Blockchain in IoT-Enabled Smart Home Network Security

Vidyashree K P
Department of Information Science and Engineering
Vidyavardhaka College of Engineering
Mysore
vidyashreekp@vvce.ac.in

Manoj M
Department of Information Science and Engineering
Vidyavardhaka College of Engineering
Mysore
manojmanjunath1425@gmail.com

Darshan V
Department of Information Science and Engineering
Vidyavardhaka College of Engineering
Mysore
darshanv18mar@gmail.com

Mohan Prakash V
Department of Information Science and Engineering
Vidyavardhaka College of Engineering
Mysore
mohanprakshv2000@gmail.com

Bharath M
Department of Information Science and Engineering
Vidyavardhaka College of Engineering
Mysore
marigowda2bharath@gmail.com

***Abstract*— In 1950s people started realizing that the value of data is much more than they knew due to which the concept of providing network security came into existence. The term network security defines that providing confidentiality, integrity, and accessibility of data to the network. Internet of things (IoT) is a technology that is growing rapidly and can be found in most of the domains which includes smart home systems (SHS). A conventional SHS is a centralized architecture where devices like sensors, LED's, voice assistants and many more are connected to a single gateway for monitoring and controlling of their activities. Due to the presence of issues like single point of failure (SPOF), rise of data loss and many other security risks in centralized architecture affects the secure data storage and transmission. Adopting blockchain-based home automation technology reduces numerous security problems which exist in the centralized architecture. So, in this paper we proposed a simple SHS network architecture using blockchain**

***Keywords*—IoT, Blockchain, Consensus, Consortium, AWS-S3.**

1. Introduction

Recently, IoT devices are used in many sectors of day-to-day life, including Smart homes. Smart home system is one of the application on Internet of things (IoT) which is gaining more popularity nowadays., where different sensors are used within the SHS through wireless connectivity. These sensors are accessible and operated by the home owners remotely. Some of the smart home IoT devices are power switches, light bulbs, locks, and many more.

IoT devices are used in many applications. These IoT devices are used to collect, store, and share data for controlling and monitoring of these devices, hence providing secure data transmission is necessary. If not there arises security concerns such as information theft, rise in data loss, vulnerability of the devices and some other cyber attacks are possible.

Despite the limited computing capacity of most IoT devices, space can still be infected by malware. IoT botnet malware is among the most frequently seen variants. The Mirai botnet has had a major and widespread impact because of poor security and access controls present in many Internet of Things devices. Numerous Mirai versions and Distributed Denial of Service(DDoS) attacks have become more frequent as a result of the public release of its source code in 2016[1]. A real-life instance of illegal hacking in which a perpetrator attempted to obtain data from a North American casino using a fish tank was made public in 2018. Despite the casino having implemented certain security measures to identify the risks, the tank is nevertheless hacked by the hacker so that they could send data to a device in Finland[2].

The Blockchain based smart home automation gateways are proposed in order to solve the issues that is present in the centralized smart home architecture and also protect home automation gateways against cyber attacks. Blockchain can be defined as a distributed ledger that tracks and

stores data or information of virtual transactions and so forth[3]. Secrecy, accessibility, integrity, and single point of attack can be avoided or reduced by implementing blockchain in the smart home system (SHS).

There are three ways that blockchain is currently being used. The first is public blockchain, also known as the permissionless blockchain, in which it allows everyone to participate in block verification and it is the massive network of interconnected nodes. It is open to anyone including miners, users, developers, and members of communities. The other method uses a private blockchain, which is also called permissioned blockchain that may only be accessed by pre-defined group of the known organization[2]. Consortium blockchain technology, which uses hybrid of public and private blockchain to implement blockchain, is the third method. In this only a predetermined group of nodes are used for block validation[4].

According to[5], the centralized conventional IoT model are compared with the blockchain model. It was found that blockchain based model was more attractive because the issues related to requirements for security in smart home network was not found in blockchain. In centralized architecture of IoT model IoT devices are connected to a single smart home gateways as mentioned in [6]. For IoT devices, a decentralized data management system is used with smart contracts used to enforce all data permissions and the blockchain used to store the audit trail of data access. Without the need for centralized system, multiple nodes can specify rules and regulations to judge their interactions through the use of smart contracts applications, which are independently enforced in the blockchain. In [7], they offer framework that stores the hash value in block and raw data is stored in storage platforms using trusted execution environment.

Many blockchain based smart home architecture are designed using Ethereum smart contracts. Ethereum is a public blockchain-based distributed computing platform which has it's own language such as Solidity and Serpent developers can write and compile using this language [8]. Ethereum can be used to combine computing systems with blockchain. This type of blockchain has difficulty of implementation and has scalability issues. It also needs huge storage and also consumes more energy.

The structure of the paper is further classified into following sections: Section 2 of the paper describes the background and related study, then section 3 consist of implementation methodology. The paper ends with conclusion and future work in section 4.

2. BACKGROUND AND RELATED STUDY

2.1. Blockchain

Blockchain is defined as a decentralized and distributed public ledger technology in peer to peer network. It uses a linked block a structure to store and verify the data and creates a tamper-proof digital platform for storing and sharing data by using a consensus mechanism to synchronize changes in data [9]. Every request is recorded in a series of blocks, each of which has a distinct digital signature for use in verification. Blockchains are the best option for storing sensitive data due to the fact that the ledger is created and maintained by everyone involved in the system equally, eliminating the need for a central controller to oversee operations.

Consensus algorithms are used to keep the same transaction records in all the nodes, which are consisted of the proving work of the transaction and the selecting policy of the block [10]. Few common consensus algorithms are PoW (Proof of Work) and PoS (Proof of Stake). The PoW is a mechanism in which the majority of nodes on the network decide on a single state it is said consensus is achieved. PoS is an alternative to PoW which reflects on the holding assets of the participating nodes.

2.2. Smart Home Network Security

Smart homes are automated structures with detection and control equipment already installed, including HVAC (heating, ventilation and air conditioning), lighting, hardware and security systems. These contemporary systems sometimes referred to as "gateways", comprise switches and sensors that interact with the central axis. IoT controls the network connectivity of these control systems, which have user interfaces that communicate with tablets, smartphones and computers. To solve the problems, present in the centralized SHS numerous solution exist, blockchain is one of the best solution which exist. Blockchain in SHS removes the single central system and replace it with distributed system where each node in system get equal priority. We

can implement a blockchain based SHS using Public, private or consortium blockchain.

Public blockchain based architecture for SHS

The authors of [11] by combining both blockchain and IoT proposed a model for smart district and provide user access to the power grid of the district. They developed a prototype where authorized users are able to work in the power grid systems through blockchain. Solar panels are setup at home and the owners can trade energy over the blockchain mechanism. Observing this system gives us information about various technical needs to implement a blockchain-based smart home system (SHS). This implementation could be a prime example of how blockchain-based IoT applications can be adopted and reduplicated in real world.

According to authors of [12] we can speed up the processing and display appropriate performance by implementing a "efficient light weight integrated blockchain (ELIB)" model for IoT systems. This model was created using public blockchain which contains two nodes overlay and smart home, operates in three layers namely consensus mechanism, certificateless cryptography, and distributed throughput management scheme (DTMS). Public permissionless blockchain make use of expensive consensus procedures, such as proof of work (PoW) proof of stack (PoS), or protocols that demand specialized hardware, like proof of elapsed time. In IoT systems where devices are diverse and power constrained, such standards do not apply. The throughput and latency demand of IoT applications, which frequently call for hundreds of transactions to be committed to the ledger within milliseconds to seconds, cannot be met by them either.

Private blockchain based architecture for SHS

A private blockchain is also called permissioned blockchain which is deployed within the organization or shred between known predefined group of participants. The writers of [14] proposed a 3-tier architecture for efficient and secure information processing. The three-tier architecture includes IoT devices connected to raspberry pie, fog computing, docker containers which provides a real-time analysis and helps in monitoring of data. This proposed architecture guaranteed that confidentiality, availability, and integrity of data and also resolved scalability issue which is present in public blockchain. This also secures the architecture from Distributed denial of service (DDoS) attacks.

Consortium blockchain based architecture for SHS

A consortium blockchain is used as the distributed ledger to record all IoT devices and their services. It serves as the main channel of communication for IoT services with their users and provides significantly greater performance and scalability and then permission-less public blockchains. The IoT network may decentralize eliminating the centralized servers that are frequently SPOF. Additionally, to protect IoT services from unwanted access, the platform can make use of access control features added by consortium blockchains. Finally, because every modification to IoT services, as well as every service request and answer, is permanently recorded on the ledger, the blockchain effectively functions as a data historian for data audits [13].

There exists a modified or hybrid consortium blockchain system called "Homomorphic consortium blockchain (HCB)". This blockchain system uses a homomorphic encryption algorithm which allows people to perform algebraic operations on the secured data which is in the form of cipher text and get encrypted results. This helps in maintaining the privacy of private or secure data [16]. The consortium blockchain differs from private blockchain, consortium blockchain uses the concept of consensus algorithm to verify the transactions. This methodology helps SHS to use the pros of both public and private blockchain.

2.3 Problem Statement

There is massive increase in the number of IoT devices and as the devices increase, security threats and problems also rises. To overcome these problems blockchain is integrated with IoT. The majority of the current structures are executed through a public blockchain, which presents a problem with scalability, and these structures are also rather intricate.
Hence providing appropriate and simplified solutions for smart homes using blockchain to reduce scalability and security issues and also improve confidentiality, integrity and availability. Practical implementation of the proposed architecture can be done by

1) Creating a plan for a smart home structure utilizing a consortium blockchain

2) Developing a functional model of a smart home web application for the aforementioned structure
3) Executing a hardware blueprint for a secure and straightforward smart home structure through the use of readily accessible IoT gadgets.

3. Methodology

The building blocks of the proposed architecture are Sensor nodes and Super node. The authorized users can communicate with the SHS. The users can send requests or get responses to the IoT devices via internet. Only the pre-chosen IoT nodes can participate in the blockchain transaction. The Super node act as the link between the IoT nodes and the requests from the users, it intermediates between them. The IoT devices will be communicating with each other and the Super node.

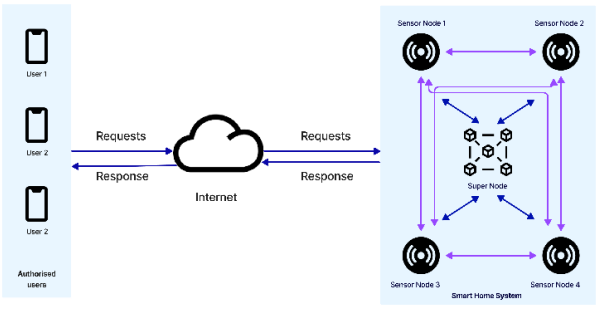

Figure 1- Proposed architecture using blockchain and IoT

In the following paragraphs we discuss about the major components of the architecture

1) Super Node (SN)

The super node is a server which works on peer-to-peer server architecture. This is used to communicate with the IoT sensor nodes. This node helps in transaction management by broadcasting last transaction to all the other IoT nodes. The Super node(SN) receives request and send replies from users through internet via RESTful API. It keeps the Ip address of registered users so that it can authenticate the users, only the devices registered can get access to the smart home system application. The authentication process is discussed in the later section of the paper.

2) IoT Sensors/Devices (SeN)

The Sensor nodes communicate with the Super Nodes (SN) and participate in the transaction verification process. The nodes can be added to the smart home system by the admin using the device's id. Once the device is added to the system a xml file for that device is created at the AWS-S3. If a user wants to communicate with any of the smart device, he sends the signal to the super node which in turn sends the signal to the sensor. The SN broadcasts the transaction to all other sensor nodes and the xml file of all the IoT sensor is updated with this transaction.

3) Transaction Verification Process

The verification of the transaction needs previous transactions to be same in all the device xml file. Whenever a new transaction happens the data is stored in all the device files hence all the file have the same previous transaction data. In the next transaction the SN checks the last 5 transactions in all the device files, if the transactions are same in all the files then and only then the transaction is approved and updated in the files. However if it finds a wrong entry in any one of the file then we can say that someone tried to gain access to device without authentication and this can be rectified using the transactions saved in other device files.

4) User Authorization

This subsection explains the process of verifying users as authorized entities. The SN grants authorization to users through the use of a RESTful API, which is an application programming interface designed to enable secure communication over the internet or between systems. This type of API utilizes REST architectural principles to create web services that allow access to system resources using a set of predefined rules. The resources can then be transferred over HTTPs by various consumers. Our proposed system utilizes the RESTful API for secure communication.

The smart home system has two types of users: Admin and General user. An Admin user is a user who has been pre-authorized and registered in SN. The admin is given the privilege to add General users to the smart home network. To add a general user, the admin will require the IMEI of the user's device. The process begins with the admin installing the smart home application as an authorized user. After

installation, the admin user can send a request through the application to add a general user.

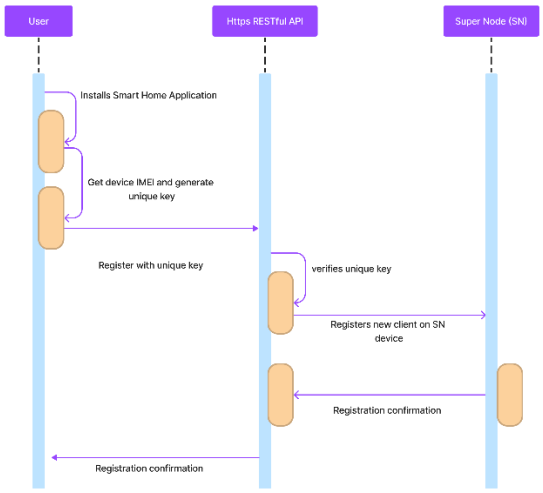

Figure 2 User Authentication

The application will then create a unique key for the General user and send it to SN via the RESTful API. After the user submits their key, the SN will validate it and add them as a new customer with a distinct ID. To communicate further within the smart home network, the admin user will provide the general user with a username and password. Whenever the user sends a request to the SN, their unique key, which is saved in the SN's database, will be used to identify them.

In the process flow the user first sends request super node (SN) the super node checks if a blockchain ledger exists, if not it creates new ledger else it generates a new block transaction and updates the blockchain ledger. After the ledger is updated, the new block is broadcasted to all other nodes using peer-to-peer server. If the broadcasting fails error message is sent else block is broadcasted to all the sensor nodes.

The broadcasted signal is caught by the SeN's listener if the block is received it is validated against last 5 transaction blocks. If validated hash value for the block is generated else if block is not validated it is rejected. The transaction data is read and target reference is checked. Target reference if matched then the action is fulfilled.

5) Hardware Implementation

In this portion, the configuration of the hardware for the blockchain execution is explained. This is achieved through the creation of a practical smart home situation that involves the utilization of three ESP8266 gadgets. To create a small smart home setup, the hardware implementation includes using a humidity and temperature sensor, buzzer alert, and a LED

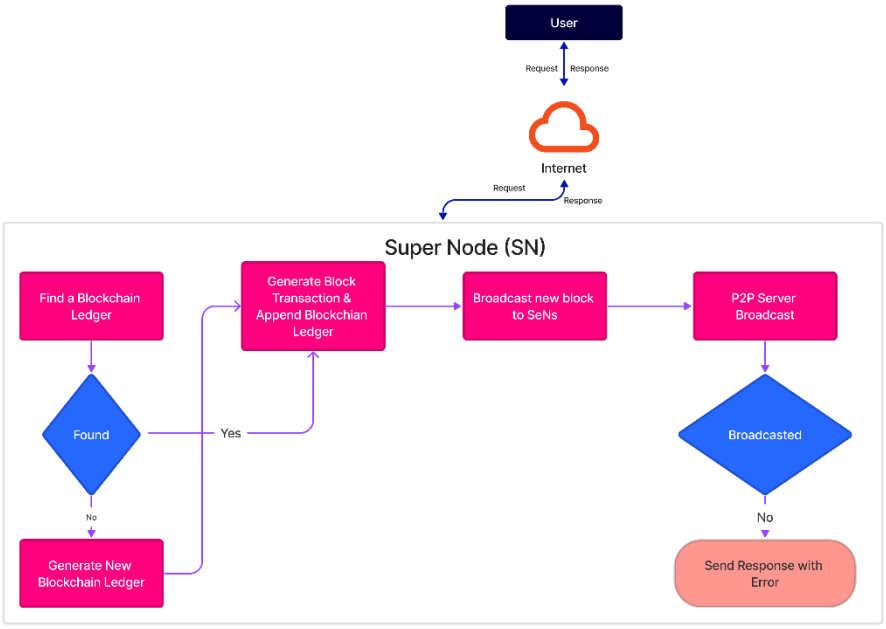

Figure 3:Process flow in SN

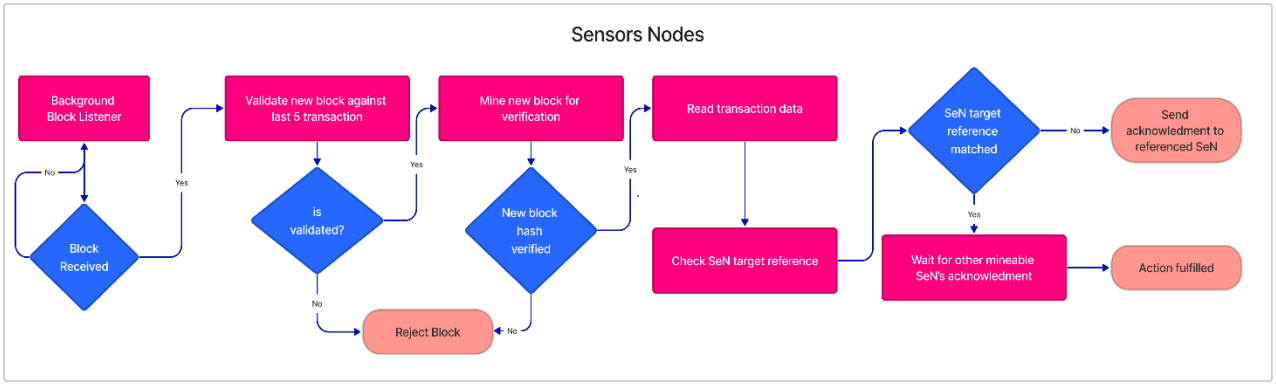

Figure 4: Process flow in SeN's

device. These components work together to create the desired functionality.

After setting up the hardware, the following task is to create a blockchain code using a suitable platform to assess its efficiency. We have used Arduino ide to code the microcontrollers and used AWS-S3 to create blocks in the blockchain. AWS-S3 was used instead of a blockchain platform was mainly to avoid the gas cost included in other platforms.
The block header contains following data:

- The previous block's hash is retained in each block to ensure the integrity of the blockchain.
- Additionally, a timestamp is included in the block to record the start and end time of the event on the device or computer and is stored as temporal information in the form of a log or metadata.
- The FromDeviceID attribute contains the address of the source device from which the transaction originates
- The ToDeviceID attribute contains the address of the destination device for which the transaction is intended.
- Additionally, status of the IoT devices is returned and stored in the block to keep track of the device status.

4. Conclusion

This paper introduces the application, existing problems, and solutions for smart homes based on a blockchain architecture. Firstly, we found several concerns involved in centralized smart home architecture such as confidentiality, integrity, and Distributed denial of service (DDoS). Blockchain was integrated into this architecture to resolve the issues in the centralized architecture. Secondly, we summarized how public, private, and consortium blockchains are integrated with smart home systems. Further, we discussed the different consensus mechanisms used in the blockchain. By noting down all the disadvantages we have implemented SHS architecture which reduces the scalability issues using blockchain. In Future research can be done to implement blockchain using a blockchain platform.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, “IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers,” *Forensic Science International: Digital Investigation*, vol. 32, Apr. 2020, doi: 10.1016/j.fsidi.2020.300926.

[2] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, “Investigating Smart Home Security: Is Blockchain the Answer?,” *IEEE Access*, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.

[3] Mohiuddin Ahmed, “Introduction to Blockchain,” 2020. [Online]. Available: https://www.researchgate.net/publication/343601688

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[5] A. Qashlan, P. Nanda, X. He, and M. Mohanty, “Privacy-Preserving Mechanism in Smart Home Using Blockchain,” *IEEE*

Access, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[6] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 9, Dec. 2020, doi: 10.1186/s13673-020-0214-5.

[7] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment," in *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, Jul. 2018, pp. 15–22. doi: 10.1109/IRI.2018.00011.

[8] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467. doi: 10.23919/ICACT.2017.7890132.

[9] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, Jan. 2019, doi: 10.1016/j.jnca.2018.10.020.

[10] D. Y. Kim, S. D. Min, and S. Kim, "A DPN (delegated proof of node) mechanism for secure data transmission in IoT services," *Computers, Materials and Continua*, vol. 60, no. 1, pp. 1–14, 2019, doi: 10.32604/cmc.2019.06102.

[11] C. Lazaroiu and M. Roscia, "Smart district through IoT and Blockchain," in *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)*, Nov. 2017, pp. 454–461. doi: 10.1109/ICRERA.2017.8191102.

[12] S. N. Mohanty *et al.*, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.

[13] R. Zhang, C. Xu, and M. Xie, "Secure Decentralized IoT Service Platform using Consortium Blockchain," Sep. 2022, doi: 10.3390/s22218186.

[14] B. Kumar Mohanta, "*Internet Of Things Enable Smart Home Security Issue Address Using Blockchain*."

[15] N. R. Pradhan and A. P. Singh, "Smart contracts for automated control system in Blockchain based smart cities," *J Ambient Intell Smart Environ*, vol. 13, no. 3, pp. 253–267, May 2021, doi: 10.3233/ais-210601.

[16] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, "Homomorphic Consortium Blockchain for Smart Home System Sensitive Data Privacy Preserving," *IEEE Access*, vol. 7, pp. 62058–62070, 2019, doi: 10.1109/ACCESS.2019.2916345.