Journal of Theoretical and Applied Information Technology

30th November 2023. Vol.101. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SMART AND SECURED SOFTWARE DEFINED NETWORKS WITH MCELIECE CRYPTOSYSTEM FOR INTERNET OF THINGS USING BLOCK CHAIN

J.V.N RAGHAVA DEEPTHI[1] ,AJOY KUMAR KHAN[2] , TAPODHIR ACHARJEE[1]

[1]Department of Computer Science and Engineering, Assam University, Silchar-788011, Assam State, India

[2]Department of Computer Engineering, Mizoram University, Aizawl 796004, India

E-mail: deepthijonnalagadda16@gmail.com ajoyiitg@gmail.com tapacharjee@gmail.com

ABSTRACT

The term Internet of Things (IoT) is used to describe everyday objects that can connect to and share data with other systems and devices over the Internet or other forms of communication with built-in sensors, processors, software, and other technologies. The primary objective is to plan and build an SDN-based IoT ecosystem with a secure communication infrastructure. The McEliece cryptosystem is used to further encrypt the block chain mechanism, and this implementation phase also includes intelligence into the data transfer mechanism. When data consisting of many processes related to controlling, routing, managing logic, etc. is sent to the SDN block, the complexity of the underlying mechanism is reduced. In a software-defined network, the data is stored in a block chain, encrypted with McEliece encryption, and then authenticated across the whole control, data, and application layers. The control plane is also used for operations and forwarding, allowing for better decision making. This study explains how SDN may be used to build a smart computational model with a wider range of features, all while keeping the underlying communication system secure. This article proposes a solution that uses the blockchain and the McEliece cryptosystem in an optimal layout to provide unprecedented levels of safety.

Keywords: *Block chain, IoT, SDN, encryption, security, delay, node, cryptosystem, data transmission, and McEliece.*

1.INTRODUCTION

The Internet of Things (IoT) is a high-tech networking method that assigns a special identification to each device connected to the network [1]. The Internet of Things (IoT) is a network of interconnected computing devices, infrastructure, services, and endpoints that enable physical and digital objects (including but not limited to computers, smartphones, and wearables) to work together to achieve a common goal. However, there are a number of security vulnerabilities that constantly cause concern inside an IoT. Some examples include denial-of-service (DoS) attacks, data theft (or data breaches), and Botnets assaults, in which multiple systems work together to take control of a victim's device and steal their private data. Edge computing and IoT frameworks use unprotected devices to expand their networks, which is a major security risk [2, 3]. Security is also compromised by the fact that some IoT devices can hop from one network to another. Zero trusts [4] is a strategy for protecting the internet and IT system that is taken into account by the standard IoT network today. Assuming they are approved, it will also mean that any type of device can join the network or use its resources. Therefore, it is simple for adversaries to bypass the firewall system in an IoT and proceed in parallel with the conventional node. Considering the wide variety of IoT devices and the fact that the vast majority of them are extremely susceptible and insecure, this might be a difficult situation. As a result, it becomes simpler for an adversary to exploit the gateway system in place in an IoT setting [5, 6].

Three-layered architecture, four-layered architecture, and five-layered architecture are just some of the current classifications of layer-based IoT operations. There are three layers in a typical software architecture setup: the application layer, the network layer, and the perception layer. In a four-layer setup, there are also support, network, and perception layers. The business layer, the application layer, the processing layer, the transport layer, and the

perception layer make up the five layers of a five-layer architecture. An examination of the various taxonomies reveals that the three-layer architecture is the most widely used in IoT implementations. Thus, a three-tiered design [7, 8] is a potential option for the proposed system. The major goal is to design and implement a trustworthy network for IoT devices based on software-defined networking. During this stage of implementation, intelligence is integrated into the data transfer mechanism, and the McEliece cryptosystem is employed to further encrypt the block chain mechanism.

There are many reasons why blockchain technology is currently considered the best long-term security strategy for the Internet of Things. A block chain is a series of linked data blocks that are secured with cryptography. Preliminary data (or blocks) are hashed using the Secure Hash Algorithm (SHA-512), and the hashed value is stored in a block along with transaction data in tree format and a timestamp [9]. Stability, traceability, process integrity, security, and speedier processing are some of the hallmarks of block chain [10]. Nonetheless, block chain has a number of stated drawbacks, including higher energy consumption, immutable data, a dependence on self-maintenance, higher costs, and the fact that the concept is still in its infancy. This restriction, however, is surmountable if the encryption mechanism employed by like blocks receives sufficient attention. The McEliece asymmetric cryptosystem [11] is used for this purpose in the proposed system. The suggested system utilizes the McEliece encryption approach's capacity to link the block chain due to the speedier method of encryption and decryption process with a greatly decreased number of steps.

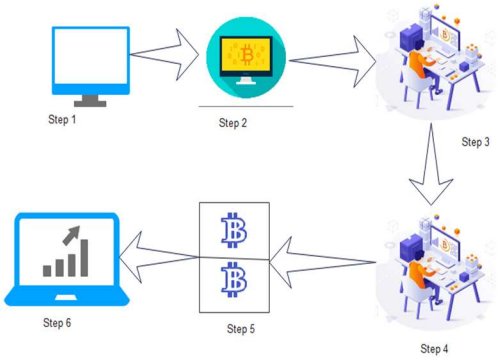

Figure 1. Process Involved in Block chain Technology

Step-1 of the block chain's activity, depicted in Figure 1, involves user-A's desire to pay money to user-B. In Step-2 operation, the system builds an initial block chain online, with each block representing a single transaction. In Step 3 of the shown procedure, the newly built block is broadcast to all participants in the network. This transaction needs to be approved by all the different kinds of systems involved, and then validated in Step 4. In Step5, this block is added to the chain, which serves as an immutable, auditable record of the transaction. Step six of the transaction entails user-B receiving the funds from user-A.

In Figure 2, many iterative actions illustrate how blockchain technology might be applied in the Internet of Things. Sensing data is the first step, followed by a measurement of the private details included therein. The third step involves carrying out interpretation using a wide variety of analytic tools. Connecting to other resources that can help with more complex analytical tasks is the fourth step. Several different types of predictive procedures also help with this. Finally, the examined data will undergo additional optimization.

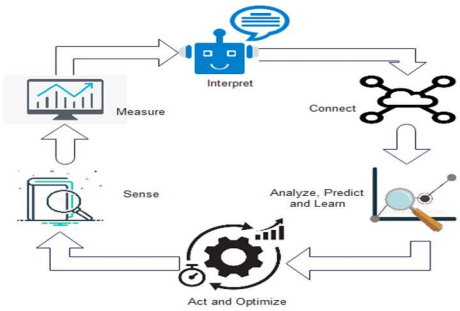

Figure 2. Integration of Block chain in IoT

Software-Defined Networking (SDN) separates the network control plane and data plane, which provides a network-wide view with centralized control (in the control plane) and programmable network configuration for data plane injected by SDN applications (in the application plane). With these features, a number of drawbacks of the traditional network architectures such as static configuration, non-scalability and low efficiency can be effectively avoided. However, SDN also brings with it some new security challenges, such as single-point failure of the control plane, malicious flows from applications, exposed network-wide resources and a

vulnerable channel between the control plane and the data plane. In this paper, we design a monolithic security mechanism for SDN based on Blockchain.

The request stream originates at the perception layer's many nodes, and is delivered to the network layer, where the distributed ledger's operational mechanism resides in the cloud. For administration at the application layer, the decentralized cloud also maintains two-way communication with the cloud in regard to a separate application. When it comes to Internet of Things (IoT) scenarios, it is the block chain application located between the network and application layer's role to manage communication amongst interacting nodes. The collected data will be processed further by the cloud's central server. In addition, SDN switches sit atop the perception layer, where the stream and request flows are evaluated, and the data flow is then sent onwards through the controller, which sits atop the network layer, where it is then communicated with the cloud server, where an algorithm is run to justify the regular or malicious nature of the communication link. The conversation has led to the development of a secure IoT communication system based on SDN and protected by blockchain technology [12, 13].

2.RELATED WORKS

As an alternative way of communication riding atop the named data networking stack, the content-centric Internet of Things' (IC-IoT) conventional design provides intriguing possibilities. The authors [Cao et al., 2018] investigate the security problem in IC-IoT and objectively state that it is less likely to be investigated due to design flaws. The authors also discover that the differential privacy (DP) method provides a broader level of data privacy. An effective security schema for user/device authentication to secure mobile payment is envisioned in [Chen et al., 2019] due to the fact that IoT interconnects a large number of smart devices that run different forms of online payment schemes. This research presents a streamlined approach to security protocol design for protecting customer data in mobile payment systems within the Internet of Things. Without respect to certificates, the solution method implements a re-signature-based strategy for authentication via the mobile payment systems protocol. Achieving higher Security with user/device privacy preservation and anonymity maintenance processes, the lightweight design enhances execution speed[15].

The authors [Hosen et al., 2019] have also dealt with a related issue in Internet of Things research. Each IoT node is free to travel in any direction at any speed, regardless of the passage of time, as depicted by the random mobility modeling presented by the system representation. However, a security framework is also presented in this study that can keep the node's data private from both internal and external threats. The system can also deal with sensing coverage issues that overlap. The system's performance score does not emphasize the precision with which it estimates delays and latency [16]. The mobile crowd sensing (MCS) for IoT does not have a means to protect user privacy. The privacy concerns in MCS prompted [Yan et al., 2019] to develop the task selection method. The results indicate that MCS has the potential for wide-area coverage, confidentiality maintenance, and efficient resource utilization [17]. The author has not dealt with the issue of edge node assaults, which are a major vector for compromising user data. Therefore, the differential privacy technique is provided [Miao, Y., et al., 2019] to lessen the data uncertainty and cut down on the data loss efficiently [18]. Table1 provides a synopsis of the aforementioned studies.

Table 1. Overview of Traditional Security Issues in IoT

Authors	Problems	Technique	Advantage	Limitation
[Cao et al.,2018] [14]	Privacy preservation of consumer data	Randomized principle based on DP-technique	Ensure consumer data privacy	Applicability is limited to only the smart grid, and the complexity of execution is unclear

[Chen et al., 2019] [15]	IoT devise/user anonymity and privacy with low traffic overhead	Re-signature based certificate-less authentication	The payment protocol design offers computational efficiency with scalable performance	The type of attacks it handles during mobile payments has not extensively discussed with the node mobility aspect
[Hosen et al.,2019] [16]	Node authentication with the minimum occurrence of overlapping sensing	ID-based authentication schema	Capable of malicious node and intrusion detection with minimized overlapping sensing	The intrusion prevention strategy is not defined and remains unclear. And also delay and latency problem is not much focused.
[Yan et al., 2019] [17]	Privacy issues in MCS	Task selection mechanism	Privacy preservation and optimal resource utilization	Not considered analysis with an edge node
[Miao,Y et al., 2019] [18]	Edge node attack	Differential privacy technique	Reduced the data loss	Not benchmarked

This section deals with the existing researches in the domain of IoT with the encryption-based security approaches. The work of [Tsai et al., 2018] 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 [19]. 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 [Liu, Z., et al., 2018]. The encryption mechanism gives improved performance and minimized computation overhead [20]. The resource-constrained IoT devices are composed of different issues like low computational ability, high latency, low bandwidth, etc. These issues are addressed in [Roy et al., 2019] with a lightweight encryption technique based on cellular automata for IoT. The technique can reduce the run time and can prevent data theft [21].

The complexity parameter is not addressed in prior work. The work of [Guo et al., 2019] 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 [22]. The work of [Hassan, W. H et al., 2019] 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 [23]. The chaotic encryption algorithm is introduced in [Thoms et al., 2019] for intelligent data transmission in IoT with key controlled neural networks. The cryptanalysis gives improved information entropy than the existing algorithm [24]. The summary of the above researches is given in Table.2.

Table 2. Overview of Encryption-based Security Schemes

Authors	Problems	Technique	Advantage	Limitation
[Tsai et al., 2018] [19]	Security of IoT	AES Algorithm	Resists different security attacks	Not addressing the issues of information centric IoT
[Wang et al., 2018] [20]	Sufficient data protection	ABE algorithm	Improved performance and minimized computation overhead	Not considered resource constrained IoT devices
[Roy et al., 2019] [21]	Resource constrained IoT devices	Lightweight encryption technique	Reduce the run time and prevents data theft	Complexity parameter is not addressed
[Guo et al., 2019] [22]	Data encryption	Reduced block encryption	Less complex and fast encryption	Not benchmarked
[Hassan, W. H et al., 2019] [23]	Authentication	Multiparty authentication based encryption	Data privacy and efficient support for 5G network	A comparative analysis is not conducted
[Thoms et al., 2019] [24]	Intelligent data transmission	Chaotic encryption algorithm	Improved information entropy	Application aspects are not discussed

From the above table, applicability is limited to only a smart grid, and the complexity of execution is unclear. The type of attacks it handles during mobile payments has not been extensively discussed with the node mobility aspect. The intrusion prevention strategy is not defined and remains unclear. Also, delay and latency problems are not much focused on, not considered analysis with the edge node, and not considered sourcing and location-aware privacy.

3. PROPOSED METHODOLOGY

In order to improve randomization during ciphering with an asymmetric encryption mode, the McEliece cryptosystem is used. This encoding method has a solid standing in post-quantum cryptography. This algorithm's decoding process is intricate because of its dependence on linear codes, which form the basis of the algorithm's primary architecture. Because of its unique set of characteristics, the McEliece encryption scheme was chosen for the proposed system. As the proposed system is deployed over an IoT environment with many nodes, encryption must be light weight. To be lightweight, an encryption algorithm should execute faster and occupy lesser memory. McEliece algorithm facilitates faster ciphering as well as a deciphering process compared to the potentially strong algorithm RSA. Although the McEliece algorithm's legacy version does not offer any process to generate a signature, amending the conventional scheme could successfully result in a signature generation [25].

Using individual data from each sensor, IoT is a more advanced communication network. The IoT facilitates the coordination of diverse cybernetic and physical systems toward the common goal of satisfying a user's need or desire. Nonetheless, there are certain safety risks. This is a persistent source of worry in the Internet of Things. The most significant security risk in cloud computing and IoT paradigms is introduced by non-secure tools that are employed to increase the range of communication. In addition, sensor nodes may hop from one channel to another, which is quite dangerous. Zero trust is currently seen as the basis for data center and IT platform security by the standard IoT platform. It also means that any device, so long as it is approved, can access the internet or the system's internal resources. Bypassing the security mechanisms of an IoT allows adversarial actors to freely move in parallel with the reliable node. This might be a challenging issue because there are different IoT systems, most of which are very sensitive and unsecured. Due to this occurrence, an adversary

can exploit the entry point method already present in an IoT environment.

The complete operation of this encryption approach is carried out in three steps as brief below:

i) Step-1-GenerationofKey

This is the first step of the McEliece algorithm. A selection of a linear code Lc is carried out by user-A. This selection is carried out from the user-A codes to be the best mechanism to perform decoding. It also renders the linear code L_c public while keeping the algorithm to perform decoding as private information. To carry out the decoding process, the proposed system has dependencies over two essential attributes, i.e., i)Information about linear code L_c and ii)Information about all the parameters that could be utilized while signifying linear code L_c from the selected group of codes. All this information is required to carry out the randomization process. The operation carried out in the process of generation of codes areas are follows:

1. A binary linear code L_c is selected as ($b1$, $b2$), which can be potentially used for rectifying e errors obtained from the large group of codes. The system then evolves for generating a potential decoding process χ due to this selection process. Consider that Fisa generator selected for the matrix of linear codes L_c while there are various generator matrices for all the linear codes L_c. However, there is a definitive selection associated with this group of codes as there is a possibility of disclosing the decoding process χ.
2. An arbitrary value of dimension ($b2$ x $b2$) is selected by user-A, a non-singular matrix of binary form B.
3. An arbitrary matrix of dimension ($b1$x $b1$) is selected by user-A, basically a matrix P form by permutation.
4. The user-A performs the computation of $b2$ x $b1$ matrix $F1$,equivalent to(BFP).
5. The public key's formulation is done as (F1,t), and the private key is formed as (BFP), where matrix P offers the possibility of encoding. It can be stored in the form of a specific parameter utilized for choosing linear code L_c.

ii) Step-2:Encryption of Message

This is the second stage of the algorithm implementation, which considers that User-B wants to forward a message *msg* to user-A, a public key defined as (F1, t) [185-190].Then the following operation takes place:

1. A message *msg* is encoded by user-B in the form of a string with the length of $b2$ of binary form.
2. A vector L_{c1} is computed by user-B as $L_{c1}=msg.F1$.
3. An arbitrary message with the vector of size n-bit is generated by user-B that possesses precisely t number of ones.
4. An encrypted message is computed by user-B as $L_c=L_{c1}+z$.

iii) Step-3:DecryptionofMessage

This algorithm's decryption process is slightly different from other existing algorithms where the steps are not the same as the encryption process [191-195]. Once the user-A receives linear code L_c from user-B that it performs the following operation:

1. A computation of(1/P) is carried out by user-A.
2. An improved linear code is computed by user-A as $L_{c1}=L_c(1/P)$.
3. The decoding algorithm χ is used by user-A for extracting L_{c1} to *msg1*.
4. Finally, the decoded message is obtained by user-A as $msg=msg1.(1/B)$.

Finally, the McEliece algorithm also carries out proof of decryption of message to ensure that the message obtained by the end-user is having data integrity. For this purpose,

$$L_{c1}=L_c.(1/P)=msg.F1.(1/P)+z(1/P)=msg.B.F+z(1/P) \quad (1)$$

In this scenario, it is feasible for Goppa code F to rectify the t errors, and the message msg BF is located at a distance of t from $L_c(1/P)$. Hence, the system can obtain rectified code as $msg1=msg.B$. Therefore, if the inverse of B is now multiplied, then it will give

$msg=msg1.(1/B)=msg.B.(1/B)$ (2)

Therefore, the outcome is matching plaintext, which proves that the decryption process is successful. Usually, the attacks that this algorithm can successfully resist are those adversaries with possession of the public key and not the private key. This algorithm can Successfully resist bruteforce attack and structural attack. However, this algorithm has certain loopholes, mainly associated with the public key's size, which is a bit larger. It is seen that even after using Goppa code with the recommended parameters, the size of the public key will be around 2^{19} bits, which is quite larger and will yield issues during implementation. Apart from this, the encrypted message is also much longer compared to the original message in plaintext. Usage of such a longer encrypted message will inevitably increase channel capacity consumption, resulting in a more vulnerable condition. This will also cause errors during transmission. Apart from this, theMcEliece cryptosystem is not applicable when it comes to the authentication process. It also lacks the signature scheme as the complete encryption process is not one to one process, and the complete algorithm is highly asymmetric. It will mean that there is no way of achieving commutation between the process of encryption and decryption. The prime reason for this adoption is mainly its faster process of performing the ciphering and deciphering process. It has lower dependencies of the number of operational steps than another existing algorithm, e.g., RSA.

The McEliece cryptosystem's adoption offers faster processing in ciphering and deciphering; however, it has a dependency on the larger size of keys. These issues are considered while developing the proposed system to evolve up with a better security system in an IoT. The prime plan of the proposed algorithm is to offer a secured communication link from the target node. The algorithm aims to mainly implement block chain to secure the information, there by 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 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:N *den*
3. $\Phi bc=f1[(x,y),A, Nden,R]i$
4. $bcvec=f2(Nden,\Phi bc)$
5. $[rt,q1,q2]=f3[(x,y),R,Nden,\Phi bc,bcvec]$
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 (Figure3),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.

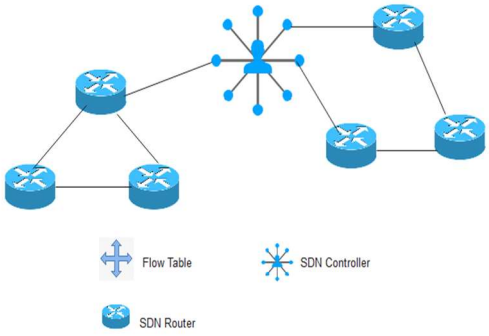

Figure 3. Stage-I (Network Deployment)

ii) Creating Block chain

The next part of the algorithm implementation is constructing a block chain of the information primarily considered an input. This operation is carried out for all node density values N_{den} existing over the deployment zone (Line-2). An explicit function $f1(x)$ is constructed, which takes the input arguments to generate a matrix of block chain Φ_{bc}(Line-3).The operation carried out for this purpose is as follows: Before implementing block chain, 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 Φ_{bc}. Hence, it is a one-point reliable source of information when any other neighboring nodes also want to communicate using the information retained within Φ_{bc}. The next part of the implementation is about exploring the single hops neighboring node from the target node whose information is obtained from Φ_{bc} matrix while constructing block chain.

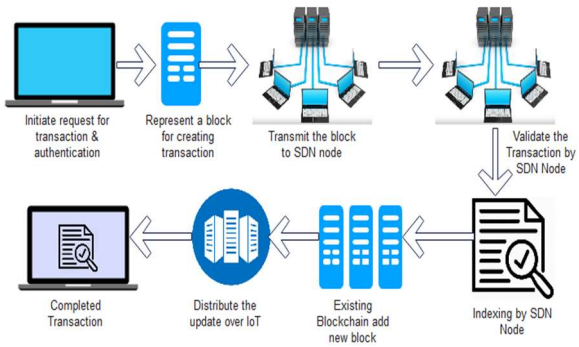

Figure 4. Stage-II (Creating Block chain)+

Figure4 highlights the mechanism used for creating and implementing the block chain in the proposed system. For this purpose, a request for a transaction is carried out, and authentication is carried out. In the proposed system, block chain 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 block chain 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 block chain:

1. 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 system constructs a highly secured digital identity using a digital signature. These keys are also used to extract the information too.

2. 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 5). It further secures the blockchain to obtain a block chain 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 N_{den} and matrix of block chain Φ_{bc}(Line-4) to generate block chain vector bc_{vec}. For all node density values, the function extracts the information about the SDN nodes from the block chain Φ_{bc} 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 block chain vectors bc_{vec} in this process (Line-4).

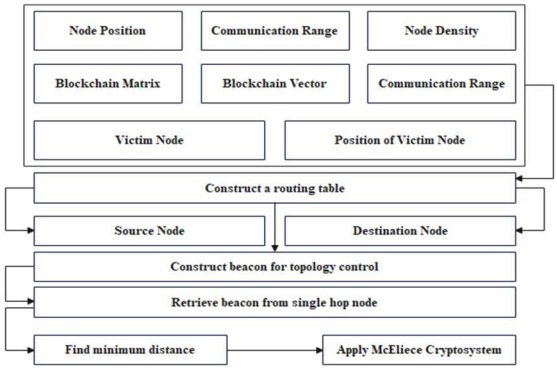

Figure 5. Stage-III(Constructing Security Wall)

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 N_{den} where a routing table is formed between the source and destination node (s_n, d_n). 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 r_t(Line-5) considering only a single hop. A beacon is formed considering the block chain matrix Φ_{bc} and block chain vector bc_{vec},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, block chain matrix, node density, and block chain vector.

Hence, this information is required to be further secured, falling in to the attacker node's captivity. This message is checked by analyzing the presence of a block chain 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 q1and q2, concerning the node density, to randomize the process of allocating secured routes to the source node and destination. However, for security purposes, the systems next process considers only routing table *r*t as it stores all the confidential current topological information (Line-6). The next part of this process is to formulate another function, *f*4(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 trap door function that ensures both forward and backward secrecy as well as is capable of identifying the illegitimate request by referring to the block chain vectors and currently formed routing table dynamically.

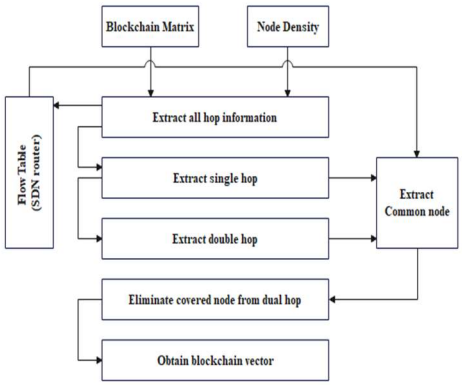

Figure 6. Stage-IV(Final Layer of Security)

Figure 6 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 by passed 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 block chain vector. Assuming that attacker has this knowledge, then the block value it generates will be different from the generated block chain 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 neighbouring 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.

4. RESULTS AND 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 m^2. 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 Result

As the proposed system implements block chain, the adoption of work [26] 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, block chain adoption could be questionable for high-end distributed computing, which is required to be testified for the proposed block chain-based method.

Transmission Delay

The network delay is anticipated to be higher if there is an inclusion of many sophisticated operations involved in securing the communication system. The proposed system uses a series of operations where the mechanism to thwart the illegitimate request, implementing the proposed block chain, 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.

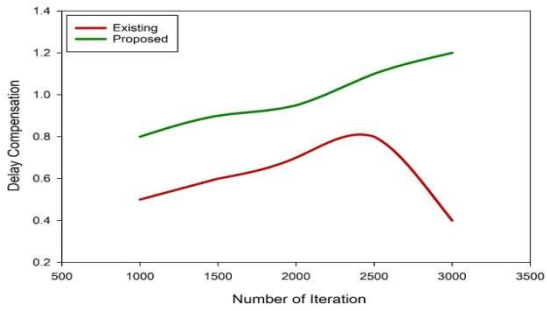

Figure 7. Analysis of Delay

The outcome is shown in figure 7 highlights that the proposed system offers approximately 45% better delay compensation in comparison to the conventional block chain method. The prime justification is: conventional block chain 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 block chain 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 pre-emptively', causing better delay compensation performance in the proposed system.

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.

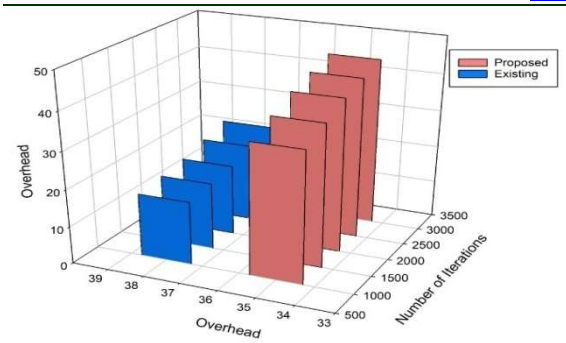

Figure 8. Analysis of Overhead

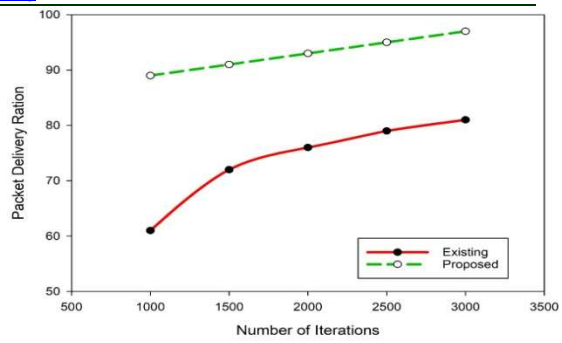

Figure 9. Analysis of Packet Delivery Ratio

Figure 8 showcases that the proposed system offers 27% reduced overhead compared to the existing block chain 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 block chain 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 block chain. Therefore, the proposed system minimizes the overhead with the increase of iteration.

Packet Delivery Ratio

Packet delivery ratio is one of the essential parameters to showcase that implemented security modelling 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 9 highlights that the proposed system offers a 37% higher packet delivery ratio than the existing block chain. The reason is existing block chain 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.

Message Size

Wing 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

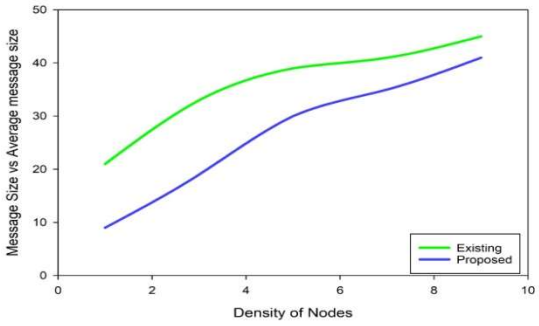

Figure 10. Analysis of Message Size

The simulation outcome shown in Figure 10 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.

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.

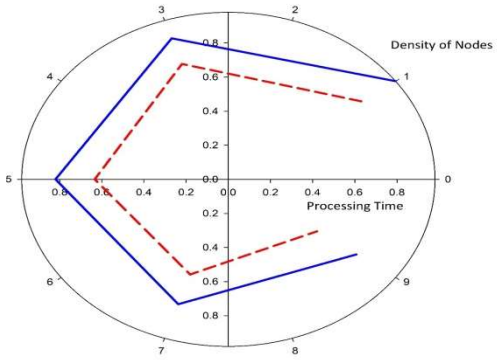

Figure 11. Analysis of Processing Time

Figure 11 showcases that the proposed system offers approximately 18% of reduced computational complexity than the existing block chain. 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.

5.CONCLUSION

An intelligent computational model has been discussed in this article. Intelligent refers to the possibility of the SDN controller abstracting separate network and transactional details of an IoT. Enhanced block chain technology, a mechanism to prevent unauthorized nodes from joining the network, and the McEliece cryptosystem are all discussed in the proposed system as potential means of providing an additional layer of security for the IoT communication system without resorting to overly complex measures. Optimized security systems will be a future addition to the IoT infrastructure.

REFERENCES:

[1] Banafa, A. (2017). IoT and blockchain convergence: benefits and challenges. *IEEE Internet of Things*, *9*.

[2] Samaniego, M., Jamsrandorj, U., & Deters, R. (2016, December). Blockchain as a Service for IoT. In *2016 IEEE*

international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 433-436). IEEE.

[3] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., &Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881-888.

[4] Azbeg, K., Ouchetto, O., Andaloussi, S. J., &Fetjah, L. (2021). A taxonomic review of the use of IoT and blockchain in healthcare applications. *Irbm*.

[5] Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z., & Peng, M. (2019). When Internet of Things meets blockchain: Challenges in distributed consensus. *IEEE Network*, *33*(6), 133-139.

[6] Meloni, A., Madanapalli, S., Divakaran, S. K., Browdy, S. F., Paranthaman, A., Jasti, A., ... & Kumar, D. (2018). Exploiting the IoT potential of blockchain in the IEEE P1931. 1 ROOF standard. *IEEE Communications Standards Magazine*, *2*(3), 38-44.

[7] Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. *IEEE Systems Journal*, *15*(1), 85-94.

[8] Mohanta, B. K., Jena, D., Panda, S. S., &Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, *8*, 100107.

[9] Humayun, M., Jhanjhi, N. Z., Hamid, B., & Ahmed, G. (2020). Emerging smart logistics and transportation using IoT and blockchain. *IEEE Internet of Things Magazine*, *3*(2), 58-62.

[10] Sharma, P. K., Kumar, N., & Park, J. H. (2020). Blockchain technology toward green IoT: Opportunities and challenges. *IEEE Network*, *34*(4), 263-269.

[11] Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076-8094.

[12] Liu, D., Ni, J., Huang, C., Lin, X., & Shen, X. S. (2020). Secure and efficient distributed network provenance for iot: A blockchain-based approach. *IEEE Internet of Things Journal*, *7*(8), 7564-7574.

[13] Wu, J., Dong, M., Ota, K., Li, J., & Yang, W. (2020). Application-aware consensus management for software-defined intelligent blockchain in IoT. *IEEE Network*, *34*(1), 69-75.

[14] Cao, H., Liu, S., Wu, L., & Guan, Z. (2018). SCRAPPOR: An efficient privacy-preserving algorithm base on sparse coding for information-centric IoT. *IEEE Access*, *6*, 63143-63154.

[15] Chen, Y., Xu, W., Peng, L., & Zhang, H. (2019). Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT. *IEEE Access*, *7*, 15210-15221.

[16] Hosen, A. S., Singh, S., Mariappan, V., Kaur, M., & Cho, G. H. (2019). A secure and privacy preserving partial deterministic RWP model to reduce overlapping in IoT sensing environment. *IEEE Access*, *7*, 39702-39716.

[17] Yan, K., Luo, G., Zheng, X., Tian, L., & Sai, A. M. V. V. (2019). A comprehensive location-privacy-awareness task selection mechanism in mobile crowd-sensing. *IEEE access*, *7*, 77541-77554.

[18] Miao, Y., Tong, Q., Choo, K. K. R., Liu, X., Deng, R. H., & Li, H. (2019). Secure online/offline data sharing framework for cloud-assisted industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(5), 8681-8691.

[19] Tsai, K. L., Huang, Y. L., Leu, F. Y., You, I., Huang, Y. L., & Tsai, C. H. (2018). AES-128 based secure low power communication for LoRaWAN IoT environments. *Ieee Access*, *6*, 45325-45334.

[20] Liu, Z., Jiang, Z. L., Wang, X., &Yiu, S. M. (2018). Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating. *Journal of Network and Computer Applications*, *108*, 112-123.

[21] Roy, S., Rawat, U., &Karjee, J. (2019). A lightweight cellular automata based encryption technique for IoT

applications. *IEEE Access*, *7*, 39782-39793.

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

[23] Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

[24] Lokshina, I. V., Greguš, M., & Thomas, W. L. (2019). Application of integrated building information modeling, IoT and blockchain technologies in system design of a smart building. *Procedia computer science*, *160*, 497-502.

[25] Shrestha, S. R., & Kim, Y. S. (2014, September). New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)* (pp. 368-372). IEEE.

[26] Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104-112.