	-	Threat	Trust, Access Control	-
Huang et al. [24]	-	Privacy	-	-	-	Access Control	-
Alqassem et al. [25]	-	Privacy	-	-	Threat	Access Control	-
Kim et al. [26]	Resource Constraint	Privacy	-	-	Threat, Control System Security	-	-
Li et al. [27]	Heterogeneity	Privacy	-	-	Threat	Trust, Access Control	-
Rahman et al. [28]	-	Privacy	Data Protection	-	Threat	Access Control	-
Proposed	Heterogeneity, Resource Constraint, Dynamic Environment	Privacy, Multicasting, Bootstrapping	Availability, Data Protection	Social Engineering	Threat, Control System Security	Trust, Access Control, Middleware	Security Service based on Security Level, Self-verification

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R7115-16-0002, Wise-IoT)

REFERENCES

[1] IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25658015

[2] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, B. Stiller, “Group key establishment for enabling secure multicast communication in wireless sensor network deployed for IoT Applications”, IEEE Access, vol. 3, pp. 1503-1511, August 2015

[3] CISCO, http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html

[4] IETF, https://tools.ietf.org/wg/6lowpan/

[5] Z.K. Zhang, M. C. Y. Cho, S. Shieh, IEEE Fellow, “Emerging security threats and countermeasures in IoT”, ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS) Singapore, pp. 1-6, April 2015

[6] D. Garcia-Carrillo, R. Marin-Lopez, “Lightweight CoAP-based bootstrapping service for the internet of things”, Sensors, vol. 16, pp. 358-381, March 2016

[7] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “Security, privacy and trust in internet of things: The road ahead”, Computer Networks, vol. 76, pp. 146-164, January 2015

[8] Z.K. Zhang, M. C. Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh, “IoT security: ongoing challenges and research opportunities”, Service-Oriented Computing and Applications (SOCA), Matsue, Japan, pp. 230-234, November 2014

[9] D. Rotondi, S. Piccione, “Managing access control for things: a capability based approach”, BodyNets, Oslo, Norway, pp. 263-268, September 2012

[10] S.-R. Oh, Y.-G. Kim, “Security analysis of MQTT and CoAP protocols in the IoT environment”, Korea Information Processing Society (KIPS) South Korea, pp. 297-299, April 2016

[11] OASIS, MQTT Version 3.1.1, http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html, 2014

[12] IETF, The Constrained Application Protocol (RFC 7252), https://tools.ietf.org/html/rfc7252, 2014

[13] Q. Gou, L. Yan, Y. Liu, Y. Li, “Construction and strategies in IoT security system”, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing (CPSCom) China, pp. 1129-1132, August 2013

[14] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, “Lithe: lightweight secure CoAP for the internet of things”, IEEE Sensors Journal, vol. 13, pp. 3711-3720, October 2013

[15] P. N. Mahalle, B. Anggorojati, N. R. Prasad, R. Prasad, “Identity establishment and capability based access control (IECAC) scheme for internet of things”, Wireless Personal Multimedia Communications (WPMC) Taiwan, pp. 87-191, September 2012

[16] B. Anggorojati, P. N. Mahalle, N. R. Prasad, R. Prasad, “Capability-based access control delegation model on the federated IoT network”, Wireless Personal Multimedia Communications (WPMC) Taiwan, pp. 604-608, September 2012

[17] J.-Y. Lee, W.-C. Lin, Y.-H. Huang, “A lightweight authentication protocol for internet of things”, International Symposium on Next-Generation Electronics Taiwan, pp. 1-2, May 2014

[18] S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad, Proposed security model and threat taxonomy for the internet of things (IoT), 1th ed., vol. 89, Berlin: Springer-Verlag, 2010, pp.420-429

[19] S.G. Hong, H. Lee, J.C. Choi, M.N. Bae, K.B. Lee, “Internet of things software platforms technology trends”, Electronics and Telecommunications Trends, vol.30, pp. 39-48, October 2015

[20] R. Roman, J. Zhou, J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, Computer Networks, vol.57, pp. 2266-2279, July 2013

[21] I. Alqassem, “Privacy and security requirements framework for the internet of things (IoT)”, International Conference on Software Engineering (ICSE) Companion India, pp. 739-741, May-June 2014

[22] Y.J. Lee, D.H. Kim, “Threats analysis, requirements and considerations for secure internet of things”, International Journal of Smart Home, vol. 9, pp. 191-198, December 2015

[23] M. Abomhara, G. M. Køien, “Security and privacy in the internet of things: current status and open issues”, Privacy and Security in Mobile Systems (PRISMS) Denmark, pp. 1-8, May 2014

[24] X. Huang, P. Craig, H. Lin, Z. Yan, “SecIoT: a security framework for the internet of things”, Security and communication networks, DOI: 10.1002/sec.1259 May 2015

[25] I. Alqassem, D. Svetinovic, “A taxonomy of security and privacy requirements for the internet of things (IoT)”, Industrial Engineering and Engineering Management (IEEM) Malaysia, pp. 1244-1248, December 2014

[26] H.-J. Kim, H.-S. Chang, J.-J. Suh, T.-S. Shon, “A study on device security in IoT convergence”, Industrial Engineering, Management Science and Application (ICIMSA) South Korea, pp. 1-4, May 2016

[27] S. Li, T. Tryfonas, H. Li, “The internet of things: a security point of view”, Internet Research, vol. 26, pp. 337-359, April 2016

[28] A. F. A. Rahman, M. Daud, M. Z. Mohamad, “Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework”, ICC (International Conference on Internet of things and Cloud Computing), United Kingdom, Article No.: 79, March 2016

[29] C. Hu, J. Zhang, Q. Wen, “An identity-based personal location system with protected privacy in IoT”, IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT) China, pp. 192-195, October 2011