

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

185,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



# Analyses of Open Security Issues for Smart Home and Sensor Network Based on Internet of Things

*Jung Tae (Steve) Kim*

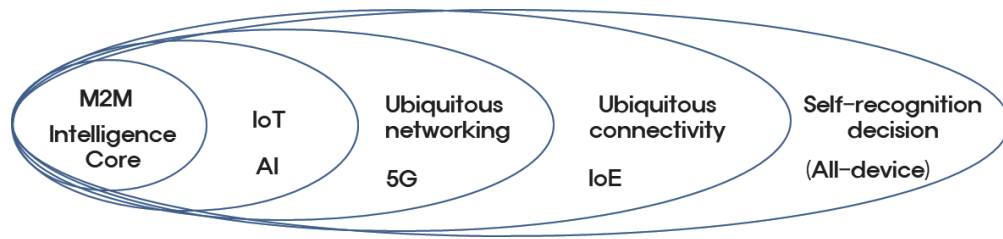
## Abstract

A lot of communication are developed and advanced with different and heterogeneous communication techniques by integration of wireless and wire connection. Conventional technology is mainly focus on information technology based on computer techniques in the field of industry, manufacture and automation fields. It consists of individual skill and technique. As new technologies are developed and enhanced with conventional techniques, a lot of new application is emerged and merged with previous mechanism and skills. The representative application is internet of things services and applications. Internet of things is breakthrough technologies and one of the innovation industries which are called 4 generation industry revolution. Many different types of object and devices are embedded in sensor node. They are inter-connected with optimized open system interconnection protocol over internet, wireless and wire medium. Most of communication is fully inter-connected with conventional techniques at point to point and end to application in general. Most of information in internet of things is weak against attack. This may induce vulnerable features to unauthorized and outside attacker over internet protocol, Bluetooth, Wi-Fi, and so forth. As high and low efficient equipment are merged into heterogeneous infrastructure, IoT communication surroundings has become more complex, Due to limited resources in IoT such as small memory, low power and computing power, IoT devices are vulnerable and disclosed with security problems. In this chapter, we analyzed security challenges and threats based on smart home network under IoT service.

**Keywords:** Security issues, Vulnerability, Attack model, Internet of Things

## 1. Introduction

IoT (The Internet of Things) is widespread, ubiquitous and becoming realized in the real world. Recently, a lot of smart sensor nodes and objects are interconnected and co-operated via the Internet protocol. The Internet of things, its devices and objects are regarded as a global network infrastructure by linking physical and virtual objects. It is implemented by the merging of data capture and communication capabilities in sensor node. IoT is used for connecting devices and sensors with small and limited resources devices to detect a lot of different devices. These kinds



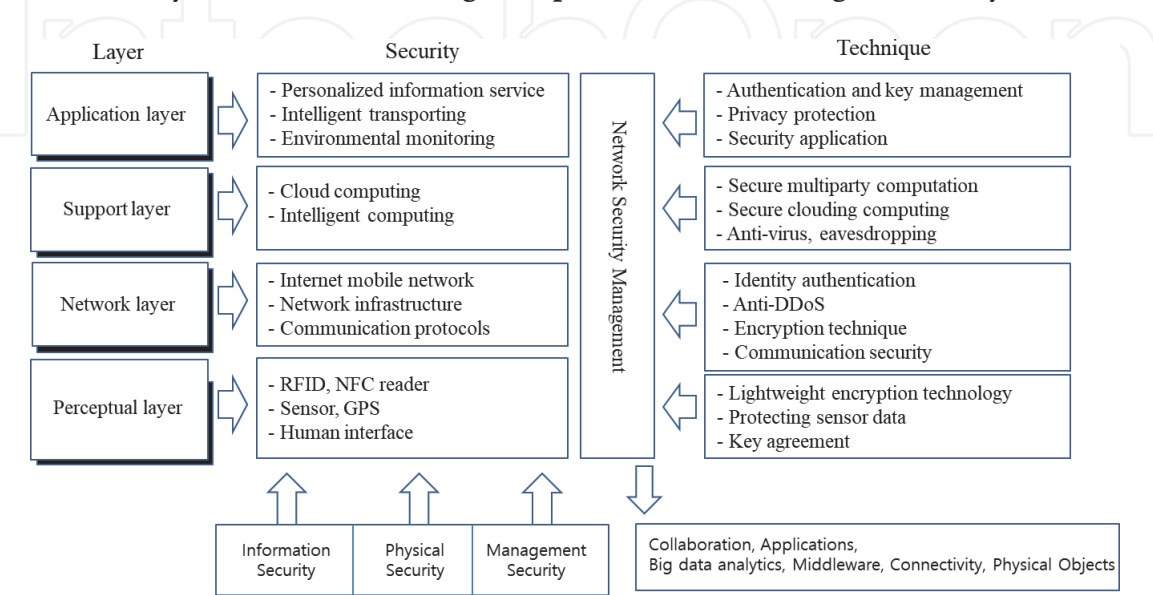
**Figure 1.**  
*Evolution of trend of IoT based on development of technology.*

of infrastructures and connectivity include existing and involving embedded sensor networks via Internet and network [1]. Recently, advanced technologies in the semiconductor enable cost effective solutions to integrate wireless sensor network and connect application with embedded processors and sensors [2]. Previous works are focused on the security mechanism and data transmission in wire and wireless sensor network. Most of the Internet of Things consist of with RFID (Radio frequency identification), sensor devices, WSN (Wireless sensor network), internet and other network, etc. Information security issues are occurred during transmission. It becomes more complicated, critical and essential problems. With a number of things, objects, sensors and actuators which is connected to the Internet, a massive and real-time data flow can be automatically connected with different protocols. Most of papers are focus on in the field of efficient and reliable mechanism of security engines. It includes many applications such as sensing, privacy, tracking, services, data modeling and protocols. The main and issues are security field because the conventional security algorithm and mechanism are not used and suitable for its application with restricted resources. To apply enhanced security and privacy, constrained devices and light-weight cryptography is required for optimal security mechanisms. Therefore, cryptography mechanisms and security protocols should be optimized to adapt constrained devices and objects or new design method to be applicable and integrating into related IoT system. Many researchers enhance try to enhance the security mechanism and schemes. They also tend to improve and develop security protocol with high speed hardware regardless of limited condition [3]. Y. W. Lim et al. proposed reduced hardware architecture and system-on-chip targeting sensor node to achieve energy efficient on the IoT healthcare sensor node. They focused on reduced hardware architecture including sensor node's power consumption and cost [4]. In addition, lightweight cryptography make an alternative idea to implement light-weight security algorithm with low computational and small capabilities. In general, IoT system should be analyzed by its original requirements such as heterogeneous, resource constraints and dynamic environment. It provides its requirement in the field of network, cloud, user, attacker, platform and service. Evolution of IoT based on development of technology is shown in **Figure 1**. This paper is mainly summarized and contributed as follows. First, we introduce and discuss the concept. There is an overview and trend of the related works in the second section. In the third section, we provided requirement and consideration of security issues for IoT System. In the fourth section, open security issues of smart home network are analyzed. Lastly, we concluded in section five.

## 2. Related works

Security requirements for IoT application will be emphasized on the importance of formulated, implemented, and enforced security policies by their needs. Christof Paar et al. proposed described detailed analysis and method to be applicable for

embedded security aspect concerning to IoT application. Regarding to traditional security solution, a lot of researcher and works have done and realized to provide embedded security system with small hardware resources such memory and low computation ability [5]. Jorge Granjal et al. surveyed and analyzed existing protocols and mechanisms for open research field. They analyzed that how existing approaches can be ensure fundamental security requirements and protect data in the field of IoT application. They also summarized the open challenges and strategies for the future work in this field [6]. Most security protocols which is used for network and internet security cannot be implemented with smart home systems related because they are low security complexity and vulnerable in smart home applications for the wireless sensor nodes. The major security issues for smart home systems are initial session key establishment between the wireless nodes and gateway or control box in smart home system. Yue Li proposed and analyzed a sort of lightweight key establishment protocol for home energy management systems. He presented an example of implementation and protocol in detail [7]. Kozlov et al. discussed about threats for privacy and security at a different architectural level of the smart home. They especially advertised to analyze privacy risk levels for privacy control mechanisms, methods, and energy aspects concerning to security, privacy, and trust. They are also evaluated an energy consumption in entire smart home infrastructure [8]. The security matters of information and network should be considered with representatives of properties such as identification, confidentiality, authentication, integrity and repudiation. In spite of a different requirement on Internet, IoT system will be applicable to the crucial and critical areas such as medical and health care, home, energy, intelligent transportation, smart factory and so on. Therefore, security needs in the IoT are more necessary and indispensable in availability and dependability. Generally speaking, the IoT can be divided into four layers [9]. The representative architecture and its configuration is described in **Figure 2** [10]. The structures of IoT are generally divided and classify into three layers. It consists of perception layer, application layer and network layer. Jeong Gi Lee et al. analyzed a current research and development trend. The main idea is that how integrated platform can be implemented with data security between different smart home nodes and devices. They implemented integration platform based on android to provide with simple development and scalability. It can be easy to access for authorized user. Smart home network based on related sensor products have a different ways of the data exchange. Its platform can be integrated easily and



**Figure 2.**  
*Basic architecture of IoT services.*

connected by heterogeneous network products and external transmission security processing for data communication. It can be supported to enable the integration of sensors [11]. Freddy K Santoso et al. proposed the implementation and design for IoT smart home system with embedded Wi-Fi system. It includes gateway to enable and activate secure communication between IoT sensor devices and control system. It allows user to control, access and configure related devices. It can be realized by smart phone and mobile devices to interface external communication and control devices [12]. Himanshu Gupta et al. presented a security framework for IoT applications using block chain technology and technique. It provided many unique characteristics such as better privacy, manageability, fault tolerance and scalability [13]. Musa G Samaila et al. proposed the IoT hardware platform security advisor. It provides three functionality features such as security requirement elicitation, security best practice guidelines. They also gave a guideline for lightweight cryptography design and implementation consideration. It includes a summary of the cryptographic algorithm [14]. Nikos Komninos et al. surveyed smart home security based on issues, challenges and countermeasures in smart grid application. They analyzed the most representative threats to smart grid environment and smart home system based on a lot of scenarios. They summarized a review of security countermeasures related to smart home as follows [15].

1. Confidentiality and privacy: Symmetric/Asymmetric encryption algorithms, zero knowledge proof systems and data obfuscation
2. Integrity: Cryptographic hashing techniques, digital watermarking, timestamps, session keys and sequence numbers.
3. Authenticity: Keyed cryptographic hash function, hash based authentication codes and MAC-attached messages
4. Non Repudiation: Mutual inspection with smart meters and unique keys for customer-AMI communication and AMI transaction logging
5. Availability: Alternative frequency channels according to hardcoded sequence, anomaly based IDSs and specification based IDSs
6. Authorization: Attribute based encryption, attribute certificates and attribute based access control system

Abdullahi Arabo analyzed cyber security challenges with the connected home ecosystem. He presented related background, motivation, development and demand for inter-connecting of different devices. The smart phone or mobile agent is used to provide a variety of function and capability to users [16]. Md. Mahmud Hossain et al. analyzed a detailed analysis of IoT system. It includes threat models, security issues, challenges and many attack models [17]. They provided a sort of open problems and issues in IoT security and privacy problems. This makes researchers to guide and solve the most critical and open problems. Pranay P. Gaikwad et al. surveyed these applications based on smart homes systems using internet of things [18]. They presented the problems and challenges which is occurred in IoT and smart homes application based on IoT system. Some solutions they proposed overcome some problems and challenges. We summarized the recent and breakthrough works in the field of security problems and privacy issues related to smart home application. A more extensive and detailed of related works have been published [19]. Monammed Ali Al-Garadi et al. surveyed of machine and deep



learning (ML/DL) methods for IoT security. They also define thematic taxonomy of ML/DL for IoT security [20].

### **3. Requirement and consideration of security issues for IoT system**

#### **3.1 Basic concept of IoT**

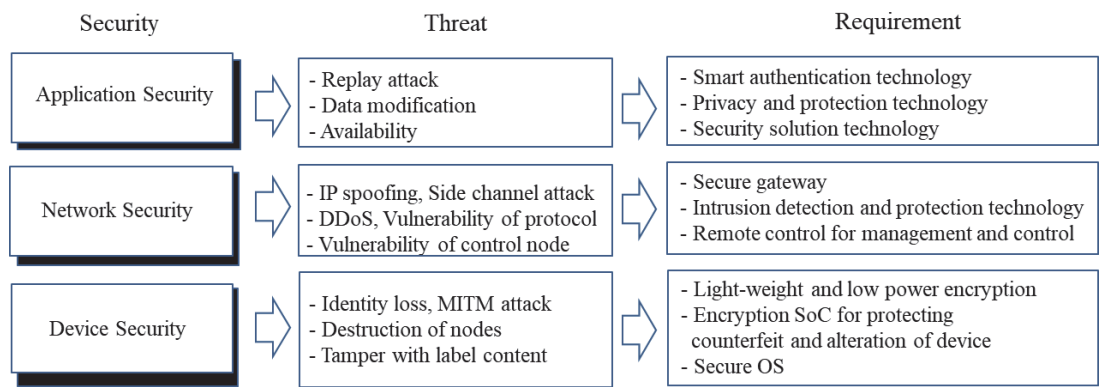
The domain of smart home environments is regarded and considered as a major factor and element for the future Internet. As a lot of homes are becoming smarter and smarter by using sensor and technology based on IoT, we can improve home security, energy efficiency, availability and comfortability. Consequently, to realize the future technology applicable to the smart home, we have to consider and treat with privacy into IoT environments. It can be identified and regarded as one of the major barriers and flaws. Because of the nature of the IoT environment, the appropriate security functions for secure and trustworthy smart home service would be applied extensively and considered importantly because the security threats will be increased and impact of security threats will be likely expanded. Jin-Hee Han et al. analyzed the requirement of security consideration for enhanced security and trustworthy mechanism in smart home system based on IoT environment [21]. As sensor nodes are widespread and utilized under ubiquitous environment, the security attacks on embedded device is increasing. The major factors include in the field of attacks such as crypto-analysis, physical, side channel, environmental, software and networks. Vijay Sivaraman et al. illustrated network-level security and privacy control for devices in smart home based on IoT. They proposed that software defined networking technology would be used to dynamically block and quarantine devices. It is based on their network activity [22]. The major security concerns for IoT system are summarized and included factors such as user identification, tamper resistant, secure S/W execution, secure content, secure data communications, identity management and secure storage. As a results of a risk and security analysis for a smart home automation system, it can be developed in collaboration with new schemes for leading industrial factors. They summarized the first steps and models of privacy and security for smart home applications. It is regarded as support and necessity for enforcing system security and user privacy, and it can help to realize the potential power in smart home environments. The typical architecture in IoT application can be divided and classify into three layers as following description [23]:

1. Perception Layer: In this layer, it collects, acquire and process the information from physical world. It is made up with two part to communicate with sensor devices and wire and wireless sensor network
2. Transmission Layer: In this layer, it transfers information in a large or long distance area. To connect and integrate information in perception layer, the information can transfer by using mobile, Wi-Fi and other communication media
3. Application Layer: In this area, it can process and service the information which is included in the layer.

Many applications provide middleware technology, computing technology and network processing in each layer. The main devices in perception layer include RFID, Zigbee and all kinds of sensors. Basic architecture of IoT service is shown **Figure 2**.

They are highly vulnerable to attacks. Several common attacks are included node capture, fake node and malicious data, denial of service attack, timing attack, routing threats, reply attack, side channel attack and mass node authentication problem. Network layer security problems have critical problems such as traditional security problem, compatibility problem, cluster security problems and privacy disclosure. In application layer, its security issues are different and more complex because of different industry or environment. The following elements should be solved with data access control, identification, data protection and recovery, authentication, ability of dealing with mass-data and software vulnerabilities in application layer. The IoT system has a particular restriction, constraints and limitation in terms of computational power, small memory and power. It makes significantly different from existing distributed systems. It can be recognized in real world that the existence of tiny computing devices is very much vulnerable to different security attacks as mentioned above. Security in level and requirement is shown in **Figure 3**.

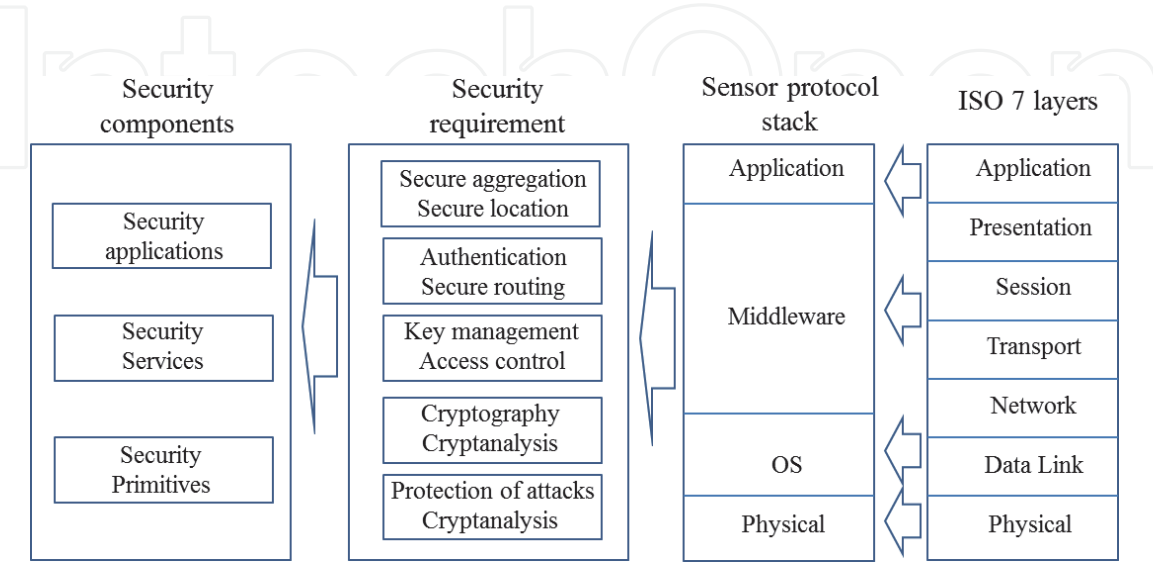
Sye Loong Keoh et al. gave an overview of the efforts and demands in the IEFT (Internet Engineering Task Force) to standardize security solutions for IoT ecosystem. They provided a detailed review with communication security solutions for IoT. Especially, they used to conjunct with standard security protocols to be applied in the CoAP (Constrained Application Protocol), and application protocol to adapt the constraints IoT devices [24]. Pranay P. Gaikwad et al. presented the architecture of IoT related to attacks model. Smart home network can be operated with household devices and home appliances. It could monitor and control remotely with different connection and control ways. When these kinds of household devices in smart homes are connected with wire or wireless Internet under standard protocols. The whole system is so called as smart home network and can be realized in IoT environment or smart homes based on IoT devices. They presented the problems and challenges which is occurred in IoT and smart home applications. Some solutions that they proposed overcome and solve some problems and challenges in real solution matters [25]. The security design can be adapted with these kinds of diverse deployment scenarios. The representative ideas have a concise set of cryptographic, single security policy framework, security mechanisms, and configuration parameters with policy-dependent. These kinds of requirement and consideration in terms of system perspectives should take into account for entire system. In spite of IoT devices are constrained with limited resources, it can be deployed with easy steps and still has a vulnerability problem. Therefore, the traditional and conventional security mechanism and algorithms cannot be straightforward realized in smart things and sensor nodes. The major and representative limitation and constraints are shown in **Table 1** [26].



**Figure 3.**  
*Level and requirement for security.*

Hardware aspect	Software aspect	Network aspect
<ul style="list-style-type: none"><li>• Computational and energy constraints</li><li>• Memory constraint</li><li>• Tamper resistant</li></ul>	<ul style="list-style-type: none"><li>• Embedded software constraint</li><li>• Dynamic security patch</li></ul>	<ul style="list-style-type: none"><li>• Mobility, scalability, multiplicity</li><li>• Multiple medium of communication</li><li>• Multi-protocol networking</li><li>• Dynamic and stable network topology</li></ul>

**Table 1.**  
*Major security constraints of IoT devices.*



**Figure 4.**  
*Basic component of security architecture.*

We analyzed the key element of security architecture with relation to sensor protocol, security demands and ISO7 layer as shown in **Figure 4**. There are many application layer protocol such as CoAP (Constrained Application Protocol), XMPP (Extensible Message and Presence Protocol) and MQTT (Message Que. Telemetry Transport), AMQP (Advance Message Queuing Protocol) [27]. Hee-jeong Kim and Jeong Nyeo Kim proposed end-to-end message security protocol based on ultra-weight cipher algorithm. This algorithm can increase security level and lower security overhead in resource limited communication [28].

### 3.2 Application of IoT services

The representative issues and services are included a lot of mechanisms. The main topics consist of end-to-end security, fault tolerance, key management, energy efficient security, trust management, IoT big data and it's forensic and so on. We also presented requirements of IoT System including basic principles as well as challenges and barriers.

#### a. Basic Principles

- Use standard and its application protocols.
- Detail protection and defense from malicious attacks.
- Secure algorithm is embedded in the system and realized with lightweight Algorithm.



- All code is implemented by authentic and trusted techniques.
- All protocols and communication is implemented by encrypted and authenticated techniques.
- All access and control to resources should be authenticated and authorized.

b. Challenges and Barriers

- Secure hardware platform is required and exploited.
- Complicated security design can be solved a cheap and mass production in silicon devices.
- A lot of vulnerable devices are revealed and plethora in the real world.
- Individual and collective risk can be monitored and assessed.
- Shared and distributed framework can be formulized and analyzed by decision making technique.
- Self-validating framework for monitoring and reasoning.

### **3.3 Security and privacy issues**

The implementation of protocols with constrained networks should be dealt with some open problems. It is induced and related to the nature and feature of the physical devices. The features are included a limited computational capacity, a low amount of memory, and a limitation on energy computation, it makes the design of these protocols too hard and complicated in nature. We give some requirements and summarize for security and privacy issues related to IoT services as follows [29–30].

a. What we need to secure

- Access to sensors, devices and objects.
- Where the IoT network is located and inter-connected.
- What kind of data is generated and communicated.
- Whether the data which is produced is in active or at rest.
- A measured temperature is moderate to devices and sensors.
- Different secure complexity and level in each devices and objects.
- Suitable gateway system for multi-function is available.

b. Threat modeling for IoT

- Complex and large system is needed to guarantee and protect the attack model

- Unattended devices is produced and is exclusive.
- Public internet is connected and established.
- Many different threats should be considered.
- Broad and wide spectrum of countermeasures is required.

#### c. IoT Security Model

- Devices are small and scale down.
- Resources cannot be intensive and compact.
- A numbers of devices are required.
- Performance should be considered.
- Comprehensibility, manageability and availabilities.
- Different risk profiles are induced.
- One size does not fit all and complex and complicated techniques are necessary.

#### d. IoT Gateway

- Adaptation and extensible platform can be utilized.
- Rapid customization using adaptors can be easy implemented.
- Multi-vendor with different standards & protocols can support.
- Common gateway platform is essential and vital in secure.
- Proxy system for device management can be used.
- Gateway is made up with data and control channels, configuration, status monitoring, and device registration and inventory, etc.
- Security and access control is embedded in gateway engine.

One of the major problems related with IoT is the heterogeneous nature of devices. Shachar Siboni et al. analyzed several specific IoT testing scenarios based on different IoT devices [31]. Daewon Kim et al. present common security requirement for IoT device identification system. The requirements are more important when the identification information is used as the sensitive data such as authentication [32]. Franco Loi et al. developed a systematic and optimized method to identify and evaluate the security and privacy on various IoT devices. They categorize the threats along four dimensions such as confidentiality, integrity, access control and reflective attacks [33].

### 3.4 Model of attacks and threats based on IoT devices

There are a various of vulnerable attacks in sensor nodes, RFID and its application because of its restricted resources. Security threats and vulnerability to sensor protocols and nodes can be classified by strong and weak attacks. Weak attacks are practical and threats by observing and manipulating the communication channel to acquire the data between a server and device tags. Replay attacks and interleaving attacks are representative examples of weak attacks model. Strong attacks are feasible threats and means for an attacker to be compromised and acquired a data on target tag. A memory of sensor is very vulnerable to be compromised and have a small resource. It can be easily attacked by side channel effect because the low cost and capability tag is unlikely to be tamper-proof. The major strong attacks are included forward traceability, backward traceability, and server impersonation and described in Ref. [34].

It is possible to identify and realized with five distinct technology and trends in the future of IT, As many devices are widespread and ubiquitous with explosion. The future of IoT will be faced with representative characteristics as follows [35–37].

1. Data deluge: Amount of data is exploded and collected and exchanged through different networks. Forecasts indicate that more than several thousands of sensors and objects will be stored and integrated in the near future. Novel and unique techniques are needed to transmit, find and fetch the data in safe.
2. Miniaturization of devices: To realize the compact and small sensor, devices will be increasingly smaller and smaller.
3. Little energy consumption: the devices and system have to reorganize its own energy or self-organization to get a power.
4. Autonomic management: the devices or systems have to control its system and have a function for self-management and self-configuration capabilities.
5. IPv6 as an integration layer: It will provide nature network.

IoT application can be realized when we have a connectivity for anything from any time, any place connectivity for anyone. The enabling of technologies and realization of IoT application should be combined with RFID, NFC, sensor, smart technology and nano-technology. The characteristics of enabling technologies are summarized [9]. Internet of things' enablers should have characteristics as follows.

1. Energy: Energy harvesting technology and low-power chipsets are critical problem to develop and evolve IoT applications.
2. Intelligence: Devices should have a capability to reform and improve for self-organization and inter-machine communication, etc.
3. Communication: As the communication technology and means enables the devices to communicate with inter-networking. New materials and Integrated on-chip technology and smart multi-band frequency antennas are required.
4. Integration: Integration of smart devices into packaging and the products can be fabricated on-chip level.

- 5. It saves a significant cost and increase the applicable and friendly for the products and objects.
- 6. Interoperability: Protocols for inter-operability have to be customized for standardization.
- 7. Standards: Open standards mainly play an import role in the success of the IoT.

In general, energy-efficient communication standards, strategy of security and privacy should be considered into interest and needs. Compatible or identical protocols at the different frequencies are needed [30]. The function of sensor IoT is described in **Table 2**.

The hardware based issues related to sensors and objects should be dealt with in politics and laws. Enablers and objects of Internet of Things have a features as following description [38].

- Manufacturing, logistics and retail sectors: Next-generation industrial artificial intelligence, smart grid, supply chain, block chain, smart factory and inventory management, remoting control maintenance, anti-counterfeiting, and so on.
- Energy and utilities sectors: Smart inspection in electricity and energy, efficient energy and consumption mechanism, smart grid in transmission, real-time operation and monitoring system, smart grid in IoT connection and so forth.
- Artificial intelligent transportation support: Telematics, GPS and wireless networks, use of in-vehicle sensor networks, collaborative road safety and efficiency technology, vehicle tracking, developing smart vehicles and traffic data collection mechanism, etc.
- Environment monitoring systems: Remote inspection and control system for monitor the behavior on wireless sensor nodes such as environment condition, monitoring of weather, detection of soil condition, etc.
- Home management and monitoring: Smart sensor nodes, secure home gateway connected to security engines, electrical appliances, smart energy control, etc.

Example of IoT based on network topology is shown in **Figure 5**. To connect sensor networks with traditional communication networks to other networks, IoT

Sensors	Function
RFID/NFC	To identify and track the sensor, object and so on.
Sensor	To collect and process the data flow To detect the changes and moving in the physical status of things and objects
Smart technology	To enhance the power of the network It is developing processing capabilities
Nano technology	To make the smaller and smaller things The ability to connect and interact in small area. It can be fabricated on chip with CMOS process

**Table 2.**  
*Function of sensor IoT.*

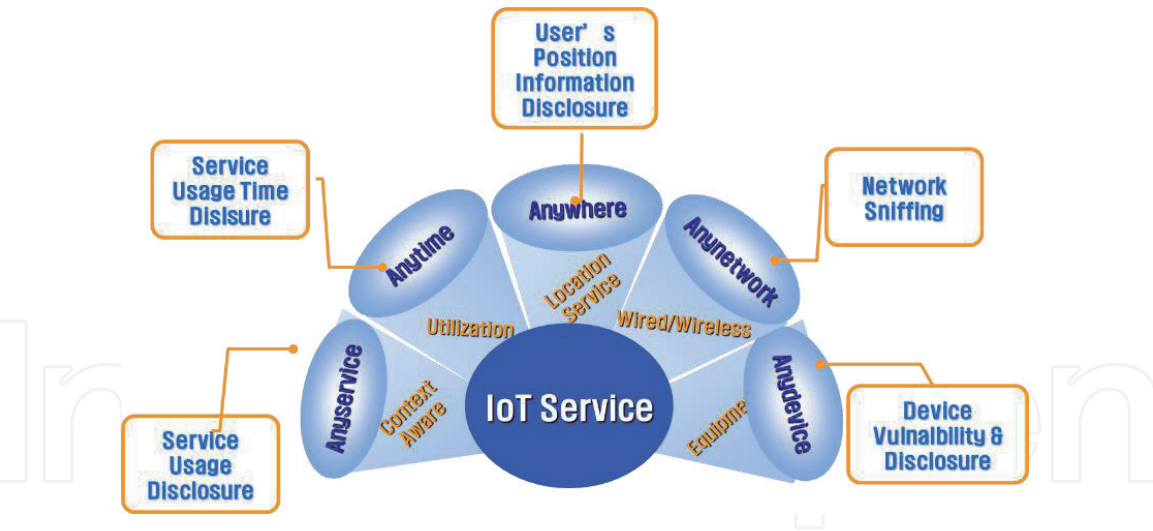


Figure 5.  
Application of IoT service [29].

gateway can provide the function of protocol conversion and device management. As a general gateway, IoT gateway has characteristics and features such as access capability with a wide range, manageability for easy, interworking protocol for efficient topology [39]. Based on the home network application, secure gateway should provide and gather internal data to collaborate and aggregate in wireless sensor networks, and data transmission among Internet, high-speed, 5G networks, DSL networks, and other network interfaces. The system requirements of IoT gateway system should be considered by employing, protocol conversion, data forwarding and management and control [36]. Example of IoT system based on network topology is shown in **Figure 6**.

To analyze the performance and security analysis of IoT architecture, we can estimate the performance analysis such as computational cost, storage requirement and communication cost and security analysis. The security elements are included factors such as data confidentiality, tag anonymity, mutual authentication, data integrity, relay attacks and forward security. The representative attack and solutions are reviewed in **Figure 7**. We analyzed reusable security requirement and used them as examples of reusable security requirements. The attacks on IoT system are included denial of service attack, physical attack, tags cloning attacks,

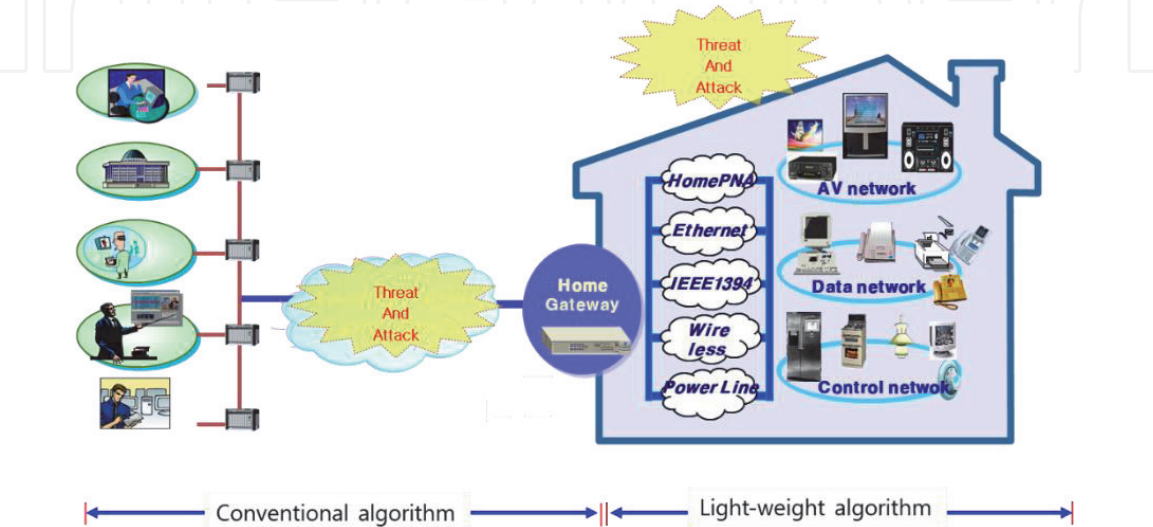


Figure 6.  
Example of IoT system based on network topology.



Security mechanism	Authentication method	Security service
Authentication	User's authentication	- PKI, OTP, certification of official recognition - Home gateway authentication - Fingerprint, vein
	Service authentication	Authentication between home service provider and home service
	Device authentication	- Authentication by certification - Home gateway is operated as authentication server
Authorization Access control	User's access control	- Access control by policy of security level - Access control profile by security level
	Device to device authentication	Necessity of access control between heterogeneous device
	Perception of situation Access control	- Restriction of user's service - Access control by location based service

**Figure 7.**  
*Characteristics of authentication method and security mechanism.*

impersonation attack, replay attack and tags tracking. Pranay P. Gaikwad et al. presented open problems and challenges [40]. Denning et al. surveyed the security and privacy matters in IoT based smart homes, and provided a strategy for reasoning about security needs. They mentioned how to conduct an attack to avoid and have a feasibility in attack model. The attractive point they propose is that the system compromise a platform and attack model caused by damage [41]. In generally speaking, smart home system can be organized and configured as shown in **Figure 7**. Smart home system consists of home gateway, home server, and smart home sensor and devices. To enhance security complexity, we should take into consideration basic security functions for the smart home system. Security functions are against security vulnerabilities and security flaws caused by device resources issues, attacks, etc. The necessity and requirement of security in authentication level can be classified by authentication and authorization level. The representative characteristics and features are shown in **Figure 7**.

Computing service with confidentiality and threat factors under ubiquitous surrounding should be regarded as vulnerable attacks and insecure services viewpoints. The major factors to be considered are as follows [42].

- Confidentiality for secure data
- Authentication and access control for authorized a user
- Integrity and non-repudiation for reliable data
- Availability and survivability for fusibility
- Privacy and authority control for authorization

Also, threat factors and features can be considered as follows.

- Sensor node attack

- Eavesdropping
- Sensing data privacy
- DOS (Denial of service)

A brief of characteristics and features of smart home network is depicted as follows.

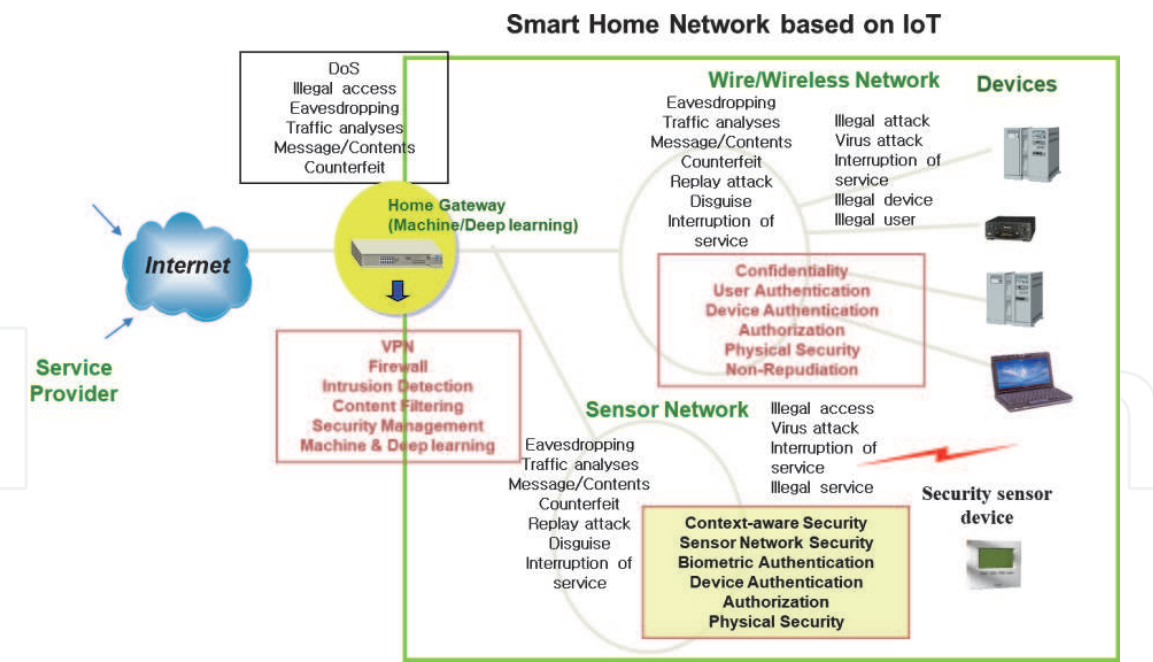
- Home network may not be isolated in sub-network and inter-connected for operability.
- Wi-Fi and PLC signals may propagate and be widespread to the next door. It can be exposed.
- Different network and addressing scheme are required.
- IP address, group and node ID is required in separated.
- Many devices have a low computational power and small memory capability.
- No public key cryptography is required. It uses a symmetry algorithm.

To enhance advanced and high complexity security, we have to take into account for intrusion protection and detection mechanism in sensor network. Especially, home gateway should be required enhanced security framework, authorized control, privacy and resilience of survival, etc. The security issues with heterogeneous connection between devices under IoT application cannot be solved with conventional cryptography techniques. Many works have done and cannot utilize existing PKI (Public key infrastructure) and lightweight schemes. Some researchers have evolved new scheme with ultra-lightweight algorithm. It has still unsolved problems. Many researcher and works tend to focus on following techniques relating to smart home network security.

- Integration of security on middleware is realized.
- New security function and schemes beyond security function of middleware are utilized.
- Safety about middleware security function can be analyzed.
- Lightweight algorithm is developed and can be suitable for its system.
- User's convenience can be provided with simple algorithm

#### **4. Open security issues for smart home network**

We analyzed and discussed the critical and essential issues for open solution of IoT related to smart home network. It mainly focuses on challenges and mechanism in application field. Example of IoT based network topology and attack model on home network is shown in **Figure 8**. We can estimate the security requirements for smart home network. It consists of device authentication, network monitoring,



**Figure 8.**  
Example of topology for attack model on smart home network.

secure session key management, physical protection, information security, and user authentication [43]. Andreas Jacobsson et al. reviewed a risk analysis related to smart home automation and control system [23].

The reviewed and related works presented have included risk analysis based approaches, security based approaches, privacy based approaches and industry based approaches. Chakib Bekara analyzed security matters and challenges for the IoT based on smart grid [44]. He considered security issues as a cyber and physical system, the IoT based smart grid will be faced with several security issues such as impersonation, eavesdropping, data tampering, authorization, control access, privacy issue, malicious code, availability and DoS issues. When dealing with security algorithms, several challenges should be considered with scalability, mobility, deployment, legacy systems, constraints resources, heterogeneity, interoperability, bootstrapping, trust management and latency and time constraints. Noy Hadar et al. proposed an innovative and creative cloud-based framework to protect attacks and threats on IoT devices. It can be applicable to cost effective solution [45].

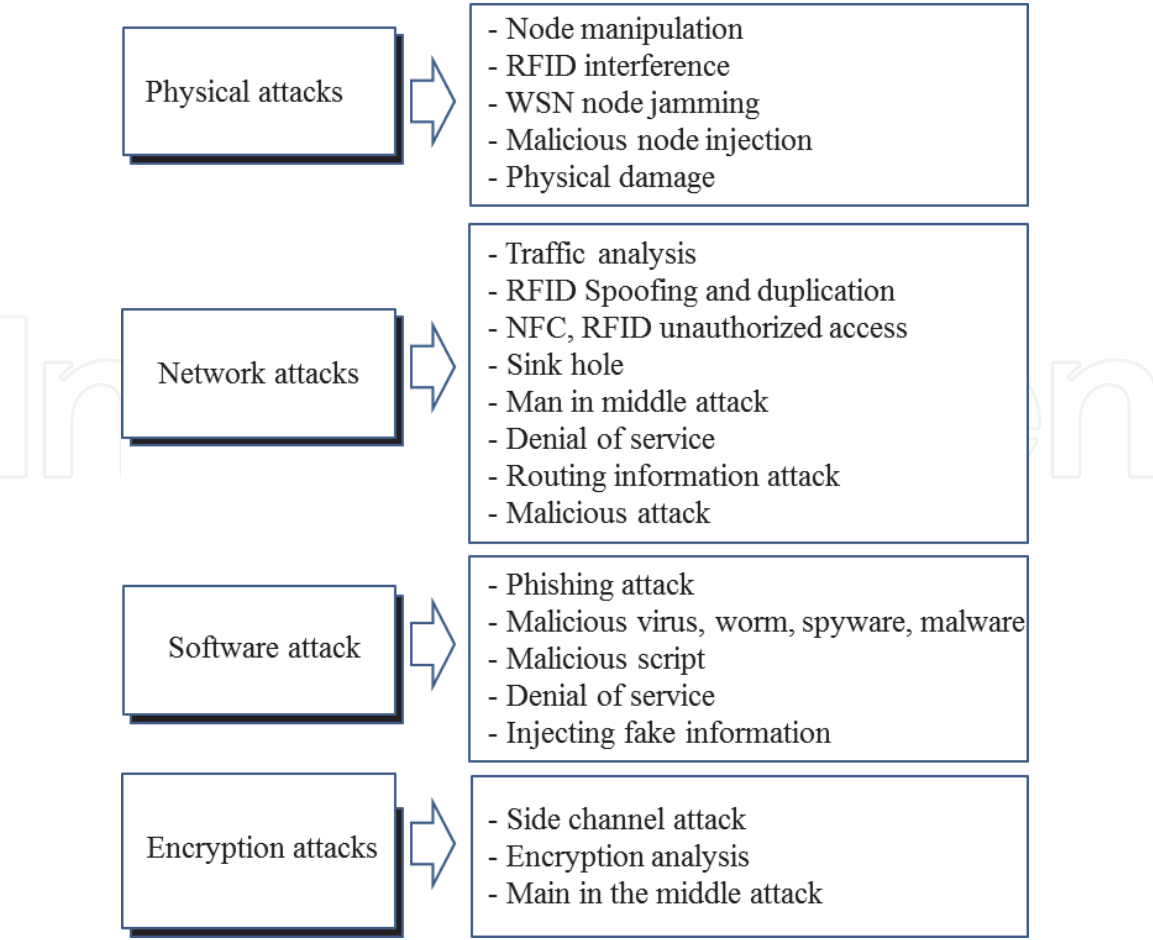
Sensors	Function
Device security	Insecurity due to device category and capability
	Software and firmware security
	Storage security
Communication security	Security service security
	Network service security
	Cryptographic security
Security service	Native service security
	Cloud service security
	Partner cloud service security

**Table 3.**  
Critical security weakness of IoT system.

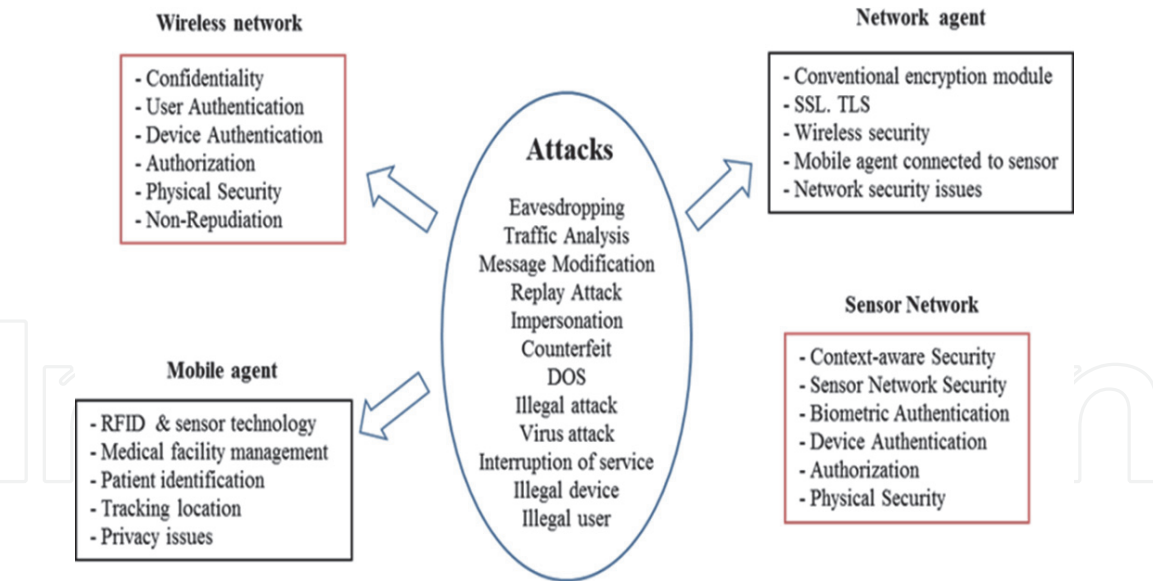
To understand IoT security issues, we should investigate the characteristics of component for the IoT sensor and network among them. It consists of sensors in home network, sensor bridge network such as home gateway and cloud. Md. Mahmud Hossain et al. analyzed critical security weakness [17]. The security characteristics of sensors are shown in **Table 3** [46].

The security challenge of devices and sensors should be solved and included as follows. We analyzed the following issues.

- a. Devices are not connected and reachable  
Most of the time, device is not connected
- b. Devices can be stolen and lost  
It makes security difficult and uncountable when the device is not attached and connected
- c. Devices are not included crypto-engines  
Strong security is difficult to solve the problem without high-speed processing power
- d. Devices have finite life  
Devices have small power and needs for self-organization and recharge mechanism



**Figure 9.**  
*Attacks model and its characteristics.*



**Figure 10.**  
*A variety of attacks on smart home network.*

- e. Devices are transportable  
Will cross borders
- f. Devices can be recognized and detected by many readers  
What data is exposed and disclosed to reader?

Characteristics of attacks and model are shown in **Figure 8**. The gateway can provide secure communication for authentication, secure session key exchange and monitoring between devices and gateway [47]. The attacks model and its characteristics are shown in **Figure 9**.

We also described the challenges of open issues for IoT's development. Trade-off between hardware, software and co-design method is needed for security framework and architecture for IoT system. We have to focus on delivering the creative and unique solutions for the state-of-the-art and innovative mechanism. It includes IoT security controls, optimized mechanisms for the new skills and extremely complex embedded applications. Example of IoT based on smart home network topology is shown in **Figure 8**. Example of attack model on home network is analyzed in literature [48]. Recent DDos (Distributed denial of service) attack and technology are developing with recent techniques and cause a high vulnerability on IoT system. It focuses on the requirement of scalable and optimized security solution. Ellia and Nayeem described common internet things and vulnerabilities [49]. A variety of attacks on smart home network is shown in **Figure 10**.

## 5. Conclusion

Internet of Things is used in many applications in different areas. IoT has been already designed for industrial wireless sensor network in many applications. It can be developed for smart homes system in the near future. Architecture of IoT and smart homes based on IoT are analyzed in this review paper. In spite of many opportunities and recent technologies, many challenges and issues are produced by a lot of attacks which is addressed in IoT. It will inherit the drawbacks of the internet used in nowadays. We discussed about security mechanisms, we also point out that



the challenges of open issues for IoT's development. Hardware and software co-design methodology is needed to fit into security framework and architecture for IoT system. We have to focus on delivering the current state-of-the-art IT security controls, optimized mechanisms for Internet of things and objects in the future works.

### **Conflict of interest**


“The authors declare no conflict of interest.”

### **Author details**

Jung Tae (Steve) Kim  
Mokwon University, Daejeon, South Korea

\*Address all correspondence to: [jtkim5068@gmail.com](mailto:jtkim5068@gmail.com)

### **IntechOpen**

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Brahim Ethem Bagci, Shahid Raza and Tony Chung, Combined Secure Storage and Communication for the Internet of Things, In Proceedings of the 2013 IEEE International Conference on Sensing, Communications and Networking, 2013, pp. 523-531.
- [2] Freddy K Santoso and Nicholas C H Vun, Securing IoT for Smart Home System, In Proceedings of the 2015 IEEE International Symposium on Consumer Electronics, 2015, pp. 1-2.
- [3] Raja Benabdessalem, Mohamed Hamdi and Tai-Hoon Kim, A Survey on Security Models, Techniques and Tools for the Internet of Things, In Proceedings of the 2014 7th International Conference on Advanced Software Engineering & Its Application, 2014, pp. 44-48.
- [4] Y. W. Lim, S.B. Daas, S. J. Hashim, R. M. Sidek, N. A. Kamsani and F. Z. Rokhani, Reduced Hardware Architecture for Energy Efficient IoT Healthcare Sensor Nodes, In Proceedings of the 2015 IEEE International Circuits and Systems Symposium, 2015, pp. 90-95.
- [5] Christof Paar and Andre Weimerskirch, Embedded Security in a Pervasive World, Information Security Technical Report, Elsevier, Vol 12, Issue 3, 2007, pp.155-161.
- [6] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, IEEE Communication Surveys & Tutorials, 2015, Vol.17, No.3, pp.1294-1312.
- [7] Yue Li, Design of a Key Establishment Protocol for Smart Home Energy Management System, In Proceedings of the 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, 2013, pp.88-pp.93.
- [8] D. Kozlov, J. Veijalainen, and Y. Ali, Security and Privacy Threats in IoT Architectures, In Proceedings of the 7th International Conference on Body Area Networks, 2012, pp.100-102.
- [9] Zhibo pang and Junzhe Tian, Ecosystem-driven Design of In-home Terminals Based on Open Platform for the Internet-of Things, International Transactions on Advanced Communications Technology, 2014, Vol.3, Issues 1, pp.369-377.
- [10] Kai Zhao and Lina Ge, A Survey on the Internet of things security, In Proceedings of the 2013 9th International Conference on Computational Intelligence and Security, 2013, pp.663-667.
- [11] Jeong-Gi Lee, Chul-Seung Yang, Hun-Ha Kim and Kang-Jin Kim, A Research and Development of Integrated Platform for Data Security between Different Smart Home Devices, Journal of the Korea Institute of Information and Communication Engineering, 2015, Vol.19, No.5, pp.1173-1179.
- [12] Freddy K Santoso and Nicholas C H Vum, Securing IoT for Smart Home System, In Proceedings of the 2015 IEEE International Symposium on Consumer Electronic, 2015, pp.11-12.
- [13] Himanshu Gupta and Garima Varshney, A Security Framework for IoT Devices against Wireless Threats, 2017 2<sup>nd</sup> International Conference on Telecommunication and Networks, 2017, pp.100-106.
- [14] Musa G. Samaila, Joao b. f. Sequeiros, Tiago Simoes, Mario M. Freire and Pedro R. M. Inacio, IoT-

HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Application in the IoT Space, IEEE Access, Jan, 2020, pp.16462-16494.

[15] Nikos Komninos, Eleni Philippou and Antreas Pitsillides, Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures, IEEE Transaction Survey & Tutorials, 2014, Vol.16, No.4, pp.1933-1954.

[16] Abdullahi Arabo, Cyber Security Challenges within the Connected Home Ecosystem Futures, Procedia Computer Science, 2015, pp.227-232.

[17] Md. Mahmud Hossain, Maziar Fotouhi and Ragib Hasan, Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things, In Proceedings of the 2015 IEEE World Congress on Services, 2015, pp.21-28.

[18] Pranay P. Gaikwad, Jyotsna P. Gabhance and Snehal S. Golait, A Survey Based on Smart Homes System Using Internet-of Things, In Proceedings of the 2015 International Conference Computation of Power, Energy, Information and Communication, 2015, pp.330-335.

[19] Romano Fantacci, Tommaso Pecorella, Roberto Viti and Camillo Carlini, Short Paper: Overcoming IoT Fragmentation through Standard Gateway Architecture, In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp.181-182.

[20] Mohammed Ali-Garadi, Amr Mohamed, and Abdulla Khalid Al-Ali, A Survey of Machine and Deep Learning Methods for Internet of Thing Security”, IEEE Communications Surveys & Tutorials, Vol.22, No.3, 2020. pp.1646-1685.

[21] Jin-Hee Han, YoungSung Jeon and JeongNyeo Kim, Security

Considerations for Secure and Trustworthy Smart Home System in the IoT Environment, ICTC 2015, pp.1116-1118.

[22] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli and Olivier Mehani, Network-level Security and Privacy Control for Smart-home IoT Devices, In Proceedings of the 8th International Workshop on Selected Topics in Mobile and Wireless Computing, 2015, pp.163-167.

[23] Andreas Jacobsson, Martin Boldt and Bengt Carlsson, A Risk Analysis of a Smart Home Automation System, Future Generation Computer Systems, 56, 2016, 719–733.

[24] Sye Loong Keoh, Sandeep S. Kumar and Hannes Tschofenig, Securing the Internet of Things: A Standardization Perspective, IEEE Internet of Things Journal, 2014, Vol.1, No.3, pp.265-275.

[25] Pranay P. Gaikwad, Jyotsna P. Gabhane and Snehal S. Golait, A Survey Based on Smart Homes System Using Internet-of Things, In Proceedings of the 2015 International Conference on Computation of Power, Energy, Information and Communication, 2015, pp.330-335.

[26] Hailong Feng and Wenxiu Fu, Study of Recent Development about Privacy and Security of the Internet of Things, In Proceedings of the 2010 International Conference on Web Information Systems and Mining, 2010, pp.91-95.

[27] Sowmya Nagasimaha Swamy, Dipti Jadhav and Nikita Kulkarni, Security Threats in the Application Layer in IoT Application”, International Conference on I-SMAC(IoT in Social, Mobile, Analytics and Cloud, 2017, pp.477-480.

[28] Hee-jeong Kim and Jeong Nyeo Kim, “A study of end-to-end message security protocol based on lightweight

- ciphers for smart IoT devices, *Journal of the Korea Institute of Information Security & Cryptology*, Vol.28, No.6, 2018, pp.1309-1317.
- [29] Shivangi Vasho, Jyotsnamayee Ram and Janit Modi, *Internet of Things (A Vision, Architectural Elements, and Security issues)*, *International Conference on I-SMAC(IoT in Social, Mobile, Analytics and Cloud)*, 2017, pp.492-496.
- [30] Jung Tae 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.
- [31] Shachar Siboni, Vinay Sachidananda, Yair Meidan, Michael Bohadana, Yael Mathov, Suhas Bhairav, Asaf Shabtai and Yuval Elovici, *Security Tested for Internet of Things Devices*, *IEEE Transaction on Reliabilities*, Vol.68, No.1, March 2019, pp.23-44.
- [32] Daewon Kim, Jeongnyeo Kim, and Yongsung Jeon, *Common Security Requirement for Device Identification System in Internet of Things*, *Advanced Science and Technology Letters*, Vol.139, 2016, pp.306-309.
- [33] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford and Vijay Sivaraman, *Systematically Evaluating Security and Privacy for Consumer IoT Devices*, *Proceedings of the 2017 workshop on IoT Security and Privacy*, 2017, pp.1-6.
- [34] Mouza Bani Shemali, Chan Yeob Yeun, Khalid Mubarak and Mohamed Jamal Zemerly, *A New Lightweight Hybrid Cryptographic Algorithm for the Internet of Things*, *The 7th International Conference for Internet Technology and Secured Transactions*, 2012, pp.87-91.
- [35] Jung Tae Kim and Hakkee Jung, *Analyses of Attacks Model and Requirement for Smart Home based on Internet of Things*, *ICFICE2017*, pp.100-102.
- [36] Jung Tae Kim, *Analyses of Secure Authentication Scheme for Smart Home System based on Internet of Things*, *IEEE Internal Conference on Applied System Innovation*, 2017, pp.100-104.
- [37] Jung Tae Kim, *Analyses and Security Requirements for Smart Home Network based on Internet of Things*, *The 11th 2016 Internal Interdisciplinary Workshop Series*, 2016. pp.100-104.
- [38] Azzedine Boukerche and Yonglin 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.
- [39] H.Chan, A.Perrig, *Security and Privacy in Sensor Networks*, *IEEE computer*, Vol.36, No.10, 2013, pp.103-105.
- [40] Pranay P. Gaikwad, Jyotsna P. Gabhane and Snehal S. Golait, *A Survey based on Smart Homes System Using Internet of Things*, *In Proceedings of the 2015 International Conference on Computation of Power, Energy, Information and Communication*, 2015, pp.330-335.
- [41] T. Denning, T. Kohno and H. M. Levy, *Computer Security and Modern Home Communication of ACM*, 2013, Vol.56, No.1, pp.94-103.
- [42] Jung Tae Kim, *Analyses of Vulnerability for Healthcare System on Internet of Things*, *The 3rd Asia Workshop on IT Convergence of KIICE2017*, 2017, pp.87-88.
- [43] Changmin Lee, Luca Zappaterra, Kwanghee Choi and Hyeong Ah Choi, *Securing Smart Home: Technologies*,

Security Challenges, and Security Requirements, Workshop on Security and Privacy in Machine-to-Machine Communications, 2014, pp.67-72.

[44] Chakib Bekara, Security Issues and Challenges for IoT-based Smart Grid, *Procedia Computer Science*, 34, 2014, pp.532-537.

[45] Noy Hadar, Shachar Siboni, and Yuval Elovici, A Lightweight Vulnerability Mitigation Framework for IoT Devices, *Proceedings of the 2017 Workshop on IoT Security and Privacy*, 2017, pp.71-75.

[46] Jung Tae Kim, Analyses of Requirement for Secure IoT Gateway and Assessment, *Information*, Vol.19, No.3, 2016, pp.833-840.

[47] Jorge Granjal, Edmundo Monterio and Jorge Sa Silva, Security for the Internet of Things: A Survey of Existing protocols and Open Research Issues, *IEEE Communication Survey & Tutorials*, Vol.17, No.3, 2015, pp.1294-1312.

[48] Jung Tae Kim, "Analyses of Security Issues for Smart Home System based on Internet of Things", *International Conference on Applied System Innovation*, 2016, pp.160-1645.

[49] Elisa Bertino and Nayeem Islam, "Botnets and Internet of Things Security", *IEEE Magazines, Computer*, Feb, 2017, pp.76-79.