National College of Ireland

Blockchain authentication in smart home IoT devices

MSc Cybersecurity

Oluwaseyi Ogunrayewa
Student ID: 20210132

School of Computing
National College of Ireland

Supervisor: Dr Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: OLUWASEYI SAMUEL OGUNRAYEWA

Student ID: X20210132

Programme: MSc CYBERSECURITY **Year:** 2022

Module: RESEARCH PROJECT

Supervisor: DR VANESSA AYALA-RIVERA

Submission Due Date: 15-12-2022

Project Title: BLOCKCHAIN AUTHENTICATION IN SMART HOME IOT DEVICES

Word Count: 6168 **Page Count** 20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: .....

Date: .....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Blockchain authentication in smart home IoT devices

Oluwaseyi Ogunrayewa
20210132

Abstract

The global market for IoT applications in smart home devices reflects the increased interest in this technology. As more and more smart home IoT devices, such as light bulbs, speech systems, sensors, automated locks, power ports/switches, etc. acquire and communicate data, users and owners of these devices must contend with the challenge of ensuring the security of their data. Using a gateway or router, many IoT gadgets in smart homes are centrally connected. This centralized structure introduces a multitude of security vulnerabilities into the network that compromise the confidentiality, integrity, and availability of network resources due to malicious attacks or single points of failure. These attacks use botnets to brute force their way into IoT devices using their default login and password combination. Authentication methods with blockchain technology offers a decentralized structure based on cryptographic techniques to protect data and counter these types of threats.

In this study, a blockchain-based architecture for IoT device authentication is proposed to aid secure data transmission between IoT nodes. The model is tested to measure security, throughput, and efficiency. NS3 simulator was used for testing IoT-specific networks and communication protocols against prevalent cyber threats like Distributed Denial of Service (DDoS) to prevent malicious nodes. The simulation findings demonstrate that having highly trusted authenticated IoT nodes helps achieve high throughput and prevent DDoS attacks.

1 Introduction

Internet of Things (IoT) is a pervasive and omnipresent network that enables monitoring and management of physical things by gathering, collecting, processing, and analysing data produced by sensor devices and intelligent objects. The development of IoT technology in recent years has prompted the conversion of conventional homes into smart, connected homes (Samrah Arif, 2020)

Data from the Statista Technology Market Outlook forecasts that over 130 million households already have at least one smart speaker, and that number may increase to 335 million over the course of the next five years. (Statista, n.d.)

According to Statista researchers, the global market for Internet of Things devices is expected to reach $1.1 trillion next year and is one sector that has mostly escaped the Covid-19 pandemic unharmed: "Homes are now even more of a focus than before during the Covid-19 pandemic. More and more consumers want to use IoT technology to digitally transform their homes, provide them voice commands, and implement extra safety measures. The Smart Home industry has been protected from sharply decreasing sales and the 2020 economic collapse by this consumer trend." For a variety of reasons, IoT networks are vulnerable to

security attacks. Each gadget is easily accessible since they are often contained and kept apart, and there are no personnel in charge of controlling or supervising these devices (Emerging Technologies, 2022).

Traditional IoT systems are centralized and connected to servers, which can cause the entire network to go down if the main server is attacked. IoT devices typically use a username and password combination for authentication.

Many IoT devices are set up by non-technical users who don't bother to modify the devices' factory default login and password. When creating a device, each manufacturer specifies a unique login and password. These default credentials can be easily exploited.

The biggest DDoS attack against Dyn, a supplier of Internet performance management services, was carried out in October 2016 using an IoT botnet (a network of computers, each of which runs a bot). Numerous websites were offline as a result, including well-known ones like CNN, Netflix, and Twitter. (Management, 2022)

Systems that have been attacked with the Mirai virus continually scan the web for IoT devices that are vulnerable before infecting them by entering in using well-known default usernames and passwords.

Blockchain has begun to be recognized in recent years as the solution to the security, trust, privacy, scalability, and dependability issues related to the IoT paradigm. Blockchain's integration with smart homes helps to address major security issues such single point of failure, confidentiality, integrity, and authentication and authorisation. The decentralized digital ledger that is the foundation of blockchain technology is protected by encryption. It runs on a distributed database that maintains a chain of blocks rather than the conventional centralized networks. Each block in a blockchain is linked to the one before it by keeping its hash, ensuring the blocks' security against manipulation.

The IoT devices can be setup using blockchain to authenticate and manage the public key infrastructure and update its functionality.

The above bring us to the following research question: How can authentication be used to prevent malicious IoT nodes that can lead to DDoS attacks and ensure secure data transmission in a smart home network

To answer that question this research deeply analyses blockchain based authentication in smart IoT home systems using an authentication value and using different metrics to evaluate the node performance when subjected to a DDoS attack in an Ns3 Simulated environment.

Additionally, the public key infrastructure is designed using blockchain so that nefarious attackers cannot take over the smart home system.

In this study, IoT smart home network will be simulated utilizing NS3 and authentication solutions will be proposed with blockchain technology and tested against cyber threats like Distributed Denial of Service (DDOS) to prevent malicious IoT sensor nodes.

The following is a summary of the paper's contributions.

1. Without the need for authentication, any node may gain entry and access the data and resources in the network. In order to protect the network from hackers, nodes must be authenticated.

2. Nodes may misbehave and discard the data packets after authentication. As a result, the nodes are evaluated using an authentication value.

3. A DDoS attack is simulated, allowing the target nodes to lose the data packets, which raises the frequency and duration of data transmissions. Hence, secure data transmission must be carried out by highly reliable authenticated nodes and the resulting metrics is evaluated.
The remainder of this paper is structured as follows: A few related system architectures with blockchain authentication in IoT devices are examined in Section II. The proposed cutting-edge blockchain-based authentication model and simulation of the framework with DDoS attack are all described in Section III. The investigation's outcomes and conclusions are presented in Section IV.

2 Related Work

This section presents a thorough overview of newly proposed blockchain architectures to address the dangers and weaknesses impacting the security of IoT smart home systems. In the realm of research, several security infrastructures have been suggested.

2.1 Node Authentication in IoT devices

An access control procedure is necessary for the IoT platform's safety in order to prevent random access by unauthorized users and cross - functional authentication of particular users (Hong, 2020). The authors of (Hong, 2020) employ a simple authentication method to identify rogue nodes in IoT networks. The BS allocates sequence numbers to the nodes in their system based on the distance between them.
Traditional IoT identification methods use the single-point-of-failure Trusted Third Party Protocol (TTP), which is centralized-based (Cui, 2020).

The Merkel Tree idea is used by the Base Station (BS) to confirm the authenticity of the nodes during communication by using the allocated sequence numbers. A blockchain-based mutual authentication system for sensor nodes is presented in (Cui, 2020). In this plan, the BSs and Cluster Heads (CHs), respectively, host the public and private blockchains. Ordinary nodes are registered using CHs, whereas CHs are registered using BSs. Smart contracts are used to register nodes and verify their authenticity.
Although identification data is kept on a public blockchain sustained by the BSs. Blockchain is used by the researchers in (Moinet, 2017) to do away with a third party's involvement in node authentication and trust assessment. Additionally, they keep on the blockchain the nodes' actions and credentials. Content access, trustworthy authentication, and trust management are not supported by existing approaches in (Moinet, 2017). The blockchain is used in (Tian, 2020) to handle keys securely in the Wireless Sensor Nodes (WSN). The blockchain contains both the nodes' public keys and identification data.
When opposed to static Sensor Nodes, dynamic WSNs have greater levels of unpredictability and extensive coverage, which raises trust concerns. Traditional Sensor Nodes often have homogenous architectures, complicated design protocols, and extra overhead (Tian, 2020). Each node's lack of traceability in the IoT network results in inefficiency and a considerable loss in industrialization. However, IoT device connections, deployment, and communication lead to private and confidential information worries (Rathee, 2020).

The current encryption standards, such Secure Socket Layer communications are made possible by Transport Layer Security (TLS) and SSL between two ends. These methods do not guarantee authentication and user anonymity (Kolumban-Antal, 2020).

2.2 Malicious Node Detection

A WSN faces a variety of difficulties and dangers when attackers are present. Various approaches are put forth to address security concerns, however they do not guarantee network efficiency and secure routing. However, because the feedback mechanism relies on the most reliable cluster nodes, there is more network overhead (Kumar, 2020).
The current smart city system has been shown to have problems with bandwidth constraints, excessive latency, scalability, privacy, and security (Sharma, 2018). Due to assaults, security vulnerabilities with IoT devices are getting worse as they multiply. The gadgets must be secured against cyberattacks. Existing options are inadequate because of problems including limited storage, a single point of failure, significant latency, and expensive processing.
Additionally, older systems have problems such as privacy issues (data is collected without the user's consent) and big data issues (accurate choices and attack detection require a vast quantity of data). This results in making poor decisions (Rathore, 2019). Mobile devices perceive and compute the data in crowd sensing networks, which reduces costs, however there is a concern about privacy leakage. Low user involvement and user-uploaded misleading information that exposes sensitive information (Jia, 2018). In the Internet of Things, information is stored centrally. Products made from shellfish are extremely sensitive, perishable, and their quality often degrades quickly.
To find and remove the malicious nodes from the network, in research papers by (Goyat, 2020) and (Kim, 2019) they evaluate the credibility of the sensor nodes. Based on how the nodes behave and interact with one another, their trust levels are calculated.
Obtaining an exact node position in a difficult and distant environment is a challenge if malicious action is carried out on cluster nodes. The localization accuracy and energy dissipation are impacted by incorrect location estimate has an impact on the Sensor Nodes' lifespan (Goyat, 2020). The changing dynamics of Sensor Nodes in (Kim, 2019) makes it a difficult issue for the localization process. The Sensor Nodes are unable to communicate the precise position due to the sectioned information in the system

2.3 Blockchain in IoT devices

Blockchain has poor performance and significant resource requirements, which are not properly handled. In a Peer to Peer (P2P) network, where storage and bandwidth are difficult to manage in IoT devices, miners also integrate the large block data and handle numerous transactions (Liu, 2019). The Internet of Things (IoT) huge data, where numerous nodes have a duplicate of the whole ledger, cannot be handled by existing blockchain technology well. Blockchain's distributed nature necessitates a lot of storage (Uddin, 2019). For low power and memory-constrained systems, the local replica of the blockchain records is not practical (Danzi, 2019). Due to its chain structure and simultaneous data updates, blockchain has a

sluggish update rate. In contrast, before connecting a transaction in a network, the two prior transactions must be validated.
Sensor Nodes (SNs) are invalid due to their finite computing resources in the earlier communications (Rovira-Sugranes, 2019). Wireless mobile devices encounter several difficulties with the PoW puzzle in the mining process in blockchain applications, which calls for strong processing power and readily available data storage (Liu, 2019).
The mining process is transferred from IoT devices to edge nodes by the authors in (Liu, 2019). As a result, they reduce the stress on IoT devices and enable the deployment of blockchain on IoT devices with limited resources. For IoT devices, a lightweight blockchain is given in (Liu, 2019). With this strategy, the authors reduce the blockchain's processing needs in industrial IoT contexts with limited resources. The lightweight blockchain solutions are also suggested for IoT networks in (Danzi, 2019) and (Kim, 2021) to lower the computational and storage needs.

2.4 Secure Routing

The dynamic behaviour of the normal nodes has been disregarded in favour of focusing on the evolution of static topology in the previous solutions. Compilation of static node data
perhaps inaccurate, which causes unreliability and network interruption. The network's dynamic nature results in energy shortage and packet delivery deterioration (Haseeb, 2019) and (Javaid, 2019). A WSN faces a variety of difficulties and dangers when enemies are present. Although several methods have been put out to address security concerns, network performance is not guaranteed. In the secure routing procedure, feedback network overhead when based on the most reliable beacon nodes (Kumar, 2020). Because establishing trust management systems like PKI is expensive and crucial to IoT vendor relationships, trust concerns frequently develop (Ramezan, 2018).
As a result, suspicious nodes participate in the routing since the current routing techniques cannot discern between the nodes' activities. A black hole attack is caused when a malicious node receives a data packet from one of its nodes and discards it without passing it on to the next node (Yang, 2019).
Multihop routing in WSNs is vulnerable to attacks from malicious nodes. A blockchain-based and Q-learning-based routing protocol is provided in (Yang, 2019) to carry out the safe routing. The plan employs blockchain to keep the routing data in a database that cannot be altered. Q-learning is utilized, however, to choose the
depending on the forwarding rate of the routing nodes, an appropriate next hop for packet forwarding Similar to author (Ramezan, 2018), route finding and route establishment activities in IoT networks are carried out via smart contracts built on the blockchain.
In addition, the authors employ bonds made of blockchain currencies to stop routing process nodes from acting maliciously. As a result, this technique has less routing overhead.
The authors of (Haseeb, 2019) describe a paradigm for safe routing in WSNs based on blockchain technology. They believe that the CHs' remaining energy may be used to forge a path to the BS. A chain of blocks containing the detected data is created in (Kumar, 2020) using a data structure like a blockchain. Additionally, the strategy chooses the appropriate data forwarding nodes based on the frequency of successful and unsuccessful data transfers.

2.5 DDoS Attack Detection

(Anhtuan Le, 2016) proposed a routing specification-based semi auto profiling technique that defines the network operations through simulation traces. The simulation traces will help to track the node behaviours. The proposed identification process will contain the legitimate protocol states with corresponding analysis while the implementation accompanied cluster heads while executing the simulation, cluster head will monitor the whole network.
To maintain the resource management the proposed system will set the cluster member activities which will send packets to neighbours and identify the cross check between the cluster heads and cluster members. The record sequence of routing information Object (DIO) and Information Solicitation (DIS) messages to control the delay transmitting complex issues related resource management in the same sequence. The simulation results reflect the successful accuracy rate in routing attacks detection also another hand the overloading will be reduced while enabling large scalability network.

3 Research Methodology

3.1 Authentication of IoT nodes in Blockchain Architecture:

The proposed decentralized IoT authentication system with blockchain was achieved by utilizing an authentication value produced by an IoT node/user and the authentication solution was simulated using NS3 simulator to mirror a real-life network architecture where different IoT nodes representing IoT devices/sensors are connected via wireless protocol. One of the IoT nodes acts as the Certification authority and approves or rejects any request from a new IoT node wishing to join the network based on the authentication value provided by the new IoT node. Data requester privacy requirements are acknowledged by blockchain authentication access module.
The certifying authority node receives the private key of the new node and validates the identity of private key message sent by new node based on the authentication value. Then the certification authority node will share the new node public key to other IoT network nodes. Before sending certificate to the new node, after which the new node is then registered in the network. Authentication of every certified node has to be registered in the network.
After every successful authentication the certification authority will provide the authorization to exchange data between existing node and new node. Through this authorization the data exchange will happen in secure way. This authentication process is simulated in NS3 by having a user provide the authentication value to add a node to the network and a graph can be plotted in NS3 to analyse different metrics like the Overhead latency, Bandwidth and Throughput increase/decrease in the network once a new node is added.

3.2 DDoS attack on IoT nodes Blockchain Architecture:

The proposed decentralized system uses a number of inputs to carry out data transactions, and if any one of the nodes does not complete the user authentication process, then the inputs will

not be processed for data transmission. The DDoS Attacker involves data transmission along with malicious activity. An attacker uses a routing path and tries to injects fake traffic into the network to flood the resource with server data requests, and ensure no bandwidth for genuine nodes. The DDoS attack exploits the inherent vulnerability in resource network. The attacker sends continuous packets of information requesting the resource for authentication. A faulty system shares the fake address, thereby the possibility for sending authentication to other nodes stops. The resource is closed without further interaction and routing path filled with forged data requests and traffic increases. The authentication procedure fails to generate any results, and network traffic related to malware activity are recorded. The proposed decentralized authentication system then limits the node's access by ensuring each node must be verified before accessing the network, thereby preventing DDoS attack.
This DDoS attack process is simulated in NS3 by overloading two different IoT networks with data requests. The two networks include an IoT network without an authentication process and the proposed IoT authentication solution. A graph is plotted in NS3 to compare the two networks and analyse different metrics like the Overhead latency, Bandwidth and Throughput increase/decrease in the network.

4 Design

In this model, IPv6 is used to facilitate communication between different IoT network node entities. Since IPv4 address space is limited IPv6 is used. Utilizing IPv6 permits the architectures to be quickly integrated into the current Internet infrastructure.

This model defines service behaviour and functionalities of IoT nodes. The architecture specifies network security. The certifying authority declares IoT node service request acceptance, user interruption and response handling. Each node will be handled based on the authentication value provided. The architecture also ensures that new IoT node request execution process does not affect the performance of the network.
Blockchain's primary idea is that it maintains a distributed and decentralized database of records across several devices, making it impossible to change a record without also changing all following blocks or getting agreement from all network nodes. The blockchain's current state must be agreed upon by all the nodes that maintain it. Based on the characteristics of the participants in the consensus mechanism, blockchains may be divided into two categories which are public and private blockchain.
Public blockchains are transparent and permissionless, allowing anybody to join and take part in the consensus mechanism without needing the consent or confidence of other network nodes. Compared to private blockchains, public blockchains require more complex consensus methods. Proof of Work (PoW), Proof of Stake (PoS), Proof of Activity (PoA), and Proof of Burn (PoB) are some of the most well-known consensus mechanisms
Private blockchains are permissioned blockchains in which every node is familiar with and trusted by every other node, and every new node joining the network must have the approval of the majority of nodes. After validation, the consensus methods in the network are comparatively easier as each node is added to the system. In this research paper, the private permissioned blockchain is utilized.

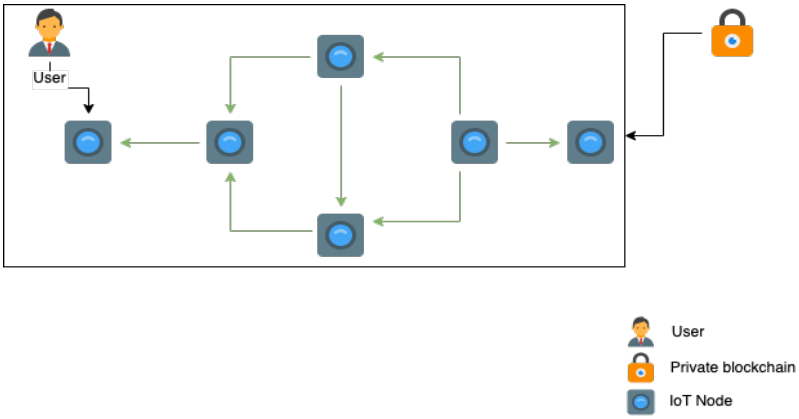

Figure 1: Private permissioned blockchain

Each block contains the block's header and body. There is no parent block for the genesis block, which is the first block on the blockchain. The block header contains the following information in that order: block version, hash, timestamp, nBits, Nonce, and Parent block hashes. The body of the block is made up of transaction data which includes the most recent public key, IPv6 addresses, the node's identification number, and authentication value

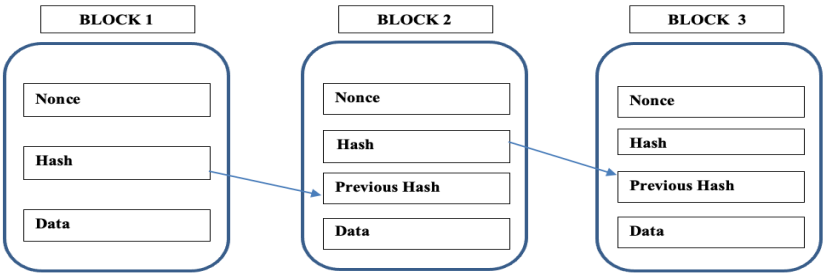

Figure 2: Blockchain structure

The proposed architecture only permits the following 3 types of transactions: addition, removal, and update. The transactions are held in a central pool, and every predetermined amount of time, the certifying authority collects them all, verifies them, creates a new block, adds it to the chain, and broadcasts it to the network. Along with the newly added transactions, the freshly created block also includes the content of the preceding block.

In this model. IoT devices and end users make up an IoT node. The Central Certifying Authority is the entryway. The CCA permits the data transfer to IoT Nodes after verifying the authentication value.

The authentication of IoT nodes involves the subsequent processes.

Step 1: The CCA determines if the Nodes are alive or not by checking their status.

Step 2: Based on the effectiveness of nodes' communications, the authentication value is determined.

Step 3: If the authentication value exceeds a certain threshold, the node is regarded valid; otherwise, it is malicious.

Step 4: Each node's authentication value ranges from 0 to 1. Nodes communicate a node-specific authentication value to the CCA upon authentication. The CCA has implemented the malicious node detection.

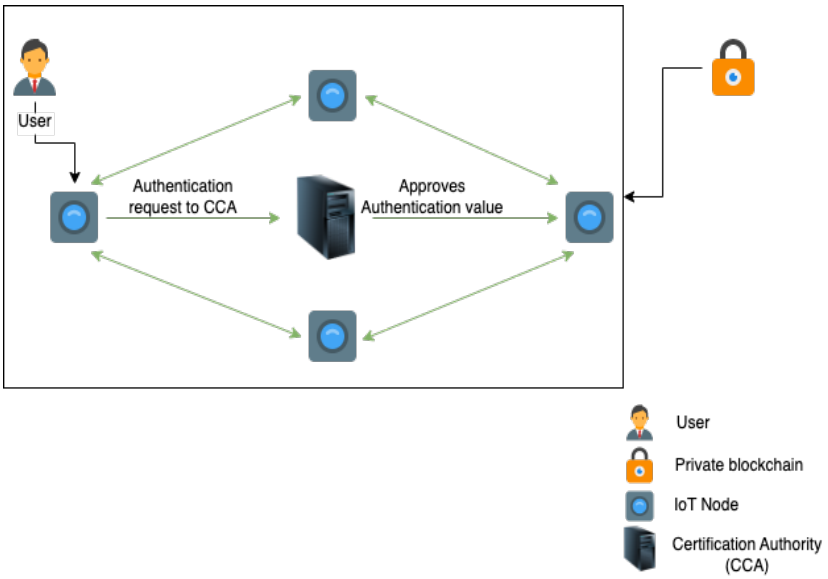

Figure 3: Authentication Model

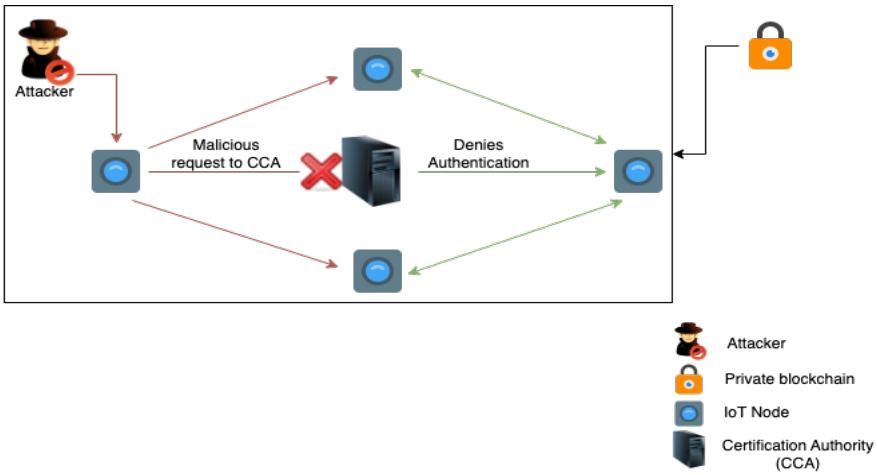

Figure 4: DDoS Prevention Model

Security issues on decentralized network are a serious challenge. For instance, DoS attack targets resource unavailability to its legitimate users. A denial-of-service (DoS) attack captures legitimate user routing path and fills it with fake traffic, it causes resource unavailability. This model is able to prevent DoS attack by requesting for an authentication value from any node that tries to join the network.

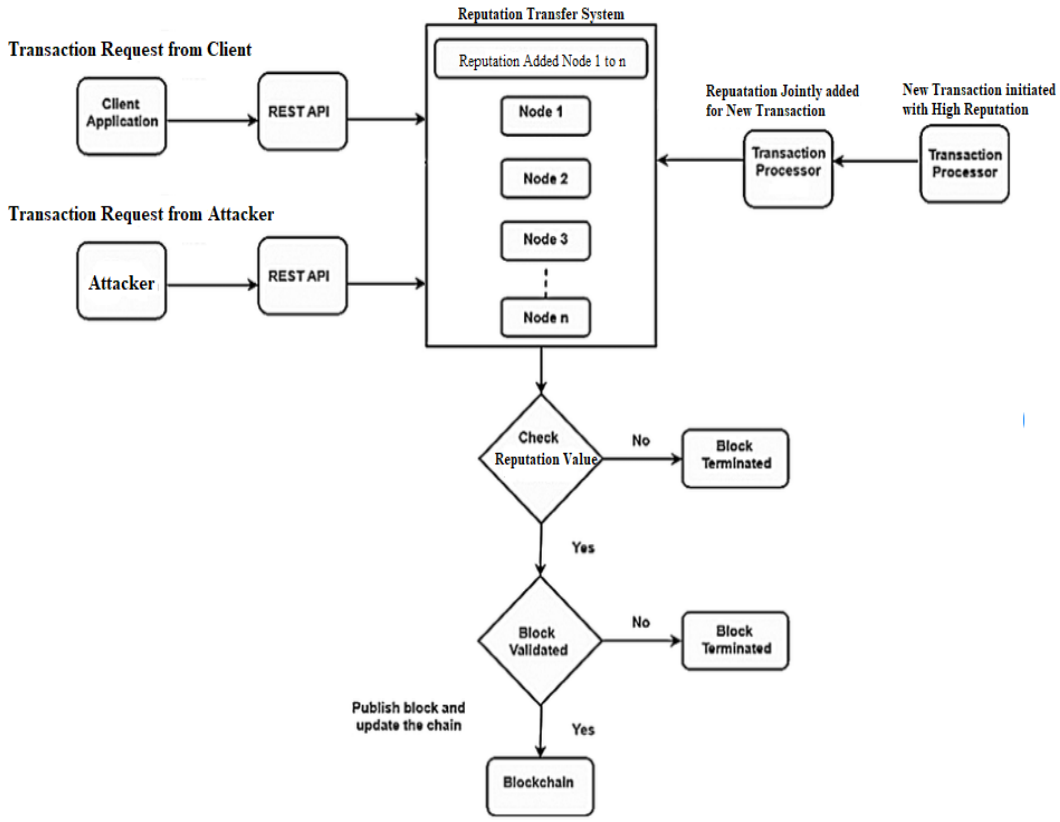

Figure 5: IoT node Authentication Flowchart

5 Implementation

The proposed system ensures security of blockchain transaction users when they initiate data transaction between source and destination. When the program runs the user is interrupted with an authentication validation system and provides authentication value. Any transaction request initiated by attacker also follows the IoT authentication system to get the authentication value. Based on authentication value it will proceed further to publish or reject the block.

The transaction is initiated with multiple users M={1,2,3,,,,,m}, m denotes users' participation with various transaction request. Each transaction request has been initiated with an authentication value. The authentication value is denoted as r.

Ri = {xi ,yi ,zi} , i € M, ----------(1)

In this equation, Ri indicates joined authentication value owned by new transaction. xi, yi, zi indicates the authentication value size required to initiate the new transaction.

This shows the joint authentication value for online transaction system. The Aim of multiple users involving multiple transaction requests is shown below,

Min ∑mi=1 {ai1xi + ai2yi +ai3zi} ----------(2),

In this equation ai1xi denote attacker transaction request processed with normal user transaction in all three cases ai2yi and ai3zi terminate attacker request based on authentication value of the system. The positive authentication value allows for new online transactions. The attacker authentication value is validated before termination from the blockchain system.

5.1 Authentication system Pseudo Code:

Authentication System Algorithm

1.Tn =Ts Ự C (Transaction Request)
2. n is number transaction requests
3.Tn – total number of transaction request.
4.if (Rv = 0,1,2,,,,,+n)
5.Attach for new transaction - New Transaction - NT(Rv)
6. if (Rv = Rv-1 ;)
7.Terminate.
8.Block validation for NT(Rv)
9.for (all transaction values are validated)
10.if (NT (Rv)>1)
11.insert new transaction NT(Rv);
12.End

Once the authentication code runs in NS3
The authentication process follows the steps below:

Step 1: Initiated authentication of IoT devices
Step 2: Blockchain IoT device data request Enquiry
Step 3: Blockchain IoT device Block reading request
Step 4: IoT device Block Authentication
Step 5: Updated Blockchain with response
Step 6: Exit

The system requests for:

- IoT Device Id
- IoT Device Name
- IoT Device Data Authentication Details
- IoT Device Authenticated Data

These parameters provided will be used as the authentication value to add and detect a malicious IoT node in the network.

5.2 Simulators

The discrete event network simulator Network Simulator 3 (NS-3) is primarily intended for research and open-source educational use. Nearly all communication protocols are supported

by NS-3, and it also supports a number of modules that enable distributed simulation and parallel simulation, among other things. To learn more about the specifics of the simulation findings, use network simulators. The output of the simulation is data that is used for this research. There are other ways to get this information, including creating PCAP traces, printing files, creating visualizations with gnu plot, and using a flow monitor. The offline animator NetAnim, which is based on the QT toolkit, is included in the NS3 package. The generated XML trace file from the simulation can be used by NetAnim to animate the ns3 network simulation. Therefore, the actions required to produce this XML trace file and set related properties must be carried out within the ns-3 simulation code. Ns3 is an open network simulator running on Linux operating system that provides different network characteristic with various applications. The system architecture is tested and validated using a NS3. The NS3 simulator was used because it is costly to test new threat models on actual networks and devices.

Other Simulators considered include NETSIM, OPNET which is a windows only commercialized simulator, CORE, OMNET++, IoTSIM and COOJA are open-source simulators but they do not offer as many protocols, network stacks and IoT devices simulation variety that NS3 offers.

6 Evaluation

6.1 Simulation configurations:

Experimental configuration setup for blockchain based authentication IoT Node value analysis system using Ns3 simulator. The simulation is executed according to IoT node authentication value and parameters showcased. The nodes are associated with transaction request and communication radius is set to 750m. The total node number is 30 and rectangle simulation area is defined with 3000 x 3000. The specifications such as total node number, rectangle simulation area and communication radius were selected randomly. The routing path stability executed successful data transmissions

Table 1: Configuration

Parameters	Value
Simulator	Ns3
Operating System	Ubuntu 16.04
Nodes	30
Simulation Area	3000x 3000m
Mac Layer	802.11g
Channel Type	Wireless Channel
Channel Bandwidth	11mbps
Transmission range	750 m
Network Layer	Peer to peer
Simulation Time	20 Mins

6.2 Evaluation Metrics

End-to-end delay is the amount of time it takes for a packet to go from its IoT source to destination across a network taken into consideration the transmission range and bandwidth in Table 1.
Throughput Delivery refers to the rate at which packets successfully travel from their IoT node source to destination taken into consideration the transmission range and bandwidth in Table 1.
Routing overhead is the extra control packets that must be sent in order for data packets to be delivered successfully. It is the proportion of data packets received at the destination node to the total number of routing control packets delivered by all nodes.
Scalability is the ability of the network to cope with increasing workloads, by expanding the network's bandwidth capacity to support new nodes
Memory Usage refers to the amount of system RAM used by IoT nodes when data is being transmitted from source to destination

6.3 Scenarios considered for Simulation System:

6.4 Experiment 1: DDoS attack

DDoS Attack captures source routing path and makes it inaccessible to legitimate users.

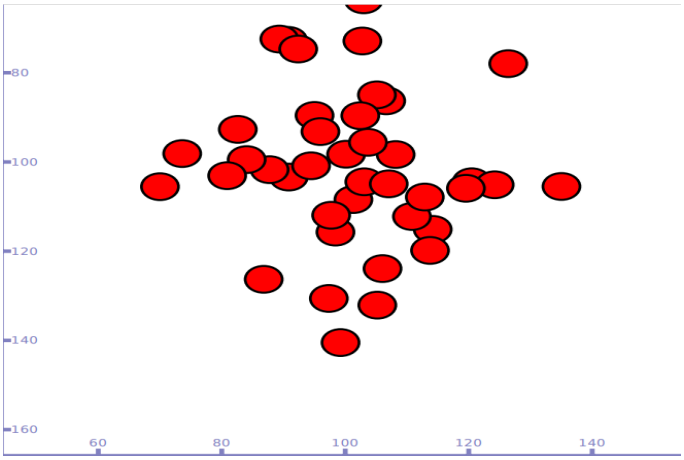

Figure 6: Injection of fake routing

Figure 6 denotes a scenario using ns3 simulator. It captures the objective of the attacker which is to purposefully manipulate resource routing and exhaust resource availability. The attacker injected malicious behaviour to the blockchain system. The simulation execution time is fixed at 20 minutes. The network simulator associated multiple nodes for the authentication of the IoT system. Authentication system added multiple nodes and each node produces its own authentication value.

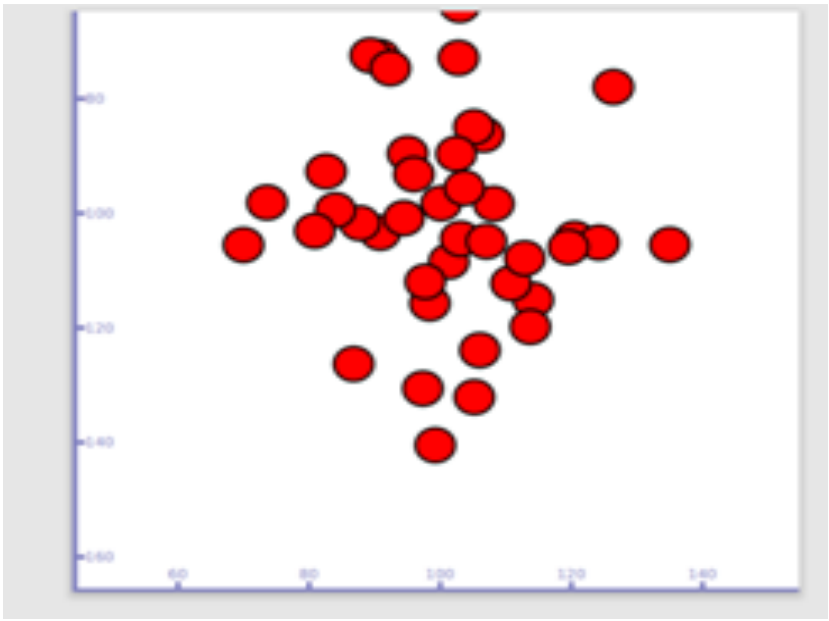

Figure 7: DDoS on proposed IoT Authentication System

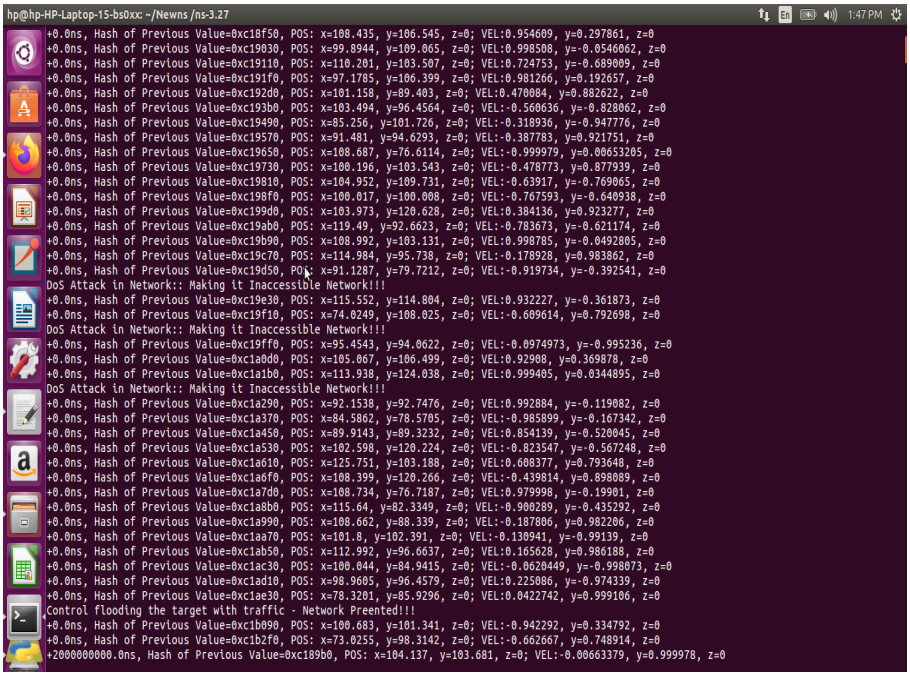

Figure 8: Malicious activity in traditional network

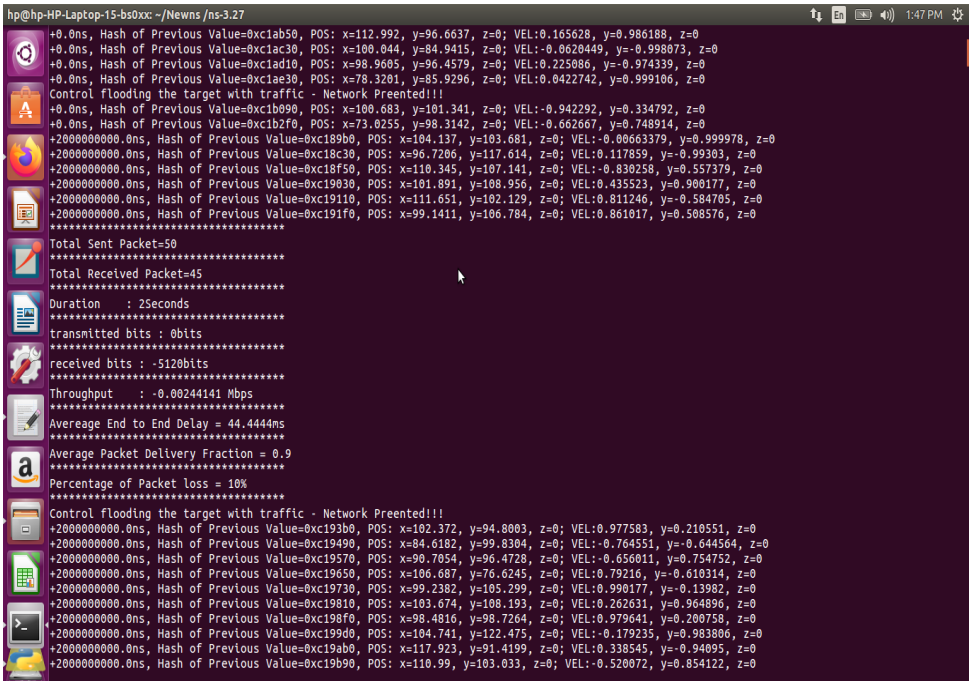

Figure 9: Flooding target with traffic

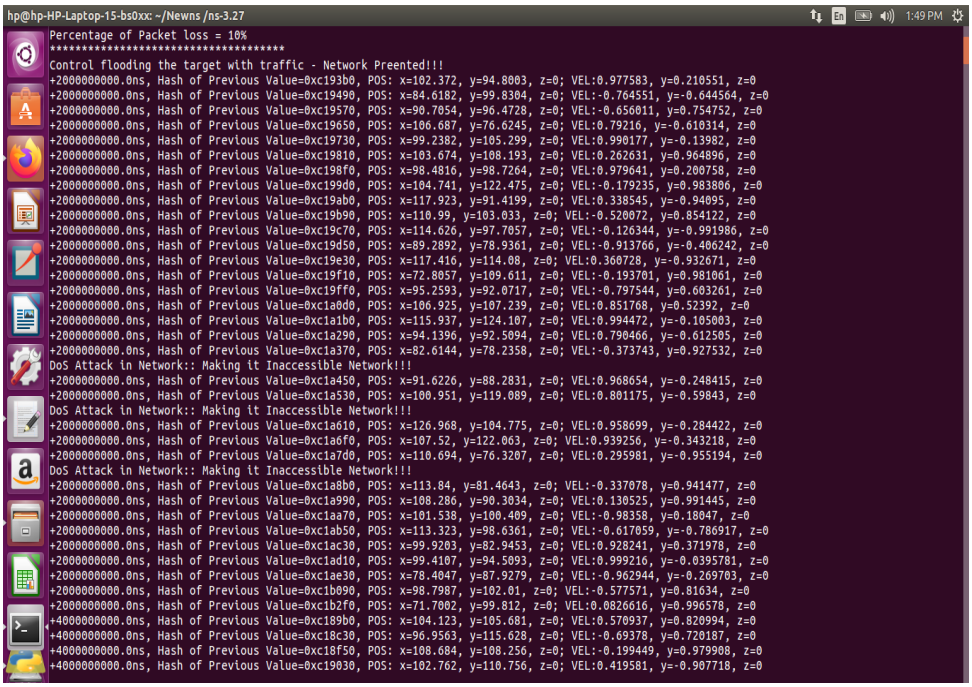

Figure 10: Attacker makes network inaccessible

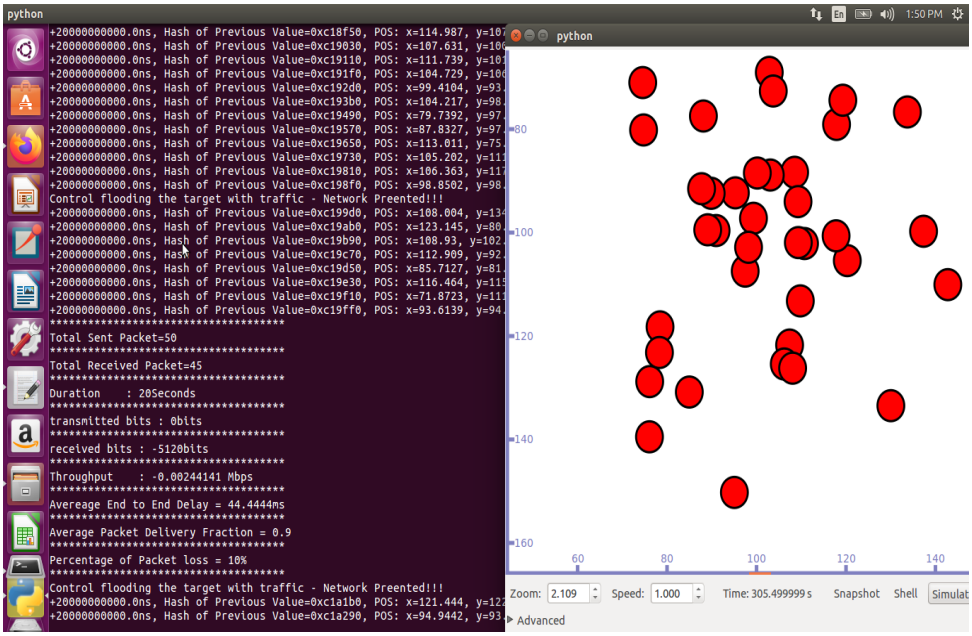

Figure 11: Proposed IoT Solution Authentication value terminates the Attacker

Figure 11 clearly indicates the attacker node has been terminated through the authentication value verification system.

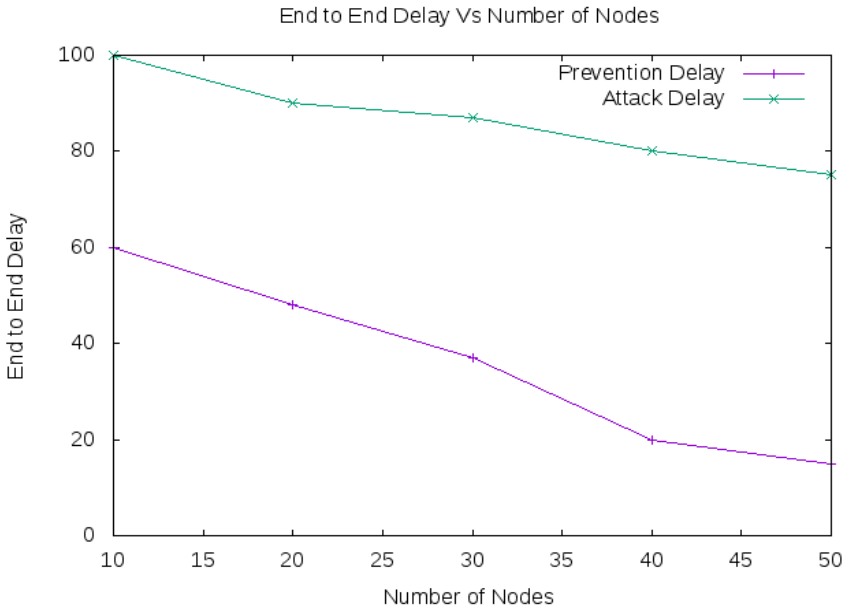

Figure 12: End to end Delay in IoT Authentication Systems

Figure 12 clearly describes attacked node response in comparison to the proposed prevention solution to measure End to End Delay. It shows that the proposed system has a lower end to end delay in transmission when compared to the malicious network.

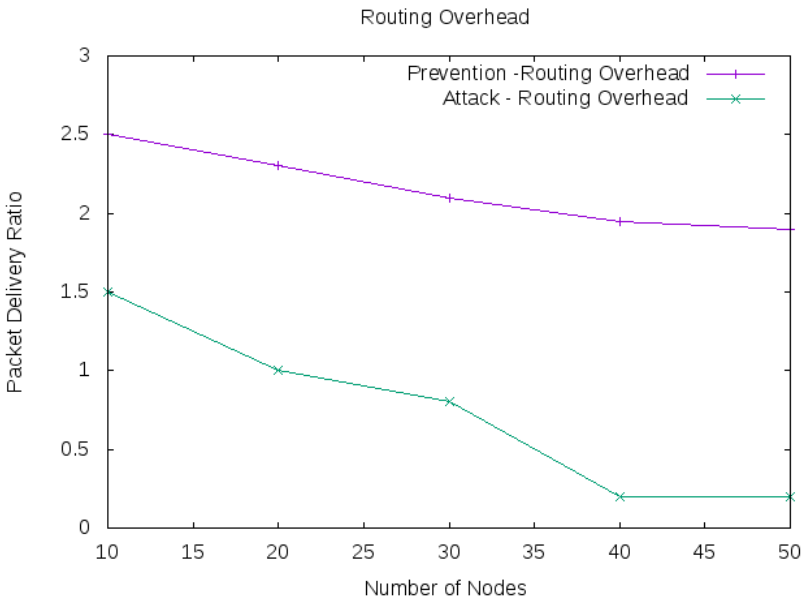

Figure 13: Routing Overhead in IoT Authentication Systems

Figure 13 clearly describes attacked node response in comparison to the proposed prevention solution to measure Routing overhead. It shows that the proposed system has high routing overhead when compared to the malicious network.

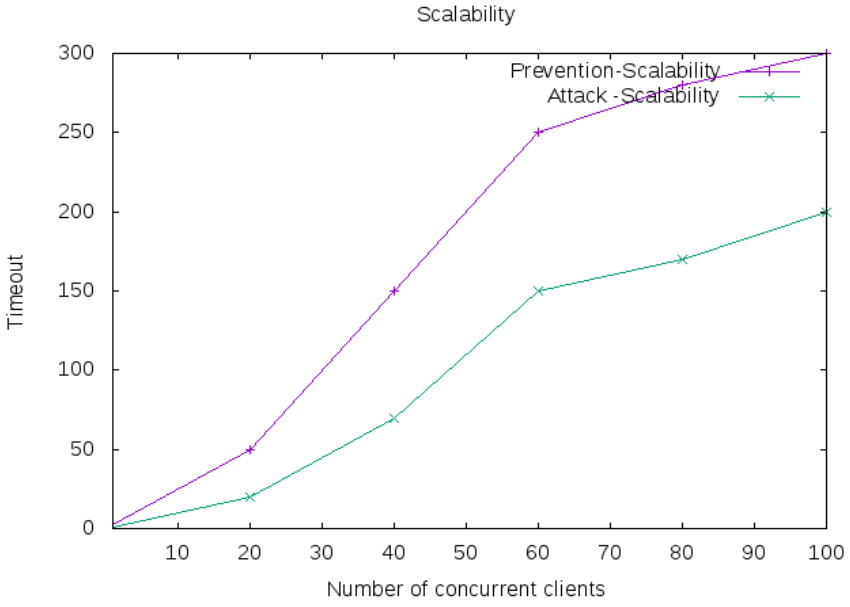

Figure 14:Scalability in IoT Authentication Systems

Figure 14 clearly describes attacked node response in comparison to the proposed prevention solution to measure Scalability. It shows that the proposed system has higher scalability when compared to the malicious network.

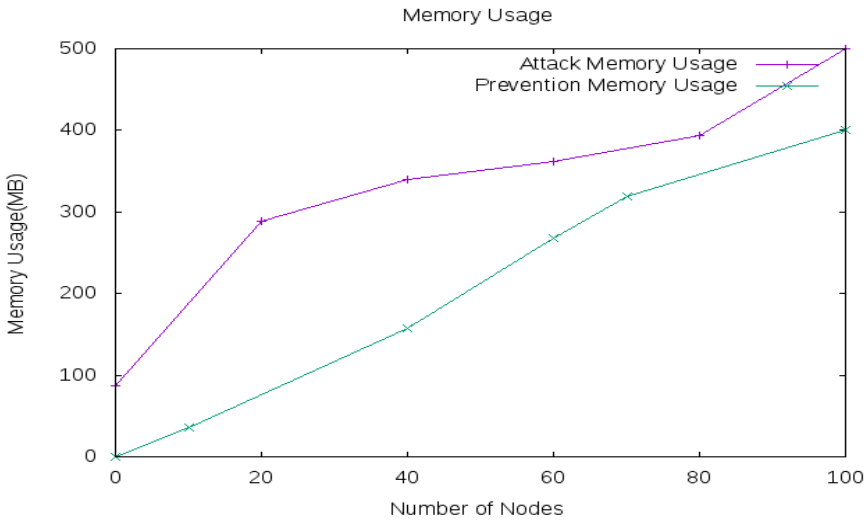

Figure 15: Memory Usage in IoT Authentication Systems

Figure 15 clearly describes attacked node response in comparison to the proposed prevention solution to measure Memory Usage. It shows that the proposed system utilises less memory when compared to the malicious network.

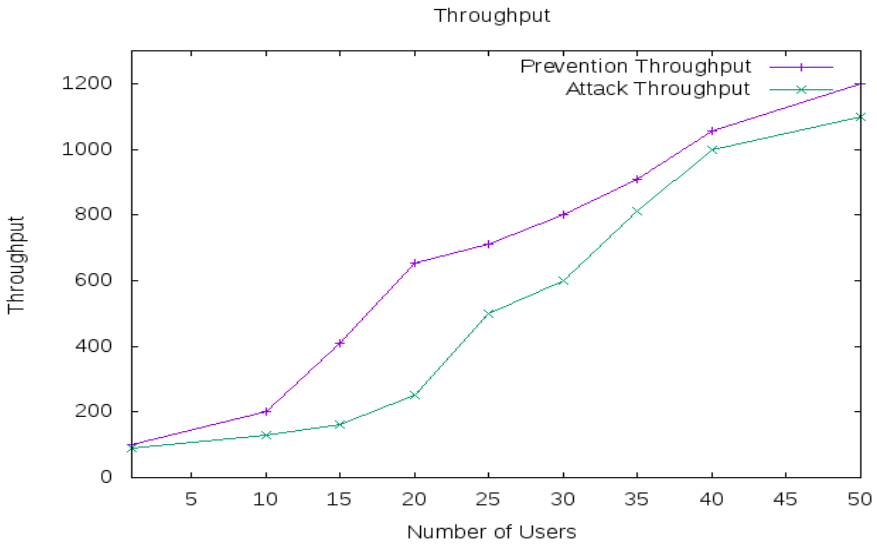

Figure 16:Throughput Delivery in IoT Authentication Systems

Figure 16 clearly describes attacked node response in comparison to the proposed prevention solution to measure Throughput. It shows that the proposed system has a higher throughput delivery when compared to the malicious network.

7 Conclusion and Future Work

A blockchain-based authentication model for secure data transfer and the identification of rogue nodes is put forth in this study. The private blockchain and smart contract are employed to accomplish the authentication objective. The nodes build the blockchain, and

after successful authentication using public key cryptography, each node's authentication value is calculated. In the presence of highly trusted nodes, the simulation findings indicate greater throughput and packet delivery ratios. As each node's reliability is evaluated, the nodes with a high trust value join the network; otherwise, they would be excluded. A modest network is used for the data transfer.

There are intentions to expand research efforts to bigger networks in the future and utilize a global public blockchain architecture with base stations, cluster heads and multi wireless sensor nodes and also incorporate machine learning into the authentication process to enable nodes automatically detect malicious request that has been previously attempted.

8 Bibliography

Anhtuan Le, Jonathan Loo, Kok Keong Chai, Mahdi Aiash, 2016. *A specification-based IDS for detecting attacks on RPL-based network topology,* s.l.: IEEE.

Ben Stephen, Arash, Robin Doss, 2021. *Detecting Internet of Things Bot,* s.l.: IEEE.

Danzi, P., Kalør, A.E., Stefanovi´c, C., Popovski, P., 2019. *Delay and communication ˇ tradeoffs for blockchain systems with lightweight IoT clients.,* s.l.: IEEE.

Emerging Technologies, 2022. *The market for smart home devices is expected to boom over the next 5 years.* [Online]
Available at: https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/
[Accessed July 2022].

Goyat, R., Kumar, G., Rai, M.K., Saha, R., Thomas, R., Kim, T.H, 2020. *Blockchain powered secure range-free localization in wireless sensor networks,* s.l.: IEEE.

Haseeb, K., Islam, N., Almogren, A., Din, I.U, 2019. *Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things,* s.l.: IEEE.

Javaid, N., Shakeel, U., Ahmad, A., Alrajeh, N., Khan, Z.A., Guizani, N, 2019. *DRADS: depth and reliability aware delay sensitive cooperative routing for underwater wireless sensor networks,* s.l.: IEEE.

Jia, B., Zhou, T., Li, W., Liu, Z., Zhang, J, 2018. *A blockchain-based location privacy protection incentive mechanism in crowd sensing networks,* s.l.: IEEE.

Kim, J.-H., Lee, S., Hong, S., 2021. *Autonomous operation control of IoT blockchain networks. Electronics,* s.l.: IEEE.

Kolumban-Antal, G., Lasak, V., Bogdan, R., Groza, B., 2020. *A secure and portable multi-sensor module for distributed air pollution monitoring. Sensors,* s.l.: IEEE.

Kumar, M.H., Mohanraj, V., Suresh, Y., Senthilkumar, J., Nagalalli, G, 2020. *Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN,* s.l.: IEEE.

Liu, M., Yu, F.R., Teng, Y., Leung, V.C., Song, M, 2019. *Computation offloading and content caching in wireless blockchain networks with mobile edge computing,* s.l.: IEEE.

Liu, Y., Wang, K., Lin, Y., Xu, W, 2019. *LightChain: a lightweight blockchain system for industrial internet of things,* s.l.: IEEE.

Management, Cyber, 2022. *IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities.* [Online]
Available at: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities
[Accessed 2022].

Moinet, A., Darties, B., Baril, J.L, 2017. *Blockchain based trust & authentication for decentralized sensor networks,* s.l.: IEEE.

Nabil Djedjigab, Djamel Tandjaouia, Faiza Medjekab, Imed Romdhanic, 2020. *Trust-aware and cooperative routing protocol for IoT security,* s.l.: IEEE.
Nakamoto, Satoshi, n.d. *Bitcoin A peer to peer electronic cash system,* s.l.: IEEE.
Ramezan, G., Leung, C, 2018. *A blockchain-based contractual routing protocol for the internet of things using smart contracts. Wireless Communications and Mobile Computing,* s.l.: IEEE.
Rathee, G., Balasaraswathi, M., Chandran, K.P., Gupta, S.D., Boopathi, C.S, 2020. *A secure IoT sensors communication in industry 4.0 using blockchain technology,* s.l.: IEEE.
Rathore, S., Kwon, B.W., Park, 2019. *Blockchain-based decentralized security architecture for IoT network,* s.l.: IEEE.
Ren, Y., Liu, Y., Ji, S., Sangaiah, A.K., Wang, J, 2018. *Incentive mechanism of data storage based on blockchain for wireless sensor networks. Mobile Information Systems,* s.l.: IEEE.
Rovira-Sugranes, A., Razi, A, 2019. *Optimizing the age of information for blockchain technology with applications to IoT sensors,* s.l.: IEEE.
Samrah Arif, Arif Khan, Sabir Ur Rehman, Muhammad Ashad and Muhammad Imran, 2020. *Investigating Smart Home Security: Is Blockchain the Answer?,* s.l.: IEEE Access.
Sergii, K., Prieto-Castrillo, F, 2018. *A rolling blockchain for a dynamic WSNs in a smart city.,* s.l.: IEEE Access.
Seyoung Huh*, Sangrae Cho*, Soohyung Kim*, n.d. *Managing IoT Devices using Blockchain Platform,* s.l.: IEEE.
Sharma, P.K., Park, J.H, 2018. *Blockchain based hybrid network architecture for the smart city,* s.l.: IEEE Access.
She, W., Liu, Q., Tian, Z., Chen, J.S., Wang, B., Liu, W., 2019. *Blockchain trust model for malicious node detection in wireless sensor networks.,* s.l.: IEEE Access.
Statista, n.d. *Smart Home technologies - Worldwide.* [Online]
Available at: https://www.statista.com/outlook/tmo/internet-of-things/smart-home-technologies/worldwide
[Accessed 2022].
Statista, n.d. *Statista.* [Online]
Available at: https://www.statista.com/outlook/tmo/internet-of-things/smart-home-technologies/worldwide
Sunghyuck Hong, 2020. *P2P networking based internet of things (IoT) sensor node authentication by Blockchain. Peer-to-Peer Networking Appl.,* s.l.: IEEE.
TAI-HOON KIM, REKHA GOYAT, MRITUNJAY KUMAR RAI, GULSHAN KUMAR, WILLIAM J. BUCHANAN, RAHUL SAHA AND REJI THOMAS , 2019. *A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks.,* s.l.: IEEE.
Tian, Y., Wang, Z., Xiong, J., Ma, J., 2020. *A blockchain-based secure key management scheme with trustworthiness in DWSNs.,* s.l.: IEEE Access.
Uddin, M.A., Stranieri, A., Gondal, I., Balasurbramanian, V., 2019. *A lightweight blockchain based framework for underwater iot,* s.l.: IEEE Access.
Yang, J., He, S., Xu, Y., Chen, L., Ren, J, 2019. *A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. Sensors,* s.l.: IEEE Access.
Yu Nandar Aung, Thitinan Tantidham, 2017. *Review of Ethereum: Smart Home Case Study,* s.l.: 2nd International Conference on Information Technology (INCIT).
Zhihua Cui , Fei Xue , Shiqiang Zhang, Xingjuan Cai , Yang Cao, Wensheng Zhang, and Jinjun Chen, 2020. *A hybrid BlockChain-based identity authentication scheme for multi WSN,* s.l.: IEEE .
Zhou, Yiyun, 2018. *Improving IoT in Smart home using Block chain smart contract,* s.l.: IEEE.