Lee *et al. Hum. Cent. Comput. Inf. Sci.* (2020) 10:9
https://doi.org/10.1186/s13673-020-0214-5

Human-centric Computing and Information Sciences

RESEARCH Open Access

A blockchain-based smart home gateway architecture for preventing data forgery

Younghun Lee, Shailendra Rathore, Jin Ho Park and Jong Hyuk Park*

*Correspondence:
jhpark1@seoultech.ac.kr
Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul 01811, South Korea

Abstract

With the advancement of Information and Communication Technology (ICT) and the proliferation of sensor technologies, the Internet of Things (IoT) is now being widely used in smart home for the purposes of efficient resource management and pervasive sensing. In smart homes, various IoT devices are connected to each other, and these connections are centered on gateways. The role of gateways in the smart homes is significant, however, its centralized structure presents multiple security vulnerabilities such as integrity, certification, and availability. To address these security vulnerabilities, in this paper, we propose a blockchain-based smart home gateway network that counters possible attacks on the gateway of smart homes. The network consists of three layers including device, gateway, and cloud layers. The blockchain technology is employed at the gateway layer wherein data is stored and exchanged in the form blocks of blockchain to support decentralization and overcome the problem from traditional centralized architecture. The blockchain ensures the integrity of the data inside and outside of the smart home and provides availability through authentication and efficient communication between network members. We implemented the proposed network on the Ethereum blockchain technology and evaluated in terms of standard security measures including security response time and accuracy. The evaluation results demonstrate that the proposed security solutions outperforms over the existing solutions.

Keywords: Smart home, Gateway, Blockchain, IoT, Security and privacy

Introduction

The functions and roles of smart homes are continuously developing due to recent developments in Information and Communication Technology (ICT) and Internet of Things (IoT) [1]. According to global market research firm Gartner, the number of smart home devices is projected to grow to 25 billion units by 2020. According to data from Stratecast, the growth rate of the global smart home market is estimated to exceed $7 billion by 2025 [2].

Smart Home refers to a private home that sends and receives data in real-time. It provides automated and intelligent services through various home devices such as TVs, lights, and refrigerators. These machines are part of the home-based communication system between devices and other environments without human intervention

[3]. Users manipulate the use of multiple home products to monitor and control themselves according to user settings based on the home's network configuration. The IoT and network environment of these smart homes are emerging as important factors. In particular, the network structure of the smart home, which is composed mainly of embedded computers, is connected to various IoT devices based on the Internet, the communication is shifting from wired to wireless [4]. Unlike how users operated each device, it is now possible to manage other devices through gateways, both inside and outside the smart home [5]. It is expected that a more efficient and systematic smart home network configuration is possible via the commercialization of 5G, a next-generation mobile communication technology, the convergence of various industries, and hardware development.

However, this change has created a gateway-oriented smart home environment. It is a structure that creates significant security vulnerabilities, as multiple devices in smart homes consist of centralized networks. In some cases, home appliances such as smart TVs and refrigerators, which are the principal components of smart homes, were hacked to send malicious mail such as phishing and spam messages. An instance includes hacking of infant monitoring cameras at home in Texas, U.S.A., to make obscene sounds on the camera [6]. These smart home appliances are often exposed due to the usage of unencrypted passwords on their wireless networks, making them the main target of hackers as a medium for DDoS attacks [7]. These problems are due to a centralized IoT system structure, and security threats are growing with the spread of the IoT era, including data forgery and tampering, access to unauthorized devices, and incorrect device control through attacks on server and gateway systems for IoT services [8, 9].

Therefore, smart home gateway networks with centralized structures should be efficiently and securely configured. An attacker can exploit a gateway's vulnerability to tampering with data generated by the gateway. Confidentiality and integrity of data must be ensured, and the availability and latency of the services offered to users in the smart home network should be considered while meeting additional security considerations. The scalability and manageability of systems should also be considered to accommodate the complexity of smart home networks.

Recently, Blockchain is employed in many next-generation applications and has become a desirable approach to provide security on a wide range of platforms, such as IoT, smart city, and many more [10]. The main reason for this, the blockchain provides decentralized and trust-free solutions, wherein online-distributed ledgers are used store data across the network in a decentralized manner. The distributed ledger provides the applications to operate in a decentralized manner without relying on a trusted or centralized intermediary. With the help of blockchain, data are exchanged in a verifiable manner among untrusted individuals that are connected in a peer-to-peer network. In the smart home, the gateway can be configured employing blockchain technology wherein data can be stored and exchanges in the form blocks of blockchain to support decentralization and overcome the problem from traditional centralized architecture. Since, data in the blockchain are exchanged in the decentralized and encrypted form, which support security requirements of confidentiality, integrity, and authentication in the smart home gateway.

Research contribution: The main contributions of the research work includes:

- We propose a blockchain-based smart home gateway network architecture to mitigate the recent challenges in existing centralized security network architecture and to counter possible attacks on the gateway of smart homes.
- We implement the proposed decentralized architecture on the Ethereum blockchain technology to support security requirements of confidentiality, integrity, and authentication in the smart home gateway.
- The performance of the proposed architecture is compared with the existing centralized security architecture. A security analysis is carried out to validate the performance of our proposed architecture.

In this paper, the proposed architecture is applied to the gateway of the existing centralized smart home by utilizing blockchain technology and proposes countermeasures against identified vulnerabilities. ID and data management for smart home gateways allow the identification and necessary information of the gateways to be recorded on blocks in the blockchain and are compared from time to time. Devices connected to a smart home network, register only those devices that are certified on the gateway. It is adding this information to blockchain blocks from time to time to identify the correct device and handle it through cryptographic communications, preventing data transmission from being leaked. The architecture classifies low data entering the gateway so that the required data can be hashed, encrypted, and stored in the internal database. Therefore, in this paper, we ensure confidentiality, integrity, and authentication, which are essential security properties required in smart home gateways. The paper identifies the flow of data at the center of the smart home gateway and includes scenario configurations and security considerations for various attacks on the proposed network.

The rest of the paper is structured as follows: "Related work" section introduces the key technologies, considerations, and previous relevant studies of blockchain-based smart home gateways. "Blockchain-based smart home gateway network" section presents the network architecture of the proposed blockchain-based smart home gateway. "Experimental analysis" section analyzes the proposed network in terms of security and efficiency of the system, and "Conclusion" section presents the conclusions of this research.

Related work

Core technologies

In this section, we will discuss core technologies that are employed to provide smart home gateway architecture for preventing data forgery.

Blockchain

Recently, blockchain technology is used in various industries, including finance, distribution, health care, and energy. Blockchain was selected as one of the key technologies to lead the fourth industrial revolution era at the 2016 World Economic Forum. Global market research institutes, Gartner, and Deloitte also selected Blockchain as one of the 2017 technology trends [11]. Blockchain is a well-known, distributed ledger technology. It can overcome the limitations of indirect and passive confidence guarantees held by traditional centralized systems and implement a decentralized system

that can assure users a direct and active trust relationship. Blockchain can be easily applied and integrated in various industries, and the integrity of the block ensures the integrity of the data [12]. Blockchain consists of a digital ledger that records transaction information that occurs on the network and is shared among network members [13]. A copy of the Ledger is distributed among each network member. When a new transaction occurs, it is authenticated with the consent of all members. The Blockchain consists of multiple blocks, which contain a number of transaction information. Since numerous blocks are chained together to form an entire blockchain, it is not possible to arbitrarily change specific data. Blocks match the data held by a majority of all users, where more than 51% of all users are identified as genuine blocks. If data of any block is modified or missing, it is easily restored as ledgers store a hash value data. It is practically impossible to change a ledger based on single transaction information. Modifying data requires hacking into a minimum of 51% of all blocks at the same time. Since distributed ledger technology is open to all members of the network, all new information is updated in real-time, and it is easy to trust and trace information. Eliminating the presence of intermediaries based on a distributed peer-to-peer network approach and without relying on traditional centralized systems increases the efficiency and transparency of transactions. It creates a fast and secure network environment at a lower cost [14]. Based on the P2P network, Blockchain is connected to an equal layer by all users, acting as a server and simultaneously as a client. This can address the problem of a server-client architecture in which multiple users are connected and managed through a centralized server in an existing network system [15].

Smart home gateway

A number of technologies for smart homes grafted as interest in the residential environment is growing due to technological development. Smart Home refers to a residential or living environment equipped with technologies that can automatically control devices and systems [16]. Managing these environments has many variable conditions, such as costs, residents' preferences, and types of buildings depending on technology. A network structure that can automatically adjust temperature and security levels, and communicate efficiently inside and outside smart homes, can provide residents with a wide range of living environments, increasing their satisfaction [17]. The gateway for devising these networks provides functionality for the following concepts:

- A variety of home network connection.
- Home Network and Internet Connections.
- Remote control and diagnosis of home appliances.
- Flexible mechanisms for software expansion and update.
- Reliable and secure remote operation method.

The implementation of these gateways aims to create a sustainable smart home that can create additional value while addressing the various vulnerabilities of existing smart homes.

Smart home gateway security considerations

Multiple devices collectively make up the smart home is controlled and monitored by communicating through the gateway [18]. Such a network configuration could expose the data in the house, result in privacy breaches, cause device malfunctions, and harm users. When a user is exposed to a smart home network implemented in each household, data collected by devices in a targeted format can be leaked [19]. There are difficulties in bringing different heterogeneous devices together in the absence of security standards for smart homes and devices. For this reason, various services cannot be provided to users smoothly. Security for gateways is essential, and the following describes the security requirements for gateways in smart homes.

- Confidentiality: Networks configured in smart homes, collect and store multiple data, including sensitive information from residents. Access to this data should be accessible only by authorized personnel and is an essential element of security for smart homes. To be confidential to the characteristics of smart homes, we use blockchain with an encryption algorithm and configure it using a key [20].
- Integrity: When data is sent and received between each configuration, no falsification shall occur during the data transmission. The hash function reduces the likelihood that these data will be falsified and allows the tracking and checking of precisely what data is recorded.
- Authentication: The function of authentication in smart home network configurations prevents an attacker from acting maliciously within a normal network from outside. Blockchain is used to verify that the network is a valid member and can take advantage of the ability to check it at a specific time to enable the correct smart home network configuration [21].

Existing research

Sivaraman et al. [22] investigated and analyzed security vulnerabilities in the smart home network layer and proposed solutions. It is possible to manage and verify the certified devices using the ISP and to operate the smart home devices even in the external internet environment. However, this approach is not efficient to provide security to internal internet environment due to lack of users data for analysis. Copos et al. [23] checked the flow of the house and the absence of confidential data using Wireshark for devices such as fire detectors during the construction of smart home devices. This approach provide a software specific solutions but it can not be comptitible with other software rather than wireshark.

Lee et al. [24] proposed an update that manages firmware updates of embedded devices using blockchain, authentication using digital signatures, and applies encryption algorithms using private keys. This mechanism does not provide security solution to a small smart home wherein small number of embedded devices are connected to each other. Bull et al. [25] proposed a gateway allowing centralized control and configuration using SDN (Software Defined Networking) in consideration of the means to provide flexible and secure communication for the rapidly increasing

number of IoT-based devices. The proposed gateway relies on centralized methodology which can be result in the problem of a single point of failure. Yin et al. [26] combined the privacy protection scheme with machine learning and proposed a novel security approach based on human-centric computing. However, this approach is less efficient in case of the unavailability of enough training data to produce machine learning model. Panwar et al. [27] discussed various security threats and their solutions in smart home. They provided a comprehensive overview of smart home security in terms various attacks statistics. Poh et al. [28] presented a privacy-preserving approach, PrivHome. It provides authentication, secure data storage and query for smart home systems. It learns and modifies the data communicated among the user, gateway, service provider, and the device to support data authentication and confidentiality. Shouran et al. [29] presented the impact of various security attacks on smart home and evaluated their impact as a low, moderate, and high to appropriate solutions for their mitigation.

The other security approaches rely on the IoT and cyber physical system security wherein various emerging technologies, such as blockchain, software defined network, and deep learning are employed [30–32].

Blockchain-based smart home gateway network

Proposed network configuration

Blockchain applied to smart home gateways is a crucial part of data transmission authentication with integrity and confidentiality between devices and other media. Although Smart Home Network has a centralized network form in each Smart Home, it was applied as a centralized to a distributed network by using blockchain at the cloud layer.

A smart home gateway based on the proposed blockchain has three layers, the device layer, gateway layer, and cloud layer. The first layer, device layer, consists of sensors and devices that collect and monitor data in the smart home network environment through various heterogeneous IoTs that are configured in a smart home. The second layer, gateway layer, stores the data generated by the Device Layer and provides it to users as needed. The third layer, the cloud layer, registers the ID for the gateway and the data processed by each gateway in the blockchain. The blocks are shared so that users can be provided with information anytime and anywhere. This can be expressed as shown in Fig. 1.

Figure 2 shows the FlowChart for the proposed architecture, which allows data from devices at the end to be collected, registered in the blockchain, and presented to users appropriately. For the data to be collected and provided to the user, the collected data undergoes hash value processing and formatting, create blocks, and verifies them periodically to maintain integrity even if data falsification occurs. Data analysis and quality maintenance should be carried out continuously to provide users with only the necessary information.

Identifying gateway devices and collecting data

IoT devices configured in smart homes are connected to one gateway, and to each device, an ID is assigned. These gateways and devices have fixed IDs and have the computing power to operate encryption and decoding algorithms with PKI and

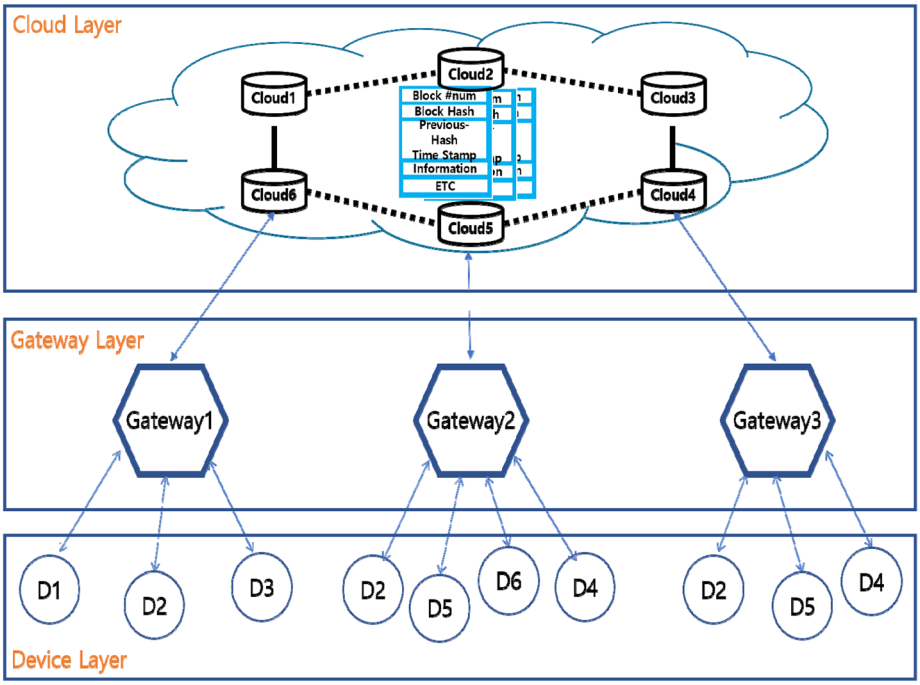

Fig. 1 Design overview of proposed network

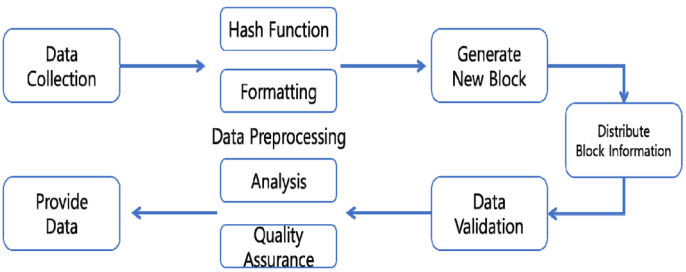

Fig. 2 Methodological flow of blockchain based cloud-enabled architecture for smart home gateway

SHA2. The certification registration and data storage processes for device and gateway interconnection protocol processes are as shown in Fig. 3.

1. Devices certified to a gateway must always be verified periodically. The Dn in the device layer attempts to register directly with or automatically connects to the gateway. The gateway requests an ID from the device that is connected or requested to obtain information about the connected device.
2. The device's gateway implements a cryptographic algorithm to encrypt the gateway information to the device and sends the message. Devices with the help of pre-shared keys decode encrypted messages.
3. Encrypted messages containing gateway information are decrypted and requested to the unregistered or unencryptable gateway when they are received.

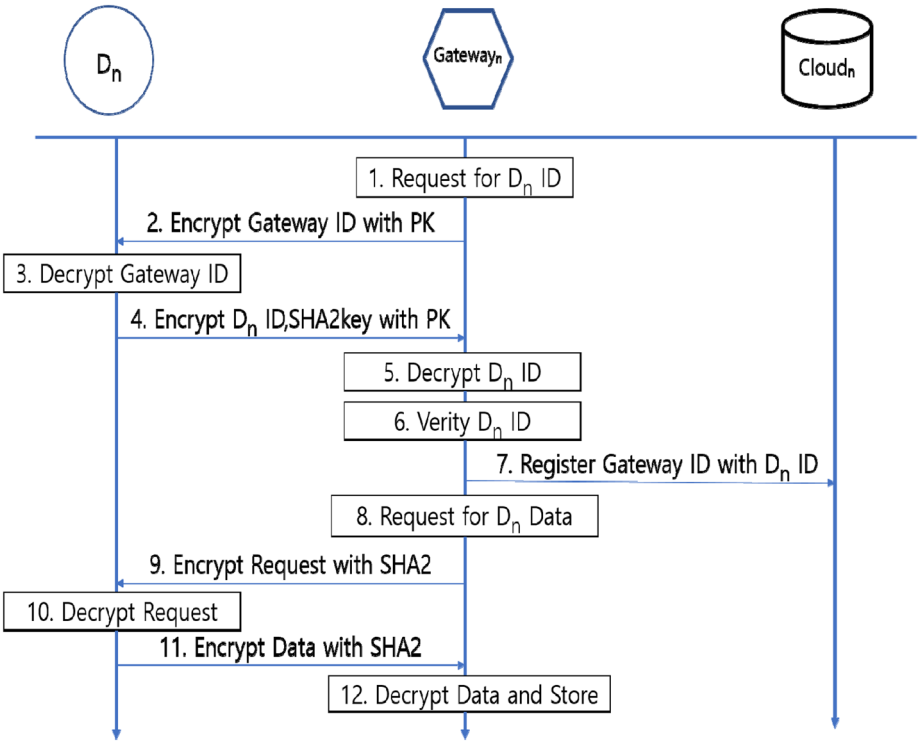

Fig. 3 Device identification and data collection

4. To share the SHA2 encryption algorithm key for continuous communication between devices and router, we encrypt device ID and SHA2 key to send messages to gateway.

5–6. The gateway decodes the transmitted messages to verify that they are registered as normal devices.

7. Once the identification procedure between the gateway and the device is complete, we store the device ID registered on the gateway in the cloud. The gateway communicates with the cloud over time to update the device ID list.

8. To collect data generated by the device, the gateway creates a request message and sends it to the device.

9. Data request messages are encrypted through the key of the SHA2 password algorithm that was validated in the previous process.

10–11. Data transfer using the device is asked to give a key to an encrypted message decoding and encryption gateway to transmit to the raw data.

12. The gateway stores the received raw data by decoding it

Gateway data management using blockchain

A network made up of blockchains guarantees the integrity of the data transmission process and records. Data generated from the end nodes participating in the network or stored in the database can be stored using the SHA-3 hash algorithm based on the

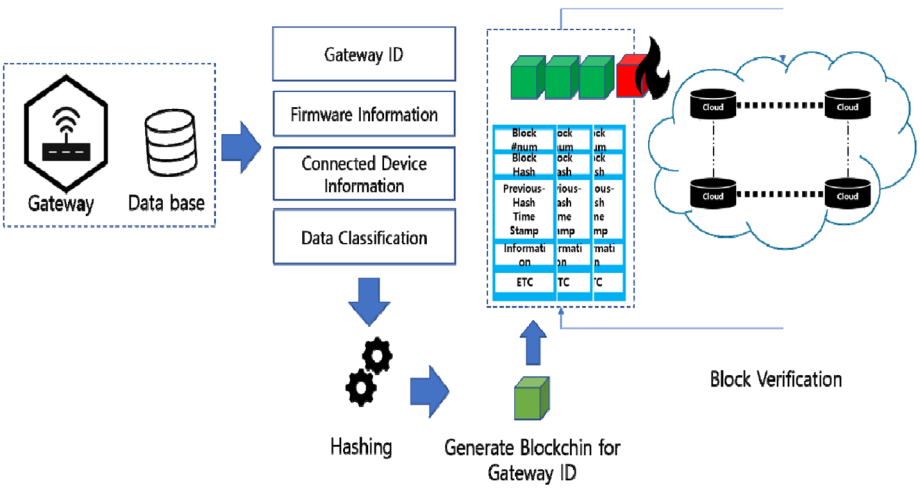

Fig. 4 Blockchain based gateway data management

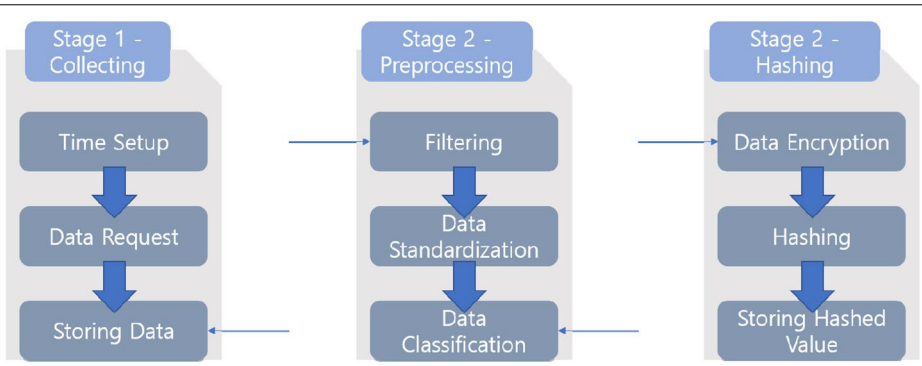

Fig. 5 Gateway data preprocessing

necessary information generated. These blocks are compared in real-time on a blockchain network in the cloud. They verify data by detecting if there is a forged blockchain. The blockchain registration and monitoring process of these gateway data can be expressed in the following Fig. 4.

Preprocessing data inside the gateway

Data generated from heterogeneous IoT devices in the smart home is transmitted to the smart home gateway consisting of various sizes and data types. The smart home gateway of the proposed architecture needs to accurately control IoT and process data according to the user's request. Figure 5 describes the process of data transfer from IoT to the smart home gateway, where data processing is divided into three categories: collection, preprocessing, and hashing.

- Stage 1. Collecting: Data generated by the device is communicated with the router for a specific time. When new data is needed at the gateway or when an event occurs, data is requested from the device. Raw data is then sent and stored in the storage device at the gateway.

- Stage 2. Preprocessing: Raw data sent from the device is preprocessed inside the gateway. For the efficiency of storage space, it filters and stores only the data needed by the router based on device ID and is stored using the standardization and classification process.
- Stage 3. Hashing: Data generated in the smart home contains sensitive information of the user so that it can be managed through encryption. The SHA256 algorithm is applied based on the password specified by the user, and the common data of the device is stored through the hash function.

Experimental analysis

This section provides the implementation of the proposed architecture to validate its performance. In implementation, the open vSwitches and several functional nodes, such as IoT devices are emulated by using Mininet [30] as an emulation environment. The Mininet was set up on the Linux server by employing 10 desktops wherein an Intel i7 processor and a 64 GB DDR3 RAM configures in a desktop. The gateways were configured by running the SDN controllers in separate VMs hosted on a Linux server [33]. The cloud server was configured by employing Amazon EC2 cloud data center [34]. The proposed architecture employed the Ethereum blockchain technology to support decentralization. In the blockchain configuration, the Ethereum Bridge in the broadcast mode [35] were used for employing an oracle in the private chain. The DApp was deployed and compiled using the Truffle development suite.

In the evaluation, the performance of the proposed network architecture was compared with the centralized network architecture. The centralized network architecture was implemented by employing security measurement at the Amazon EC2 cloud data center whereas the security measurement in the proposed architecture was carried out at the gateway layers. The performance comparison is illustrated in Figs. 6, 7 wherein standards evaluation metrics of the security response time and accuracy were measured with the variation in the quantity of data traffic. It can be clearly observed from Fig. 6 that the proposed network architecture outperformed over the traditional centralized architecture. It is due to the proposed architecture employed the blockchain at the gateway layer that

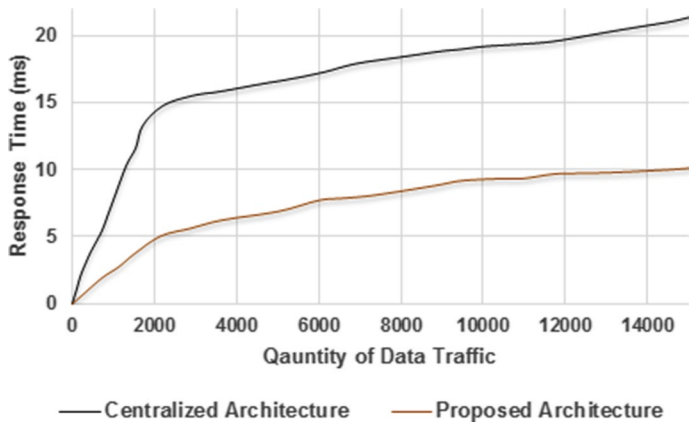

Fig. 6 Measurement of security response time with the variation in the quantity of data traffic

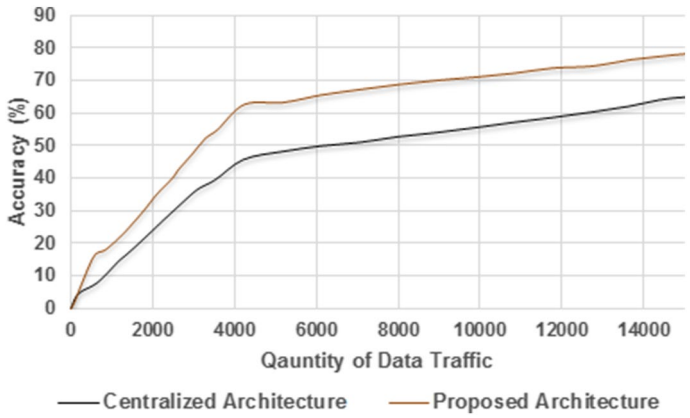

Fig. 7 Measurement of accuracy with the variation in the quantity of data traffic

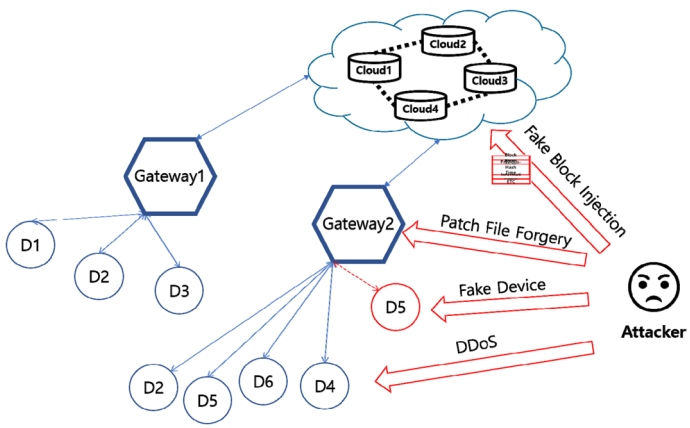

Fig. 8 Attack scenarios on proposed architecture

further provides faster response and more accurate to security measurement as gateway is closer to IoT device than cloud. The more accurate security measurement of proposed architecture demonstrates that blockchain employed in it is effective to preserve the security requirements of confidentiality, integrity, and authentication in the smart home.

Security analysis: Attack techniques on existing smart home gateways are continually changing as the environment changes to the network and the IoT. Especially, IoT devices have limited computing power and battery capacity. In this network environment, an attacker can set various attack scenarios according to the target device. Figure 8 shows the attack scenario for the proposed smart home gateway architecture.

Patch file forgery attack: A forgery attack against a patch file is a method of attacking a specific device through a connected router or the patch file itself [36]. In the proposed architecture, if a patch is applied to a device through a tampered patch file, it can result in device malfunction, permission change, eavesdropping, and data deletion. The proposed architecture ensures the integrity of centrally distributed patches for batch updates of devices and strengthens the security of the management server itself.

ZeroDay Attack: Zero-day attack is a technique that attacks when a patch for a software vulnerability is not available [37]. Because of the lack of countermeasures possible against such vulnerabilities, such attacks cannot be prevented, and any device

can be compromised. The proposed architecture supplements with periodic security updates, whitelists and blacklists, and blocks attacks through real-time monitoring of changes.

Blockchain 51% Attack: It is a hacking attack that attempts to profit by manipulating transaction information after securing more than 50% of the hash nodes of the entire blockchain nodes [38]. In other words, a 51% attack means that a malicious attacker has powerful hash computing power in excess of 50% of the whole network. The attacker can create new blocks and add them to the blockchain network faster than other honest nodes so that other nodes can store forged data. The attack forces other blocks to adopt a blockchain that contains forged data. However, in order for the 51% attack to succeed in the proposed blockchain-based architecture, the hash power of all nodes participating in the blockchain network must be greater than the sum of the hash computation power. In addition, the number of nodes participating in the architecture increases, which can effectively defend against attacks. Therefore, the blockchain 51% attack on the proposed blockchain-based architecture is impossible.

DDoS: Distributed Denial of Service (DDoS) attack results in the disruption of services provided by a server by flooding it with traffic from compromised devices [39], [40]. If an attack occurs on an existing centralized smart home gateway network, authentication and integrity services are stopped. The proposed architecture prevents DDoS traffic during data processing by not providing loops such as If/While/for in basic IoT request scripts. Applying the resource consumption limit of blockchain, the attacker can not proceed indefinitely. In addition, DDoS attacks on the entire blockchain network are impossible on all nodes at once. This depends on the environment in which the nodes are distributed. Finally, we compared our proposed work with the existing work in terms of security architecture, methodology, research gap, and proposed approach to validate significance of our research (Table 1).

Table 1 Summary of comparison of our research work with existing works

Research work	Security architecture	Methodology	Research gap	Proposed approach
Sivaraman et al. [22]	Centralized	Manage and verify the certified devices using the Internet Service Provider	Does not provide security to internal internet environment due to lack of user's data for analysis	Employ blockchain to manage and verify the certified devices
Copos et al. [23]	Centralized	Check the flow of confidential data using Wireshark for devices	Provide a software specific solution	Does not use any software like Wireshark
Lee et al. [24]	Centralized	Manages firmware updates of embedded devices using blockchain	Does not provide security solution to a small smart home wherein small number of embedded devices are connected to each other	Provide a scalable solution using blockchain
Bull et al. [25]	Centralized	Employ centralized control and configuration using SDN to provide flexible and secure communication	Can be result in the problem of a single point of failure	Support a decentralized solution using blockchain

Conclusion

In this paper, we proposed a blockchain-based data tamper-proofing gateway architecture for the existing smart home gateway environment and IoT. This architecture provides the following solutions to minimize the confidentiality, integrity, and authentication issues of the heterogeneous IoT and centralized gateways that make up the smart home. The SHA2 encryption algorithm is applied to solve the confidentiality and authentication problems that occur in smart home gateway and heterogeneous IoT. In addition, blockchain technology is used to maintain the integrity of data stored in the gateway. The data transformation algorithm is implemented in the architecture by efficiently shaping raw data. Three considerations and scenarios are presented to analyze the proposed architecture over existing research, which demonstrates the effectiveness of the proposed architecture over previous studies. However, our proposed network architecture has some limitation in teams of additional computational complexity by blockchain operation. The proposed work can be enhanced by employing the concept of mobile edge computing to offload the computation.

Acknowledgements
The authors thank everyone for their support and review for this study.

Authors' contributions
YL and SR conceived of the presented idea. YL designed the proposed framework, performed the security analysis. YoL, JiHP and SR discussed the related works, drafted the manuscript. JoHP supervised the research. All authors discussed the results and contributed to the final manuscript. All authors read and approved the final manuscript.

Funding
This study was supported by the Research Program funded by the SeoulTech (Seoul National University of Science and Technology.

Availability of data and materials
Not applicable

Competing interests
The authors declare that they have no competing interests.

Received: 29 December 2019 Accepted: 29 January 2020
Published online: 17 March 2020

References

1. Sun, R., Xi, J., Yin, C., Wang, J., Kim, G. J. (2018). Location privacy protection research based on querying anonymous region construction for smart campus. Mobile information systems, 2018
2. Robles RJ, Kim TH, Cook D, Das S (2010) A review on security in smart home development. Int J Adv Sci Technol 15:13–22
3. Park JH, Salim MM, Jo JH, Sicato JCS, Rathore S, Park JH (2019) CIoT-Net: a scalable cognitive IoT based smart city network architecture. Human Compu Inf Sci 9(1):1–29
4. Wang J, Gao Y, Liu W, Sangaiah AK, Kim HJ (2019) Energy efficient routing algorithm with mobile sink support for wireless sensor networks. Sensors 19(7):1468–1494
5. Mittal Y, Toshniwal P, Sharma S, Singhal D, Gupta R, Mittal VK (2015) A voice-controlled multi-functional smart home automation system. In: 2015 Annual IEEE India conference (INDICON), 2015
6. Schiefer M (2015) Smart home definition and security threats. In: 2015 ninth international conference on IT security incident management & IT forensics, 2015
7. Xiong B, Yang K, Zhao J, Li K (2017) Robust dynamic network traffic partitioning against malicious attacks. J Netw Comput Appl 87:20–31
8. Pongle P, Chavan G (2015) A survey: attacks on RPL and 6LoWPAN in IoT. In: 2015 international conference on pervasive computing (ICPC), 2015
9. Gu K, Yang L, Yin B (2018) Location data record privacy protection based on differential privacy mechanism. Inf Technol Control 47(4):639–654
10. Sharma PK, Rathore S, Park JH (2018) DistArch-SCNet: blockchain-based distributed architecture with li-fi communication for a scalable smart city network. IEEE Consum Electr Mag 7(4):55–64
11. PR Wire (2016) Gartner: blockchain and connected home are almost at the peak of the hype cycle. https://prwire.com.au/pr/62010/gartner-blockchain-andconnected-home-are-almost-at-the-peak-of-the-hype-cycle. Accessed 28 Dec 2019

12. Sharma PK, Moon SY, Park JH (2017) Block-VN: a distributed blockchain based vehicular network architecture in smart city. JIPS 13:184–195
13. Sanchez I, Satta R, Fovino IN, Baldini G, Steri G, Shaw D, Ciardulli A (2014) Privacy leakages in smart home wireless technologies. In: 2014 international carnahan conference on security technology (ICCST), 2014
14. Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B (2017) Blockchain technology innovations. In: 2017 IEEE technology & engineering management conference (TEMSCON), 2017
15. Rathore S, Pan Y, Park JH (2019) BlockDeepNet: a Blockchain-based secure deep learning for IoT network. Sustainability 11(14):3960–3974
16. Chandramohan J, Nagarajan R, Satheeshkumar K, Ajithkumar N, Gopinath PA, Ranjithkumar S (2017) Intelligent smart home automation and security system using arduino and Wi-fi. Int J Eng Comput Sci (IJECS) 6:20694–20698
17. Chen M, Yang J, Zhu X, Wang X, Liu M, Song J (2017) Smart home 2.0: innovative smart home system powered by botanical IoT and emotion detection. Mob Netw Appl 22:1159–1169
18. Lin H, Bergmann N (2016) IoT privacy and security challenges for smart home environments. Information 7:1–15
19. Singh S, Sharma PK, Park JH (2017) SH-SecNet: an enhanced secure network architecture for the diagnosis of security threats in a smart home. Sustainability 9:1–19
20. He S, Zeng W, Xie K, Yang H, Lai M, Su X (2017) PPNC: privacy Preserving Scheme for Random Linear Network Coding in Smart Grid. KSII Transact Internet Inf Sys 11(3):1–10
21. Xie K, Ning X, Wang X, He S, Ning Z, Liu X, Qin Z (2017) An efficient privacy-preserving compressive data gathering scheme in WSNs. Inf Sci 390:82–94
22. Sivaraman V, Gharakheili HH, Vishwanath A, Boreli R, Mehani O (2015) Network-level security and privacy control for smart-home IoT devices. In: 2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), 2015
23. Copos B, Levitt K, Bishop M, Rowe J. (2016) Is anybody home? Inferring activity from smart home network traffic. In: 2016 IEEE security and privacy workshops (SPW), 2016
24. Lee B, Malik S, Wi S, Lee JH (2016) Firmware verification of embedded devices based on a blockchain. In: international conference on heterogeneous networking for quality, reliability, security and robustness, 2016
25. Bull P, Austin R, Popov E, Sharma M, Watson R (2016) Flow based security for IoT devices using an SDN gateway. In: 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud), 2016
26. Yin C, Zhou B, Yin Z, Wang J (2019) Local privacy protection classification based on human-centric computing. Human Comput Inf Sci 9(1):33
27. Panwar N, Sharma S, Mehrotra S, Krzywiecki Ł, Venkatasubramanian N (2019) Smart home survey on security and privacy. arXiv preprint. arXiv:1904.05476
28. Poh GS, Gope P, Ning J (2019) Privhome: privacy-preserving authenticated communication in smart home environment. IEEE Trans Depend Secur Comput. https://doi.org/10.1109/TDSC.2019.2914911
29. Shouran Z, Ashari A, Priyambodo T (2019) Internet of things (IoT) of smart home: privacy and security. Int J Comput Appl 182:3–8
30. Rathore S, Park JH (2018) Semi-supervised learning based distributed attack detection framework for IoT. Appl Soft Comput 72:79–89
31. Sharma PK, Rathore S, Jeong YS, Park JH (2018) SoftEdgeNet: SDN based energy-efficient distributed network architecture for edge computing. IEEE Commun Mag 56(12):104–111
32. Kim NY, Rathore S, Ryu JH, Park JH, Park JH (2018) A survey on cyber physical system security for IoT: issues, challenges, threats, solutions. J Inf Process Syst 14(6):1–10
33. Huang X, Yu R, Kang J, Xia Z, Zhang Y (2018) Software defined networking for energy harvesting internet of things. IEEE Internet Things J 5(3):1389–1399
34. Magurawalage CMS, Yang K, Hu L, Zhang J (2014) Energy-efficient and network-aware offloading algorithm for mobile cloud computing. Comput Netw 74:22–33
35. Rathore S, Kwon BW, Park JH (2019) BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network. J Netw Comput Appl 143:167–177
36. Choi BC, Lee SH, Na JC, Lee JH (2016) Secure firmware validation and update for consumer devices in home networking. IEEE Trans Consum Electron 62:39–44
37. Palani K, Holt E, Smith S (2016) Invisible and forgotten: Zero-day blooms in the IoT. In: 2016 IEEE international conference on pervasive computing and communication workshops (PerCom Workshops), 2016
38. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) DDoS in the IoT: mirai and other botnets. Computer 50:80–84
39. Lin IC, Liao TC (2017) A survey of blockchain security issues and challenges. IJ Netw Secur 19:653–659
40. Salim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput 10:1–44

Publisher's Note