International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/214509 Volume 9, Issue 4, July – August (2022)

RESEARCH ARTICLE

Blockchain-Based Model for Smart Home Network Security

Abdualrahman Johari
Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
G200004912@seu.edu.sa

Raed Alsaqour
Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
r.alsaqor@seu.edu.sa

Received: 06 July 2022 / Revised: 15 August 2022 / Accepted: 19 August 2022 / Published: 30 August 2022

Abstract – Network security is a vast topic that combines processes, devices, and technologies. Network security is the group of rules and configurations. This designed to protect the information and networks' integrity, accessibility, and confidentiality using software and hardware. The network nowadays has become complex, which is changing the threat environment. Similarly, smart homes are also becoming prone to security threats. Due to that, ensuring network security is very important. The vulnerabilities of the smart home network can exist in many areas, including users, location, data, and applications. Some smart devices in smart homes may lack system hardening and can have hardcoded passwords, or the passwords can be found without any encryption inside the device or the software. Security of the smart home network is a high priority of the connected devices so that hackers do not get access to sensitive and personal data. Otherwise, this may risk the entire network of the smart home. This research will provide a model to analyze various security concerns of the smart home network. For this research, a qualitative method such as a case study analysis will be done for conducting this research study. In addition, relevant information through the secondary data collection method will be collected. Investigation of various security threats related to smart home networks will be performed, and Blockchain Technology will be used technologies to mitigate the security issues and secure and protect the smart home network secured and protected. In this research, the novel, decentralized, and innovative approach to blockchain technology will be presented, which will be used to enhance the security architecture of the smart home network.

Index Terms – Blockchain, Smart Home Network, Network Security, Security Threats, Modeling, Cyberattack.

1. INTRODUCTION

Among the current Internet of Things (IoT) based blockchain applications, blockchain technology is expanding significantly in home automation systems. Using sensors connected to wireless networks, homeowners may remotely operate their appliances [1]. Security doors, led lights, and boost converters are examples of devices with limited data processing capabilities. As the market for these products has developed rapidly, numerous new security challenges have emerged [2]. Academics have given these devices a lot of consideration as an important research issue. Furthermore, the special security risks created by these devices have not been adequately addressed by specific security procedures. It is no secret that blockchain, a distributed database based on cryptographic principles, is receiving a lot of interest for its potential to play a part in safeguarding the IoT. Blockchain-based IoT solutions are a cutting-edge replacement for centralized, traditional approaches that have significant problems with the demand for home automation. The study of global Internet development and usage trends in [3, 4], it is anticipated that by 2022, there will be 29 million smart home items available, a huge increase from the current 6.5 million. Furthermore, according to [5], in the current year, it is predicted that there will be about 700 million smart automation and control devices, up from the previously predicted 500 million. It is getting harder to keep such devices secure as the amount and diversity of home automation continue to expand dramatically.

This research aims to examine different home automation network security problems. Case study analyses will be used as a qualitative approach for this research. Secondary data gathering methods will also be used to gather important information. Numerous security concerns to technology systems will be investigated. Blockchain innovation will be utilized to mitigate security problems and defend the home automation network. This research analyzed the security of home automation by introducing blockchain-based technology and examine some of the recently proposed smart house designs that use blockchain. The research developed

RESEARCH ARTICLE

basic but secure home automation architecture using the blockchain and discuss the drawbacks and benefits of using this design.

The proposed architecture will identify the need to reduce request time, utilize cloud storage, and include users in the blockchain validation process. The following are the most significant contributions made by this research:

- Evaluate the security challenges associated with smart household infrastructures and create home automation architecture based upon that Blockchain network.
- A functioning prototype of a Building Automation Mobile App for suggested architecture will be developed and exhibited.
- The suggested architecture's results will be compared to the centralized security infrastructure to determine which is superior.
- It developed a hardware implementation for a basic secured smart home architecture by evaluating it with smart devices that are widely accessible.
- Propose a blockchain-based home automation gateways network design to minimize current issues in centralized network security architectures and defend against prospective assaults on home automation gateways.

Following is how the remaining sections of the essay are structured: Section 2 examines the background and related literature, Section 3 outlines the research methodology, and Section 4 presents the proposed model. Security assessment is covered in Section 5. The results and analysis are shown in Section 6. Finally, the paper is concluded and potential future work is discussed in Section 7.

2. BACKGROUND AND RELATED WORK

2.1. Blockchain

A blockchain system of recorded information makes hacking to change the entire system difficult or impossible [6]. Blockchain technology is now one of the most popular research motives. It is a decentralized blockchain platform that can only be updated by adding new entries. It is protected by encryption. It offers a framework for processing trusted transactions without the intervention of a third party. Each request is documented in a sequence of blocks, each with a unique digital certificate for verification purposes. The fact that the ledger is engendered and managed to maintain by all people involved equally inside this system, and therefore there is neither the main controller to organize the operation, blockchains store structure is designed, and unchanging documentation in a secured network manner makes them ideal for storing sensitive information [7]. Each node is permitted to join safely since blockchain is based on a peer-to-peer (P2P) networking model. When a node or user enters the blockchain platform, that node and user receive a complete copy of the ledger. If an incremental request is produced, a block is constructed and sent to every device in the network for verification. Once the block has been verified by all the other stations and determined to be unaltered, it is recorded on the block's blockchain. To validate the authenticity of a block, every one of the devices in the system must agree [8]. When receiving a blockchain for verification, every other network device compares it to its blockchain; the other nodes within the network refuse any blocks that have been manipulated.

The operation of a blockchain is depicted in Figure 1. A block that reflects the desired transaction is produced once the transaction has been requested. The block is then distributed to all network nodes after that. The nodes then verify the transaction. The block is added to the current blockchain after receiving a reward for the proof of work. The transaction can then be designated as finished after this operation.

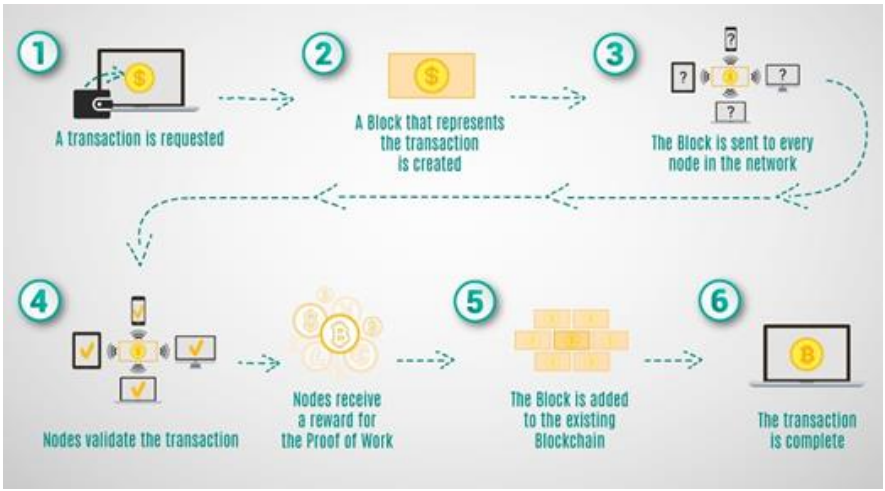

Figure 1 Working Process of Blockchain

RESEARCH ARTICLE

2.2. Smart Home Network Security

Nowadays, with the help of smart home technology, it has become very easy to do various kinds of work, such as making a grocery list, and this method helps to monitor the access points of the house. Smart homes offer a variety of benefits through innovative equipment and can add value to the homeowner. The present age is highly dependent on technology, and it is very common for IoT devices to gain popularity [5]. The use of smart home devices protects homeowners from insecurity and ensures their security. Because of all the major security measures, this is their primary advantage. A simple and secured smart home framework is based on a refined version of the blockchain, known as the Consortium blockchain. Smart home devices use a kind of security automation via cameras to monitor the outside. A type of lock is also used to attach the buttons. In addition, if any irregular behavior can be detected in the home, special notifications are shown. Many use such devices to establish power over their family security and obtain transparent information about it. However, smart home devices might not always provide accurate and precise information. Like other devices, these devices allow hackers to use various tools to make threats and gain access by creating access points. Security vulnerabilities, in this case, can create promotions that homeowners will never know about and are unlikely to be unaware of. These threats can occur in various ways: malware infiltration, data theft, data leaks, death penalty failures, and denial of service. However, homeowners should explore other alternatives to promote greater security and take great care of their smart home systems to avoid facing such a dangerous digital environment.

Figure 2 shows how the user connects to a smart home. The smart home combines smart lights, smart locks, smart sockets, smart appliances, an alarm system, smartwatches, and smart TVs. The smart home connects with a cloud server, health care providers, entertainment providers, etc. The user's needs and requirements can be fulfilled as soon as possible.

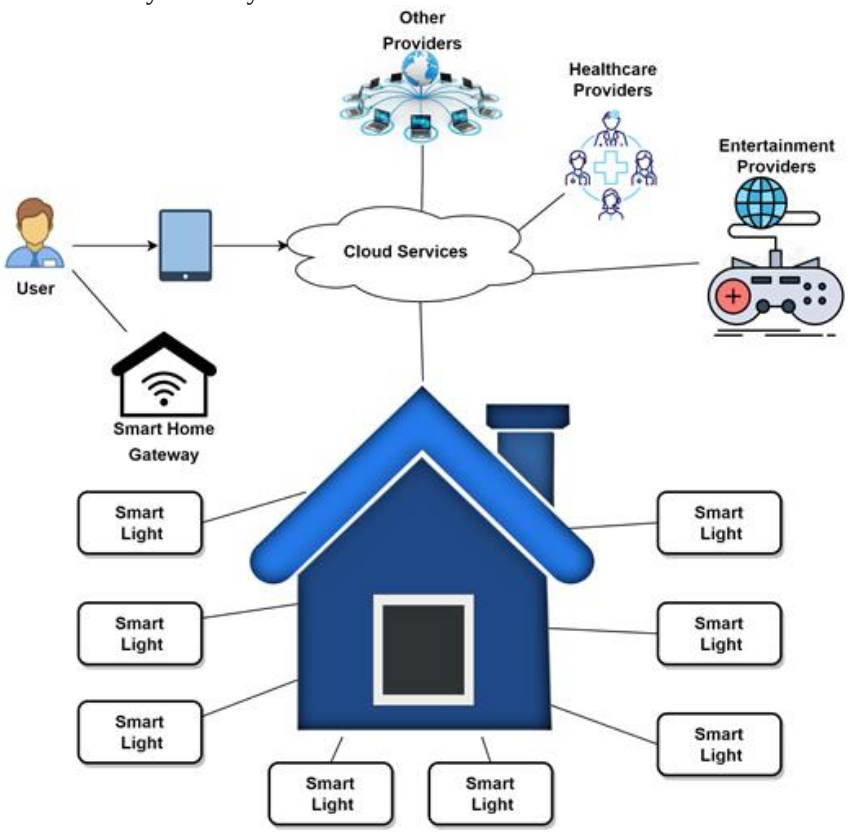

Figure 2 Smart Home Security

2.3. Related Work

According to [9], with the advancement of technology, users can now use certain options. A notable example is a blockchain, the most popular and widely used technology. With blockchain, people can solve most cybersecurity issues, and it is currently very popular in the cryptocurrency market.

According to [10], the blockchain architecture with an IoT-based system is an attractive alternative to the conventional

RESEARCH ARTICLE

centralized model, but it has significant issues addressing the requirement for security in smart homes.

Numerous IoT-based devices are linked together and centered on a smart home's gateways, as was explained in [8]. A gateway plays a big part in a smart home. However, due to its centralized structure, there may be security issues with certification availability and integrity. The authors suggested a blockchain-based gateway for smart homes to overcome the security flaws and protect the network from potential attackers. Gateway, device, and cloud are the three levels that make up the network. The authors claim that in order to enhance decentralization and resolve problems associated with conventional centralized design, the blockchain will be integrated at the gateway layer, where data is stored and transferred in the form of blockchain blocks. Almost every user is familiar with and knowledgeable about their smart home devices. According to [11], Due to their constrained processing and storage capabilities, IoT-based devices like lightbulbs, door locks, and power switches have become increasingly vulnerable to security threats as the number of IoT devices used in smart homes has increased exponentially. By encouraging the adoption of blockchain technology and investigating some of the already suggested architectures for smart homes utilizing blockchain technology, Arif et al. aimed to investigate the security of smart homes.

In [12], the authors introduced a resource-efficient blockchain-based solution for private and secured IoT. The approach was made achievable by a new use of computing resources in a typical IoT setting. The black check technique, in which data are loaded over extremely secure channels, is a decentralized way of preserving data. Users now find it simpler to securely keep their data and offer transparency attributable to this. Blockchain technology is the greatest solution to safeguard a community's shared data and can offer secure data storage.

The authors in [13] proposed a homomorphic consortium blockchain to preserve smart-home-security privacy based on a traditional smart-home system. To further validate operational nodes and the security transactions for smart homes, they included verification services made up of verification nodes to their model.

According to [14], security and privacy in IoT are two of the biggest challenges, mainly due to the massive scale and distribution nature of IoT-based networks. Decentralized security and privacy can be offered through blockchain-based methods. The majority of resource-constrained IoT devices cannot handle the delay, high energy use, and computing overhead needed. Authors in [14] presented a lightweight instantiation of blockchain specifically geared for utilization in IoT by eliminating the proof of work and the concept of coins. Table 1 summarises the advantages and disadvantages of securing smart homes with blockchain by analyzing papers by various authors.

Table 1 Relevant Studies on Advantages and Disadvantages of Securing Smart Homes with Blockchain

Related Studies	Advantages	Disadvantages	Methodology
[10]	Blockchain can improve efficiency and speed, as it can complete time-consuming processes and automate them, maximizing efficiency.	Transparency is a huge issue in the present industry. The organizations tried to implement more regulations and rules. With blockchain, smart homes can use a completely decentralized network, which does not require centralized authority and improves the system's transparency.	Using an attribute-based access control system to authenticate users of smart homes and IoT devices allows for real-time communication between home users and a fully validating private blockchain node.
[9]	As a substitute for end-to-end encryption, blockchain is helpful in the development of a common security protocol. Forming an uniform API framework allows it to be used to secure private messages.	It is expensive, and network connectivity is one of the common issues the owners will encounter. The setup and configuration are too complex.	- The network is based on the Ethereum blockchain, and security, reaction speed, and accuracy are measured. - Ethereum is a decentralized, open-source blockchain that supports smart contracts.
[8]	One of the benefits of blockchain is its low cost. It allows data to be submitted peer-to-peer without centralizing the controls.	Blockchain has a difficult process of implementation, and scalability is an issue.	- The confidentiality and authentication issues are resolved by using the SHA2 encryption technique. - The integrity of the data kept in

RESEARCH ARTICLE

			the gateway is maintained using blockchain technology. - The design effectively shapes raw data to perform the data transformation algorithm.
[11]	Combining other technologies with blockchain can strengthen privacy agreements and enhance secure communications.	It needs huge storage; most of the blockchain consumes too much energy.	- Cloud computing and the consortium blockchain were combined. - To make smart homes safe and secure, the architecture for smart homes was designed to provide secrecy, integrity, scalability, and availability.
[12]	It is secure and encrypted by design with so many independent nodes to verify the updates to the chain before the updates.	It can be destroyed, so there is a requirement for a better way to handle this. Whenever the data are updated, the nodes required are not ideal for the commercial blockchains needed for the network to be fast and secure.	Utilization of computing resources in a typical IoT environment (such as smart homes) and application of a Deep Extreme Learning Machine (DELM).
[13]	The block can be verified and inspected by all parties, which can help improve trust and access to the data.	It has a high implementation cost. Accessing the information stored by blockchain requires a private key, but the wallet will be in danger if it does not work.	Built a modified form of the Smart Home System (SHS). Following that, translate this concept to the consortium blockchain architecture.
[14]	Encryption with blockchain can help secure the IoT-based devices, making it impossible to overwrite existing data records.	Blockchain is highly energy-dependent, and it is not a distributed computing system.	

2.4. Problem Statement

The rapid increase in home devices on the market has raised numerous security problems [15]. This is due to such equipment's small power and storage, making people vulnerable to various cyber-attacks, including ransomware. This is why security solutions in the distribution among those devices have gained prominence as a required study field among academics due to their importance [16]. Following are some research questions that will be found in this research.

1. Is it feasible to leverage blockchain protocols to establish security architecture for smart products and home connections from a technical standpoint?
2. How do existing network architectures react to resource unavailability when subjected to the blockchain-based protection implementation described in the linked paper?
3. How will applying the conceptual methodology for users and suppliers affect the security (consumers' network resilience and dependability) of the networks of both service providers and consumers?

3. RESEARCH METHODOLOGY

The methodology adopted in this research involves a blockchain-based smart home gateway consisting of three components: the cloud layer, the gateway layer, and the device layer. The device layer comprises sensor devices that gather and collect information in the smart home communication network via diff erent IoTs installed in a smart home. The gateway layer holds the data produced by the Device Layer. It makes it available to users as required. The cloud layer stores data processed by every gateway and the gateway ID in the blockchain. The modules are distributed to access content from anywhere at any time. Figure 3 illustrates this methodology.

Figure 4 depicts the suggested architecture's flowchart, allowing data from devices at the end to be acquired, recorded in the blockchain, and suitably displayed to users. To gather and transmit information to the user, the data collected

RESEARCH ARTICLE

undergoes hash code encoding and structuring, creates blocks, and validates them regularly to ensure validity even if data falsification happens. To offer clients only the needed data, analysis of data and quality control should be performed constantly.

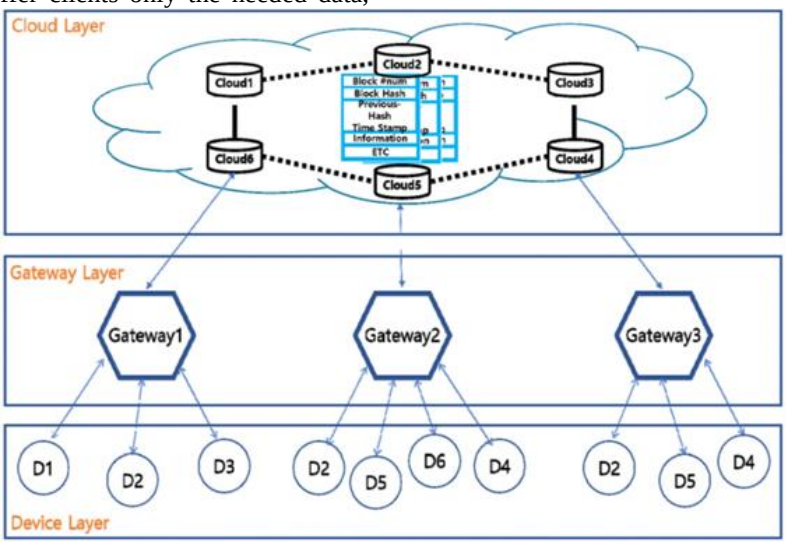

Figure 3 Design Overview

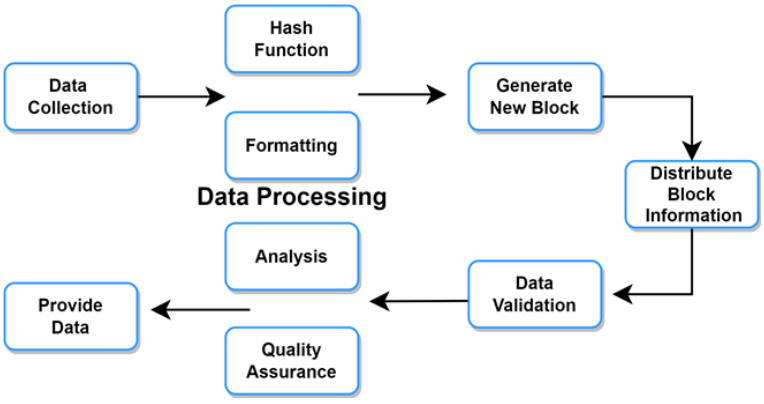

Figure 4 Blockchain Methodological Flow

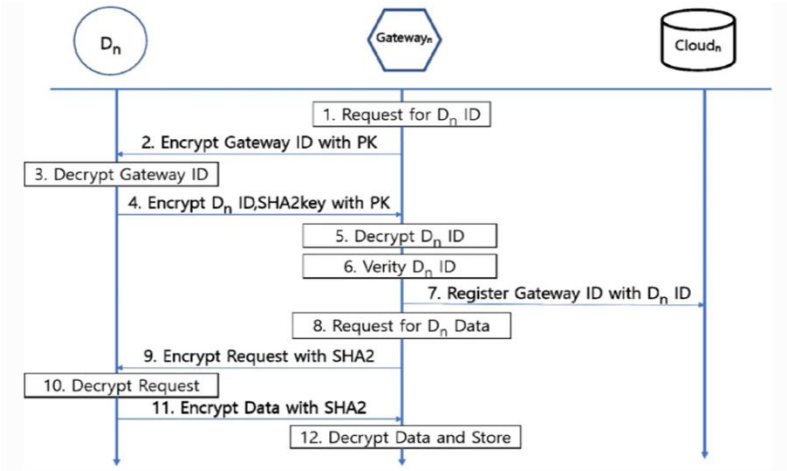

Figure 5 Data Collection and Device Identification

RESEARCH ARTICLE

3.1. Data Collection and Gateway Device Identification

In our methodology, IoT nodes in smart homes are linked to a single gateway, and an ID is issued to every component. These nodes and gateways have unique IDs and the processing power to run SHA and PKI cryptography and decryption methods. Figure 5 depicts the adopted methodology's certification verification and data storage operations for gateway and node connectivity protocol activities.

3.2. Data Preprocessing within the Gateway

Data of diverse quantities and file formats are delivered to the smart home gateway from various IoT devices in the smart home. The suggested architecture's smart home gateway must accurately control IoT and process information based on the user's request. Figure 6 illustrates the data transmission process from IoT to the smart home gateway. Data processing is classified into three stages: collecting, preprocessing, and encryption.

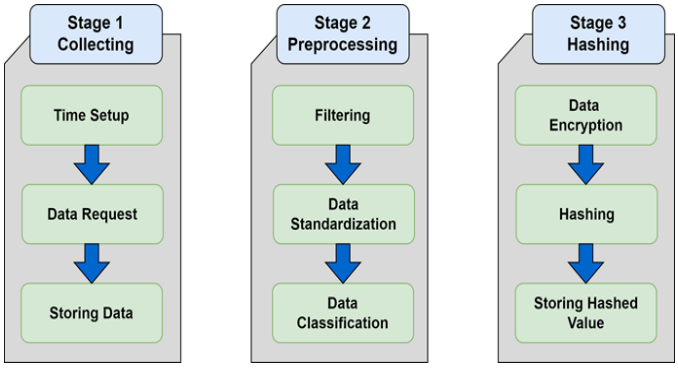

Figure 6 Data Preprocessing

Stage 1. *Data collection*: The device communicates with the gateway for a set time. Data is solicited from the device when additional data is required at the gateway or when an incident happens. The original data is sent and saved in the gateway's memory stick.

Stage 2. *Preprocessing*: The data sent from the gadget is preprocessed within the gateway. It classifies and preserves only the data required by the gateway depending on the device ID and is saved using the normalization and categorization procedure to maximize storage capacity.

Stage 3. *Hashing*: Because the data produced in the smart home comprises sensitive data about the user, it must be protected via encryption. The SHA256 method depends on the user's password, and the hash value is used to record the device's relevant data.

4. PROPOSED MODEL IMPLEMENTATION

The proposed model implementation is depicted in Figure 7. The system's primary agents and constituents are introduced one by one. The data collected from sensors varies by product and originates from sensing data in the home, such as brightness, moisture, and temperature, medical data collected by wearable devices, photographs collected by surveillance devices, and video and audio feeds. The requester is any entity that gains access to the data of smart appliances. The entity that depends on smart home information to ensure service availability is typically called the data requester. This implementation used architecture in [17] to implement our blockchain, as illustrated in figure 7.

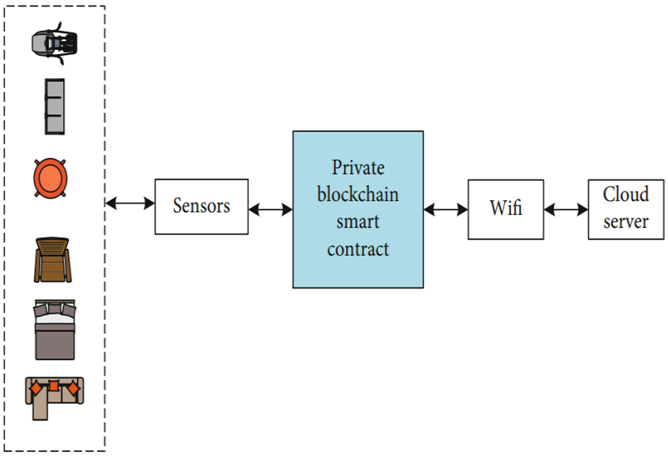

Figure 7 Overall Architecture of Implemented Smart Home Network

This part implements the conceptual model to validate its functionality. Mininet is used as an emulation platform to imitate open vSwitches and numerous functional components, including IoT devices, in implementation. The Mininet was built upon the Linux platform using 2 workstations, each with 32 GB DDR3 RAM and an Intel i7 processor. The gateways were set up by running the SDN managers in different virtual machines (VMs) on a Linux platform. The cloud server was set up using the Amazon EC2 infrastructure. To enable decentralization, the suggested model made use of Ethereum blockchain technology. The Ethereum Bridge in broadcast mode was utilized in the chain setup to deploy an oracle in the private blockchain. The Truffle developer kit was used to launch and build the decentralized application.

The implementation is carried out in a virtual setting utilizing the Mininet simulator. In the developed model, two workstations are first installed as hosts to generate traffic. A virtual controller (POX device) redirects all traffic to the main SDN controller. The intruder attempts to obtain access to the SDN controller. However, the simulated controller accumulates actions from the vSwitches, taking flow table entries into account in the physical SDN controller (C0). The POX manager then uses the blockchain protocol to determine if the transaction is legitimate or not based on previously recorded data in the routing table. The vSwitches validate the

RESEARCH ARTICLE

flow entries once the controller updates them. This is accomplished by inspecting the information of each request submitted by the vSwitches. Every vSwitch's response is treated as a single block it sends to the controller. These transactions are collected and transmitted to the POX manager, which constructs a Blockchain using the suggested technique and verifies it using C0. C0 sends the flow rules as soon as the values in the table are changed. The implementation setup and findings are documented and evaluated. In the network architecture constructed with Mininet, two workstations, h1 and h2, are launched. Furthermore, as shown in Figure 8, further hosts, namely h3 to h8, were launched with a controller C0 and a single vSwitch.

After the network is established, the workstations and virtual controller, i.e., POX manager, are named. The workstations are linked to the POX device, and traffic is routed through the POX console, as shown in Figure 9. The blockchain system is comprised of certain activities upon which the mining process is carried out using proof of work as a resolution method. Figure 10 combines nonce bits, the extrinsic bits, to form a blockchain. The consensus protocol demonstrates how the blockchain operates. Thus the time required to mine the packets or transactions is depicted in Figure 11. In this case, the estimated duration to mine on a 2-bit nonce is 0.24 seconds, which is excellent for the case under consideration. The more nonces introduced, the longer blockchain will take to encode.

```
mininet@mininet-vm:~$ sudo mn --topo single,8 --controller=remote,port=6633
[sudo] password for mininet:
*** Creating network
*** Adding controller
Unable to contact the remote controller at 127.0.0.1:6633
*** Adding hosts:
h1 h2 h3 h4 h5 h6 h7 h8
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1) (h3, s1) (h4, s1) (h5, s1) (h6, s1) (h7, s1) (h8, s1)
*** Configuring hosts
h1 h2 h3 h4 h5 h6 h7 h8
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> xterm h1 h2
mininet> xterm h3 h4 h5 h6 h7 h8
```

Figure 8 Implementation of the Proposed Model

```
DEBUG:core:Platform is Linux-4.2.0-27-generic-x86_64-with-Ubuntu-14.04-trusty
INFO:core:POX 0.2.0 (carp) is up.
DEBUG:openflow.of_01:Listening on 0.0.0.0:6633
INFO:openflow.of_01:[00-00-00-00-00-01 1] connected
INFO:iplb:IP Load Balancer Ready.
INFO:iplb:Load Balancing on [00-00-00-00-00-01 1]
INFO:iplb.00-00-00-00-00-01:Server 10.0.0.1 up
INFO:iplb.00-00-00-00-00-01:Server 10.0.0.2 up
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.2
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.2
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.2
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.2
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.2
DEBUG:iplb.00-00-00-00-00-01:Directing traffic to 10.0.0.1
```

Figure 9 POX Controller in Action

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/214509 Volume 9, Issue 4, July – August (2022)

RESEARCH ARTICLE

```
Mining block 1...
Block mined:0067e5e1fcb60b9151484777725246427b51d95ccaedf0f3c813a09fdbf182af
Mining block 2...
Block mined:008d6a1546b6df1f75f93e0d71a49a34a93ca15a142fa4e782fd66989494e703

[Done] exited with code=0 in 0.243 seconds
```

Figure 10 Time Consumed for Mining in the Implementation Simulation 1

```
Mining block 1...
Block mined:0067e5e1fcb60b9151484777725246427b51d95ccaedf0f3c813a09fdbf182af
Mining block 2...
Block mined:008d6a1546b6df1f75f93e0d71a49a34a93ca15a142fa4e782fd66989494e703

[Done] exited with code=0 in 0.246 seconds
```

Figure 11 Time Consumed for Mining in the Implementation Simulation

5. SECURITY ASSESSMENT

As the network and IoT environments evolve, exploitation tactics on conventional smart home access points are always evolving. IoT systems, in particular, have finite computer power and battery lifetime. An intruder in this communication network can configure numerous attack patterns based on the target computer. Figure 12 depicts the proposed smart home gateway design's assault model adopted from Lee et al. (2020).

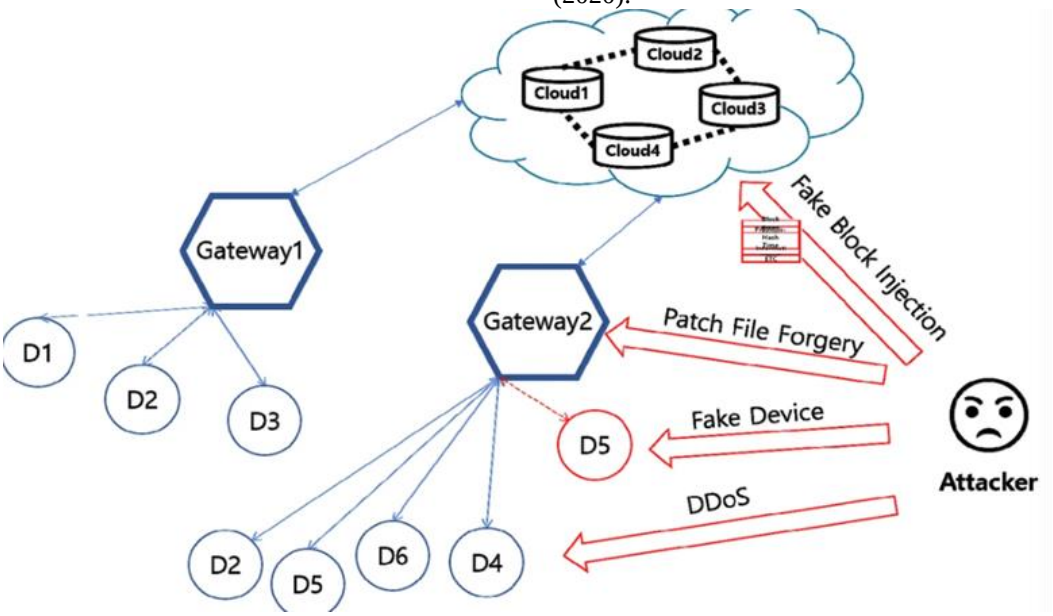

Figure 12 Attack Scenarios on the Implemented Smart Home Network

Patch file forgery: This exploit targets a specific gadget through a linked gateway or the patch config file [18]. Suppose a patch is installed on a computer using a corrupted patch file. In that case, it can lead to system failures, privilege modification, espionage, and data destruction under the proposed design. The suggested architecture protects the integrity of centrally deployed updates for batch equipment security patches and increases the administration server's protection.

Fake block injection (Blockchain 51% exploit): A malicious attack aims to benefit by changing transaction data after acquiring more than 50% of the hashing units of the total blockchain endpoints [19]. A 51 percent exploit indicates that a malicious actor possesses a hash compute capacity that exceeds 50 percent of the total network. Therefore, other endpoints can hold false data; the intruder can produce new blocks and add them to the blockchain network quicker than other nodes. The exploit compels other transactions to use a

RESEARCH ARTICLE

blockchain with falsified data. Nevertheless, for the suggested blockchain-based design's 51 percent attack to prevail, the hash capacity of all participating nodes in the blockchain platform should be higher than the sum of the hashing computing capability. Furthermore, the number of sensor nodes operating in the design grows, increasing the design's ability to defend against cyberattacks [19]. As a result, the presented blockchain-based smart home network architecture is immune to the blockchain 51% exploit.

DDoS: This exploit disrupts a server's operations by overloading it with traffic from infected computers [20]. Verification and authenticity capabilities are disabled if an attack happens on a traditional centralized smart home access network. The outlined design eliminates DDoS traffic throughout data processing by avoiding using loops like If/While/for in simple IoT inquiry codes. The intruder cannot continue unabated using the blockchain's resource consumption restriction. Furthermore, DDoS attacks on the whole blockchain network are unfeasible on all devices simultaneously. This is affected by the nature in which the terminals are located.

Fake device (IP Spoofing) attack: Fake device attack is a cyber-attack where anyone tries to fool other computer systems by posing as a genuine individual using a computer, tool, or system. It's among the techniques hackers use to obtain computer access to extract confidential material from them, convert them into hordes (computer systems seized for malicious usage), or conduct Denial-of-Service (DoS) assaults. A fake device attack is a most often used sort of faking.

6. RESEARCH RESULTS AND DISCUSSIONS

Mininet simulator was used to create a smart home network simulation model. Mininet is an open-source exploratory Internet of Things service that offers a generic API for smart app development. Several fundamental elements of the smart home system are included, such as embedded temperature, light, and moisture sensors, as well as IEEE 802.15.4 radio-integrated transmitters. The smart home network experimental setup devices are separated into two servers/hosts. Each host has four devices, three of which are home terminal equipment, and one is a vSwitch. Every host creates a separate smart home system by building a separate gateway application in Java and storing the forwarding table, service catalog, and data table in the MySQL database. The IEEE 802.15.4 guidelines are used for equipment and service discovery smart home systems. Every host represents a real-world home outfitted with smart home technology.

The applicability of the authentication protocol in a smart home context is first examined. The equipment of the smart home simulation environment, as per the concept suggested in this work, comprises a smart electronic endpoint unit and a home gateway host. The minimum group authentication scheme is uplinked on these systems, and the simulation findings are shown in the figure below. The ordinate in Figures 13 and 14 represents the mean time spent in various stages of the system during the operation of 100, 200, 300, and 400 instances, respectively, and the distance between A, B, and C symbolizes the 3 phases of signature verification, signature generation, and key generation in the authentication protocol.

The time taken by the smart home devices performing each cycle of the authentication protocol is visible in Figures 13 and 14, suggesting that the authentication scheme has high stability and is within the appropriate time range of real application situations. Figure 15 depicts the overall mean time spent on each of the two devices' three stages. Figure 15 shows that the authentication technique suggested in this work performs well in meeting security features and computation complexity. As a result, based on simulations in the previous chapter, the minimum authenticated key agreement method described in this work may match the acceptance criteria of smart home contexts and have a promising application possibility. The simulation platform is then used to create a smart home authentication mechanism based on blockchain to demonstrate the feasibility of the proposed concept. This section will cover the operational specifics, including blockchain and a smart home ecosystem. The system's efficiency is then assessed via simulated experiments.

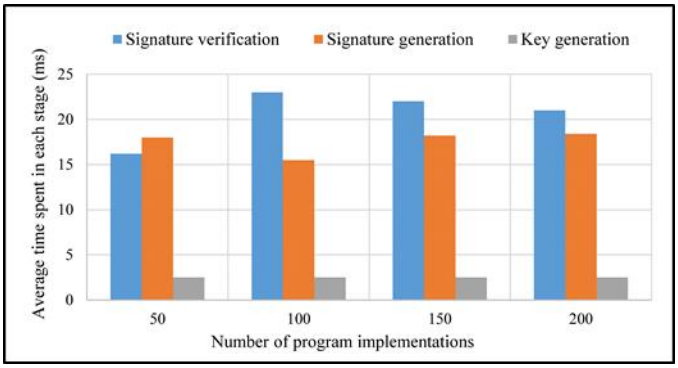

Figure 13 The Average Outcome of the Smart Home Terminal Device's Signature Method Examination

The latency in the blockchain experiments was adjusted to one second. The delay of attribute formation, attribute allocation, and policy formation procedures for four special activity arrival rates were investigated. Attribute formation describes the properties created to be assigned to the key generated in the key generation step, attribute allocation describes the properties or features allocated to a key in the signature generation, and policy formation highlights the policies associated with a particular signature in signature verification. Figures 16-18 show that the delay rises as the

RESEARCH ARTICLE

block grows. In Figure 16, if the attribute creation arrival time is 10, the delay time climbs to 145 milliseconds since the preserved events slow down the writing pace of events inside the blockchain as the block size grows and the message queue fills up.

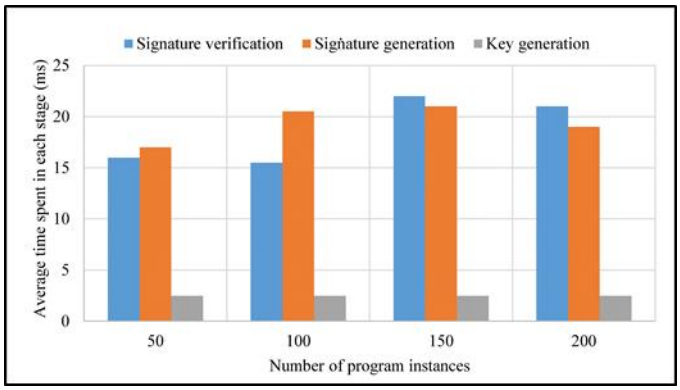

Figure 14 The Average Outcome of the Smart Home Gateway Server's Signature Method Assessment

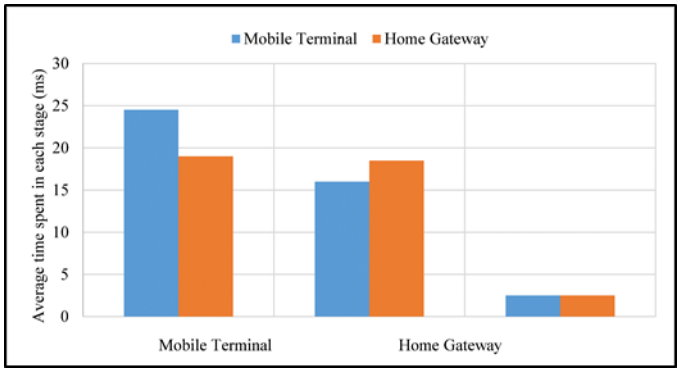

Figure 15 The Average Outcome of the Signature Method Test Done by Several Smart Home Products

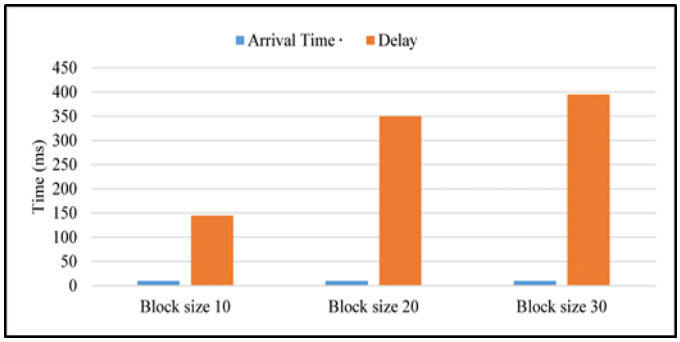

Figure 16 Transaction Delay for Attribute Creation

According to experimental data, attribute allocation takes more time than the other two procedures (attribute formulation and policy development). The experimental findings of the simulation platform demonstrate that by determining the appropriate model parameters for the blockchain network, the access control efficiency of the blockchain network may be enhanced. Tests yielded the best settings of block size 20 and transaction rate 40 operations per second, with a data resource access delay of roughly 1s.

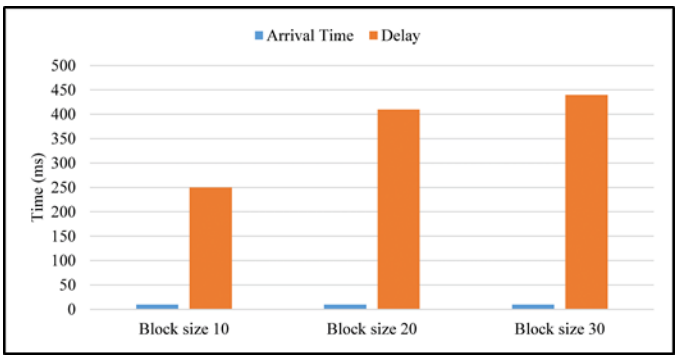

Figure 17 Transaction Delay for Attribute Allocation

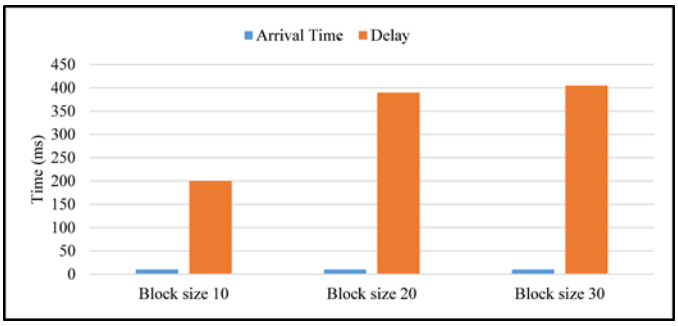

Figure 18 Transaction Delay for Policy Formulation

7. CONCLUSIONS AND FUTURE WORK

The model proposed in this work can handle smart home service access requests quicker than the conventional smart home network. Furthermore, the more authentic peer endpoints in the endorsement policy, the stronger the network's level of security and the greater the connectivity and computation complexity. The smart home system may balance security and usability by configuring proper security settings. Based on the simulation findings, the suggested access control strategy may match the real implementation needs while maintaining adequate security settings. Furthermore, the architecture offers the following options to decrease the centralized gateways that comprise the smart home's privacy, security, and authentication concerns. The encryption method is used to overcome the difficulties of secrecy and validation that arise in smart home gateways.

Furthermore, blockchain technology is employed to ensure the integrity of the data kept in the gateway. The data processing method is applied in the architecture by optimally molding raw data. Three considerations and cases are offered to compare the proposed design to current research, demonstrating its efficacy above earlier investigations.

RESEARCH ARTICLE

Blockchain technology can establish new doors for cutting-edge smart home systems. Nevertheless, some difficulties must be addressed before blockchain is widely adopted in the smart home infrastructure.

- Developing an interoperable system is difficult due to many blockchain systems' varied file formats and transaction runtimes. Information security is a big problem, and it is linked to three states: data leaving the source, data in motion, and data arriving at the target device. Another challenge when designing an interoperable framework is the different consensus processes used by independent blockchain systems. Transporting data from one blockchain to another is necessary to create a smooth application development environment. Smart home blockchain technology to reduce processing time Blockchain for smart homes that are flexible: Whenever the quantity of devices in the system rises, the scalability of the smart home blockchain falls considerably. This is because the multiplication of nodes increases the danger of data inconsistency owing to varying throughput.
- Centralized systems may be retained since homeowners seek a smooth service with the least hardware expense. A typical blockchain's heavyweight hardware architecture is a strain for a small smart home network, where devices have limited resources. As a result, lightweight blockchain technology necessitates increased acceptance and long-term durability and scalability. Considerable research has attempted to provide lightweight frameworks by incorporating shared overlay networks, cluster heads, data structures for block headers, etc. Nevertheless, such research yields only a modest decrease in storage and is based on security assumptions. These assumptions result from a lack of comprehensive testing to guarantee vulnerability in real-world settings.

The proposed system for the smart house network environment has to be improved further to solve the following specifications:

- Mutability and Ongoing Access Control: given the volatility of a smart home IoT ecosystem, access monitoring is needed to manage and regulate access even after it has been granted, and often users require a quick modification. Furthermore, access limits must be used as a consumable, non-refundable quantity of accessibility to some services. For example, the available time for children to use the PlayStation on holiday needs monitoring, and access should be withdrawn promptly (ongoing control) if it is depleted (mutability).
- Conflicts: users may not have policy disagreements since the proposed platform does not include any unfavorable policies; rather, it uses restrictive allocations to prevent a position from being granted certain privileges. Nevertheless, it is conceivable for administrator agendas to conflict. Various users, for example, set the smart thermostat to varying temperature settings. Because customers anticipated discrepancies to be handled autonomously based on a survey of access control demands in a smart home, it is strongly advised that a policy mediation mechanism be implemented into a smart home's access control scheme.

REFERENCES

[1] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," International Journal of Distributed Sensor Networks, vol. 15, p. 1550147719844159, 2019.

[2] A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, and A. Ghosh, "Blockchain-based model for expanding IoT device data security," in Advances in Applications of Data-Driven Computing, ed: Springer, 2021, pp. 61-71.

[3] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," Computers & Electrical Engineering, vol. 83, p. 106585, 2020.

[4] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, et al., "Blockchain for edge of things: applications, opportunities, and challenges," IEEE Internet of Things Journal, vol. 9, pp. 964-988, 2021.

[5] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, "A blockchain-based energy trading platform for smart homes in a microgrid," in 2018 3rd international conference on computer and communication systems (ICCCS), 2018, pp. 472-476.

[6] 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, 2019.

[7] B. Mbarek, M. Ge, and T. Pitner, "Blockchain-based access control for IoT in smart home systems," in International Conference on Database and Expert Systems Applications, 2020, pp. 17-32.

[8] 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, pp. 1-14, 2020.

[9] Z. Shahbazi, Y.-C. Byun, and H.-Y. Kwak, "Smart Home Gateway Based on Integration of Deep Reinforcement Learning and Blockchain Framework," Processes, vol. 9, p. 1593, 2021.

[10] 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.

[11] 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.

[12] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, et al., "A machine learning approach for blockchain-based smart home networks security," IEEE Network, vol. 35, pp. 223-229, 2020.

[13] 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.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017, pp. 618-623.

[15] A. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," Expert Systems, vol. 39, p. e12753, 2022.

[16] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, "Managing smart home appliances with proof of authority and blockchain," in

RESEARCH ARTICLE

International conference on innovations for community services, 2019, pp. 221-232.
[17] K. Liao, "Design of the Secure Smart Home System Based on the Blockchain and Cloud Service," Wireless Communications and Mobile Computing, vol. 2022, 2022.
[18] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," Human-centric Computing and Information Sciences, vol. 7, pp. 1-12, 2017.
[19] K. Kolias, "Kolias C., Kambourakis G., Stavrou A., Voas J," DDoS in the IoT: Mirai and other botnets, Computer, vol. 50, pp. 80-84, 2017.
[20] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," The Journal of Supercomputing, vol. 76, pp. 5320-5363, 2020.

Authors

Abdualrahman Johari works as the Head of Compliance in the private sector, Riyadh, Saudi Arabia. He received his Master's in Cyber Security from Saudi Electronic University, Saudi Arabia in 2022, and a BSc in Computer Networks from Jazan University, Saudi Arabia in 2013. He holds many certificates in the IT field, such as CompTIA Security+, CEH, Certified Blockchain Expert, ITIL, Cisco CCNA R&S and CCNA Security and others.

Raed Alsaqour is an Associate Professor at the College of Computation and Informatics, Saudi Electronic University, Riyadh Branch, Kingdom of Saudi Arabia. He received his Ph.D. in Wireless Communication Systems from the National University of Malaysia, Malaysia in 2008, MSc in Distributed Systems from University Putra Malaysia, Malaysia in 2003, and BSc in Computer Science from Mutah University, Jordan in 1997. He is a member of IEEE, ACM, and IAENG. His research interests include wireless, ad hoc and vehicular networks, routing protocols, simulation, and network performance evaluation.

How to cite this article:

Abdualrahman Johari, Raed Alsaqour, "Blockchain-Based Model for Smart Home Network Security", International Journal of Computer Networks and Applications (IJCNA), 9(4), PP: 497-509, 2022, DOI: 10.22247/ijcna/2022/214509.