International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.201-208
http://dx.doi.org/10.14257/ijsia.2015.9.10.18

# Requirement of Security for IoT Application based on Gateway System

Jung Tae Kim

*Department of Electronic Engineering, Mokwon University, 302-318, Korea*
*jtkim3050@mokwon.ac.kr*

***Abstract***

*An integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of the wireless network in open wireless network and the unique security mechanism used in each one of these networks. The security consideration should satisfy a concise set of cryptographic and security mechanisms, single security policy framework, and configuration parameters policy-dependent. This may require consideration of system perspectives, taking into account the entire system and device lifecycle, ease-of-use and ease-of-deployment. Finally, we analyzed requirement of IoT security gateway system to improve vulnerability of sensor node.*

***Keywords:*** *RFID, Internet of things, Authentication, Security protocol*

## 1. Introduction

IoT (Internet of things) is the combination of a variety of information sensing devices such as radio frequency identification (RFlD) devices, infrared sensors, global positioning systems, and Internet. To form a huge network, all sensor devices are connected to the network to facilitate the identification and management, which ultimately provides a full of services to people which is based on the integration of applications in everywhere. More than 15 billion computer and Internet-enabled devices will be connected to the cloud and each other in what is commonly called the Internet of Things (IoT). Connectivity is imperative to realize the power of the IoT, which can be allowed by gaining insight from data provided by these connected devices. Many applications of Internet of Things (IoT) exist in every place. But many works focuses on an architecture having a central unit (cloud server) running web applications for dual-way communications with both remote sensors and actuators. The sensor networks will be remote, running on mobile Internet connections that may have irregular drops in the Internet connection [1]. IoT applications show that low cost devices may be connected and accessible over the Internet. The function of sensor devices can be implemented with sensor readings, sending control commands or receiving alarm messages. A wireless sensor network can be utilized for local applications so that it may operate without a gateway until now. But for IoT usage there is a need of gateways in present days. For example, energy companies need a way to remotely read their meters. This type of usage demands high level of security in every part of the system. Transmission of information security issues becomes more complicated and essential to a variety of communication channel. Traditional security of a single network environment cannot guarantee secure data transmission of IoTs. In general, we should consider privacy and data protection. Information security is complementary requirements for IoT services. The potential applications of IoT are limitless and will give an economic benefits, healthy condition, cooperative community and private lives. We also consider that information security is perceived as a basic requirement in the provision of IoT services for the industry [2]. However, the Internet was not built for highly secure

ISSN: 1738-9976 IJSIA

communications. Therefore mechanisms such as secure socket layer or TLS (Transport Layer Security) are added on the original TCP/IP protocol used in the Internet [3]. The IP protocols are taken into consideration in many concerns until now. But the nature of IoT devices and IoT architecture is faced with its own challenges in securing every IoT solution. Some new security mechanisms are developed with these kinds of constraints. The requirement of the solution has direct correlation with the cost and time to the market. Therefore every solution has its own business requirements which may or may not be stringent. Many works focuses on an architecture having a central unit such as cloud server running web applications for dual-way communications with both remote sensors and actuators. The sensor networks will be remote, running on mobile Internet connections that may have irregular drops in the Internet connection. A lot of researchers study and deal with low cost devices which are connected to and accessible from the Internet. Open standards will be the key enablers for the success of the IoT. Finally, energy-efficient communication standards, security and privacy and use compatible or identical protocols, should be are needed in different requirement and surroundings.

## 2. Related Works

Chibiao Liu and Jinming Qiu proposed an integrated approach to secure the data transmission of the WLAN-based IoT applications. Meanwhile, they analyzed experiments and theoretical analysis to study the performance of the proposed integrated security approach. It shows that the integrated approach is a new and effective way to secure the data transmission of the WLAN related to IoT applications [4]. Romano fantacci, etal, analyzed the smart building technologies and the overall full smart cities environment. They proposed enhanced feasibility and sustainability of proposed system. But standard gateway architecture is needed [5]. Qian Zhu, etal, proposed an IoT gateway system based on Zigbee and GPRS protocols according to the typical application and presented the data transmission between wireless sensor networks and mobile communication networks, protocol conversion of different sensor network protocols, control function for sensor networks, and gave an implementation of prototyping system [6]. Chibiao Liu, etal, proposed an integrated approach to secure the data transmission of the WLAN-based on IoT application. They performed experiments and theoretical analyses to study the performance of the proposed integrated security approach method, it shows the integrated approach is new and effective way to secure the data transmission pf the WLAN related to IoT application [7]. Antonio F. Skarmeta, etal, proposed a decentralized approach for security and privacy challenges in the Internet of things. They provided a concise description of some of the major challenges related to these areas. It still need to be overcome in the coming years for a full acceptance of all IoT stakeholders involved and a distributed capability based on access control mechanism which is built on public key cryptography to cope with some of these challenges [8]. To realize the security on IoT system, new ultra-cryptography is needed because it provides low computation and limited resources such as small area and limited memory. To cope with these limited drawbacks, Mouza Bani Shemaili, etal, proposed a new lightweight hybrid cryptography algorithm for the Internet of things. They analyzed and proposed some of the available lightweight cipher, and new algorithm that can fit low computation devices [9]. Hossein Shafagh and Anwar Hithnawi proposed a public key cryptography framework for the Internetwork of things. They first identified necessary components of an interoperable secure end-to-end communication while incorporating public-key cryptography and evaluated involved computational and communication overheads [10]. Zeng Bohan, etal, proposed encryption node design in Internet of things based on fingerprint features. In order to ensure the security of sensitive data transmitted between the nodes, and access permission control for the sensing node, a pairs of encryption node, and access control node are designed based on AES (Advanced Encryption Standard) algorithm, and AES security coprocessor of CC2530 is used. The software and hardware design methods of the encryption node are presented. The data transmission experiments between the nodes are carried out. They evaluated that the encryption nodes can achieve wireless encryption transmission for the node's data, so its security can be ensured [11].

## 2. Requirement of IoT System

Cryptosystem is basis of information security. In the traditional network, there are two uppermost forms of cryptographic applications such as point to point encryption and end to end encryption. As far as we know, their system can be merged with the IoT framework [12, 13]. Generally, the node of sensor layer is low speed CPU such as single chip system. Encrypt and decrypt programs cannot use large storage and high-power. So Encryption mechanism in IoT should be lightweight. Compared with traditional network, sensor nodes in IoT deployed in an unattended environment, there are some new characteristics in sensor network. First, wireless link signal is very weak. Second, node is exposed. Third, network topology is dynamic [14]. Emergence of IoT will generate only when strong security solutions are in place. The standards must define different security features to provide confidentiality, integrity, or availability of services. The issues related to identity objects must be dealt with in politics and legislations. Enablers of Internet of Things have following characteristics [15].

a) Manufacturing, logistics and retail sectors: product authentication and anti-counterfeiting, next-generation industrial automation and supply chain management, inventory management, track & trace, remote maintenance, service and support.

b) Energy and utilities sectors smart electricity and water transmission grids, real-time monitoring of sewage systems, efficient energy and water consumption at homes enabled by connected devices to the grid.

c) Intelligent transportation systems support for vehicular ecosystems, use of in-vehicle sensor networks, telematics, GPS and wireless networks for developing smart vehicles, vehicle-to-vehicle and vehicle to roadside communication for collaborative road safety and efficiency, vehicle tracking, traffic data collection for traffic management etc.

d) Environment monitoring systems wireless sensor nodes to monitor weather, environment, civil structures, soil conditions etc.

e) Home management and monitoring use of sensor nodes, smart applications, wireless networks, home gateways for applications such as home security, elderly care, smart energy control etc.

For example, in the case of home network application, IoT gateway system should support internal data collaboration and aggregation in wireless sensor network and data transmission among Internet, 3G networks and other network interfaces. The requirement of IoT system included data forwarding, protocol conversion, and management and control [6]. Theoretical analysis to study the performance of the proposed integrated security approach; it shows that the integrated approach is a new and effective way to secure the data transmission of the WLAN related IoT applications [4]. The implementation of protocols in constrained networks has to deal with some problems related to the nature of the physical devices. The limited computational capacity, the low amount of memory, and the constraints on the energy computation, make the design of these protocols hard and complicated. We introduced requirement of security and privacy issues related to IoT system as follows [16].

a) What do we need to secure

- Access to devices and applications.
- From anywhere in the IoT network.
- And to the data they generate.
- Whether that data is in motion or at rest.

- A body temperature sensor and a thermostat both measure temperature.
- But you must be able to secure them differently.
- Especially on e.g. a multi-tenant home gateway.

b) Threat Modeling for IoT

- Large, complex systems.
- Unattended devices.
- Connected via the public internet.
- Many different threats to consider.
- Correspondingly broad spectrum of countermeasures.

c) IoT Security Model

- Down to very small devices.
- Can't be too resource intensive.
- To large numbers of devices.
- Performance.
- Comprehensibility & manageability.
- To different risk profiles.
- One size doesn't fit all.

d) Basic Principles

- Use standards wherever possible.
- Defense in depth.
- All IoT applications run in a secure container.
- All code is signed and only trusted code will be executed.
- All communications are encrypted and authenticated.
- All access to resources must be authenticated and authorized.

e) Challenges and Barriers

- IoT technologies fall into hardware exploits category.
- Cheap mass production implies shoddy security design.
- There will be a plethora of vulnerable devices.
- Optimistic and somewhat static characterizations of history and stable societies.
- Monitoring and assessment of individual and collective risk.
- The formulization and analysis of a framework for shared distributed decision making by autonomous agents (human or machine).
- Self-validating framework for monitoring and reasoning.

f) IoT Gateway

- Multi-vendor Adaptation & Extensible Platform.
- Rapid customization using adaptors.
- Multi-vendor support with different standards & protocols.
- Common gateway platform.
- Proxy for Device Management.
- Device registration & discovery, data & control channels, inventory, alarms, configuration, status monitoring.
- Security & Access Control.

g) The security challenge

- Devices are not reachable.
- Most of the time a device is not connected.
- Devices can be lost and stolen.
- Makes security difficult when the device is not connected.
- Devices are not crypto-engines.
- Strong security difficult without processing power.
- Devices have finite life.
- Credentials need to be tied to lifetime.
- Devices are transportable.
- Will cross borders.

- Devices need to be recognized by many readers.
- What data is released to what reader

## 3. Example of Topology for IoT Gateway

The typical IoT application architecture can be divided into three layers. As the bridge to connect sensor networks with traditional communication networks, IoT as a fusion of heterogeneous networks, not only involves the same security problems with sensor network, mobile communication network and the Internet, but also more particular ones, such as privacy protection problem. The structure of IoT is generally divided into three layers, including perception layer, network layer, and application or service layer. The characteristics of IoT layers are described [17].

1) Perception layer: It is the information origin and the core layer of IoT. All kinds of information of the physical world used in IoT are perceived and collected in this layer, by the technologies of sensors and wireless sensors network.

2) Network layer: This layer, also called transport layer, including access network and core network, provides transparent data transmission capability. By the existing mobile communication network, radio access network, wireless sensor network and other communications equipment

3) Service layer: This layer, also called application layer, includes data management sub-layer and application service sub-layer. The data management sub-layer provides processing complex data and uncertain information, such as restructuring, cleaning and combining, and provides directory service, market to market service, Quality of Service (QoS), facility management, geomatics, etc. Some systems support some technology such as network processing, computing technology, and middleware technology as the processing layer. IoT gateway can provide the functionalities of protocol conversion and device management. The representative characteristics of IoT have a wide range of access capability, management and protocol interworking. The security of information and network should be equipped with these properties such as identification, confidentiality, integrality and repudiation. Different requirements from Internet, the IoT will be applied to the crucial areas of national economy, medical service, health care, and intelligent transportation. Therefore security needs in the IoT will be higher in availability and dependability. In general, the IoT can be divided into four key levels [18]. Figure 1 shows that the level architecture of the IoT [19].

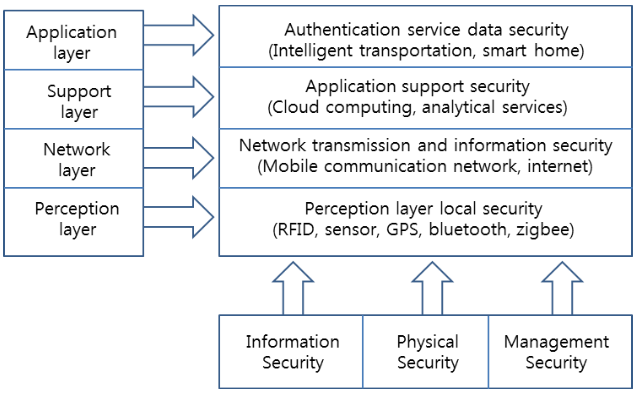
Application layer
Support layer
Network layer
Perception layer
Authentication service data security
(Intelligent transportation, smart home)
Application support security
(Cloud computing, analytical services)
Network transmission and information security
(Mobile communication network, internet)
Perception layer local security
(RFID, sensor, GPS, bluetooth, zigbee)
Information Security
Physical Security
Management Security

**Figure 1. Security Architecture of IoT**

The fundamental differences between the IoT domain and the Internet domain can be classified by the host and network capabilities as well as the respective network topology. Each dimension shows challenges for standard IP security protocol to perform there functions in the IoT domain. The challenges have to consider device capabilities, network capabilities and network topology. For example, The Intel Gateway Solutions for IoT offers companies a key building block to enable the connectivity of legacy industrial devices and next generation intelligent infrastructure to the IoT. It integrates technologies and protocols for networking, embedded control, enterprise-grade security, and easy manageability on which application-specific software can run. The Intel Gateway Solutions for IoT enables [20]: 1) Connectivity up to the cloud and enterprises. 2) Connectivity down to sensors and existing controllers embedded in the system. 3) Pre-process filtering of selected data for delivery. 4) Local decision making, enabling easy connectivity to legacy systems. 5) A hardware root of trust, data encryption, attestation, and software lockdown for security. 6) Local computing for in-device analytics.

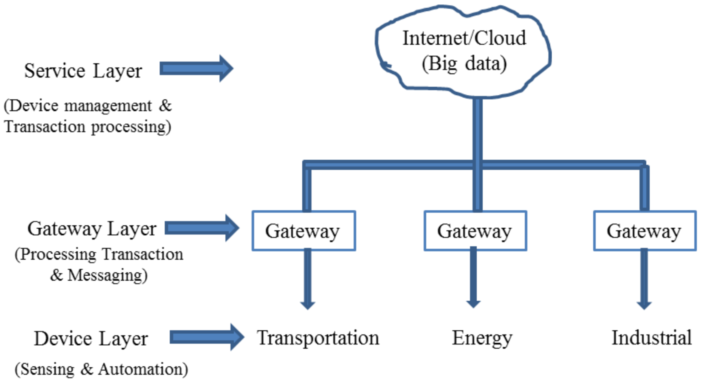

**Figure 2. Topology of Gateway of IoT**

The main functions of IoT gateway are required following capabilities such as multi-vendor adaptation and extension platform, proxy for device management, security and access control, standard web interfaces for data interfacing, and control and gateway hardware platform.

## 4. Conclusions

A consequence of requirements for the IoT is that legacy devices may become a security and privacy liability. Security vulnerabilities of devices should therefore be monitored and solved. It might be useful to consider a set of devices in the IoT. We surveyed and analyzed a requirement of security issues for IoT system and security challenges for Internet of things. The requirement can be considered for some security options and approach that can be used for IoT solutions.

## Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2013-052980)

## References

[1] H.-J. Seo and H.-W. Kim, “Network and Data Link Layer Security for DASH7”, Journal of information and communication convergence engineering, vol. 10, no. 3, (**2012**), pp. 248-252.

[2] L. Li, “Study on security architecture in the Internet of Things”, 2012 International conference on Measurement, Information and Control, (**2012**), pp. 374-377.

[3] P. Huss, N. Wigertz, J. Zhang, A. Huynh, Q. Ye and S. Gong, “Flexible Architecture for Internet of Things Utilizing an Local Manager”, International Journal of Future Generation Communication and Networking vol. 7, no. 1 , (**2014**), pp. 235-248.

[4] C. Liu and J. Qiu, “Study on a Secure Wireless Data Communication in Internet of Things Applications”, International Journal of Computer Science and Network Security, vol. 15 no. 2, (**2015**), pp. 18-23.

[5] R. Fantacci, T. Pecorella, R. Viti and C. Carlini, “Short Paper: Overcoming IoT Fragmentation through Standard Gateway Architecture”, 2014 IEEE World Forum on Internet of Things, (**2014**), pp. 181-182.

[6] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin, “IoT Gateway: Bridging Wireless Sensor Networks into Internet of Things”, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, (**2010**), pp. 347-352.

[7] C. Liu and J. Qui, “Study on a Secure Wireless Data Communication in Internet of Things Applications”, International Journal of Computer Science and Network Security, Vol.15, No.2, (2015), pp. 18-23.

[8] A. F. Skarameta, J. L. Hernandez Ramos and V. Moreno, “A Decentralized Approach for Security and Privacy Challenges in the Internet of Things”, 2014 IEEE World Forum on Internet of Things, (2014), pp. 67-72.

[9] M. B. Shemaili, C. Y. Yeun, K. Mubarak and M. J. Zemerly, “A New Light Hybrid Cryptographic Algorithm for The Internet of Things”, The 7th International Conference for Internet Technology and Secured Transaction**, (2014),** pp. 87-92.

[10] H. Shafagh and A. Hithnawi, “Poster Abstract: Security Comes First, A Public-key Cryptography Framework for the Internet of Things”, 2014 IEEE International Conference on Distributed Computing in Sensor Systems, (**2014**), pp. 135-136.

[11] Bohan, X. Wang and K. Zhou, “Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530”, 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, (**2013**), pp. 1454-1457.

[12] W. Yao, C.-H. Chu and Z. Li, “The Use of RFID in Healthcare: Benefits and Barriers”, IEEE International Conference on RFID Technology and Applications, (**2010**), pp. 128-134.

[13] L. Li, “Study on Security Architecture in the Internet of Things”, 2012 1ntemational Conference on Measurement, Information and Control (MIC), (**2013**), pp. 374-377.

[14] Q. Wen, X. Dong and R. Zhang, “Application of Dynamic Variable Cipher Security Certificate in Internet of Thing”, Proceedings of IEEE CCIS2012, (**2012**), pp. 1062-1066.

[15] A. Boukerche and Y. Ren, “A Secure Mobile Healthcare System Using Trust-based Multicast Scheme”, IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, (**2009**), pp. 387-397.

[16] J. T. Kim, “Requirement of IoT Security Gateway To Improve Vulnerability of Sensor Node”, 2015 International Conference on Future Information & Communication Engineering, vol. 7, no. 1, (**2015**), pp. 435-428.

[17] C. Liu, Y. Zhang and H. Zhang, “A Novel Approach to IoT security based on immunology”, 2013 Ninth International Con-ference on Computational Intelligence and Security, (**2013**), pp. 771-775.

[18] Z. Pang and J. Tian, “Ecosystem-Driven Design of In-Home Terminals Based on Open Platform for the Internet-of Things”, ICACT Transactions on Advanced Communications Technology, Vol.3, Issues 1, (**2014**), pp. 369-377.

[19] . Zhao and L. Ge, “A Survey on the Internet of Things Security”, 2013 Ninth International Conference on Computational Intelligence and Security, (**2013**), pp. 663-667.

[20] Product Brief Intel® Gateway Solutions for the Internet of Things, (**2014**), pp. 1-1.

## Author

**Jung Tae Kim,** he received his Ph.D. degrees in Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI (Electronic Telecommunication Research Institute), where he worked as senior member of technical staff. In 2002, he joined the department of electronic engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of information optical security technology that includes network security system design, RFID&USN and wireless security protocol.