Blockchain based Smart Door Lock system

Donhee Han
Department of Electronic Engineering
Sogang University
Seoul 04107, Korea
xsun10x@sogang.ac.kr

Hongjin Kim
Department of Electronic Engineering
Sogang University
Seoul 04107, Korea
chii92@sogang.ac.kr

Juwook Jang
Department of Electronic Engineering
Sogang University
Seoul 04107, Korea
jjang@sogang.ac.kr

***Abstract*—** IoT (Internet of Things) has a large portion of our life. This is manifested by the large number of connected devices. With the exponential growth of IoT devices, IoT security is becoming important. In particular, Smart Door Lock system is extremely important because it is closely related to the safety of the user. However, the data sent and received of existing Smart Door Lock system is vulnerable to forgery and hacking. To improve these security issues, we propose a Smart Door Lock system based on blockchain. Also, this provides data integrity and non-repudiation. Lastly, we propose an algorithm that the Smart Door Lock system judge some situations around itself and operates based on data sent from sensors.

***Keywords*—** Blockchain, Data security, Internet of Things, Smart Door Lock system

I. INTRODUCTION

Home security system is a process for enhancing the quality of resident's life by facilitating a secure environment [1]. Recently, Smart Door Lock system has widely been used as a major part of home security system. Smart Door Lock system is considered as a smart authentication access control based on authenticated person to lock/unlock the door in home [2]. However, in many cases, an intruder has tried to penetrate home by circumventing the lock system [3]. Here in this paper we enhance the security of Smart Door Lock system by using IoT and blockchain technology.

The blockchain is a distributed database of records or public ledger of all transactions that have been executed and shared among participating parties. Each transaction in the public ledger is verified by Consensus of a majority of the participants in the system. Once entered, information can never be erased and it is called Data Integrity [4]. Authentication is that Each transaction is digitally signed using the private key of the participant that made the transaction.

In this paper we propose a blockchain based Smart Door Lock system that can guarantees Data Integrity, Authentication. We also propose an algorithm that how the Smart Door Lock system judge particular events around itself by using data sent from sensors and then operates.

II. BLOCKCHAIN PROPERTIES

A. How a blockchain network runs

Nodes in the blockchain network form a peer-to-peer network by repeating the following process:

1. Nodes interact with the blockchain network via a pair of private/public keys. They use their private key to digitally sign their own transactions and they are addressable on the network via their public key. Every signed transaction is broadcast by a node that creates the transaction [5].
2. The transaction is then verified by all nodes in the blockchain network except the node that creates the transaction. In this step, invalid transactions are discarded. It is called *verification.* (The process of *verification* refers to Section Ⅱ-*B. Verification.)*
3. Each node collects the transactions that have been validated in a certain time into a block and implements a proof-of-work finding a nonce for its block. When a node finds a nonce, it broadcasts the block to all nodes [6]. This is a process called *mining*.
4. All nodes select a block broadcasted for the first time and verify that the block (a) contains valid transactions, and (b) references via hash the correct previous block on their chain. If that is the case, they add the block to their chain and apply the transactions it contains to update their block chain. If that is not the case, the proposed block is discarded. This marks the end of current *mining* round [5].

B. Verification

Blockchain technology ensures the elimination of the double-spend problem, with the help of public-key-cryptography, whereby each node is assigned a private key a public key shared with all other nodes [7]. When a signed transaction is broadcast by a node that creates the transaction, all receiving nodes verify the transaction by decrypting a signature with a public key of a sending node. If a signature verification result is true, the signed transaction is verified that the sending node is not changed.

C. Proof-of-Work

The proof-of-work involves scanning for a value that when hashed with SHA-256. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. In a blockchain network, all nodes implement the proof-of-work for each *mining* round by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later

978-1-5090-4032-2/17/$31.00 ©2017 IEEE

blocks are chained after it, the work to change the block would include redoing all the blocks after it [6]. In this paper, we suggest that the number of zero bits is small to guarantee a real-time blockchain network, about 3 to 4 zero bits are required.

III. DESIGN OF PROPOSED SMART DOOR LOCK SYSTEM

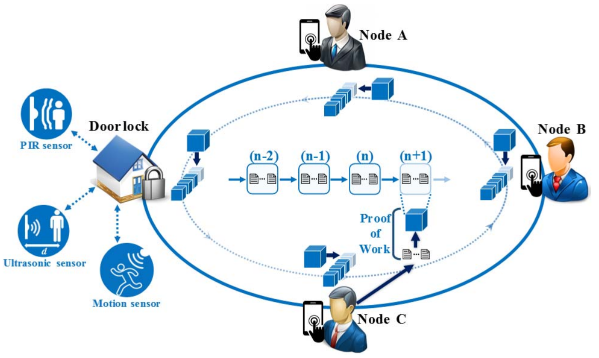

Figure 1. Blockchain based Smart Door Lock system

A proposed Smart Door Lock system is shown in Figure 1. In (n+1) *mining* round, all nodes in the blockchain network try to create a (n+1) block and broadcast it. After that, the first received block is added to their chain. Since all transactions in the block are unchangeable, data integrity is guaranteed by implementing the proof-of-work.

A. Proposed smart door lock

A block diagram of proposed smart door lock is shown in Figure 2. The proposed smart door lock consists of a control module that is a CPU, a door OPEN/LOCK operator that controlled by the control module, a communication module for TCP/IP and Bluetooth/Zigbee communication, a GPS module for measuring a distance, a data storage and three sensors.

A PIR sensor detects a snooper outside the door. If the snooper is detected, then an ultrasonic sensor detects the snooper for measuring a distance between the smart door lock and the snooper [8]. Use of a motion sensor is slightly different from the aforementioned two sensors. It detects an indoor intruder when the smart door lock is in the LOCK state.

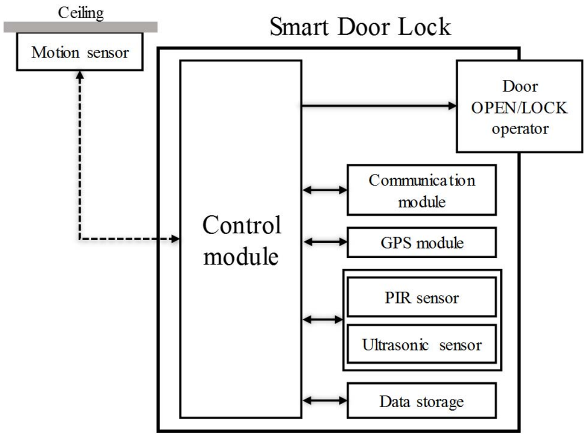

Figure 2. Block diagram of smart door lock

B. Smart door lock OPEN/LOCK control

Algorithm that how a user in blockchain network controls the smart door lock is shown in figure 3. When a smart door lock receives a transaction that contains OPEN/LOCK control message and a GPS information from the user called a node, it begins to verify the transaction whether an authenticated node broadcasted the transaction. This process is to prevent a situation that an intruder circumvents a lock system. If the verification result is true, the smart door lock checks whether the control message is OPEN. The GPS information of the node is used to measure a distance between the smart door lock and the node in case of the OPEN control message. The smart door lock operates according to the control message in two following situations: An authenticated node sent (a) LOCK message or (b) OPEN message and *d* is lower than preset range. Lastly, the smart door lock broadcasts a result of the operation to the blockchain network.

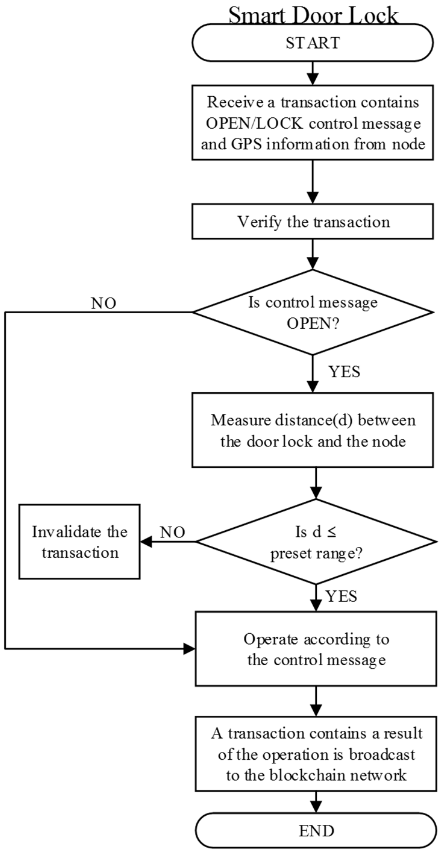
Smart Door Lock
START
Receive a transaction contains OPEN/LOCK control message and GPS information from node
Verify the transaction
Is control message OPEN?
NO
YES
Measure distance(d) between the door lock and the node
Is d ≤ preset range?
NO
Invalidate the transaction
YES
Operate according to the control message
A transaction contains a result of the operation is broadcast to the blockchain network
END

Figure 3. Smart door lock control algorithm

C. Intrusion detection

Indoor intrusion detection algorithm of Smart Door Lock system is shown in Figure 4. When a smart door lock is in the LOCK state, a motion sensor attached to a ceiling detects an indoor intrusion. If an intruder is detected and the smart door lock receives data from the motion sensor for preset time, the smart door lock determines that the indoor intrusion has happened. Lastly, the smart door lock broadcasts a transaction that contains an alarming message to the blockchain network.

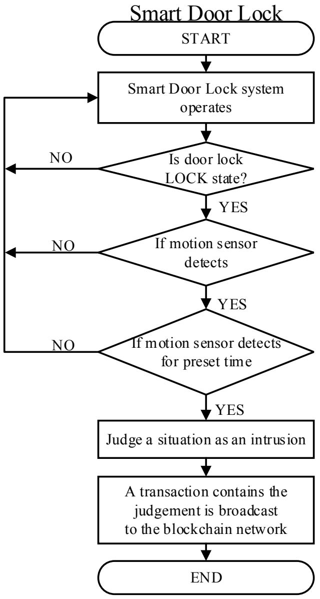
Smart Door Lock
START
Smart Door Lock system operates
Is door lock LOCK state?
NO
YES
If motion sensor detects
NO
YES
If motion sensor detects for preset time
NO
YES
Judge a situation as an intrusion
A transaction contains the judgement is broadcast to the blockchain network
END

Figure 4. Indoor intrusion detection algorithm

Outdoor intrusion detection algorithm of Smart Door Lock system is shown in Figure 5. If PIR sensor detects a snooper outside the door, an ultrasonic sensor detects the snooper for measuring a distance between the smart door lock and the snooper. In next step, if *d* is lower than preset range and the smart door lock receives data sent from the PIR sensor for preset time, then the smart door lock determines that the outdoor intrusion has happened. Lastly, the smart door lock broadcasts a transaction that contains an alarming message to the blockchain network.

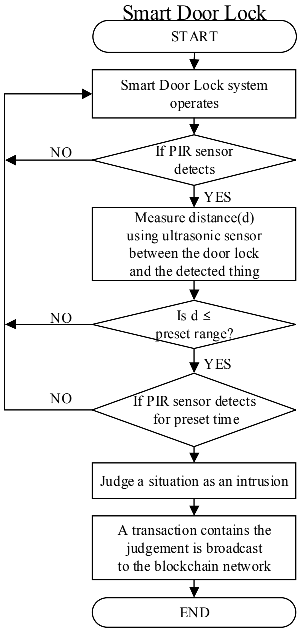
Smart Door Lock
START
Smart Door Lock system operates
If PIR sensor detects
NO
YES
Measure distance(d) using ultrasonic sensor between the door lock and the detected thing
Is d ≤ preset range?
NO
YES
If PIR sensor detects for preset time
NO
Judge a situation as an intrusion
A transaction contains the judgement is broadcast to the blockchain network
END

Figure 5. Outdoor intrusion detection algorithm

IV. CONCLUSION

We have designed the Smart Door Lock system based on blockchain. The blockchain applied to the Smart Door Lock system guarantees authentication, non-repudiation and data integrity. It prevents an unauthenticated user from participating in the blockchain network. Also, three sensors used in this system and smart door lock guarantees that all indoor/outdoor intrusion are detected immediately.

Future works will be carried out to expand blockchain network with applying smart city and also operate directly according to numerous sensor data. So, the proposed system can be configured as a robust network.

ACKNOWLEDGMENT

This research was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. 2015-0-00183, A Study on Hyper Connected Self-Organizing Network Infrastructure Technologies for IoT service)

REFERENCES

[1] S. Solanke, N. Sonawane, V. Ugale and S. A. Khoje, “Home Security Using Image Processing and IOT,” International Journal of Emerging Technologies in Engineering Research, vol. 5, pp. 23–26, June 2017.

[2] Sura Mahmood Abdullah, “Design secured Smart Door Lock based on Jaro Winkler Algorithm,” Tikrit Journal of Pure Science, vol. 21, pp. 154–159, June 2016.

[3] O. Doh and I. Ha, “A Digital Door Lock System for the Internet of Things with Improved Security and Usability,” Advanced Science and Technology Letters, vol. 109, pp. 33–38, August 2015

[4] M. Crosby, Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman. (2015). “Blockchain Technology Beyond Bitcoin,” Sutardja Center for Entrepreneurship&Technology, http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf (accessed June 20, 2017).

[5] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Constracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, May 2016.

[6] S. Nakamoto. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf (accessed June 21, 2017).

[7] M. Pilkington. (2016). “Blockchain technology: Principle and applications,” *Research Handbook on Digital Transformations*

[8] A. Carullo and M. Parvis, “An Ultrasonic Sensor for Distance Measurement in Automotive Applications,” IEEE SENSORS JOURNAL, vol. 1, pp. 143–147, August 2001.