Int. J. Nonlinear Anal. Appl. 14 (2023) 1, 1697–1715
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.6899

Blockchain simulation model for a communication system in IoT devices

Ahmed Ali Talib Al Khazaali, Sefer Kurnaz*

Electrical and Computer Engineering, Altinbas University, Istanbul, Turkey

(Communicated by Javad Vahidi)

Abstract

Blockchain technology has drawn in a ton of consideration from specialists, designers, and organizations lately, and its execution has revived interest in various applications, including e-finance, e-medical care, savvy homes, the Internet of Things, government-managed retirement, coordinated factors, and others. Most of the blockchain-related examinations in the writing have been viewed as designing execution centred, with hypothetical framework investigation getting undeniably less consideration; in any case, the current work is simply ready to show the mining system. For better comprehension of the functional and hypothetical elements of the blockchain, a model in view of the lining hypothesis is advanced in this review. In this article, we have explored the joining of IoT with blockchain technology and gave a top to bottom investigation of the blockchain-empowered IoT and IIoT frameworks. The cutting-edge research is arranged into information capacity and the executive's method, enormous information and distributed computing procedure (money and information inspecting), and modern areas (store network, energy, and medical services area). The sagacious conversation in view of the various classifications is likewise introduced in the paper.

Keywords: Blockchain technology, Simulation Model, IoT, Communication System
2020 MSC: 94C60, 00A72

1 Introduction

IoT is a sophisticated form of networking of different computing and communication devices using unique identifiers of each device. To achieve a collaborative environment, IoT integrates various technologies such as hand-held digital devices, industrial machinery, animals (or) people, or any physical-digital entities to work together to achieve the application's purpose. However, there are various security issues few of them are Denial-of-service (DoS) attacks, Data Theft (or) Data Breaches, Botnets attacks where several systems to take control of the victim's system, to extract the victim's confidential data this consistently matter of concern within an IoT. Unsecured devices are the main security concern in frameworks of edge computing and IoT as they are used to increase network coverage. There are also devices within an IoT that can migrate from one to another network, which causes a serious threat to Security. In present times, the conventional IoT network considers the concept of zero trusts, which is a mechanism for safeguarding the infrastructure of the internet and the IT system. It will also mean that it allows any form of devices to join the network or access the resources within a network that assumes that they are also authorized. Hence, it

*Correspoding Author
Email addresses: ahmed.al-khazaali@ogr.altinbas.edu.tr (Ahmed Ali Talib Al Khazaali), sefer.kurnaz@altinbas.edu.tr (Sefer Kurnaz)

Received: March 2022 *Accepted:* July 2022

is not difficult for the adversaries to go parallel with the regular node after bypassing the firewall system in an IoT. This is potentially a challenging situation as there are various IoT devices, and most of them are highly vulnerable and unsecured. This phenomenon makes an adversary job easier to utilize the gateway system present in an IoT environment.

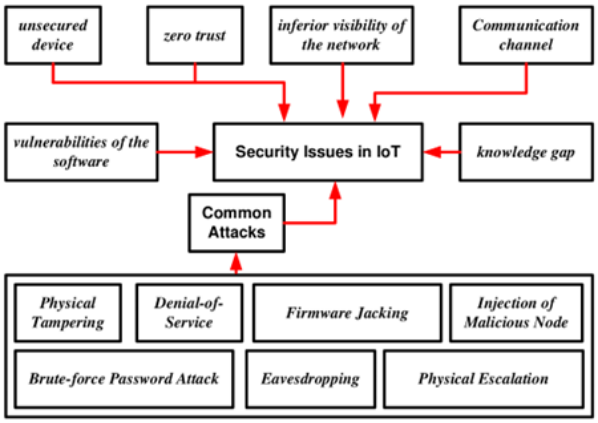

Figure 1: Taxonomy of Security issues in an IoT

At present, various protocols are used in an IoT communication system that already has a reported security issue and is known to negatively influence the complete networking system. There are various forms of attacks in an IoT; however, some of the common attacks in an IoT environment are

- Physical Tampering: Threats to unauthorized tampering on the physical device are possible when the devices run in an environment which cannot be accessed by the people.
- Denial-of-Service: It is one of the most reported attacks in both cloud environment and IoT where the complete network and servers are paralyzed, rendering it easier for attackers to access the network or fulfill other malicious intentions.
- Firmware Jacking: If the network is compromised, then the updates for upgrading the firmware are also possibly compromised, and when such compromised firmware update reaches hardware, it infects them too as there are failed authentication of the source of firmware update origination point.
- Injection of Malicious Node: The malicious nodes are physically deployed by the adversary among the regular normal IoT devices. The malicious nodes can carry out various forms of illegitimate control of the network and illegal sniffing of data.
- Brute-force Password Attack: Such attacks are also deployed to access the devices in vulnerable IoT environments.
- Eavesdropping: The vulnerable communication channel can be compromised and intercepted by the adversary node. The adversary can steal all the sensitive data certain weak spot in the communication channel.
- Physical Escalation. Various forms of the flaws associated with the operating platforms, hardware, and software can be misutilized by the attacker to have illegitimate access to the IoT resources.

2 Literature Review

This section deals with the existing researches in the domain of IoT with the encryption- based security approaches. The work of [16] described a secure communication mechanism by improving the conventional Advanced Encryption Standard (AES) algorithm. The encryption mechanism resists different security attacks and also minimizes the encryption power. The system has not addressed the issues of information-centric IoT. Sufficient data protection can be achieved using attribute-based encryption (ABE) mechanism consisting of Cipher text policy introduced in [18]. The encryption mechanism gives improved performance and minimized computation overhead. The resource-constrained IoT devices are composed of different issues like low computational ability, high latency, low bandwidth,

etc. These issues are addressed in [13] with a lightweight encryption technique based on cellular automata for IoT. The technique can reduce the run time and can prevent data theft. The complexity parameter is not addressed in prior work. The work of [6] has presented a reduced block encryption mechanism for the IoT where less complex and fast encryption is achieved. The block encryption mechanism yields reduced computations and offer higher Security that supports low powered IoT devices. The work of [20] has introduced a multiparty authentication-based encryption mechanism for narrowband IoT terminals. The encryption mechanism is based on certificates policy, which provides data privacy and efficient support for the 5G network. The chaotic encryption algorithm is introduced in [14] for intelligent data transmission in IoT with key controlled neural networks. The cryptanalysis gives improved information entropy than the existing algorithm.

The above research does not address information-centric IoT issues, not considered resource-constrained IoT devices; complexity parameter is not addressed, not benchmarked, a comparative analysis is not conducted, and application aspects are not discussed.

The benchmarking of the IoT applications with the Encryption scheme is not addressed in existing works. Benchmarking of symmetric encryption mechanism is described in [15] for IoT applications' cloud storage. The dynamic symmetric encryption mechanism outcomes suggest the trade-off between cloud performance and Security with the existing system. The throughput and error performance is not analyzed for IoT applications. [11] introduced a lightweight encryption scheme for IoT where the performance is analyzed for error and throughput with and without coding in the Additive White Gaussian Noise (AWGN) channel. The system yields better Security without affecting the processing time, reduced errors, and better performance. The encryption mechanism does not discuss a combination of both probabilistic and lightweight encryption schemes. The smart healthcare IoT application's secure surveillance model is presented in [9], where both probabilistic and lightweight encryption schemes are used. The scheme offers reduced storage, improved bandwidth, and reduced transmission cost with improved patient data security in IoT systems. The hybrid lightweight proxy encryption is not incorporated in prior research for securing the IoT environment. In [10], a hybrid re-encryption scheme is presented where the re-encryption process is efficient and minimizes encryption and decryption. However, the hierarchical attribute-based encryption (HAE) is not presented for the IoT based healthcare system. [4] described a Cipher text policy with the HEA algorithm to protect the healthcare data's key leaking. The study has not discussed the encryption mechanism for IoT smart grid. A lightweight and secure sign encryption mechanism is described in [7] for IoT based smart grid. The outcomes suggest that the security system offers better security and reduced cost and communication resources than existing security schemes.

Throughput and error performance is not analyzed from the above table, not considered a combination of encryption scheme; hybrid lightweight proxy encryption is not incorporated in hierarchical attribute-based encryption (HAE), not considered, not discussed encryption mechanism, not considered security analysis with different applications.

The security aspects for Bigdata based IoT multifactor authentication factors are not discussed with IoT systems. The scalable, secure authentication mechanism for IoT- bigdata systems is discussed in [2] with lightweight cryptography. The authentication scheme offers three-level authentication during user login, data authentication, and data access. The outcomes give improved computational time, Security, improved encryption, and decryption time. The system does not consider the resource-constrained IoT device security in Fog based IoT. A work of [3] has presented an encryption protocol for IoT devices with a resource constraint problem. The system gives supporting results for resource-constrained fog based IoT. The application of IoT for the 5G scenario is not addressed in prior work. In [1], a quantum walk-based data security is presented in support of 5G IoT. The quantum walks with encryption mechanism gives secure data transmission and security features. [5] has given a collective matrix factorization (CMF) mechanism for accurate data transmission and a homomorphic encryption mechanism for data security. A sensitive hashing is used to preserve the index structure, giving improved Security supporting real-time IoT applications. A collaborative study of [8] has presented a chaining encryption algorithm for IoT networks with low power wide area networks. The outcome suggests significant Security of IoT networks but not performed benchmarking. A secure surveillance system with probabilistic image encryption for the IoT systems is presented in the work of [12].

The technique can detect the surveillance system's suspicious activities with better accuracy, bandwidth improvement than traditional techniques. The analysis of the encryption scheme over the multimedia IoT is not explained in previous work. Design and its analysis of lightweight encryption mechanism based on compressive sensing are found in [17]. The analysis suggests that the system can handle the different forms of attacks, but it is not benchmarked with the existing research. Multi-authority access control is introduced in [19] for cloud storage security. The access control security scheme can achieve better security with reduced computational overhead and storage cost.

It is being observed that these approaches have not considered resource constraint parameters, Not involved data security with 5G applications, Not benchmarked, and Analysis of the encryption scheme is not conducted.

3 Research Problem

The problems identified and addressed in this part of the study are as follows:

- *Incapability to resist unknown attackers:* Existing IoT environment majorly depends upon the definition of attack, without which constructing a security system is almost challenging. IoT using the cloud as a backend is highly exposed to unknown vulnerabilities, and it requires a mechanism that can identify and resist unknown attackers.
- I*mprovisation to blockchain:* At present, blockchain technologies are reportedly characterized by various issues, e.g., lack of scalability towards large computing environment (especially in a distributed environment), excessive resource utilization, and leads to complexity in operation, entries of blockchains are immutable. Blockchain is one of the potential security systems that require improvement before deployment over a large IoT environment.
- *Lack of cost-effective security:* Existing security schemes in IoT are either very specific to attack or are highly complex in their operation. This complexity acts as an impediment towards data transmission performance in IoT. This problem must be addressed to balance the demands of both security and data transmission in a larger network.
- *More usage of iterative encryption:* The existing encryption methods used in IoT must be improvised due to larger keys over IoT devices with limited resources. There is a need for a more progressive security system and less on the iterative encryption system to secure IoT communication system.

4 Research Methodology

The proposed research work is carried out using an analytical research methodology. The prime task is to design and develop a secure communication framework in an IoT ecosystem over the Software-Defined Network (SDN). This part of implementation also incorporates intelligence in the data transmission mechanism where the McEliece cryptosystem further encrypts the blockchain mechanism's potential. The overall mechanism is simplified as the data being transmitted to the SDN block consisting of multiple operations associated with controlling, routing, managing logic, etc. The data are arranged in blockchain, while McEliece encryption is used for ciphering the chain that is followed by authentication operation over the application, control, and data plane in a software-defined network. Further operational and forwarding plane is used for control plane for effective decision making. The overall architecture of the proposed system is as follows in Figure 2:

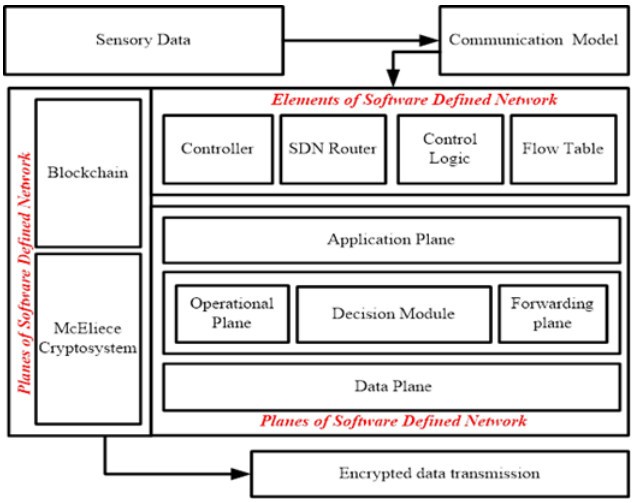

Figure 2: Overall Architecture of Proposed System

The proposed system considers a specific form of secured architecture, considering sensor nodes as an IoT device. The proposed system makes use of a module that is responsible for generating blockchain, and it uses an authorization server along with the network controller system in IoT. A unique identifier is used for indexing the data.

Normally, every application has a data flow coupled with it, and the administrator can dynamically control it. The study assumes that the administrator knows information about the destination node associated with each flow's identity. Therefore, the controller will be capable of computing the flow information of the routes.

The complete design of the proposed system is based on the fact that there is a need to construct a secure communication channel between the SDN node and its controller. There is a higher possibility of insertion of the malicious packet in the communication channel that would further invite the attacks, e.g., distributed denial of service or even steal certain confidential data associated with the higher layers that cannot facilitate security. There is also a need to secure data transmission between all applications because the link layer is not completely capable of facilitating full transmission security as encryption and decryption are carried out over all the hops one by one. The proposed study also assumes that all the network users unanimously trust the SDN controller as it will perform construction, management, and update all the network protocols.

To offer a resilient communication system, it is essential to ensure that SDN nodes secure communication with the IoT controller system. The proposed system architecture consists of three essential modules viz. i) controller of SDN, ii) block chain generator, and iii) validation server. Irrespective of any form of communication scheme among the IoT devices, all the entities involved can communicate. Being a common location entity, the proposed SDN architecture controller can manage the network's control plane in both a centralized and decentralized manner. The routing behaviour is defined dynamically with forwarding protocols associated with flow tables in SDN nodes. The algorithms are executed by the controller using the local representation connected to the state of a network. It carries out the estimation of the entries made in the data flow table per the existing routing policies.

The proposed system uses the block chain to secure the data. A generator module is designed explicitly for this purpose, which takes part in key generation in a later phase using the McEliece algorithm. All the forms of receiving and obtaining the Authorization request are carried out by the validator server to let the SDN node join the network. The node access evaluates the credential that is stored in the database. After the node's successful authentication, the information about the identity and credential is stored within a local database, maintaining a list of authorization.

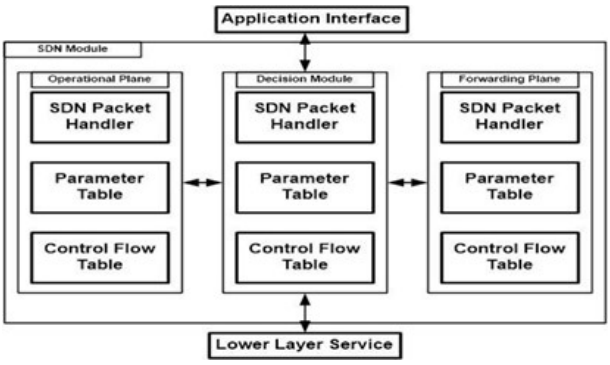

Figure 3: Proposed SDN Architecture

Figure 3 highlights the proposed SDN architecture that is designed over an IoT environment. Following the principle of RFC 7426, the standard architecture of SDN is developed along with an inclusion of the security system using blockchain. The architecture is designed to offer a good communication bridge between the reception services of data and data transmission. A closer look into Fig.4.1 shows three essential modules viz. operational plane, decision module, and forwarding plane. Following are the functionalities developed in each of the actors:

- *Operational Plane:* This actor carries out proper updating and manages all significant information associated with the node's state. It can check the status of adjacent IoT nodes, their level of resource availability, etc. A definitive memory is formed to store this parameter in the form of the matrix. It can also use a control flow table to route the data packets to certain particular IoT nodes
- *Decision Module:* It is one of the prime actors in the proposed SDN architecture responsible for managing incoming and outgoing data packets, configuring a queuing system, data transformation, etc. This actor's core job is to make the raw data packet suitable for processing as per the SDN module's internal structure. Finally, this packet is transmitted either to the operational or to the forwarding plane.
- *Forwarding Plane:* This actor is mainly responsible for managing different data packet types as per the programmed operation embedded within it over the flow table. This actor can transmit the data packet to the

consecutive node, reject it, or transmit it back to the upper layer (provided it has contacted its destination IoT node). In the absence of any rule of matching, this actor performs a querying SDN controller to know the process of data packet handling. All the data packets that are found unmatched are stored until and unless the system has received the response.

The proposed system represents a *flow table* as a definitive data structure in its passive form that retains all forms of information associated with the data forwarding process. The decision module further evaluates the presence of encryption of the blockchain for a higher level of security. The *security module* is responsible for decrypting the ciphered data. Further, the SDN layer performs the processing of the obtained plaintext data packet. The blockchain and cryptography process using the McEliece system is carried out by a security module where the core target is to facilitate an interactive interface exclusively for the decision module for operating on the blockchain and encryption operation.

Figure 4 highlights the computational architecture for the proposed SDN Controller system, which plays a contributory role in the architecture building process. The SDN nodes facilitate the connectivity with the network nodes. Apart from the decision module, there are other operations blocks, too, viz. *management plane* and *control plane*. All the internal and external data packets are subjected to transformation with the SDN module's aid by the decision module in an interface.

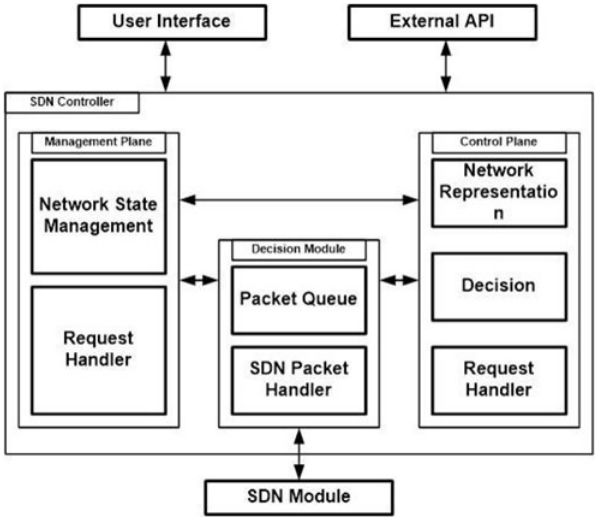

Figure 4: Computational Architecture of Proposed SDN Controller

This module checks the request message's allocation concerning either the control plane or management plane. The briefing of the functionalities of these elemental planes is as follows:

- *Management Plane:* The up-gradation of the information associated with the network is maintained by this plane. The information of the control plane is fed with the network representation by this plane. This plane also performs interaction with the operational plane associated with transmitting the request beacon information and updates of all the status connected with the IoT nodes. An alternative measure for evaluating the IoT nodes' parameters is carried out by this plane to resist any form of overhead without any need to perform querying from the given network topology.
- *Control Plane:* All the decision associated with secured communication among the IoT nodes and identification of the malicious users via a security module is carried out by this plane. The purpose is to facilitate a robust and resilient route for data delivery in IoT systems. The network nodes can be configured with the flow configuration based on the request.

The routing operation utilizes the consolidated information about the network. The validation server and the blockchain operations perform a simplified operation. The validation server possesses the dependency of the repository associated with all the legitimate IoT nodes. It also requires to carry out alerting the connected elements of the network concerning the authorization status. The blockchain is responsible for securing the transaction-based information

associated with routing for safeguarding the beacons' internal information and topology control. The proposed system develops a beacon of 8 bit, and its frame format is shown in Figure 4, which is used for carrying out network task in SDN. The frame format's design is carried out so that it is suitable for any format of a packet in the network layer of IoT. The complete design of the beacon frame format is carried out based on RFC 4944.

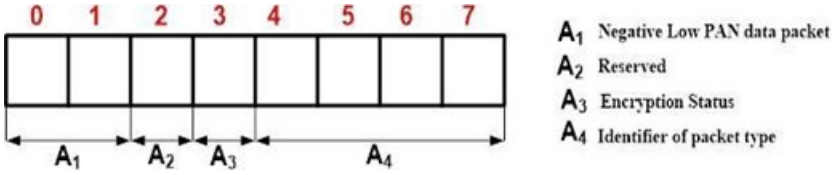

Figure 5: Proposed Beacon Frame Format

Figure 5 shows that the initial two bits of frame length are predefined allocated for handling a low personal area network (6lowPAN), and hence it is configured to 0. A similar reservation of zero is also carried out for the third bit in the frame format. The status of the encryption is checked from a fourth bit in the packet frame. In contrast, residual bits of information is used for representing conventional data types of a packet associated with the SDN, i.e., data packet, request of flow, configurational set up of data flow, response update status, request update status, information associated with adjacent IoT nodes, request and response of loading of proposed logic over SDN router with specific indexing process, assessing a request for constructing blockchain, etc. The proposed system transmits the application data using its data packet and its connected address information associated with the source IoT node and flow identity. The complete process of communication among the essential actors is shown in Figure 6.

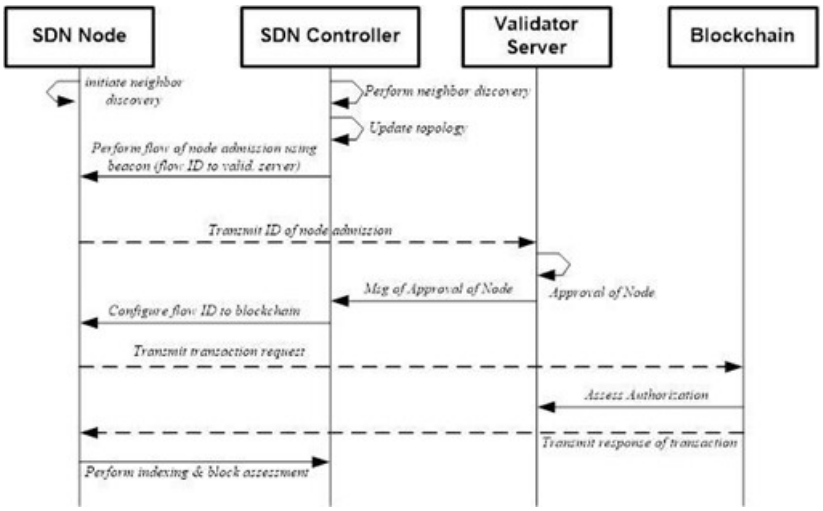

Figure 6: Complete process of security

According to Figure 6, the following steps of operations are carried out: The node forwards the request packet of authorization while the validator node carries out the node's identification. Response information about the authorization is forwarded back by the validator node. During this time, the reply flow associated with the authorization module's respective flow table and control flow table are configured by the SDN controller. An intermediate node relays the message of authorization response to the IoT node, which forwards indexing for supporting the security program loading by the blockchain matrix after receiving by the node. The blockchain matrix obtains this data packet and evaluates the confidential information that resides within the validator server. The blockchain then forwards a response with an index value generated new to offer better forward secrecy. Any intermediate node further relays the response message to the target IoT node. The secured communication between the validator server and the SDN controller is now established, which finally permits forwarding the flow request. After completing the transaction by blockchain, the node is now added by the SDN controller to the matrix with information about all secured IoT nodes.

The final step of the proposed architecture is to offer encryption using the McEliece cryptosystem. However, it should be noted that an encryption system is an iterative scheme and suffers from the simplified recovery of the plaintext if there is a similar public key usage more than one time. On the other hand, the McEliece cryptosystem

is also faster in operation than the potential RSA algorithm. Hence, the proposed system mechanizes a scheme to cover up this algorithm's loophole by adding another mechanism to resisting any node that is found to be illegitimate. The idea is to improvise the McEliece approach to secure the blockchain so that the information about the SDN router's topology control should be encrypted. Before encryption, it must not fall victim to the adversary. Hence, the mechanism is as follows: the proposed system chooses the adjacent nodes of the SDN router where an IoT node is supposed to select the blockchain vector in a single hop from the double hops. This is done to ensure that even if there is an attack, it cannot propagate more than one hop. For an effective identification of an illegitimate request, the proposed system formulates two rules as follows (Figure 7).

- Normally an attacker will choose to select a victim node with the lowest resources and higher connectivity. In case such, the node positioned in single- hop N8 in Figure 7 (no other double hop is present beyond it) will propagate a control message that consists of neighboring node information. The root node N1 to that node must confirm that such a single node should not disclose any further information. It will mean that N8 will not disclose any information about N5-N7 and N2-N4 to any requester node.
- The second rule is to evaluate the control message for joining the new node network; the root node N1 must assess if the new node is already present in its list of neighboring nodes such that no such information is present in the transmitting node control message. It is positioned at a higher distance of multi hops from N1 from a security viewpoint. Once this condition is satisfied, the system further performs another operation where it checks if N8 has selected any new unknown node whose neighboring node is N8 itself.

This rule checks for the authenticity and intention of the node. The first rule's accomplishment is carried out by checking the control message to evaluate if they alerted the transmitting node represented in the neighboring node. The identification of the malicious node is carried out by looking for the topology control message. In the presence of any information of entries of the blockchain already selected by the N8 and then it permits it to reach the unknown node in double hops, it will mean that the new node may be a curious victim node controlled by an attacker. According to the proposed policy, the authenticated list of blockchains are already indexed and maintained by various SDN nodes, and an attacker does not possess this information, and hence attacker ends up generating a genuine request for joining the network; however, the only difference is that it will not be able to generate any such blockchain index which fails authentication by the blockchain matrix. This mechanism ensures that the proposed system can resist the malicious node or victim node, or any regular node that is curious to join the network illegitimately. This mechanism is a highly improved version of optimizing blockchain followed by finally encrypting it with McEliece cryptosystem that further offers another security layer.

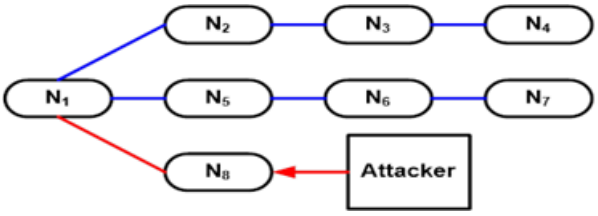

Figure 7: Mechanism to Thwarting Illegitimate Request of Joining Network

5 Algorithm Implementation

The prime plan of the proposed algorithm is to offer a secured communication link from the target node. The algorithm aims to mainly implement blockchain to secure the information, thereby facilitating a higher degree of privacy and confidentiality. However, the algorithm further offers a second layer of encryption using the McEliece cryptosystem, making the information furthermore ciphered near impossible for an attacker to break it. One essential fact to understand in the algorithm construction is that the complete operation and deployment are carried out over the controller system. SDN routers are finally responsible for formulating the secure link among the IoT device in communication. The transactional information associated with the flow table is responsible for managing the routing table. Hence, all the node performing communication is assumed to be compliant with the protocols relayed by the SDN–controller system and obey the link generated. The essential step of operation being carried out by the proposed algorithm are shown as follows:

Algorithm 1 Algorithm for Jain Secure Communication Link (JSCL)

Input: *A, x / y, Nden, R*
Output: *link*
Start
1: *init* A, (x, y), Nden, R
2: For i=1: *Nden*
3: Φbc=$f1$[(x, y), A, Nden, R]i
4: bcvec $f2$(Nden, Φbc)
5: [rt, q1, q2]=$f3$[(x,y), R, Nden, Φbc, bcvec]
6: link=$f4$[(x,y), A, Nden, R, Φbc, sn, dn, rt, vn]
7: End
End

The input to the algorithm is A (Simulation area), *x / y* (Positional information), *Nden* (Node density), and *R* (communication radius), which after processing yields an outcome of the link (secured link). The steps of the operation carried out by the algorithm and its respective discussion of the rationale behind its formulation are as discussed below:

i) Network Deployment:

It should be noted that the proposed system has an inclusion of the SDN-based network in an IoT ecosystem. The deployment stage consists of randomly deploying the IoT devices with specific node density Nden over a specific deployment area, i.e., A. The communication radius R of the node can be highly flexible, which depends on the application deployed over an IoT. The deployment area is a flexible parameter that can be scaled up or down based on the application's demands. In this deployment (Figure 8), it is essential to consider the SDN operation within the deployed IoT device. There are two types of nodes in an IoT in this mechanism, i.e., controller and SDN router. The controller runs a control logic while the SDN router has possession of the flow table. In the existing system, the control logic is run by the regular node, and there is no inclusion of the flow table. All the necessary input information can be considered to carry out network deployment (Line-1). Hence, the proposed deployment offers the inclusion of entities that can extract more bundles of information and higher processing capability to find the routes' reliable information.

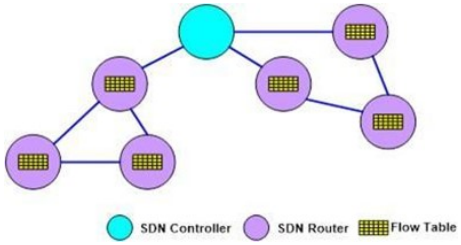

Figure 8: Stage-I (Network Deployment)

ii) Creating Block chain

The next part of the algorithm implementation is constructing a blockchain of the information primarily considered an input. This operation is carried out for all node density values Nden existing over the deployment zone (Line-2). An explicit function $f1$(x) is constructed, which takes the input arguments to generate a matrix of blockchain Φbc (Line-3). The operation carried out for this purpose is as follows: Before implementing blockchain, the algorithm considers all the IoT devices, mainly focusing on source node sn and destination node dn, followed by obtaining the relative distance between them. Consideration of this distance parameter makes the proposed system applicable to both static nodes and mobile nodes as the algorithm perform its security operation based on this distance and therefore offers uniformity in its computation irrespective of the positive of the IoT nodes. The algorithm also checks that only the information associated with communicating nodes are retained so that there is no unnecessary wastage of memory usage. All this information is retained within matrix Φbc. Hence, it is a one-point reliable source of information when any other neighboring nodes also want to communicate using the information retained within Φbc. The next part of the implementation is about exploring the single hops neighboring node from the target node whose information is obtained from Φbc matrix while constructing blockchain.

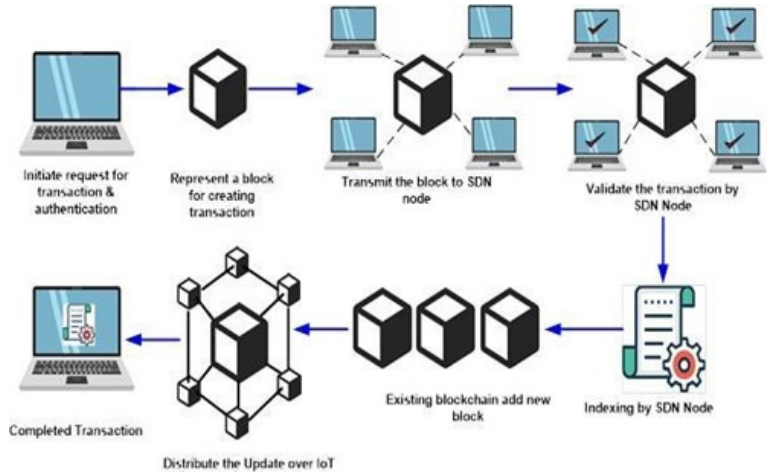

Figure 9: Stage-II (Creating Blockchain)

Figure 9 highlights the mechanism used for creating and implementing the blockchain in the proposed system. For this purpose, a request for a transaction is carried out, and authentication is carried out. In the proposed system, blockchain will represent the transaction information of the input arguments considered (Line-3). This block will then be transmitted to all the IoT devices assumed to be a legitimate member within the network. The proposed system assumes a certain primary authentication system for all the legitimate nodes before being deployed within a network. Once the nodes perform validation of the transaction, they receive an index starting the proof of work. The algorithm then adds this block to the current blockchain while the update distribution is carried out over the complete network, which ends the transaction's successful completion. Following are the brief of operation of the proposed blockchain:

- The proposed block chain's primary implementation is basically to carry out authentication with the aid of cryptographic keys and all the input arguments stated in Line-3. This information acts as identified for the user, which can be used for accessing their data. As the source node carries a private key within itself and it also has a public key. Usage of both the keys' forms, the systemconstructs a highly secured digital identity using a digital signature. These keys are also used to extract the information too.
- The next step of implementation is authorization, which is carried out by the controller system in SDN. The controller performs the transaction's approval before adding the respective block to formulate a chain system. The complete authorization is only considered to be valid when all the IoT devices agree with the transaction to be valid. A specific index is offered to all the IoT nodes which participate in verifying the transaction. The controller can use the SDN router for this information dissemination process, followed by constructing a flow table.

iii) Constructing Security Wall

The proposed system constructs a security wall's unique logic to offer the resistance between the intruder and the common IoT node (Figure 10). It further secures the blockchain to obtain a blockchain vector for securing itself against unknown malicious requests spreading from single and double hop nodes. This algorithm's design's core basis is the possibility of intrusion by a dynamic adversary who could change their attack strategy, which may not be defined within the control logic in the SDN router. Hence, the SDN router needs to have the capability to identify the malicious request from an illegitimate node in IoT and resist them to protect the entire network. For this purpose, an explicit function $f2(x)$ is constructed, which takes the input arguments of node density Nden and matrix of blockchain Φbc (Line-4) to generate blockchain vector bcvec. For all node density values, the function extracts the information about the SDN nodes from the blockchain Φbc which is a single hop. The identification of double hop further follows this operation. A similar operation is further carried out to narrow down the search for common single hops of the target node, followed by extracting information about single hop from the double hop neighboring nodes. Considering the coverage for the target node, the system extracts information about the identity of the single-hop node and common nodes existing between two double-hop IoT nodes. This process leads to finding the IoT node, which has the highest coverage, and this node is required to be protected. Therefore, the exploration will lead to the generation of all the block chains and their associated

connectivity (vector), further required to be protected (Line-5). However, the algorithm considers only the unique blockchain vectors bcvec in this process (Line-4).

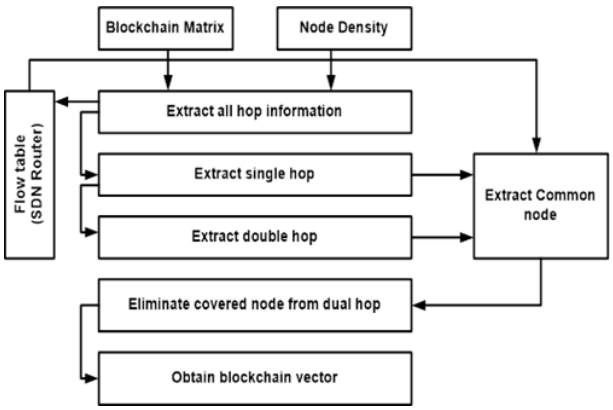

Figure 10: Stage-III (Constructing Security Wall)

iv) Final Layer of Security

This is the final layer of security, which is continuing with the prior stage of security wall formation. This operation is carried out by constructing a function $f3(x)$, which takes all the prior parameters as an input argument (Line-5). This operation mainly focuses on secure routing between IoT nodes via an SDN router. The process involved in it is as follows: the function is applied considering all the node density Nden where a routing table is formed between the source and destination node (sn, dn). The function checks if the local interface address is found to be equivalent to the destination node address. In such a case, it stores the next-hop information for constructing a routing table rt (Line-5) considering only a single hop. A beacon is formed considering the blockchain matrix Φbc and blockchain vector bcvec, which is used for finding the neighboring nodes with a single hop. This message is essential as it can be used to control the topology of the current IoT node connectivity to secure them. The topology control message will consist of information about the single-hop node, blockchain matrix, node density, and blockchain vector. Hence, this information is required to be further secured, falling into the attacker node's captivity. This message is checked by analyzing the presence of a blockchain vector from the SDN node. Finally, the route is formed using the minimum distance between the source and destination. The function further generates two random parameters q1 and q2, concerning the node density, to randomize the process of allocating secured routes to the source node and destination. However, for security purposes, the system's next process considers only routing table rt as it stores all the confidential current topological information (Line-6). The next part of this process is to formulate another function, $f4(x)$, to encrypt this routing information (Line-6) generate a secured communication channel. The complete encryption process is carried out using the McEliece cryptosystem, which follows the conventional steps of key generation and message encryption.

This process's novelty is that conventional adoption of this encryption results in resistivity from structural attacks and brute force attacks only. Still, the algorithm's proposed design increases the resistivity of any other forms of attackers whose information is not priory known. Therefore, the major advantage of the proposed design in this last part of the implementation of the algorithm is that it constructs a robust trapdoor function that ensures both forward and backward secrecy as well as is capable of identifying the illegitimate request by referring to the blockchain vectors and currently formed routing table dynamically.

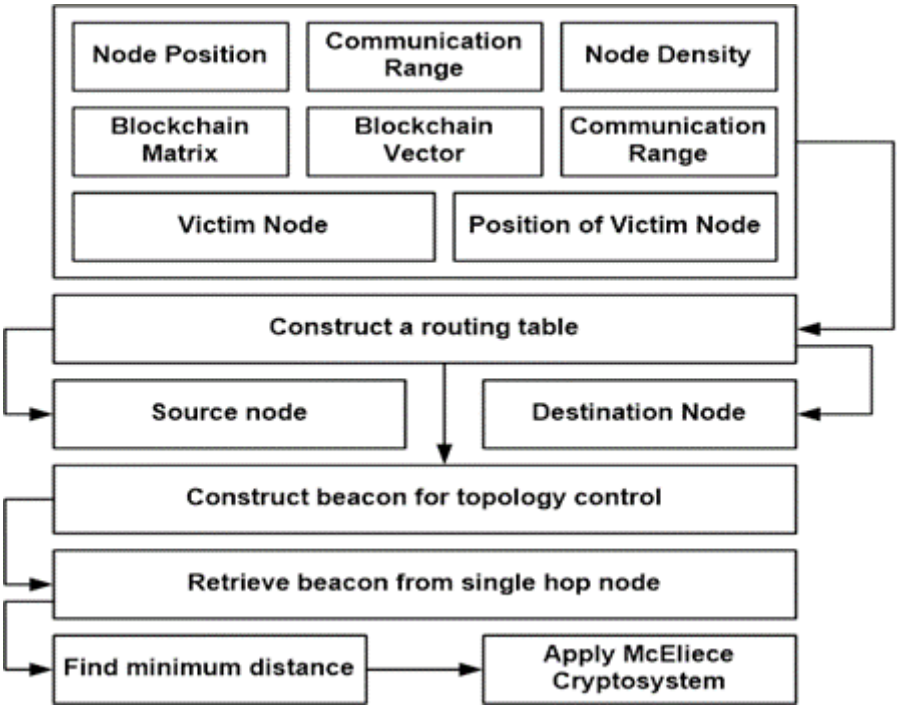

Figure 11: Stage-IV (Final Layer of Security)

Figure 11 showcases the process flow of the final stage of implementation, which considers the victim node's presence and its respective position within the simulation area A. The core idea is that the victim node (controlled by an attacker) should not be given any form of access to join the network. However, in such a case, the algorithm could be bypassed as the victim node's identity will be found valid within the constructed routing table. Still, it will be undergoing an immediate computation of an updated blockchain vector. Assuming that attacker has this knowledge, then the block value it generates will be different from the generated blockchain obtained from the topology control message. This confirms that the victim node is about to perform the malicious activity, and they are barred from participating in forwarding any message to their immediate neighboring nodes. On the other size, the complete communication between the source and destination node is encrypted by the McEliece cryptosystem. Therefore, the proposed system carries out a secure communication system in an IoT environment.

6 Result Discussion

This section discusses the results that have been obtained after implementing the proposed logic discussed in the prior section. Scripted in MATLAB and normal windows environment, the proposed system implements the logic of intelligence in the security implementation in developing a computational model. The simulation outcome of the proposed system is carried out concerning simulation parameters used, the strategy of analyzing results, and comparative analysis with multiple performance parameters.

Simulation Parameters

The proposed system is designed mainly considering an IoT test scenario that deploys Soft Defined Network (SDN) concept for better security formulation. The simulation is carried out considering 500-1000 nodes randomly deployed over a simulation area of 900 x 1000 m2. The data traffic rate is considered 1 bit of message for every second associated with one IoT node. The time of data traffic is considered to be 20 seconds. The communication radius is considered to be 40 meters

Strategy of Analyzing Results

A closer look into the computational model's proposed intelligent system shows that it offers security to the IoT nodes with SDN. For an effective benchmarking, the proposed system is required to be compared with the existing security protocols in IoT, i.e., Transport Layer Security (TLS) and datagram TLS (DTLS), Trusted computing group (TCG), OAuth 2.0, Simple Authentication and Security Layer (SASL). However, they are highly symptomatic in securing only a specific form of the attacker. There are existing block-chain based methods to where privacy

concerns have been emphasized for sharing data packet using blockchains. As the proposed system implements blockchain, the adoption of work is considered an existing system. The proposed model's analysis is carried out considering performance parameters of delay, overhead, packet delivery ratio, throughput, average message size, and processing time. The rationale behind adopting these parameters is that a robust encryption-based approach should offer better communication performance and security. Moreover, blockchain adoption could be questionable for high-end distributed computing, which is required to be testified for the proposed blockchain-based method.

Comparative Analysis of Delay Compensation

The network delay is anticipated to be higher if there is an inclusion of many sophisticated operations involved in securing the communication system. The propose system uses a series of operations where the mechanism to thwart the illegitimate request, implementing the proposed blockchain, and McEliece cryptosystem is used. Hence, it is essential to assess the end-to-end delay in the presence of increasing iteration, where each iteration means an increase of traffic load randomly over the defined IoT system.

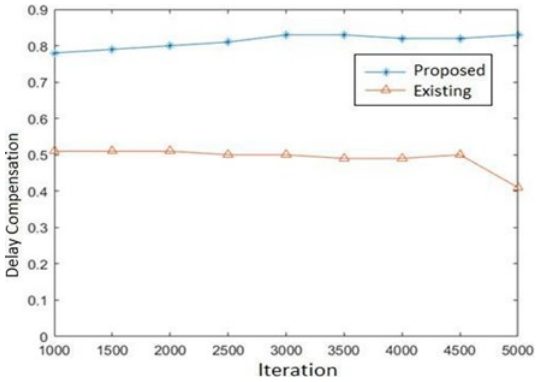

Figure 12: Analysis of Delay Compensation

The outcome is shown in Figure 12 highlights that the proposed system offers approximately 45% better delay compensation in comparison to the conventional blockchain method. The prime justification is: conventional blockchain doesn't support scalability, which reasons for the inclusion of more time with the increase of traffic load as seen from increasing iteration, and hence they don't perform well for offering delay compensation. The proposed system has an extensive usage of blockchain where the information is better indexed and updated by the SDN controller leading to lesser inclusion of parameters and faster identification of the malicious node. This results in better delay compensation. Moreover, the management plane usage offers rich information about the duration preemptively, causing better delay compensation performance in the proposed system.

Comparative Analysis of Overhead

Owing to the inclusion of many IoT devices, there are possibilities of the higher generation of data, which could eventually increase the network overhead. Hence, the incorporation of an intelligent factor in the proposed system will mean an efficient usage of information by the SDN controller for resisting network overhead. Therefore, a better form of security approach is anticipated to exhibit reduced overhead, which is testified here.

Figure 13 showcases that the proposed system offers 27% reduced overhead compared to the existing blockchain approach. Although with the inclusion of the McEliece cryptosystem, there is a possibility of matrices of larger dimension, the proposed algorithm offers the entire authentication directly by the blockchain matrix with the aid of final index generated by the

SDN controller, which compensate the issues of the larger key size of McEliece cryptosystem. Apart from this, approval of the node is carried out in the validator server and not in the SDN controller, which reduces the final load on the SDN controller while securing the blockchain. Therefore, the proposed system minimizes the overhead with the increase of iteration.

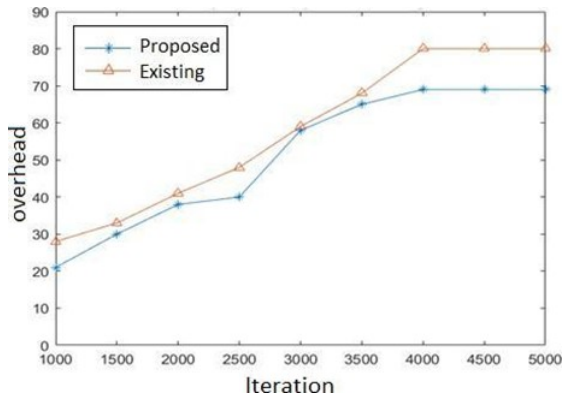

Figure 13: Analysis of Overhead

Comparative Analysis of Packet Delivery Ratio

Packet delivery ratio is one of the essential parameters to showcase that implemented security modeling doesn't affect the data delivery process ratio to check if there is a lightweight feature in the proposed system. A lightweight security protocol should always offer a satisfactory packet delivery ratio to ensure that data transmission never gets affected while the security module is busy handling the malicious nodes. The analysis is carried in the probability of undefined attackers who are *curious* to join the network illegitimately by forwarding requests to join.

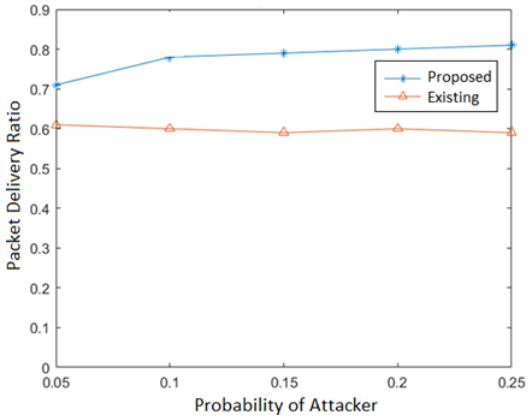

Figure 14: Analysis of Packet Delivery Ratio

Figure 14 highlights that the proposed system offers a 37% higher packet delivery ratio than the existing blockchain. The reason is existing blockchain generates a large chain of blocks with more focus on proof of work that highly resources consuming. On the other hand, the proposed system includes a decision module between the management and control plane, which can handle the SDN packet more efficiently. Moreover, by indexing the blocks, the process becomes quite faster at the end of validation, resulting in a faster completion time of assessment resulting in freeing SDN nodes used for data transmission. The higher availability of such SDN nodes also contributes towards increasing the packet delivery ratio.

Comparative Analysis of Throughput

Although the packet delivery ratio is computed, the proposed analysis also computes throughput because it represents the dissemination of information over an IoT network. This parameter could further offer an edge towards standardizing data transmission speed over an SDN-based IoT network. Hence, with an increase in an attacker's probability, throughput could be affected as the type of attack strategy is completely unknown.

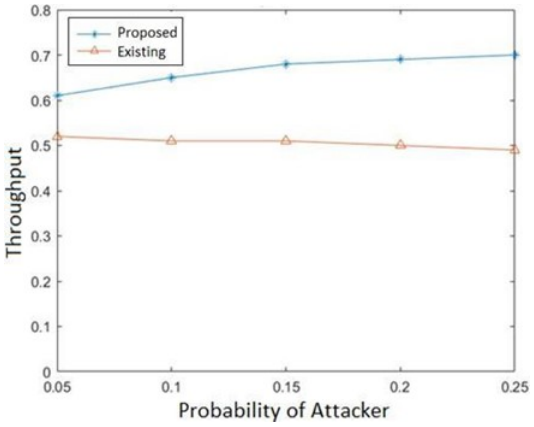

Figure 15: Analysis of throughout

Figure 15 highlights that the proposed system offers 39% of better throughput performance than the existing approach. The prime reason behind this is that the proposed system offers a request handler as a common operation between management and control planes in the SDN controller. This results in identifying the illegitimate request faster by matching with the index value generated by the blockchain vector with that of a malicious user that never matches. This results in a takeover of the SDN packet handler's sub module in the decision module, resulting in faster disseminating the data packet. This operation is absent in the existing blockchain. The complex operation of block maintenance is present, resulting in overutilization of blocks and making the controller busy, resulting in reduced throughput.

Comparative Analysis of Message Size

Owing to a large number of nodes and massive distributed traffic, there are possibilities that certain nodes failed to receive reception. Assuming that the IoT nodes are sensor nodes, it carries out retransmission, which is required to ensure that the data packet reaches its destination node. Hence, this results in an increasing exchange of beacons (or control message). Although the beacon's size is only 8 bits, it can go higher in case of excessive transmission, especially for concurrent users in an IoT. Hence, the ideology is to assess the dependency of the larger message size to confirm successful transmission over increasing node density.

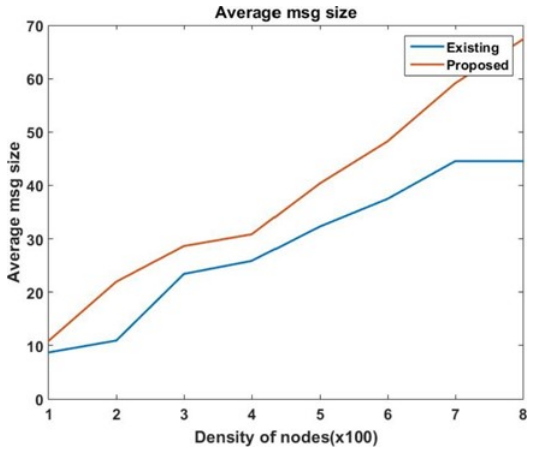

Figure 16: Analysis of Message Size

The simulation outcome shown in Figure 16 shows that the proposed system offers approximately 40% of reduced dependencies of beacons to complete the transaction. The prime reason behind this is the packet format, which carries full information even in the smaller size message. Apart from this, the consistent upgrading of the blockchain index further reduces the dependency of the legacy message used during encryption. This significantly reduces the dependency on a greater number of messages. However, existing blockchain will require maintaining complete information within the blocks, giving rise to an increase in complexity. Hence, they are inefficient for a larger number of nodes in IoT.

The next part of the analysis studies the performance parameter of CPU Utilization time, which is when the time is spent right from initialization to the encoded data being split by the proposed blockchain approach.

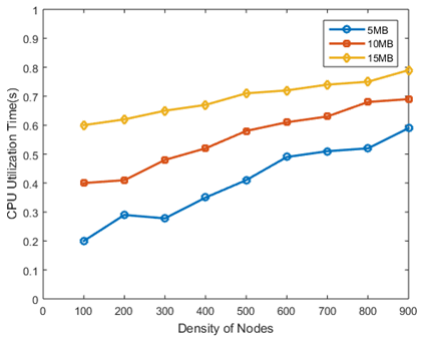

Figure 17: Impact of message size on CPU utilization Time (normal scenario)

Figure 17 highlights the reduced size of the message offers reduced CPU utilization time, increasing the size of the message. In a normal scenario, there are no intrusion events, which lead to the usual allocation of network and computing resources. Such allocation is definitive for the 5 MB size of the message. With an increase in message size, this allocation of CPU resources increases slightly more, as seen on 10MB and 15MB of message size of increasing node density. A slight increase of CPU utilization time is seen for 5MB messages when the node's density is 200; this is due to the proposed system when the primary and secondary algorithm is done with execution and splitting algorithm initiates. This results in a slight increase in CPU utilization time; however, it is just one time. The system normalizes soon as the routing table is already constructed that. A similar assessment is also carried out for the attack scenario showcased in Figure.4.17.

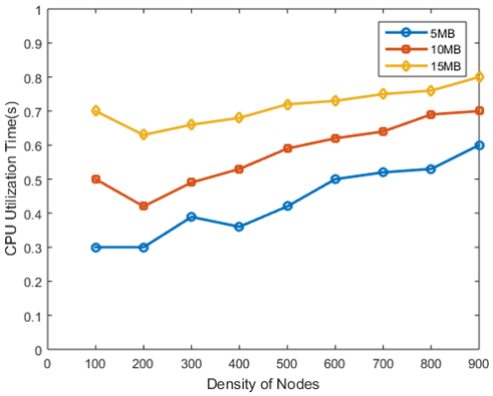

Figure 18: Impact of message size on CPU utilization Time (attack scenario)

Usually, in the attack prone situation, the attacker node tries to assist in data forwarding and act exactly like a normal node to gain its trust. Under such a scenario, the attacker attempts a greater number of message forwarding by deploying other victim nodes. This increases the CPU utilization time to approximately 10% compared to the normal scenario of communication. The CPU utilization time further increases when the message's size is increased by 5MB in every test case considered with an increase of node density. Therefore, this is one of the indicative patterns which distinguishes a stable communication environment from the attack environment. Another justification behind this outcome is that attackers' presence increases the number of message sizes, too, even if the node's density remains constants (owing to the spoofing exercised by the attacker. Therefore, even if the attack doesn't occur, the presence of the attacker and their preliminary activities can be captured using this graphical outcome.

Comparative Analysis of Processing Time

At present, conventional block chain usage has many reports associated with its computational complexity, and apart from this, it already has scalability issues. There is also an inclusion of encryption and the proposed concept of resisting illegitimate requests to join the network. Hence, this algorithm must be tested for computational complexity, which could also offer evidence of the lightweight nature. The processing time of the proposed system refers to

the complete time incurred right from the initialization level to the decoded of the blocks' encoded splits from the authenticated system.

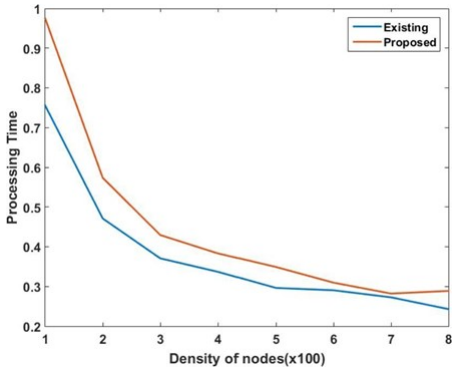

Figure 19: Analysis of Processing Time

Figure 19 showcases that the proposed system offers approximately 18% of reduced computational complexity than the existing blockchain. The prime reason behind this is proposed intelligence in the form of information processed by the decision module, which reduces previous steps' dependencies due to the potential trapdoor function. Hence, the overall processing time is reduced in this regard as compared to the existing system. Apart from this proposed system maintains the entries of the block in the form of the index, which can be stored in memory without any possibility of disclosure by the attacker as it supports both forward and backward secrecy.

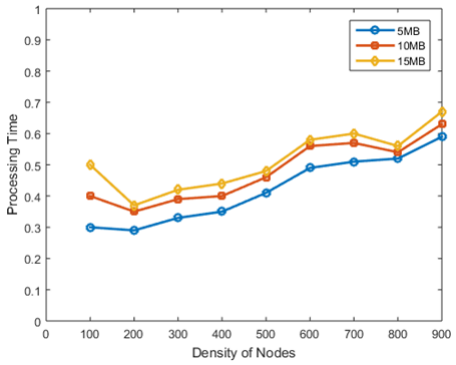

Figure 20: Impact of message size on Processing Time (normal scenario)

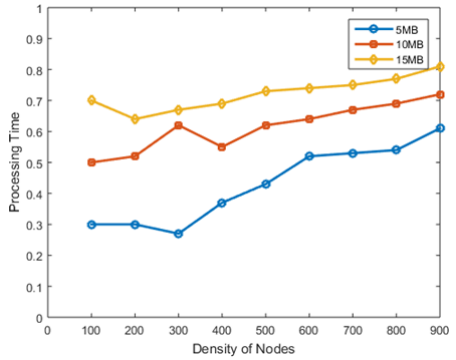

Figure 21: Impact of message size on Processing Time (Attack scenario) Figure 21 and Figure **??** show that the proposed system exhibits increasing processing time in the attack environment compared to the normal scenario. Similar justification resides here as discussed in outcomes of Figure 17 and Figure 18.

7 Summary

This Paper has discussed an intelligent model of computation. The term intelligent represents the potential of abstracting distinct network and transactional information of an IoT by the SDN controller. The proposed system discusses improved blockchain technology, a mechanism to resist any node from joining the network illegally, and McEliece cryptosystem for a more added security layer towards IoT communication system without using any sophisticated or complicated system.

References

[1] A.A. Abd EL-Latif, B. Abd-El-Atty, and S.E. Venegas-Andraca, *Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption*, Phys. A: Statist. Mech. Appl. **547** (2020), 123869.

[2] S. Atiewi, A. Al-Rahayfeh, M. Almiani, S. Yussof, O. Alfandi, A. Abugabah, and Y. Jararweh, *Scalable and secure big data iot system based on multifactor authentication and lightweight cryptography*, IEEE Access **8** (2020), 113498–113511.

[3] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako, and E. Djaba, *Encryption protocol for resource-constrained devices in fog-based iot using one-time pads*, IEEE Internet Things J. **6** (2019), no. 2, 3925–3933.

[4] X. Chen, Y. Liu, H.-C. Chao, and Y. Li, *Ciphertext-policy hierarchical attribute-based encryption against key-delegation abuse for iot-connected healthcare system*, IEEE Access **8** (2020), 86630–86650.

[5] C. Guo, J. Jia, Y. Jie, C.Z. Liu, and K.-K.R. Choo, *Enabling secure cross-modal retrieval over encrypted heterogeneous iot databases with collective matrix factorization*, IEEE Internet Things J. **7** (2020), no. 4, 3104–3113.

[6] X. Guo, J. Hua, Y. Zhang, and D. Wang, *A complexity-reduced block encryption algorithm suitable for internet of things*, IEEE Access **7** (2019), 54760–54769.

[7] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari, S.S. Ullah, M.A. Khan, and S.J. Khattak, *A lightweight and formally secure certificate based signcryption with proxy re-encryption (cbsre) for internet of things enabled smart grid*, IEEE Access **8** (2020), 93230–93248.

[8] A. Jalaly Bidgoly and H. Jalaly Bidgoly, *A novel chaining encryption algorithm for lpwan iot network*, IEEE Sensors J. **19** (2019), no. 16, 7027–7034.

[9] J. Khan, J.P. Li, B. Ahamad, S. Parveen, A.U. Haq, G.A. Khan, and A.K. Sangaiah, *Smsh: Secure surveillance mechanism on smart healthcare iot system with probabilistic image encryption*, IEEE Access **8** (2020), 15747–15767.

[10] O.A. Khashan, *Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment*, IEEE Access **8** (2020), 66878–66887.

[11] Y.M. Khattabi, M.M. Matalgah, and M.M. Olama, *Revisiting lightweight encryption for iot applications: Error performance and throughput in wireless fading channels with and without coding*, IEEE Access **8** (2020), 13429–13443.

[12] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S.W. Baik, *Secure surveillance framework for iot systems using probabilistic image encryption*, IEEE Trans. Ind. Inf. **14** (2018), no. 8, 3679–3689.

[13] S. Roy, U. Rawat, and J. Karjee, *A lightweight cellular automata based encryption technique for iot applications*, IEEE Access **7** (2019), 39782–39793.

[14] G.R.W. Thoms, R. Muresan, and A. Al-Dweik, *Chaotic encryption algorithm with key controlled neural networks for intelligent transportation systems*, IEEE Access **7** (2019), 158697–158709.

[15] Y.-W. Ti, C.-F. Wu, C.-M. Yu, and S.-Y. Kuo, *Benchmarking dynamic searchable symmetric encryption scheme for cloud-internet of things applications*, IEEE Access **8** (2019), 1715–1732.

[16] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, *Aes-128 based secure low power communication for lorawan iot environments*, IEEE Access **6** (2018), 45325–45334.

[17] A.S. Unde and P.P. Deepthi, *Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia iot*, IEEE Trans. Circuits Syst. II: Express Briefs **67** (2019), no. 1, 167–171.

[18] S. Wang, K. Guo, and Y. Zhang, *Traceable ciphertext-policy attribute-based encryption scheme with attribute level user revocation for cloud storage*, PloS One **13** (2018), no. 9, 203225.

[19] S. Xiong, Q. Ni, L. Wang, and Q. Wang, *Sem-acsit: secure and efficient multiauthority access control for iot cloud storage*, IEEE Internet Things J. **7** (2020), no. 4, 2914–2927.

[20] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, *Certificateless multi-party authenticated encryption for nb-iot terminals in 5g networks*, IEEE Access **7** (2019), 114721–114730.