Block chain based data security enhanced IoT Server Platform

Jin Hyeong Jeon
Graduate School of Ajou University
Knowledge Information Security
206, World cup-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do,
Republic of Korea
Jinhyeong9905@gmail.com

Ki-Hyung Kim
Graduate School of Ajou University
206, World cup-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do,
Republic of Korea
kkim86@ajou.ac.kr

Jai-Hoon Kim
Graduate School of Ajou University
206, World cup-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do,
Republic of Korea
jaikim@ajou.ac.kr

***Abstract*— In this paper, we propose a new IoT server platform by introducing a block chain and store sensor data in a block chain. Mobius selected IoT server platform, Mobius authenticates IoT devices conforming to oneM2M standard, receives real-time sensor data, stores information and data in Mysql server and manages it. However, Mysql's Mobius configuration has many vulnerabilities and threats to security, and many of them have not been addressed yet. This paper propose a data storage method by constructing a block chain as a database instead of a general / conventional server construction method such as Mysql server in the server configuration method by introducing such a block chain.**

Keywords*— *IoT; security; Database; Block Chain

I. INTRODUCTION

Mobius is an open IoT server platform that complies with oneM2M standard, authenticates IoT devices, receives real-time sensor data, stores and manages information and data in Mysql server. Recently discovered as a vulnerability of Mysql, the vulnerability is a deodorization method using SQL injection and remote access, utilizing the transmission method using the http protocol ruling.

In this research, we introduce block chains to the IoT platform and use the open source of Ethereum, one of several virtual currencies, to store and manage real - time sensor data in blocks. Propose a new open IoT server platform that does not use Mysql. We also propose a method and structure for storing real - time sensor data in a block by using smart contract in etherium.

II. VIRTUAL CURRENCY BLOCK CHAIN RELATED RESEARCH

A. *Ethereum[4]*

Ethereum is the virtual currency developed by Vitalik Buterin, the platform. It is a virtual currency derived from an existing bit coin. While bit coins concentrate on settlement and transaction related systems, Ethereum transparently passes various applications such as contracts, SNS, e-mails, electronic voting, as well as transactions and settlement based on the core technology blockchain Provide extensibility so that it can act on it. As it is based on BlockChain, these will of course be decentralized applications. Therefore, this is abbreviated as DApp or dApp (deep).[4]

B. *Smart Contract[4]*

The first block chain based smart contract is a bit coin script. Transactions are automatically executed according to the conditions for creating and sending scripts in OPCODE of source language for bit coin transactions. However, bit coin scripts can not use loops, and there is a limit that can not manage information other than the balance of bit coins. Due to the unique structure of the block chain When allowing loops with bit coin scripts, if an infinite loop occurs on the door during script conditions, the entire network can be stopped. Users can easily do DoS (Denial of Service) attacks via infinite loops. Ethereum is a smart contract specialized block chain platform that has come up to overcome the limitations of these bit coin script systems. I have created a smart contract that allows saving and looping of various states which are limitations of the bit coin scripting system. Here, a fee is generated every time each line is executed, the limit of the fee on the network is set, and the infinite loop is prevented. Creating an infinitely repeated condition Running Smart Contract stops when reaching the commission limit in the middle of the spin.[4]

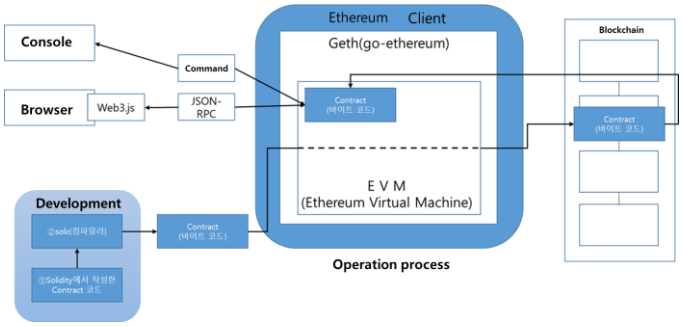

Fig. 1. Ethereum operation process[4]

C. *Mobius IoT Platform server configuration.*

The Mobius platform manages various IoT Device information in order to provide IoT (Internet of Things) service based on oneM2M international standard and combines these IoT Device access control, authentication, user management, multiple IoT services It provides a platform for serving through applications. [7]

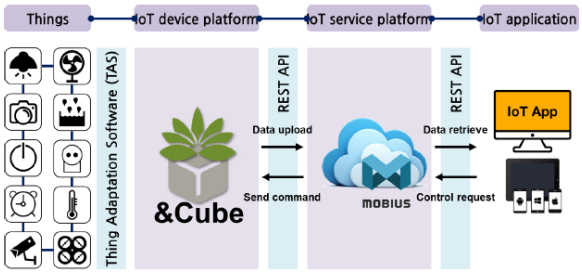

Fig. 2. Mobius basic structure diagram[7]

III. RELATED RESEARCH

A. *IoT security control system[]*

Here propose IoT security control system design based on Secure Pi. It is a new security control system SCC that can monitor the status of Secure Pi. SCC consists of SCC-Client, SCCServer, SCC-Web and Database as shown in [Fig 3]. SCC manager monitors Secure Pi through web browser.

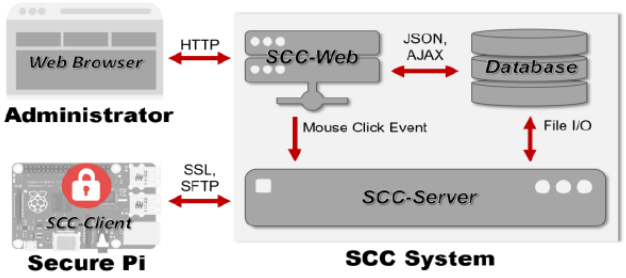

Fig. 3. Structure of SCC System

The proposed IoT security system satisfies oneM2M security requirements and monitors Secure Pi devices based on TPM, a hardware security chip. However, if a vulnerability is found in the database of the server platform where the IoT sensor data is stored, data threats will occur from attackers. In this paper, we propose a new IoT server platform architecture by introducing a block chain instead of the device monitoring system proposed by IoT security control system. We propose a method to prevent data forgery by storing sensor data in a block chain.

IV. MYSQL VULNERABILITY

A recent serious vulnerability in MySQL was discovered in September 2016. As a remote or local attacker, it affects the default Mysql server by manipulating the Mysql configuration file (my.cnf), and it is said to be applied from the moment the DB is rebooted. The vulnerability could also be exploited through authenticated My SQL DB access and SQL injection. If an attacker successfully exploits that vulnerability, it can steal root privileges and trigger arbitrary code. This can result in a complete attacker mastering the DB. The vulnerability is not disclosed in detail. In a number of contexts, exploit CVE-2016-6662 is a remote vulnerability that can be exploited remotely to gain root privileges. It is a vulnerability that is easier to exploit than CVE-2016-6662. CVE-2016-6662, CVE-2016-6663 These two vulnerabilities have not yet been resolved. Mysql is an old database technology, and it is also widely used by general users and service companies. However, as it is heavily used, the vulnerability is likely to occur each time the attacker is exposed to the technology. In this paper, we propose the prevention of forgery and falsification of sensor data and user data based on block-chain in IoT service by using Ethereum network as database instead of general purpose database server such as Mysql.

V. SUGGESTED CONFIGURATION WITH BLOCK CHAIN

In this study, we utilize Etherium as a DB server instead of using the conventional general DB server by utilizing the existing IoT platform server, Mobius, and additionally the Ethernet network. The IoT device information and the sensor data are stored in a block chain of the etherium network to make it more secure and easy to manage. The proposed structure is shown in [Fig 4].

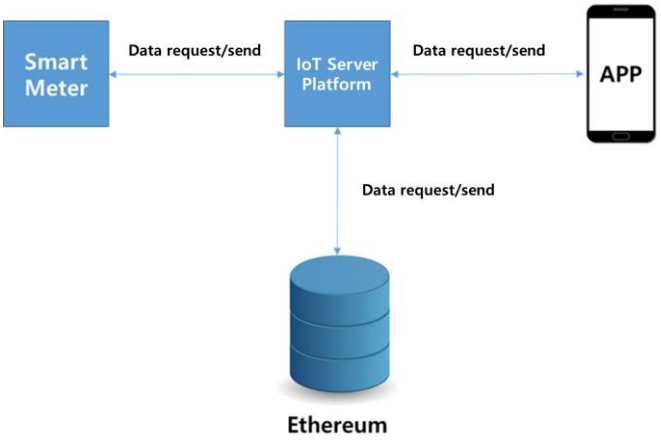

Fig. 4. Suggested configuration with block chain

To use Ethernet as a DB server, you must use Web3.js, a library that can request Ethernet APIs from the IoT server platform. Web3.js can be used to receive smart contracts in Ethernet block chain in real time via Json-RPC. The data is stored in struct information of each user who subscribes in the Android App. In addition, when transmitting data, it confirms the smart meter information that each user has on the smart contract, thus ensuring reliable data. The data storage process is shown in [Fig 5].

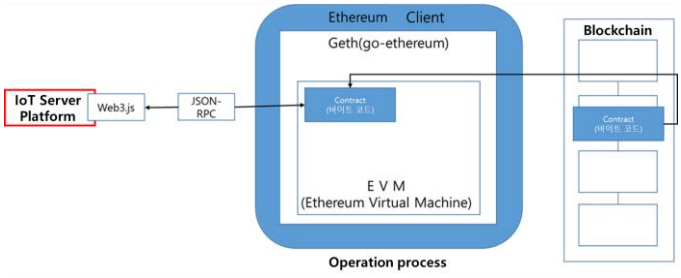

Fig. 5. Data storage process

Through the new IoT server platform that introduces the block chain proposed in this study, the data information is not vulnerable to attacks against the central server such as DD oS attack compared to the existing central server processing through the block chain structure, It also has the advantage of saving costs through storage. Since the block chain has a distributed p2p network, new users have the advantage of being able to communicate without a reliable third party.[2] In addition, since the data is transmitted in the virtual currency trading mode of the block chain, it is difficult to forge data when the packet is leaked, and the data can not be forged even after being stored in the block chain.

Users who have subscribed to the Android APP in this way will have their respective dummy wallet addresses. With the Smart Contract of Etherium, users can request and confirm the sensor data in real time. In addition, smart contracts allow electricity, water and gas Will be able to charge for Android APP. In this paper, we propose a block chain for IoT platform. As a result of using the system proposed in this study, user, IoT device information and sensor data are all resolved in reliability and integrity.

VI. Security Analysis

Using the existing IoT server platform, sensor data is stored on the general-purpose database server in a state that the sensor data is not secure at all. This would allow an attacker to exploit a vulnerability in the database server to attempt to forge or steal data. However, if we use the Block chain based data security enhanced IoT Server Platform proposed in this study, data security is based on block - chain. First, the IoT server platform transmits data to the Ethernet network to store data as shown in [Fig 6].

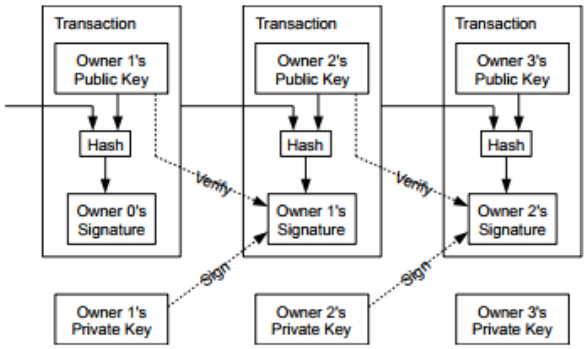

Fig. 6. Data transmission security process[1]

Hash the sensor data of the user's public key at the time of data transfer, and sign the entirety of the transaction details insured by the data with the user's secret key. The public key and secret key are used to prevent forgery and corruption in data transmission.[1]

Second, when a user requests a data, the smartcard evaluates the wallet address of the requested message against the dictionary's registered wallet address to confirm that the data is the user. Therefore, the user can not confirm the information of another user, and the attacker can not confirm the data itself because he does not know the secret key of the users. Finally, sensor data is stored in the actual Ethereum network as shown in [Fig 7].

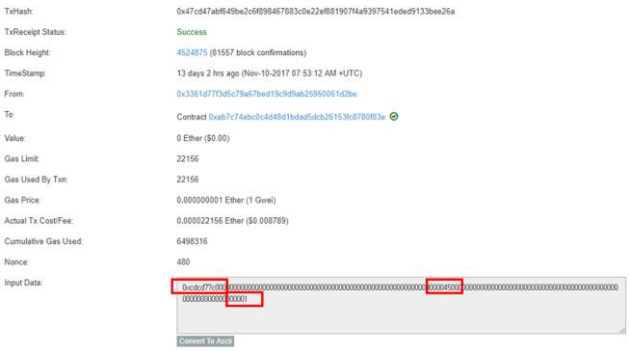

Fig. 7. Status of transaction data

As shown in [Figure 7], when the input data part is hashed in the data transmission, the data is recorded and transmitted in a divided manner, thereby preventing forgery and deodorization of the data.

VII. Conclusion and Future Research

In this research, we introduced a block chain and proposed a public fee system service configuration of IoT platform with enhanced security, and utilized Smart Contract, encryption method and authentication method of Ethereum block chain. In future research, concrete system design and development will be promoted with respect to utility fee system service method of IoT platform with enhanced security, introducing block chain.

ACKNOWLEDGMENT

This study was conducted as a result of the study of the "Future Master of Science Program in the Department of Knowledge and Information Engineering, Employment Contract Type" by the Ministry of Creation Science and the Korea Internet Promotion Agency.

REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Oct 2008.

[2] Antonopoulos, Andreas M, Mastering Bitcoin: unlocking

[3] digital crypto-currencies, OReilly Media, 2014.

[4] Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper.

[5] "Proof of stake versus Proof of work", Bitfury Group, Whitepaper, 2015.

[6] Device authentication in Smart Grid System using Blockchain, Sung-HoonLee, KAIST, 2016

[7] Installation Guide Mobius_v2.0.0_KR, KETI, 2017