International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 14 (2018) pp. 11648-11652
© Research India Publications. http://www.ripublication.com

# Security and Privacy Measures on Data Mining for Internet of Things

**Sung Woon Lee[1], Thokozani Vallent[2], Hyunsung Kim[3]**

*[1]Department of Information Security, Tongmyong University, Korea.*

*[2]Department of Mathematical Sciences, University of Malawi, Malawi.*

*[3]Department of Cyber Security, Kyungil University, Korea. &*
*Department of Mathematical Sciences, University of Malawi, Malawi*

*(Corresponding author)*

## Abstract

Although Internet of things (IoT) bring in a great development in the ubiquitous computing world by virtue of connecting intelligent collaborative objects to the Internet anywhere and anytime, there are still security and privacy concerns on its operations. As IoT is expanding, organizations need to move quickly to building in security and privacy measures in its designed architecture. This study defines security requirements and challenges that are common in IoT and their solutions, ranging from simple things like authentication to trust management. Protecting data during network transit is also very important concern in the measures.

**Keywords:** Internet of things; Security; Privacy; Data Mining

## INTRODUCTION

The emergent growth of technology based on the Internet has led to the booming Internet of things (IoT) concept [1-3]. IoT is a technology where objects around us will be able to connect to each other and communicate via Internet. With the increasing number of applications to the use of IoT, there is a necessity for protecting the security and privacy of various entities involved in the system.

In general the term IoT generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not resembling the normally computers, allowing these devices to generate exchange and consume data with minimal human intervention [4]. The term IoTs is used interchangeably with cyber physical systems (CPS) which refers to the combination of closely integrated physical processes, networking and computation. Thus the potential realization of IoT result into a hyper-connected world which take advantage of advancements and interoperability in: ubiquitous connectivity, widespread adoption of IP-based networking, smart grid, miniaturization, big data and the rise of cloud computing to offer new capabilities previously not possible. It is no secret to expect major transformation in many aspect of the way we live by virtue of adoption and implementation of the new technology. As such IoT is an emerging topic of technical, social, and economic significance for the upcoming technological era. Since IoT is based on network of intelligent devices, it faces the same cyber threat associated with CPS. The main barriers for expansion of the IoT are privacy, security and trust in spite of its myriad benefits. Thus the hyper connectivity of IoT raises the important issues of security and privacy [5-6]. Thus there is an imperative need to achieve the required state of security and privacy to convince consumers into utilizing the technology [7]. The attempt to address the threats would take varied approach including distributed approach designed for IoT environment in which the smart devices themselves are making context-aware authorization decisions. This brings in scenario where the smart device communication would be coupled with an end-to-end authentication, integrity and non-repudiation. Thus the proposed study will seek to provide solutions to the questions.

## IoT SCOPE AND ARCHITECTURE

IoT enables things to be connected anywhere and anytime using any service or network. An easy to implement an IoT system mainly depends on identifying the proper discovery, identification, configuration and manipulation of interconnected devices and sensors [8].

A classification of IoT elements is proposed in [9] from a higher level perspective;

- Hardware: This level includes sensors, central units and built-in communication hardware. Due to the limited resources in sensors, they are usually utilized in sensor networks where multiple sensors are linked together. A central unit in IoTs has ability of storing, processing, and delivering data to users.
- Middleware: It consists of storage and computation tools for data analyses. Cloud computing is the integrity of several traditional technologies such as hardware virtualization, service-oriented architecture, load-balancing, distributed computing, grid computing, utility computing and autonomic computing. It can be considered as a natural step forward from the grid-utility model.
- Presentation: There are visualization and interpretation tools in this level. These tools are designed for various applications and can be accessed from any platform.

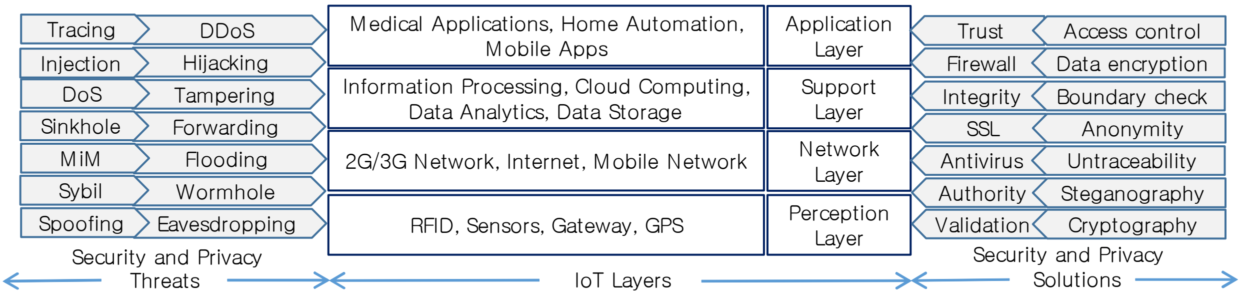

Fig. 1 shows an architecture of IoT, which should be an open architecture using open protocols to support a variety of existing network applications. Likewise, it should additionally incorporate security, adaptability and semantic representation middleware to promote data world integration with Internet [10]. The architecture in Fig. 1 has the following layers:

- Perception layer: The sensor technology, embedded technology, nano technology and tagging technology are located in this layer. It identifies unique objects and collects information from the physical world with the help of its sensors.
- Network Layer: It contains sensor networks, optical fiber communication networks, broad television networks, 2G/3G communications networks, fixed telephone networks and closed IP data networks for each carrier. Transfer of collected data from sensors, devices, etc., to an information processing system is under the responsibility of this layer.
- Support Layer: It works as information processing systems which takes data in one form and processes it into another form. All data are stored in a big database and will be available when there are any demand.
- Application Layer: There are applications in this layer which are developed for user requirements or industry specifications including smart traffic, precise agriculture, smart home, mining monitor, etc.

## SECURITY THREATS OF IoT

This section examines the existing threats in IoT systems as shown in the left side of Fig. 1. Each layer in IoT has their intrinsic threats but this section will just consider the meaning of threats because they are related with each other and it is not easy to classify the threat into any specific layer.

- Spoofing: It is initiated with a fake broadcast message sent to sensor network by the attackers. It makes to assume its originality falsely which makes it appearing from the original source. It is quite often that this scenario is results in the attacker obtaining full access to the system making it vulnerable.
- Signal jamming: It is a type of denial of service (DoS) attack that it occupies the communication channel between the nodes and hinders them from communicating with each other.
- Device tampering: The attacker captures the sensor node physically replaces the node with their malicious node. This type of attack usually results in the attacker gaining total control over the captured node and harms the network.
- Eavesdropping: Wireless characteristics of RFID system make it possible that attacker sniffs out the confidential information such as password or any other data flowing from tag-to-reader or reader-to-tag making the system vulnerable.
- Selective forwarding: In such attacks, malicious nodes do not forward some messages and selectively drop them, ensuring that they cannot propagate later on. The attacker who is responsible for suppression or modification of packets originating from a select few nodes can sometimes forward the remaining traffic not to reveal her wrongdoing. There are different types of selective forwarding attacks.
- Sybil attack: It is clarified as a malicious device illegitimately taking on multiple identities. An attacker can be in more than one place at once as a single malicious node. It presents multiple identities to other nodes in the network reducing the effectiveness of fault tolerant schemes.
- Sinkhole attack: It is defined by intense resource contention among neighboring nodes of the malicious node for the limited bandwidth and channel access. It results in congestion and can accelerate the energy consumption of the nodes involved. With sink holes forming in a sensor network, it is vulnerable to several other types of denial of service attacks.
- Wormhole: This form of DoS attack induces relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunneling of bits of data over a link of low latency.
- Man-in-the-middle attack (MiM): This attack is a form of eavesdropping in which the unauthorized party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information.
- Flood attack: High traffic in channels is the main disrupting effect of this attack which congests the channel with an

unusually high number of useless messages. Basically, a single malicious node sends a useless message which is then replied by the attacker to create a high traffic.

- Tampering with data: The attack appears when a person from the inside tampers the data for personal benefits or commercial benefits of any third party companies.

- DoS Attack: It shuts down the system which results in unavailability of the services.

- Unauthorized access: The attacker can easily infiltrate into the system and damage the system by preventing the access to the related services of IoT or deleting sensitive data. Hence, an unauthorized access can be fatal for the system.

- Sniffer/loggers: Attackers can introduce sniffer/logger programs into the system that take important information from the network traffic. The main goal of the sniffer is to steal passwords, files, and e-mail text.

- Injection: Attackers may enter code directly into the application that is executed on the server. This is a very common attack, easy to exploit, and can cause some bad results such as data loss, data corruption and lack of accountability.

- Session hijacking: This attack reveals personal identities by exploiting security flaws in authentication and session management. This type of attack is very common and effects of attack are really important. With the identity of someone else, attacker can do anything the real user can do.

- Distributed DoS (DDoS): Its working principle is the same as the traditional DoS attack. However, it is executed by multiple attackers at the same time.

## SECURITY AND PRIVACY MEASURES OF IoT

Management of security and privacy at the IoT environment is a major challenging issue as many heterogeneous devices are networked and organized to form big data. This section measures security and privacy shown in the right part from Fig. 1, which are for the solutions to cope from the threats [11-13].

- Privacy: Data privacy means that the user is able to control when, how, and to what limit personal information will be collected, used, and shared. It can affect user confidence and people’s lives. In an IoT environment, connected systems may communicate with each other, transmit collected, treated or control exchanged data. The capabilities of system’s connections during various processes imply many security and privacy issues in the dynamic world of IoT, regarding constraints of maintaining the meaning of the handled information.

- Access privacy: It emphasizes the manner how people can access to personal information. It is important to highlight the need for efficient policies and mechanisms to manage different types of data and fit various situations in IoT contexts. This group may include blocking approaches, lightweight protocols and data sharing, and accessing technique.

- Untraceability: Different communication sessions in IoT associated with the same object should not be linkable. An adversary cannot link the communication activities of a particular object together and thus establish the device’s profile, which contains much private information.

- Location privacy: An object’s current and past location in IoT should not be disclosed to adversaries.

- Context privacy: An adversary should not be able to learn the exact access context information (duration, type of service request, etc.) of an object without the object’s prior approval or knowledge.

- Anonymity: The identity of the origin and/or the destination of a conversation is hidden from adversaries unless it is intentionally disclosed by the object. Anonymity impacts location privacy, because as long as an object is anonymous, location privacy is preserved. Anonymity mechanisms should allow the object to use the IoT services while protecting the identity or other identification information from possible abuse. For keeping the object anonymous, there should not be possibility to link any parameters of the object identity with any context-based information.

- Authentication: It is the process of confirming entity’s identity using a login and additional information to sign in, such as passwords, PIN, smart cards, digital certificates, biometrics, etc. It is used to prevent unauthorized access to resources.

- Access control: An access control system aims to control who can do what on which resource. It assigns and verifies the permission granted to a user allowing him/her (or not) to perform some operation on some resource(s). When designing an access control system for IoT environments, some functional parameters must be considered as delegation support, access right revocation, granularity, scalability, time efficiency, and security.

- Trust: Establishing, negotiating, updating and revoking trust among entities in IoT context is an essential task. The main difficulty to overcome is the engagement of unfamiliar and unpredictable entities during trust mechanism. Due to their heterogeneous and irregular composition, it becomes necessary to define different evaluation of trust for things, humans, and services. To guarantee success in a trust negotiation operation, credentials of involved parties must be exchanged and verified; then mutual trust can be established. Contrarily to classic schemes where trust is built in a centralized manner and prior trust relationships are established, managing trust in dynamic and distributed environment is a very challenging research activity.

IoT enables objects to become active participants. They become able to recognize events and changes in their environment, and react more or less autonomously without human intervention. Computer networks, instead of just being networks of calculators that process data, will become intelligent networks capable of sensing, perceiving and recognizing, acting and reacting, and will continue to evolve towards more autonomy. As illustrated in Fig. 2, in parallel with the increasing autonomy of objects to perceive and act on the environment, IoT security and privacy should move towards a greater autonomy in perceiving threats and reacting to attacks, based on a cognitive, systemic approach [12]. Fig. 2 summarizes three IoT security research axes: efficient security for tiny embedded networks, adaptive, context-aware and user-centric security, and a cognitive, systemic approach to securing the IoT.

**Cognitive and systemic IoT security and privacy**

10. Responsibility and liability enforcement
09. Trust models for the cloud of things
08. Autoimmunity
07. Identification, authentication and credentials managements

**Adaptive, context-aware security and privacy**

06. Security sharing in mobile ubiquitous environments
05. Adaptive security profile and policy management
04. User centric, context-aware privacy

**Security and privacy for tiny embedded networks**

03. Secure protocols for low power lossy networks
02. Scalable and efficient key management
01. Energy efficient cryptography

**Figure 2.** Research axes for IoT security and privacy [12]

An urgent prerequisite for securing IoT is the development of efficient security mechanisms for embedded networks with scarce resources. Current developments demonstrate the resource scarcity of the devices and technologies that will be part of IoT. Consequently, much research work is being devoted to developing efficient, robust and low consumption security and privacy solutions for embedded computing for low power lossy networks.

It is essential to adapt important security and privacy subsystems such as key management, authentication, privacy management and so on.

## REMARKS

IoT is an emerging technology that has attracted a considerable number of researchers from all around the world. There have been major contributions making this technology adapted into our daily life. However, there are lots of key issues addressing security and privacy concerns of IoT and they need more research efforts to be solved.

In this paper, security and privacy measures of IoT were reviewed substantially. Requirements and challenges of security and privacy measures in IoT were analyzed and collected. All kinds of security and privacy threats that may be critical in the IoT in different fields have been discussed and classified with respect to layers of IoT architecture. Finally, the security and privacy directions have been provided for these threats.

## ACKNOWLEDGEMENT

Corresponding author is Hyunsung Kim. This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

## REFERENCES

[1] A. Gorave and V. Kulkarni, "Discrimination Aware Data Mining in Internet of Things (IoT)," International Journal of Computer Applications, vol. 159, no. 3, pp. 39-42, 2017.

[2] L. Loeb, "A Security Protocol for the Internet of Things," Security Intelligence, https://securityintelligence.com/a-security-protocol-for-the-internet-of-things/, 2015.

[3] J. A. Stankovic, "Research Directions for the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.

[4] A. F. Skarmeta, J. L. Hernandez-Ramos and M. V. Moreno, "Decentralized Approach for Security and Privacy challenges in the Internet of Things," Proceedings of 2014 IEEE World Forum on Internet of Things, pp. 67-72, 2014.

[5] K. Rose, S. Eldridge and L. Chapin, "The Internet of Things: An Overview, Understanding the Issues and Challenges of a More Connected World," Internet Society, 2015.

[6] Y. Ashibani and G. H. Mahmoud, "Cyber Physical Systems Security: Analysis, Challenges and Solutions," Computers and Security, vol. 68, pp. 81-97, 2017.

[7] J. Matherly and S. Ridley, "How the Internet of Things is Creating New, Unexplored Territories and The Insecurity of Things," IQT Quarterly, vol. 6, no. 4, pp. 14-20, 2015.

[8] S. C. Arseni, S. Halunga, O. Fratu, A. Vulpe and G. Suciu, "Analysis of the Security Solutions Implemented in Current Internet of Things Platforms," Proceedings of IEEE Grid, Cloud & High Performance Computing in Science, pp. 1-4, 2015.

[9] A. Shawish and N, Salama, "Cloud Computing: Paradigms. Inter-Cooperative Collective Intelligence: Techniques and Applications," Studies in Computational Intelligence, vol. 495, pp. 39-67, 2014.

[10] E. Leloglu, "A Review of Security Concerns in Internet of Things," Journal of Computer and Communications, vol. 5, pp. 121-136, 2017.

[11] H. Kim, "Privacy Preserving Security Framework for Cognitive Radio Networks," IETE Technical Review, vol. 30, no. 2, pp. 142-148, 2013.

[12] A. R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou, "A Roadmap for Security Challenges in Internet of Things,"

Digital Communications and Networks, DOI:http://dx.doi.org/10.1016/j.dcan.2017.04.003.

[13] H. Kim, "Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS," Sensors, vol. 14, pp. 23742-23757, 2014.