IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 35-43
www.iosrjournals.org

Block chain-Enabled Security for Connected Homes

M.Rajpriya
PhD Research scholar, Department of Computer Science and Applications
St. Peter's Institute of Higher Education and Research, Chennai, Tamil Nadu, India.

R.Subhashini
Assoc. Professor, Department of Computer Science and Applications
St. Peter's Institute of Higher Education and Research, Chennai, Tamil Nadu, India.

ABSTRACT
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). In smart homes, various IoT devices are connected to each other, and these connections are centered on gateways. The role of gateways in smart homes is significant. However, their 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. We implement the proposed decentralized architecture on Ethereum blockchain technology to support security requirements of confidentiality, integrity, and authentication in the smart home gateway. Data generated from the end nodes participating in the network or stored in the database can be stored using the SHA-2 hash algorithm based on the necessary information generated. These blocks are compared in real-time on a blockchain network in the cloud to detect and prevent any instances of tampering or forgery.

Keywords: *Smart home, Gateway, Blockchain, IoT, Security and integrity.*

I. Introduction

The emergence of smart home technology has led to the development of an intelligent and automated environment that allows users to control their home devices through a network of interconnected systems [1]. However, this system also poses significant security risks due to the centralized structure of the smart home gateway network[2]. In some cases, hackers have exploited vulnerabilities in smart home appliances to launch malicious attacks [3]. Therefore, it is essential to efficiently and securely configure smart home gateway networks to protect against these security threats.

Blockchain technology has emerged as a promising approach to provide security on a wide range of platforms, including IoT and smart city networks [4]. Blockchain provides decentralized and trust-free solutions by storing data across the network in a decentralized manner. This technology allows for data to be exchanged in a verifiable manner among untrusted individuals that are connected in a peer-to-peer network. In the smart home, blockchain technology can be used to configure the gateway, store data, and exchange it in the form of blocks to support decentralization and overcome the problem from traditional centralized architecture. This approach ensures security requirements of confidentiality, integrity, and authentication in the smart home gateway.

This research proposal aims to investigate the potential use of blockchain technology in securing smart home gateway networks. The proposed research will focus on designing a block chain-based smart home gateway network that can protect against various security threats, including data forgery and tampering, access to unauthorized devices, and incorrect device control. The scalability and manageability of the proposed system will also be considered to accommodate the complexity of smart home networks. The findings of this research will provide a basis for the development of more secure and efficient smart home gateway networks, which can help prevent security breaches and ensure the safety of smart home users.

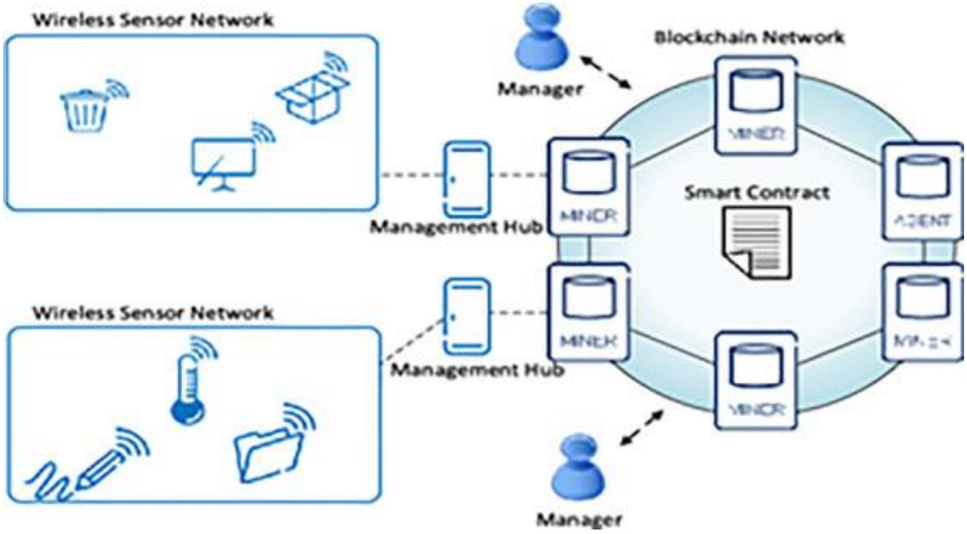

Figure 1. Decentralized access control system having IoT along with Blockchain Network

II. Related works

Blockchain

Blockchain technology has gained widespread adoption in various industries, such as finance, distribution, healthcare, and energy. It is a well-known, distributed ledger technology that has been recognized as a key technology to lead the fourth industrial revolution era [5]. The blockchain can overcome the limitations of traditional centralized systems by implementing a decentralized system that can assure users of a direct and active trust relationship.

One of the unique features of blockchain is its ability to integrate and be applied across various industries, ensuring data integrity [6]. It consists of a digital ledger that records transaction information and shares it among network members, with each member holding a copy of the ledger. When a new transaction occurs, it is authenticated with the consent of all members. The blockchain consists of multiple blocks, each containing a number of transaction information that cannot be arbitrarily changed [7]. Blocks match the data held by a majority of all users, and any modified or missing data is easily restored as ledgers store a hash value data.

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 approach addresses the problem of a server-client architecture in which multiple users are connected and managed through a centralized server in an existing network system. Therefore, the integration of blockchain technology in various industries provides greater security, transparency, and efficiency to the network [8].

Smart home

As the interest in smart homes grows, a number of technologies have been developed to automate and control devices and systems within residential environments. These environments have varying conditions, such as costs, preferences, and building types, which require a network structure to efficiently adjust temperature, security levels, and communication both inside and outside the home. The gateway for these networks aims to provide a range of functionalities, including home network and internet connections, remote control and diagnosis of home appliances, software expansion and update mechanisms, and a reliable and secure remote operation method. The goal of implementing these gateways is to create sustainable smart homes that can add value while addressing the vulnerabilities of existing smart homes.

Smart home gateway security considerations

Smart homes, with their multiple interconnected devices, offer many conveniences but also present security challenges. The gateway, which controls and monitors communication between devices, is a critical component for ensuring the security and privacy of smart homes. In this article, we'll discuss the key security requirements for smart home gateways.

Confidentiality

To protect the sensitive data collected by smart home networks, confidentiality is crucial. Only authorized personnel should have access to this data. Blockchain technology, combined with encryption, can ensure confidentiality for smart homes. Using a key, we can encrypt the data and store it on a blockchain, which restricts access to authorized users only.

Integrity

Ensuring the integrity of data is another critical security requirement for smart home gateways. Data transmission must be secure, with no falsification occurring during the transfer. A hash function can be used to detect any alterations to the data, making it possible to track and verify what data has been recorded.

Authentication

To prevent malicious actors from gaining access to a smart home network, authentication is necessary. Blockchain technology can verify the identity of network members and ensure that only authorized devices can access the network. By periodically checking the network's validity, blockchain technology can provide an added layer of security to smart homes.

III. Proposed Network

The proposed smart home network configuration is built upon blockchain technology, which enables secure authentication with integrity and confidentiality for data transmission between devices and other media. By using blockchain at the cloud layer, the previously centralized Smart Home Network can be transformed into a distributed network.

The smart home gateway based on the proposed blockchain has three layers: the device layer, gateway layer, and cloud layer. The device layer comprises sensors and devices that collect and monitor data in the smart home network environment using various heterogeneous IoTs. The gateway layer stores the data generated by the device layer and provides it to users as needed. The cloud layer registers the ID for the gateway and the data processed by each gateway in the blockchain. The blocks are shared, enabling users to access information at any time and from anywhere.

By using blockchain technology, the proposed network configuration enhances the security and privacy of smart home networks. Data transmission is authenticated, ensuring that only authorized users can access the data, and the data is kept confidential. Additionally, by transforming the smart home network from a centralized to a distributed network, the system becomes more resilient and resistant to attacks.

In summary, the proposed smart home network configuration using blockchain offers a secure and efficient solution for managing and protecting data in smart home networks.

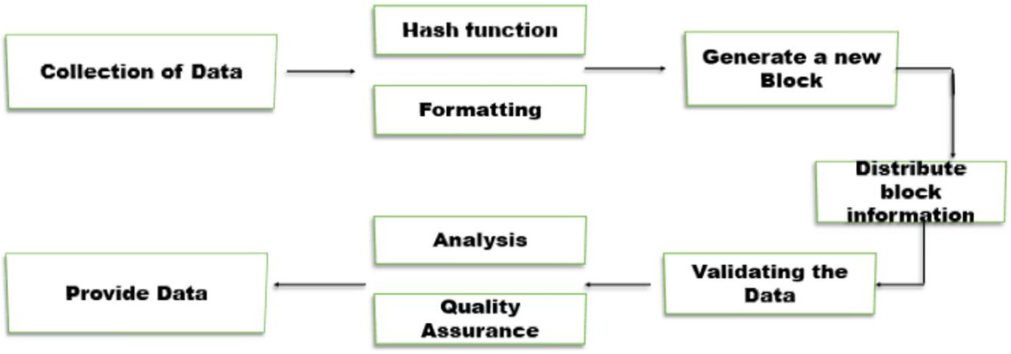

Fig 2. Designing a BlockchainEnabled Cloud Architecture for Smart Home Gateway: A Methodological Framework

Figure 2 shows the flowchart for the proposed architecture illustrates how data can be collected from devices and registered in the blockchain, and then presented to users in a meaningful way. To collect and provide this data to the user, the collected data undergoes hash value processing and formatting, which creates blocks. These blocks are then periodically verified to maintain their integrity, even if there is an attempt at data falsification. Additionally, continuous data analysis and quality maintenance must be carried out to ensure that users receive only the necessary and accurate information.

Recognizing gateway devices and acquiring data

Smart home IoT devices are linked to a central gateway, and each device has a designated ID. Both the devices and gateway have a fixed ID and the processing capability to execute encryption and decoding algorithms using PKI and SHA2.

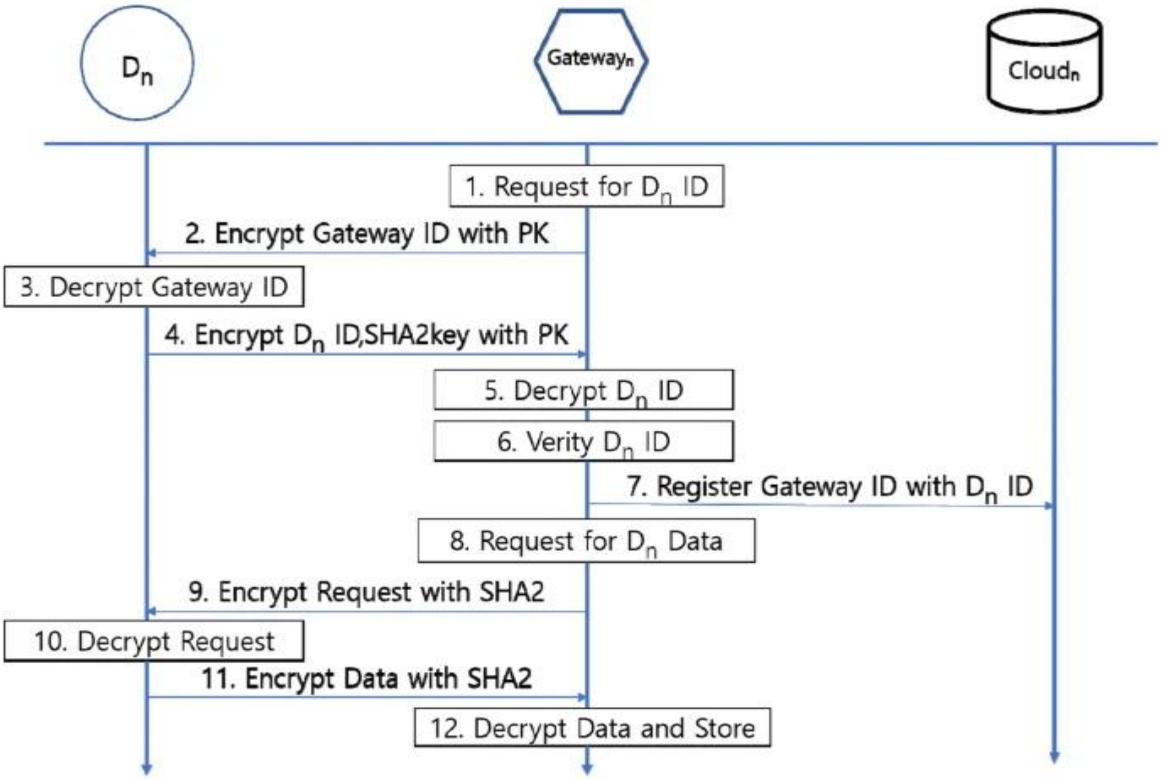
D$_n$
Gateway$_n$
Cloud$_n$
1. Request for D$_n$ ID
2. Encrypt Gateway ID with PK
3. Decrypt Gateway ID
4. Encrypt D$_n$ ID,SHA2key with PK
5. Decrypt D$_n$ ID
6. Verity D$_n$ ID
7. Register Gateway ID with D$_n$ ID
8. Request for D$_n$ Data
9. Encrypt Request with SHA2
10. Decrypt Request
11. Encrypt Data with SHA2
12. Decrypt Data and Store

Figure 3 displays the process of certification registration and data storage for the device and gateway interconnection protocol.

To ensure the security of the smart home network, devices that are certified to a gateway are periodically verified. The device layer, represented by Dn, can register with or automatically connect to the gateway. To request information about the connected device, the gateway requests an ID from the device that is connected or requesting to connect. Once an ID is obtained, the gateway uses a cryptographic algorithm to encrypt the gateway information to the device, and the message is sent. The device then decodes the encrypted message using pre-shared keys. If an unregistered or unencryptable gateway is detected, encrypted messages containing gateway information are decrypted and requested. To establish continuous communication between devices and the router, the SHA2 encryption algorithm key is shared by encrypting the device ID and SHA2 key to send messages to the gateway. The gateway decodes the transmitted messages to verify that they are registered as normal devices. Once the identification procedure between the gateway and device is complete, the device ID is registered on the gateway and stored in the cloud. The gateway communicates with the cloud over time to update the device ID list. To collect data generated by the device, the gateway creates a request message and sends it to the device. Data request messages are encrypted using the key of the SHA2 password algorithm that was validated in the previous process. To transfer data, the device is asked to provide a key for decrypting the encrypted message, which is then encrypted and transmitted to the raw data. Finally, the gateway stores the received raw data by decoding it.

Gateway data management using blockchain

The use of blockchain in a network ensures the transmission and record-keeping of data with high integrity. To store data generated by end nodes or stored in the database, the SHA-2 hash algorithm is used to create blocks that contain the necessary information. These blocks are compared in real-time on a cloud-based blockchain network, which verifies the data by detecting any instances of a forged blockchain. The gateway data registration and monitoring process can be visualized through the diagram presented in Figure 4.

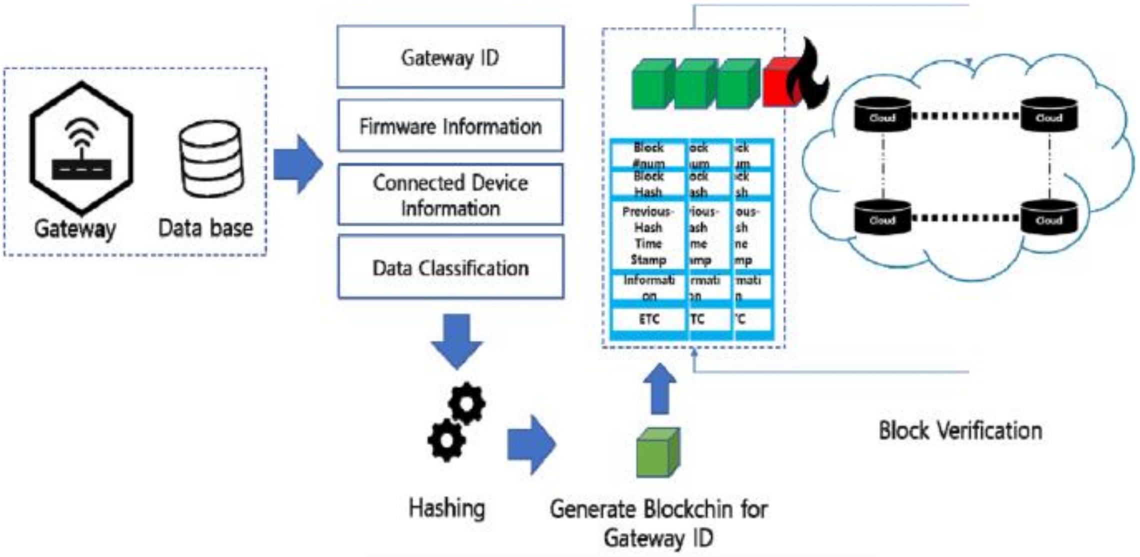

Figure 4. Blockchain based gateway data management

Performing data preprocessing within the gateway

The smart home gateway in the proposed architecture is designed to handle the transmission of data from heterogeneous IoT devices in smart homes. This gateway is capable of processing data of varying types and sizes while ensuring accuracy in IoT device control and data processing according to the user's needs. Figure 5 illustrates the process of data transfer from IoT devices to the smart home gateway, which involves three distinct categories of data processing: collection, preprocessing, and hashing.

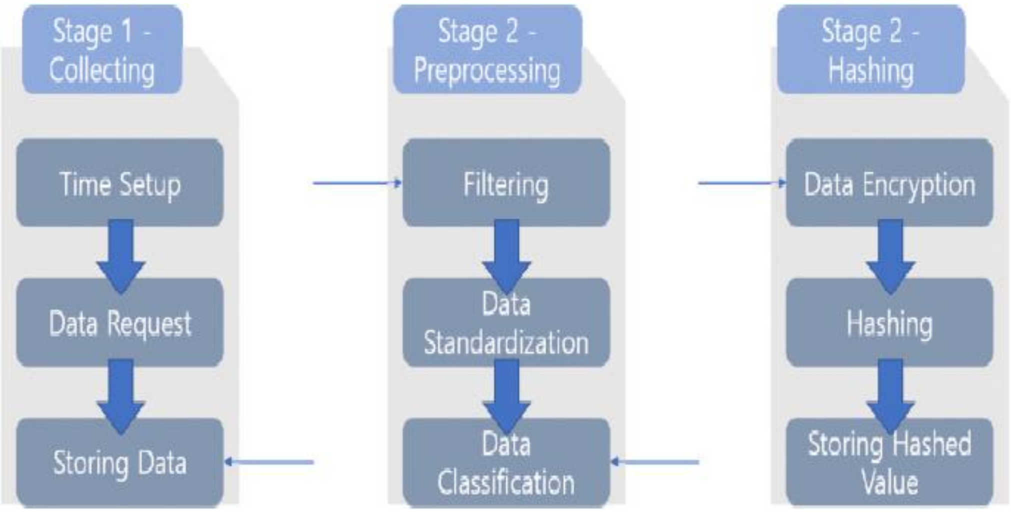

Figure 5. Performing data preprocessing within the gateway

Step 1: Data Collection - The device generates data that is communicated to the router for a specific period of time. When the gateway requires new data or when an event occurs, the device is requested to send data. The raw data is then transmitted and stored in the storage device at the gateway.
Step 2: Data Preprocessing - The raw data sent from the device is preprocessed inside the smart home gateway. The gateway filters and stores only the data required by the router, based on device ID, and uses a standardization and classification process to store the data efficiently.
Step 3: Data Hashing - Data generated in the smart home often contains sensitive information, which requires encryption. To encrypt the data, the user specifies a password, and the SHA256 algorithm is applied to store the common data of the device through the hash function.

IV. Experimental Analysis:

From Figure 6, it is evident that the proposed network architecture surpasses the traditional centralized architecture. This is attributed to the use of blockchain technology in the gateway layer, which enables faster response times and more precise security measurements since the gateway is in closer proximity to the IoT device than the cloud. The precise security measurements provided by the proposed architecture prove that the use of blockchain is an effective means of maintaining the confidentiality, integrity, and authentication requirements in smart homes.

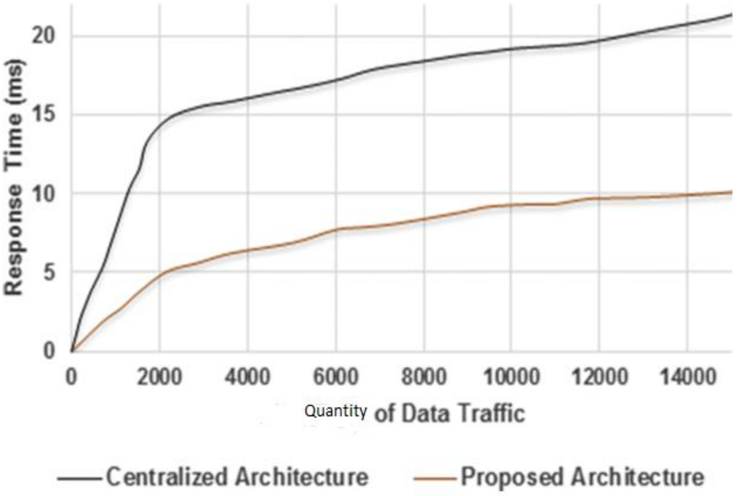

Figure 6. Evaluation of security response time under varying data traffic loads

V. Security Analysis

The security analysis of smart home gateways is an ongoing process due to the constantly evolving attack techniques employed by malicious actors in the ever-changing network and IoT environment. As most IoT devices are designed with limited computing power and battery capacity, they are particularly vulnerable to attacks. Consequently, attackers can easily exploit weaknesses in the system and create various attack scenarios targeting specific devices.

To maintain the security of smart home gateways, continuous vigilance and proactive measures are necessary to detect and mitigate any potential vulnerabilities before they can be exploited by attackers. With the increasing prevalence of IoT devices in modern households, securing smart home gateways has become a critical concern to prevent unauthorized access to personal data and privacy breaches. Therefore, it is crucial to stay updated with the latest attack techniques and invest in robust security measures to protect against potential attacks.

Blockchain 51% Attack

A 51% attack is a type of hacking attack that aims to manipulate transaction information in order to gain profit. This attack occurs when a malicious actor gains control of more than 50% of the hash nodes in the entire blockchain network. This essentially means that the attacker has access to a powerful hash computing power that exceeds that of other nodes in the network. As a result, the attacker can create and add new blocks to the blockchain network at a faster rate than honest nodes, thus allowing them to store and add forged data to the network. The attack is successful when other blocks in the network are forced to adopt the blockchain that contains the forged data.

However, it is important to note that in order for a 51% attack to succeed in a blockchain-based architecture, the hash power of all participating nodes must be less than that of the attacker. This means that the number of nodes in the architecture must be increased to effectively defend against attacks. With the increase in nodes, the blockchain network becomes more decentralized and the likelihood of a 51% attack decreases. In the proposed blockchain-based architecture, a 51% attack is impossible due to the increased number of nodes participating in the network, which effectively mitigates the risk of an attacker gaining control over the majority of the network's hash power.

Zero Day Attack

A zero-day attack is a type of hacking technique that exploits software vulnerabilities for which a patch or fix is not yet available. These attacks can be particularly devastating because there are no countermeasures or protections in place to prevent them from occurring. As a result, any device can potentially be compromised by a zero-day attack, making it a serious threat to cyber security.

However, in the proposed architecture, measures have been put in place to supplement security against such attacks. The architecture is designed to receive periodic security updates, which can help to identify and address vulnerabilities before they can be exploited by attackers. In addition, the use of whitelists and blacklists can help to block unauthorized access and prevent malicious activity from occurring. Real-time monitoring of changes is also implemented to detect any suspicious activity and take immediate action to mitigate potential threats.

VI. Conclusion

The proposed research paper introduces a blockchain-enabled data security gateway architecture designed to address the confidentiality, integrity, and authentication issues that arise in the smart home gateway environment and IoT. The architecture provides a comprehensive solution to these problems by implementing the SHA2 encryption algorithm to secure smart home gateways and heterogeneous IoT devices, while also utilizing blockchain technology to ensure data integrity. The effectiveness of the proposed architecture is evaluated through the presentation of three considerations and scenarios, which show that the proposed architecture outperforms existing research in terms of data security and integrity. However, it is important to note that the proposed architecture may introduce additional computational complexity due to the operation of blockchain. To address this limitation, the research proposes the concept of mobile edge computing, which can offload computation and further enhance the proposed architecture.Overall, the proposed blockchain-based data tamper-proofing gateway architecture offers a robust solution for securing smart homes and IoT devices.

References

[1]. 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

[2]. Gu K, Yang L, Yin B (2018) Location data record privacy protection based on differential privacy mechanism. Inf Technol Control 47(4):639–654

[3]. Xiong B, Yang K, Zhao J, Li K (2017) Robust dynamic network traffic partitioning against malicious attacks. J Netw Comput Appl 87:20–31

[4]. 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):55–64Return to ref 10 in article

[5]. X. Chen, Z. Wei, X. Jia, P. Zheng, M. Han and X. Yang, "Current Status and Prospects of Blockchain Security Standardization," 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom), Xi'an, China, 2022, pp. 24-29, doi: 10.1109/CSCloud-EdgeCom54986.2022.00014.

[6]. W. Cai and J. Qu, "Systematic Research on Information Security Based on Blockchain Technology," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 900-903, doi: 10.1109/ICEARS53579.2022.9751814.

[7]. A. K. Yadav and V. P. Vishwakarma, "Adoptation of Blockchain of Things(BCOT): Oppurtunities & Challenges," 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2022, pp. 1-5, doi: 10.1109/ICBDS53701.2022.9935985.

[8]. D. Lamken et al., "Design patterns and framework for blockchain integration in supply chains," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 2021, pp. 1-3, doi: 10.1109/ICBC51069.2021.9461062.

[9]. X. Wang, A. Badshah, S. Tu and M. Waqas, "Blockchain-Based Security Management Platform," 2021 2nd Asia Symposium on Signal Processing (ASSP), Beijing, China, 2021, pp. 118-121, doi: 10.1109/ASSP54407.2021.00026.

[10]. Z. Gong-Guo and Z. Wan, "Blockchain-based IoT security authentication system," 2021 International Conference on Computer, Blockchain and Financial Development (CBFD), Nanjing, China, 2021, pp. 415-418, doi: 10.1109/CBFD52659.2021.00090.

[11]. 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

[12]. Shouran Z, Ashari A, Priyambodo T (2019) Internet of things (IoT) of smart home: privacy and security. Int J Comput Appl 182:3–8

[13]. alim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput 10:1–44

[14]. T.Tantidham and Y. N. Aung, "Emergency Service for Smart Home System Using Ethereum Blockchain: System and Architecture," IEEE International Conference on Pervasive Com-puting and Communications Workshops (PerCom Workshops), pp. 888–893

[15]. B. Putz and G. Pernul, "Detecting Blockchain Security Threats," 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2020, pp. 313-320, doi: 10.1109/Blockchain50366.2020.00046.

[16]. [16] C. Su and X. Li, "A Review of Blockchain Consensus," International Conference on Intelligent Computing, Automation and Applications (ICAA), pp. 598–604, Nanjing, China,25–27 June 2021.

[17]. M. Conoscenti, A. Vetrò and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature review," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, 2016.

[18]. F. Alkurdi, I. Elgendi, K. S. Munasinghe, D. Sharma and A. Jamalipour, "Blockchain in IoT Security: A Survey," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW, Australia, 2018, pp. 1-4, doi: 10.1109/ATNAC.2018.8615409.

[19]. E. Fernando, Meyliana and Surjandy, “Blockchain Technology Implementation in Raspberry Pi for Private Network,” International Conference on Sustainable Information Engineering and Technology (SIET), pp. 154–158, 2019

[20]. H. Yang, Y. Bai, Z. Zou, Q. Zhang, B. Wang and R. Yang, "Research on Data Security Sharing Mechanism of Power Internet of Things Based on Blockchain," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2020, pp. 2029-2032, doi: 10.1109/ITAIC49862.2020.9338843.