Journal of Digital Convergence
Vol. 17. No. 12, pp. 235-241, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.12.235

Research on a New Approach to Enhance IoT Security Using Blockchain Technology

Sunghyuck Hong
Professor, Baekseok University, Division of ICT

블록체인 기술을 이용하여 IoT 보안 강화를 위한 새로운 접근방법 연구

홍성혁
백석대학교 ICT학부 교수

Abstract The structure of the IoT can be divided into devices, gateways, and servers. First, the gateway collects data from the device, and the gateway sends data to the server through HTTP protocol, Websocket protocol, and MQTT protocol. The processing server then processes, analyzes, and transforms the data, and the database makes it easy to store and use this data. These IoT services are basically centralized structures with servers, so attacks on the entire platform are concentrated only on the central server, which makes hacking more successful than distributed structures. One way to solve this problem is to develop IoT that combines blockchain. Therefore, the proposed research suggests that the blockchain is a distributed structure, in which blocks containing small data are connected in a chain form, so that each node agrees and verifies the data with each other, thereby increasing reliability and lowering the probability of data forgery.

Key Words : IoT, Server, Data Security, Blockchain, platform

요 약 IoT의 구조는 크게 디바이스, 게이트웨이, 서버로 나눌 수 있다. 먼저 디바이스로부터 게이트웨이는 데이터를 수집하고, 게이트웨이는 HTTP 프로토콜, 웹소켓 프로토콜, MQTT 프로토콜을 통해 서버로 데이터를 송신한다. 그 후 처리서버에서 데이터를 가공, 분석, 변환, 하며 데이터베이스는 이러한 데이터들을 저장하고 활용을 쉽게 한다. 이러한 IoT 서비스는 기본적으로 서버가 있는 중앙 집중형 구조라는 특징 때문에 전체 플랫폼에 대한 공격이 중앙 서버로만 집중되어 분산형 구조보다 해킹 성공 확률이 높다. 이를 해결하기 위한 하나의 방안으로 블록체인을 결합한 IoT가 개발되고 있다. 따라서, 제안하는 연구는 블록체인은 분산형 구조로 소규모 데이터들이 담긴 블록들이 체인 형식으로 연결되어 각 노드들이 서로 데이터를 합의, 검증하는 단계를 거쳐 신뢰성을 높이고 데이터 위변조 확률이 낮추는 방안을 제안한다.

주제어 : 사물 인터넷, 서버, 데이터 보안, 블록체인, 플랫폼

*This paper was supported by 2019 Baekseok University Fund.
*Corresponding Author : Sunghyuck Hong(sunghyuck.hong@gmail.com)
Received September 16, 2019 Revised October 26, 2019
Accepted December 20, 2019 Published December 28, 2019

1. Introduction

IoT (Internet of Things) refers to the technology of assigning IP addresses to objects and maintaining network communication between people, objects, objects and objects. IoT has been used in many places in our life as a field where the concept has not been developed for a long time and the technology is still developing, such as wearable devices, smart home, autonomous vehicles. With the growth of this technology, the Internet of Things is increasingly gathering a lot of data around our lives, and its security is becoming even more important because of the nature of the data that it contains. However, since the existing Internet has a centralized structure, it has a security problem that it can not be sure whether the data is manipulated centrally or artificially, and it is difficult to respond to risks such as leakage of important data [1].

The composition of this study is as follows. In Chapter 2, we describe the principles of IoT, security loopholes and actual damage cases. In Chapter 3, we discuss the characteristics of block chains and their applications to IoT, examples and examples of IoT platforms using block chains, And the necessity of strengthening security accordingly, and the use of a block chain for this purpose.

2. IoT

2.1 Overview of IoT

2.1.1 Configuring the IoT Architecture

Fig. 1, the components of IoT can be divided into devices, gateways, and servers. Among them, the gateway plays a role of relaying devices that can not directly access the Internet to the Internet [2-4].The server can be roughly divided into three roles, each called a front-end part, a processing part, and a database part. Fig. 2, the front-end part acts as a transmission / reception server. The receiving server receives data from the device and the gateway, and forwards the data to the processing part. The transmission server transmits the data received from the processing server back to the device. Fig. 3 shows a role of gateway briefly.

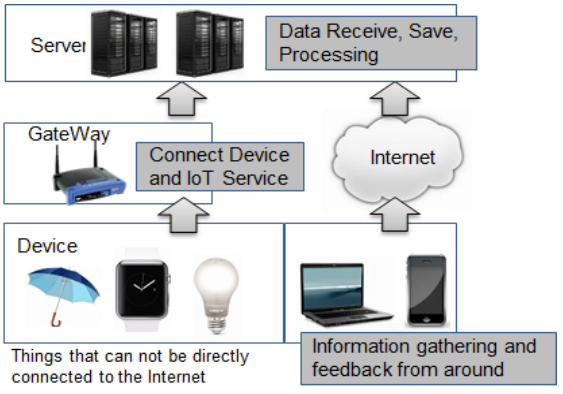

Fig. 1. Configuration of IoT Architecture

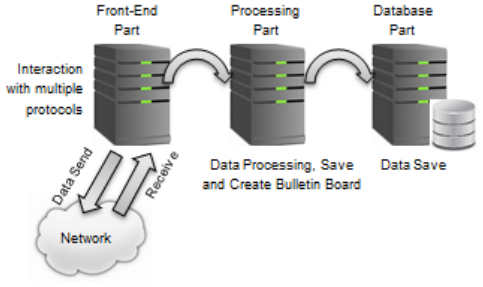

Fig. 2. Configuration of IoT Server

2.1.2 Data Collection Steps

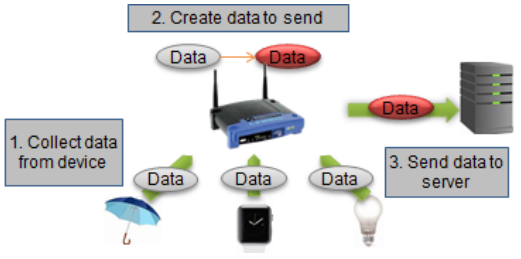

Fig. 3. Role of Gateway

The gateway collects data from the device, which consists of three functions: connection function with device, data processing function, and transmission function to server.

- Connection with devices: Devices and gateways are connected to various interfaces.
- Data processing: Data received from the device is converted into numbers and strings that can be transferred from the gateway to the server, rather than directly to the server.
- Transmission to server: Send data transmission interval and protocol to server according to server side [5].

2.1.3 Data Receiving Step

The receiving server acts as an intermediary between the device and the system for the purpose of receiving data transmitted from the device literally. Methods for transferring data from the device to the server include HTTP protocol, Web socket, and MQTT. Fig. 4 shows HTTP on OSI Application layer.

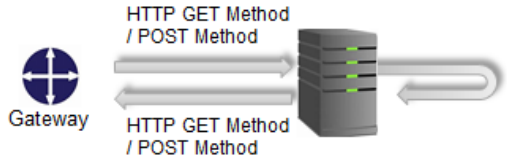

Fig. 4. HTTP Protocol

The HTTP protocol is the most widely used and simple protocol, and the device accesses the server using the HTTP GET or POST method, and sends the data through the request parameter or BODY [3]. Fig. 5 shows a Web-socket protocol which explains bidirectional communication between a getway and server.

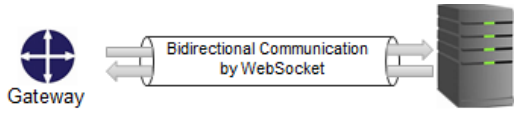

Fig. 5. Web-socket Protocol

The web socket protocol is a communication protocol for realizing socket communication on the Internet, and can continuously transmit and receive data between the browser and the server in both directions. The HTTP protocol has to establish a connection every time data is transmitted, whereas the web socket can continue to send and receive data once the connection is established [6-8].

MQTT is a protocol created by IBM and continues to evolve into open source and is an IoT-specific communication protocol. MQTT allows IoT to communicate with multiple devices. In addition, the MQTT is characterized by its simple message size and protocol structure, which allows it to operate in a narrow bandwidth and low reliability environment [4]. In short, it is a lightweight protocol that is suitable for IoT service. There is also movement to move.

2.1.4 Data processing steps

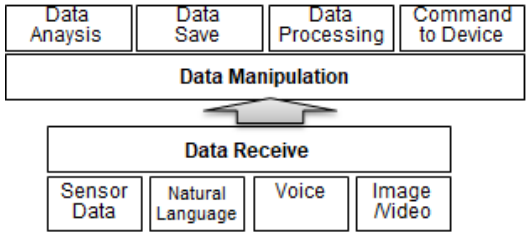

Fig. 6. Data manipulation

The processing server is a part that processes the received data, and it can store the data or convert it easily, and extract new data from the existing data in Fig. 6. There are two representative processing methods for data analysis and processing: batch processing and stream processing. In batch processing, data is first stored in a database, and data is acquired at a predetermined time and processed [9]. Because batch processing is important to process all data within a fixed time, distributed processing based software is used to efficiently process the larger number of data to be processed. Stream

processing processes data arriving at a processing server in sequence without storing data, in contrast to batch processing, which is a method of collecting and processing data at a time.

2.1.5 Data storage step

The database facilitates the storage and utilization of data and also searches for data that matches the conditions. With a database, you can easily find out a single piece of data by combining multiple pieces of data.

2.1.6 Device control step

The transmission server controls the device by transmitting data to the device again. The data transmission method using HTTP, Web socket, and MQTT is used again as a method of transmitting this data.

2.2 Platform based on oneM2M Mobius

We will briefly introduce the structure of Mobius, a platform developed by Korea Electronics and Information Technology Research Institute (KETI) based on oneM2M among various IoT platforms, and in Chapter 3, we propose a simple structure combining block chain with this platform. Mobius is a platform that uses oneM2M. OneM2M is called "M2M", which is a kind of communication between different countries. The structure of the Mobius platform is as follows in Fig. 7.

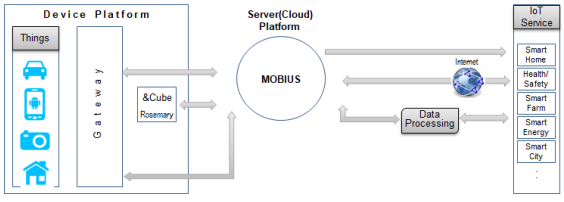

Fig. 7. Structure of Mobius

2.3 Security loopholes in IoT

Due to the centralized nature of the attack, the probability of a successful hacking attack is higher than that of a distributed one [6]. This large number of current IoT platforms is characterized by a centralized structure that is difficult to adequately block network security threats.

2.4 IoT Security Threat Example

2.4.1 Examples of InseCam Sites

There is InseCam with a server in Russia, a website that hacks and broadcasts CCTV all over the world. According to the article, 11,000 CCTVs leaked from the United States were leaked to the website, and Korea came in second with 6536. This leaked CCTV could be hacked as long as it was connected to the Internet. Especially, CCTV is being used in a lot of times, and there is a lot of damage especially in Korea where video is often connected to the Internet instead of outputting through the inside. This is a serious hacking problem because it can be directly linked to invasion of privacy and violent crime [10].

2.4.2 Mirai Malware Cases

In October 2016, a DDoS attack against DYN (Dean), a major DNS provider, resulted in about 1,200 major websites in the United States that were paralyzed for three to four hours. However, IOT devices such as home appliances were used in this DOS attack. This was an attacker who infected the Mirai malware that IoT devices were vulnerable to security threats and exploited them for attacks, using tens of millions of IP addresses for attacks. And this Mirai malicious code has been developed every day and used in a more subtle way [8]. (Security News)

2.4.3 Automobile Test Hacking Example

In July 2015, Andy Greenberg, a reporter for Wired magazine, conducted a smart car hacking experiment with security expert Chris Balak. This hack was a success, but it was to remotely raise the radio sound of a running car, to blow the air

conditioner at maximum wind speed, and to stop the car engine artificially. If we hacked it for the purpose of crime, it could happen any loss of life. As a result, there has been a growing demand for smart car research as well as the preparation of car jacking [9]

3. IoT using block chain

3.1 Public Blockchain & Private Blockchain

Block chaining can be divided into Public Blockchain and Private Blockchain according to network closure. Private Blockchain is an administrator who supervises the usage of each user, and an administrator peer exists, and only a few allowed nodes can join the network [10]. Therefore, it is difficult to say that the administrator has a certain degree of authority and it is a completely decentralized structure. However, since the authorized nodes can agree and manage the data, the security is good. Fig. 8 shows public and private blockchain.

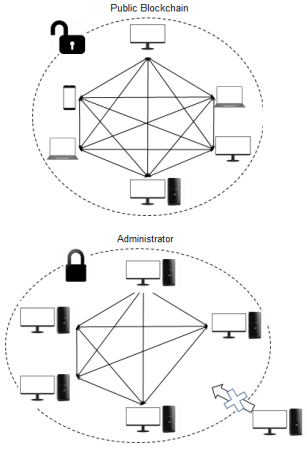

Fig. 8. Public Blcokchain, Private Blockchain

Table 1 below compares the differences between the two.

Table 1. Comparison of characteristics between Public Blockchain and Private Blockchain

	Public Blockchain	Private Blockchain
Decentralized	High	Low
Processing Speed	Low	High
Data Closure	Low	High
Application Field	Virtualized Currency, DNS	IoT

3.2 IoT Platform with Block Chain

The Watson Internet platform receives data from the device using the MQTT protocol, actively analyzes the data, and interfaces with the IBM block-chain platform. Therefore, although it can inherit the advantages of confidentiality and transparency of the block chain, it is incompatible with IoT, which does not conform to IBM's proprietary specifications [11]. IOTA is a block-chain platform developed to solve this problem because the data transaction speed is too slow. 11, the more nodes are generated, the faster the processing speed becomes [12]. However, it also has the limitation that it is not suitable for storing data received from devices on the Internet. Fig. 9 shows general blockchain and IOTA.

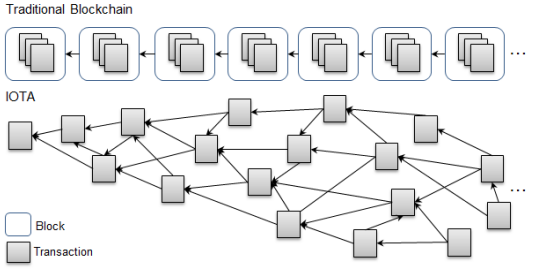

Fig. 9. Traditional Blockchain vs. IOTA

3.3 Reason why Blockchain is secure

Blockchain relies heavily on encryption technology to achieve data security. One very important encryption feature here is hashing. Within the blockchain, these output values, called hashes, are used as unique identifiers for

data blocks. The hash of each block is generated in relation to the hash of the previous block, through which the blocks are linked together to form a blockchain. These hash identifiers play an important role in maintaining blockchain security and immutability. Hashing is also used in the consensus algorithm used for transaction verification. Therefore, blockchain uses a computational infeasible [11-14].

4. Conclusion

As IT technology has evolved day by day, the world is now moving into the fourth industrial revolution. IoT, one of the 4th industrial revolution technologies, is a technology that connects various networks with each other by embedding various sensors and communication devices into one common household objects. It is a collection of private data very closely related to our privacy. And is transmitted and received [15]. If these sensitive data are hacked and leaked, it can lead to crime as well as personal privacy leakage, so the demand for security is increasing with the development of IoT. In this study, we proposed a block chain as one of the security measures. Many companies are now addressing security by combining block chains with IoT security. January 15, 2019 Coindesk will conduct a survey of digital security company Gemalto, which has 950 tech and business professionals around the world, in a recent survey of 2018 IoT block chain From 19 percent to 9 percent. In addition, 91% of companies that do not currently use block-chain technology have the potential to consider accepting this technology in the future [15]. The application of the block chain has just emerged as a security measure in IoT and it is in the early stage of development, so it is a field to be noticed in the future.

REFERENCES

[1] L. Hang & D. Kim. (2019). Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors, 19(10),* 2228. doi:10.3390/s19102228

[2] C. Z. IZhang. (n.d.). Economics of Internet of Things (IoT): Market structure analysis. *Managing the Internet of Things: Architectures, Theories and Applications,* 137-154. doi:10.1049/pbte067e_ch8

[3] J. Freer, B. Beggs, H. Fernandez-Canque, F. Chevrier & A Goryashko. (1995.). Moving object surveillance and analysis for camera based security systems. *Proceedings The Institute of Electrical and Electronics Engineers. 29th Annual 1995 International Carnahan Conference on Security Technology.* (pp. 67-71). doi:10.1109/ccst.1995.524735

[4] Root characteristics of some important trees of eastern forests : A summary of the literature. (1980). doi:10.5962/bhl.title.150066

[5] J. A. Kurtz. (2017). Hacking Wireless Access Points. *Hacking Wireless Access Points,* 93-107. doi:10.1016/b978-0-12-805315-7.00007-3

[6] N. Pathak & A. Bhandari. (2018). Implementing Blockchain as a Service. *IoT, AI, and Blockchain for .NET,* 211-242. doi:10.1007/978-1-4842-3709-0_8

[7] J. H. Jeon, K. Kim & J. Kim. (2018). Block chain based data security enhanced IoT server platform. 2018 *International Conference on Information Networking (ICOIN).* (pp. 941-944). doi:10.1109/icoin.2018.8343262

[8] F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma & A. Jamalipour. (2018). Blockchain in IoT Security: A Survey. *2018 28th International Telecommunication Networks and Applications Conference (ITNAC).* doi:10.1109/atnac.2018.8615409

[9] Y. H. Joh. (2014). A Framework for IoT-Based Convergence Personalized Menu Recommendation System. *Journal of the Korea Convergence Society, 5(4),* 147-153.

[10] H. M. Jung, K. Jeong & H. J. Cho. (2017). A Design for Security Functional Requirements of IoT Middleware System. *Journal of the Korea Convergence Society, 8(11),* 63-69.

[11] H.J. Kim, H. S. Lee, B. J. Choi & Y. H. Kim. (2019). Machine Learning-based Quality Control and Error Correction Using Homogeneous Temporal Data Collected by IoT Sensors. *Journal of the Korea Convergence Society, 10(4),* 17-23.

[12] J. H. Oh & K. H. Lee. (2016). Attack Scenarios and Countermeasures using CoAP in IoT Environment. *Journal of the Korea Convergence Society, 7(4),* 33-38.

[13] M. J. Lee. (2015). A Game Design for IoT environment.

Journal of the Korea Convergence Society, 6(4), 133-138.

[14] C. R. Seo & K. H. Lee. (2016). ARP Spoofing attack scenarios and countermeasures using CoAP in IoT environment. *Journal of the Korea Convergence Society, 7(4),* 39-44.

[15] S. Sun Yoo & S. T. Kim. (2017). Development of Intelligent Gateway for IoT office service in small size. *Journal of the Korea Convergence Society, 8(11),* 37-42.

홍 성 혁(Sunghyuck Hong) **[정회원]**

· 2007년 8월 : Texas Tech University, Computer Science (공학박사)
· 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
· 관심분야 : 블록체인, 사물인터넷 보안, 경량보안프로토콜
· E-Mail : shong@bu.ac.kr