JOURNAL OF BASIC SCIENCE AND ENGINEERING

EFFICIENT A LIGHTWEIGHT MULTI-ZONE DAG BLOCKCHAIN FRAMEWORK FOR SECURING MEDICAL DATA IN FOG-BASED IOT APPLICATIONS

[1] Kolakaleti Divya Sree, [2]Aswin Kumer S V
Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh 522302, India.
E-Mail id: durga123456sri@gmail.com, and svaswin@gmail.com

Abstract:
Blockchain technology is regarded as a promising security solution for medical data applications linked to the Internet of Things (IoT). The fundamental purpose of blockchain networks in medical care is to ensure security. Blockchain has a linear structure that expands with the amount of transactions entered. This rise in size is the fundamental hurdle to blockchain adoption, making it unsuitable for resource-constrained IoT applications. Furthermore, conventional consensus algorithms such as PoW, PoS, and safer agreement techniques based on the Proof-of-Work (PoW) paradigm are being developed to solve these difficulties. This engineering framework prioritizes the security of information from IoT device sensors. This paper solves these concerns by introducing a novel lightweight blockchain topology and consensus approach. The Multi-Zone Direct Acyclic Graph (DAG) Blockchain (Multizone-DAG-Blockchain) framework is proposed for fog-based IoT applications. In this application, fog computing technology is combined with IoT to offload IoT workloads to fog nodes, lowering IoT device power consumption. A non-clone able physical function-based validation technique (DPUF-VM) verifies multiple authentication certificates on the blockchain to ensure that both IoT and fog nodes are who they claim to be. Each transaction on the blockchain is saved as a hash function using the lightweight Cube Hash algorithm and signed with the Four-Q-Curve method. Sensitive data is encrypted and stored in the cloud. Fog nodes protect data while lowering IoT nodes' energy consumption and complexity. To begin, the fog node does a redundancy analysis using the Jaccard Similarity (JS) metric. It then does a sensitivity analysis with the Neutrosophic Neural Intelligent Network (N2IN) algorithm. A simple proof-of-authentication (PoAh) method is given for transaction validation, and the bi-objective spiral optimization (BoSo) algorithm picks the best consensus node to do it. This approach is optimized for energy consumption, storage cost, response time, and throughput.
Keywords: *Iot, medical health care application, Multi zone DAG blockchain; dynamic PUF; lightweight PoAh consensus; BoSo node selection; four-q-curve encryption; IoT environment.*

1. Introduction

The combination of blockchain, the Web of Things (IoT), and deep learning has the potential to change clinical consideration by providing a solid and safe observing framework for touchy clinical information [1, 2]. Here, the main goal is to create a blockchain-based healthcare system that safeguards patient privacy. This framework will use deep learning techniques and a reasonable agreement convention to ensure the categorization, veracity, and accessibility of health care information while enabling advanced information research and knowledge [3, 4]. The healthcare industry generates vast amounts of sensitive data, such as patient medical records, clinical images, genetic information, and data from wearable technology [5, 6]. Maintaining data privacy is critical for both regulatory compliance and patient trust. Blockchain technology is an appealing solution because traditional, constrained systems struggle to ensure data confidentiality and safety [7, 8]. The innovation of blockchain is that it provides a decentralized, immutable record that is transparent,

truthful, and easily identifiable. The medical services industry stores its data in a distributed network of hubs. Blockchain enhances security and prevents unauthorized modifications or tampering [9]. Furthermore, it does away with the need for a centralized authority, allowing patients more autonomy over their information [10, 11]. Through wearable technology, sensors, and clinical hardware, the Web of Things (IoT) powers a variety of ongoing patient information, playing a crucial role in the medical services industry [12]. However, it is crucial to send and keep this data securely in order to safeguard patients' privacy. Information can be safely and openly shared among authorized members while maintaining patient anonymity and categorization by integrating IoT devices with a medical care blockchain [13]. Predictive analytics, therapy recommendation, and disease detection are just a few of the healthcare areas where deep learning algorithms have demonstrated outstanding results [14]. By utilizing the vast amount of safely stored healthcare data on the blockchain, deep learning models can be taught to enhance healthcare outcomes, enable personalized medication, and provide insightful knowledge [15]. Various strategies can be used in this setting to maintain security. Encryption, information anonymization, and secure multi-party calculation (MPC) are strategies used to protect private clinical data while saving the capacity to lead adroit investigations [16]. With homomorphic encryption, scrambled information can be used for estimations, keeping up with security the whole way through the handling pipeline. Despite the fact that work is progressing to build agreement conventions that utilize profound learning, blockchain frameworks normally utilize exemplary agreement conventions like Evidence of Work (PoW), Verification of Stake (PoS), and Functional Byzantine Adaptation to Internal Failure (PBFT). These conventions influence the registering ability of profound learning models to achieve agreement and settlement on the blockchain [17, 18]. Overall, the integration of a profound learning agreement convention-based, medical services-safe blockchain into the Web of Things has the potential to transform the medical care sector by ensuring the protection, clarity, and security of information across the board [19]. However, these credentials can be easily hacked by attackers. On the other hand, the physically tilting PUF is the hardware-based security credential embedded in every IoT device [19]. Therefore, PUF-based authentication becomes a promising research direction. Although authentication prevents unwanted access, data still needs to be protected from attackers [20]. For data security, cryptographic techniques play a central role. In general, encryption algorithms are widely used to ensure data security in the IoT [21]. Due to their complexity, these algorithms are not suitable for the IoT environment because devices have limited resources. This makes highly complex algorithms unsuitable for the IoT environment. Therefore, lightweight encryption algorithms have become an essential solution for securing the IoT [22]. However, the following research questions are still unanswered in IoT and need to be addressed: What is the performance of authenticated IoT nodes using lightweight and dynamic credentials? How do I use cryptographic functions to secure transactions performed by IoT nodes? How can we make the blockchain as lightweight as possible for the IoT environment to be efficient? In this paper, we answer these research questions through optimal blockchain integration. Furthermore, the algorithms used with the lightweight blockchain are also the main culprits for heavy computation in the blockchain environment.

1.1 Research Aim and Motivation

This research aims to reduce the heavy computational needs and constraints of the IoT-blockchain technology. This research topic focuses on lightweight blockchain infrastructure, lightweight consensus, and lightweight security protocols for these purposes the developed secure IoT environment in terms of initial authentication and sensitive data security.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

This research topic mainly focuses on the existing problems in IoT ecosystems. The current blockchain technology is not suitable for the resource-constrained IoT environment. Although some applied lightweight blockchain-based methods on IoT, there is still high complexity. Indeed, most lightweight blockchain solutions focus on lightweight consensus algorithms. However, the structure of blockchain also increases complexity because the IoT environment is broad-spectrum. Besides, the involvement of redundant data from IoT nodes rapidly increases the bulk of the blockchain. Even in lightweight consensus algorithms, the consensus nodes are selected randomly or in the round, inefficient. Furthermore, the algorithms used with the lightweight blockchain are also the main culprits of heavy computation in the blockchain environment.

1.2 Major Contributions

The principal contribution of this topic is the design of new Multi-DAG technology for the IoT environment. The essential contributions of this work are as follows; Firstly, a lightweight authentication performed by the dynamic validation mechanism of PUF with the support of blockchain. In this process, a random identifier is dynamically generated and approved at any moment to guarantee its validity. Secondly, the encrypted data stored is validated in the blockchain by consensus. We propose a lightweight proof of authentication (PoAh) consensus. Moreover, we minimize the consensus complexity by selecting the optimal node through the Bi-Objective Spiral Optimization (BoSo) algorithm. Thirdly, we propose a secure IoT environment based on the multi-zone DAG blockchain (Multizone-DAG-Blockchain) that reduces complexity and energy consumption. Three significant aspects are enhanced. Firstly, lightweight authentication, secondly, lightweight data encryption, and thirdly lightweight consensus algorithm design. Fourthly, all transactions are handled in a new Multi-Zone DAG Blockchain infrastructure (Multizone-DAG-Blockchain) that is lightweight and scalable. Bulk is further decreased by using the Cube Hash algorithm and the Four-Q Curve-based signature algorithm in the blockchain. Finally, For the incoming IoT data, the fog node performs a Jaccard similarity-based redundancy analysis, including a neutral neural intelligent network (N2IN) sensitivity analysis. Then, for all sensitive data, the fog node applies lightweight encryption based on the four-quarter curve.

1.3. Problem Definition

A proposed distributed authentication device in a Fog-IoT environment is based on distributed blockchain technology. The significant issues with the above approach are numerous. Firstly, the access of non-authorized users is minimized, but the proposed approach is overly complex due to ECDSA and SHA-1, which have very high computational complexity. Secondly, authentication is based on unprotected parameters such as system ID and public address, which are easily falsifiable. Moreover, the public address is published to all nodes through a public network, increasing its vulnerability. Thirdly, the PoW (proof of work) consensus algorithm is used, which is complex and increases resource consumption. In PoW, all participating nodes must validate transactions and broadcast the evidence. If one node has a higher load or fewer resources, that node will have higher resource consumption.

A lightweight blockchain uses a lightweight consensus algorithm, the so-called synergistic multiple proofs. However, the proposed blockchain structure is not scalable, even though it uses a blockchain filter. Since the IoT network is always large-scale and generates millions of data, using the conventional blockchain structure is not suitable. In the IoT environment, data redundancy is the principal problem that leads to the blockchain's unlimited growth. This work also stores the redundant data in the blockchain, increasing its size. Here, the consensus algorithm is executed by the IoT nodes, which are limited in resources. The IoT nodes do not have enough resources to validate every

transaction in the network, leading to high surcharging levels. An Efficient Lightweight Integrated Blockchain (ELIB) design has been proposed; the lightweight consensus algorithm works by limiting the number of blocks generated in the blockchain. However, defining the arbitrary nature of blocks is a heavy process that increases time consumption. This waiting time applies to all transactions in the network. In principle, the IoT network involves millions of transactions, which increases the overall time consumption. In the IoT network, data redundancy is a significant problem; with a massive amount of redundant data, the blockchain's size increases. Furthermore, all the IoT nodes also increase the space complexity as the blockchain copy has to be kept in each node. A fog-based blockchain and network architecture (BFAN) has been proposed. Although PoW consensus provides security to validate transactions through complex and heavy computation, the deployment of fog nodes does not resolve the issue as IoT nodes still execute the consensus algorithm, which is inefficient. IoT nodes are resource-constrained and do not have enough resources to run PoW in the network. The use of SHA-2 and ECDSA further increases the complexity, with even a lower level of security. Data encryption is enabled for all data, increasing the size and complexity of the network. These mentioned research problems are still not solved in the IoT Major Contributions

1.4 Major Contributions

The principal contribution of this work is the design of a new Multi-DAG technology for the IoT environment. The essential contributions are as follows:

- ***Lightweight Authentication:*** We introduce a lightweight authentication mechanism performed by the dynamic validation mechanism of PUF with the support of blockchain. In this process, a random identifier is dynamically generated and approved at any moment to guarantee its validity.
- ***Encrypted Data Validation:*** The encrypted data stored is validated in the blockchain by consensus. We propose a lightweight proof of authentication (PoAh) consensus mechanism. Additionally, we minimize the consensus complexity by selecting the optimal node through the Bi-Objective Spiral Optimization (BoSo) algorithm.
- ***Secure IoT Environment***: We propose a secure IoT environment based on the multi-zone DAG blockchain (Multizone-DAG-Blockchain) that reduces complexity and energy consumption. Three significant aspects are enhanced: lightweight authentication, lightweight data encryption, and lightweight consensus algorithm design.
- ***Scalable Blockchain Infrastructure***: All transactions are handled in a new Multi-Zone DAG Blockchain infrastructure (Multizone-DAG-Blockchain) that is lightweight and scalable. The bulk is further decreased by using the CubeHash hash algorithm and the Four-Q Curve-based signature algorithm in the blockchain.
- ***Data Redundancy and Sensitivity Analysis:*** For the incoming IoT data, the fog node performs a Jaccard similarity-based redundancy analysis and a neutral neural intelligent network (N2IN) sensitivity analysis. For all sensitive data, the fog node applies lightweight encryption based on the Four-Q Curve.

2. Related Works

Multi-level blockchain system (MBS) [23] for the IoT environment, the main advantages were the blockchain's speed and flexibility. For this purpose, the blockchain implementation is in multiple levels, the micro-level (IoT level), the gateway level blockchain (cluster heads of the IoT network), and the macro-level blockchain (platform level). The data generated by the IoT devices were collected and stored in the massively distributed ledger to improve the security level. The deployment is complex and is not suitable for the resource-constrained IoT environment.

Lightweight consensus algorithm, known as proof of block and transaction (PoBT) [24], The proposed consensus algorithm minimizes IoT nodes' time waste and memory. The PoBT consensus algorithm is integrated into the Hyper ledger fabric framework. However, the consensus algorithm is still executed by a random IoT node, which increases the complexity

Distributed blockchain is employed to authenticate IoT devices [25]. For this purpose, a cross-domain authentication scheme (xDBAuth) [26], aims to contribute as a trusted third-party signer. For validation, proof of authenticity and integrity (PoAI) enable access to IoT nodes. However, authentication by considering only the IoT identity is insecure and unreliable. Although PoAI is a lightweight consensus executed by resource-constrained devices, which increases the complexity. Though, a blockchain-based distributed security mechanism has been proposed. The security architecture was composed based on software-defined networking (SDN), blockchain, and fog computing. SDN is used to monitor network streams, while blockchain aims to strengthen network security. Besides, fog computing reduces the latency of the IoT network. The consensus algorithm is executed by the IoT nodes, which consume enormous resources.

Multiple wireless sensor networks compose an IoT environment. To avoid the single point of failure, this work [27] proposes a Blockchain-based identity authentication mechanism. The blockchain network provides different identities for these nodes and validates the authentication. This work uses PoW for validation, which is not practical for resource constrained IoT nodes.

This paper proposes a blockchain-based security scheme for secure data transmission [28]. This work mainly focuses on the blockchain's overhead reduction to make it suitable for the resource-constrained IoT environment. for this purpose, it uses a symmetric key encryption algorithm to validate and grant permission to IoT nodes; and a numeric signature in the ring structure. The conventional blockchain is computationally heavy and involves a large number of calculations

The proposed IoT network as shown in Fig. 1 is built in three tiers: the IoT perception tier, the blockchain and fog tier, and the cloud tier.

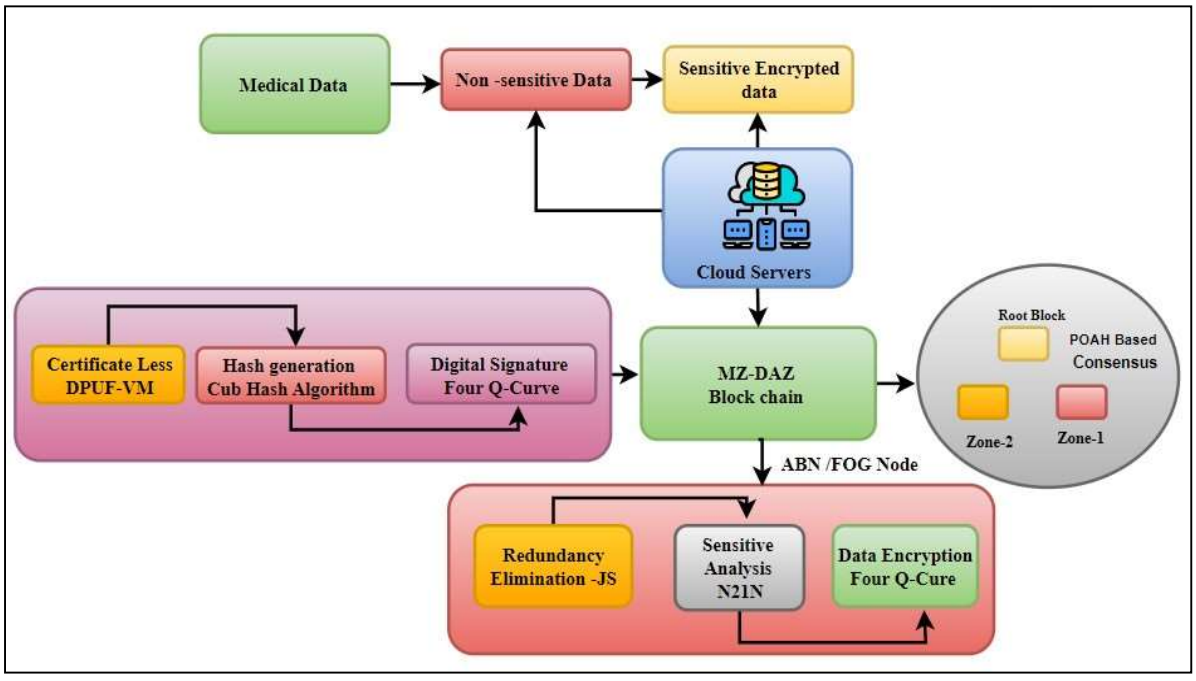

Figure 1: Proposed tri-level multizone-DAG-blockchain architecture

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

The first tier includes n a number of IoT sensors (S1,S2,S3…Sn)(S1,S2,S3…Sn). These sensors are supposed to perform specific tasks and do not contribute to blockchain validations, so-called passive block nodes (PBNs). The first layer includes a blockchain gateway (BGW) as well. The PBNs or IoT devices are responsible for creating data and initiating transactions. The second tier consists of a m number (F1, F2,F3…Fm) (F1,F2,F3…Fm). of fog nodes (FNs) known as active block nodes (ABNs). The ABNs or FNs are responsible for validating transactions in the blockchain. This system's main objective is to decrease the energy consumption and complexity of PBNs by transferring the validation process to ABNs as shown in Fig. 1.

The proposal provides efficiency through the following processes:

- Lightweight DPU-VM based authentication
- Lightweight data encryption
- Lightweight consensus algorithm

3.Proposed Methods

3 .1. Lightweight DPU-VM based authentication

IoT nodes and fog nodes are authenticated using a Dynamic Physically Unclonable Functions based Validation Mechanism (DPUF-VM) with the blockchain's assist. We proposed a dynamic approach in which a random identifier (RID) is dynamically generated for each IoT node. All IoT devices and fog nodes initially register their identity with the blockchain network, in which the identity is stored as a hash function. A novel idea of DPUF-VM is to change the RID dynamically based on the device ID and the previously detected value by the concerned sensor. The process of DPUF-VM is explained in the following steps:

Step-1: The first step is device registration. In this step, the devices register the identification information to the blockchain through BGW. For the sensor index i, the identification pieces of information are sensor ID SID (i) S$ID(i)$, MAC address SMAC(i)S$MAC(i)$, PUF(SC−R(i)) S$C{-}R(i)$), and the sensor's last detected value ρiρi. The random ID's generated as follow:

$$RiD(i) = SiD(i) \otimes \rho_i \tag{1}$$

This random ID's (RID)RID) changed at each time based on the current sensed value.

Step-2: The second step is device registration. The credentials are stored in the blockchain as hash values at this step. Furthermore, the Cube Hash algorithm is proposed for hash generation.

The output is given for an hs-bit string as follow:

$$H(x) = R_{Int\ rounds+}\frac{r}{bs} + R_{finround} - hs(x) \tag{2}$$

Our hashed properties can be R_{ID}, S_{ID},S_{MAC} or S_{C-R}

Step-3: The third step is device authentication. The Si triggers authentication with the sending of an authentication request to the BGW. Then the BGW requests a random certificate with a digital signature. The RCERRCER is generated based on the RIDRID and SMACSMAC as follows,

$$RCER = H\big(RiD(i) = SiD(i)\big) \otimes SMAC \tag{3}$$

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

Likewise, the digital signature generation for PUF is given as follows,

$$DS = Sign\ (S_{C-R}) \quad (4)$$

For PUF Signing purpose, we based on Four Q-Curve signing algorithm, designated as follow,

$$\in \left(f_p^2\right): x^2 + y^2 = 1 + gx^2y^2 \quad (5)$$

where p is a prime number, and is a non-square in f_p^2. This curve, dubbed "Four Q". p is defined to generate digital signature. First, the hash is generated for PUF by using Cube Hash algorithm. In the order of l, the random selected i is from [1, l−1], the curve point computed as follow,

$$\left(x_1, y_1\right) = lxG \quad (6)$$

where G is the generator known in advance, to calculate the r from the curve point, the computation is as follow,

$$r = x_{1,}\ modl \quad (7)$$

$$S = l^1(z + rSK)modl \quad (8)$$

The pair (r, s) is the digital signature, while SK is the private key of the concerned device responsible for submitting the authentication credentials as $RCER = Sign\ (R_{C-R})$

Step-4: The fourth step is device validation. Upon reception of the authentication information, BGW validates it through a signature verification procedure.

If the credentials are identical to those in the blockchain, the device is authenticated. Otherwise, the request is denied. The DPUF- VM process is described in Fig. 2.

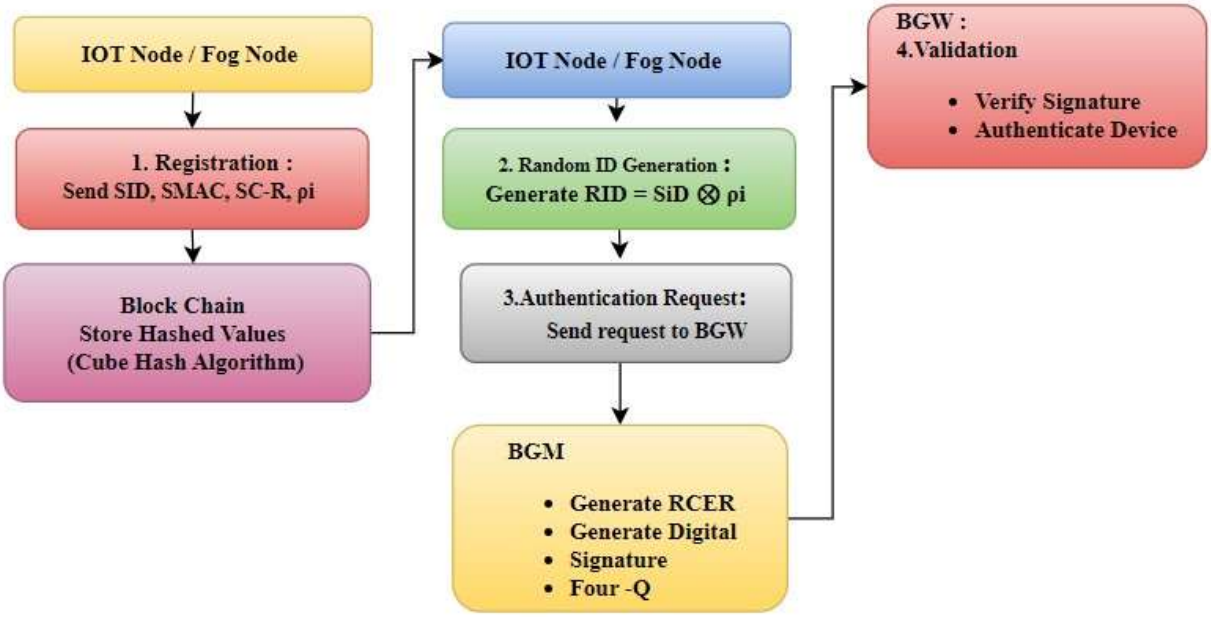

Figure 2: Proposed DPUF-VM authentication

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

In the same way as IoT nodes, fog nodes are likewise authenticated by BGW in order to guarantee a high level of security.

Cube Hash Generation Algorithm

```
def rotate_left(x, n):
    return ((x << n) & 0xf0xffffffff) | (x >> (32 - n))
def permutation step(state):
    for i in range (128):
        state[i] = rotate left(state[i], (i % 32) + 1)
    for i in range (64):
        temp = state[i]
        state[i] = state [64 + i]
        state [64 + i] = temp
    for i in range (128):
        state[i] = (state[i] + state [(i + 1) % 128]) & 0xffffffff
def cube hash (input data, output size=32):
    state = [i for i in range (128)]
        # Process each 128-byte block of input data
    for i in range (0, len (input data), 128):
        block = input data [i:i + 128]
        if len(block) < 128:
            block += bytes ([1]) + bytes ([0] * (127 - len(block)))
        for j in range (128):
            state[j] ^= block[j]
        permutation step(state)
       # Finalization
    for _ in range (10):  # Example number of final permutation steps
        permutation step(state)
        # Output extraction
    output = b''
    for i in range (output size):
        output += state[i].to bytes (1, 'little')
    return output
```

3.2 Lightweight Data Encryption

After successfully authenticating the IoT, the data is transmitted from the IoT nodes to the fog nodes. The fog nodes apply a lightweight encryption mechanism depending on the sensitivity level of the received data. The fog nodes perform two primary operations, initially eliminating redundancy and then encrypting the data. The fog node performs redundancy elimination by JS calculation for the received data (SD1, SD2,…, SDu). The calculation is performed as follows,

$$JS(SD_{u,}SD_v) = \frac{|SD_u \sqcap SD_v|}{|SD_u \sqcap SD_v|} \quad (9)$$

If the output of the algorithm JS between two data is small, then the input is redundant, and one of the inputs is removed from the data set. The leading factor in the growing size of the blockchain is the storage of redundant values in the blockchain. For this purpose, the fog node starts by eliminating

all redundant data from the collected data. Also, the data encryption increases the input size, which leads to an increase in the size of the blockchain. To deal with this issue, we would only apply encryption to sensitive data. For sensitivity analysis, the fog node uses the N2IN algorithm. The N2IN algorithm is associated with an artificial neural network (ANN) and a Neutrosophic Intelligence algorithm. The sensitivity is determined based on the detected reading ρ, the sensor type (STST), and the sensor location (SLSL) for the received data. The neutrosophic set is like a fuzzy set, however it performs better than fuzzy sets [15] the collected data initialized in the input layer of N2IN. In the hidden layers, the weight value of each data is calculated by the neutrosophic intelligence. This weight value calculation is performed on the hidden layers, and the weight value of each data is adjusted. Based on the above approach, the N2IN performs a sensitivity analysis. All sensitive data is encrypted using the Four-Q-curve. For all sensitives SDiSDi, the fog node applies encryption. Then, the encrypted data (Encrypted[SDiSDi]) is stored as a new transaction in the blockchain.

The Algorithm Logic of NZIN

If ρ is abnormal & S_T is sensitive && S_T sensitive
Then SD is sensitive
Apply Encryption
Send SDi-Encrypted to the Cloud level
Else,
SDi is non –Sensitive
Send SDi to the Cloud level
End If

3.3 Efficient Lightweight Consensus Algorithm

The consensus algorithm is the primary method used to validate each and every blockchain transaction. There is a need to modify the current consensus algorithm due to its high processing cost and complexity. Similarly, there are numerous scalability and complexity issues with the blockchain's current traditional linear layout. Consequently, we suggest a brand-new multizone-DAG-blockchain architecture. The IoT perception layer in the suggested architecture is divided into several zones, each of which has its own zone for managing transactions. Fig. 3 displays the Multizone-DAG-Blockchain model.

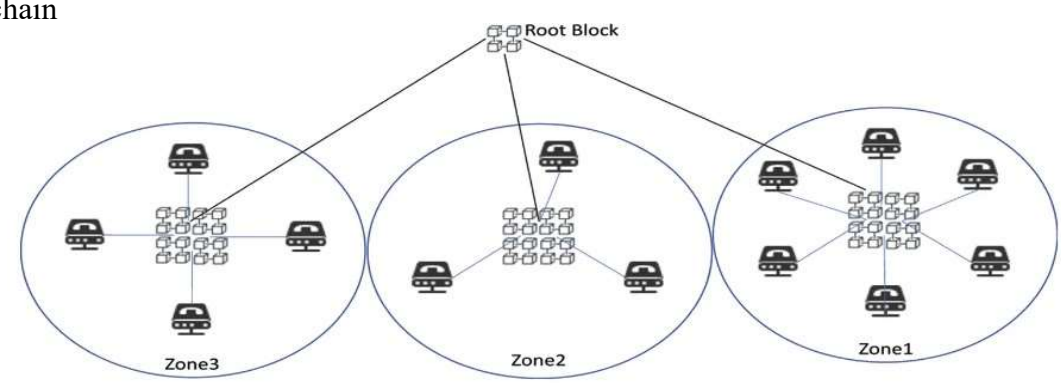

Figure 3: Multizone DAG blockchain design

In a fundamental sense, the DAG blockchain promotes scalability and minimizes complexity compared to the regular blockchain. As each transaction is added in the form of new blocks in the

regular blockchain, the blockchain grows exponentially. This phenomenon is addressed in the DAG-based blockchain, in which the graph GG is composed over transactions. In the proposed Multizone-DAG-Blockchain model, a number vv of directed acyclic graphs (DAGs) are constructed as $G1,G2,\ldots,GvG1,G2,\ldots,Gv$ for vv number of zones. That is, we obtain multiple DAGs with corresponding transactions for multiple zones. The ii-th graph is defined as $G=\{Sj,E,W\}G=\{Sj,E,W\}$ with $Sj\in ZiSj\in Zi$. $SjSj$ is the set of IoT sensors located in zone ii ($ZiZi$), EE is the set of edges between $SjSj$, and WW is the weight function presented as $E\subseteq(Sj\times Sj)E\subseteq(Sj\times Sj)$ and $W\subseteq(Sj\times Sj)\rightarrow RW\subseteq(Sj\times Sj)\rightarrow$R. The GG is entirely directed so that there are no cycles in the graph. In the Multizone-DAG-Blockchain, the transactions are the vertices (VV), and the blocks contain all transactions. The root block of the Multizone-DAG-Blockchain is the genesis block, and the $GjGj$ is a finite graph of $\{V,E\}\{V,E\}$. The arrival of each transaction at each time tt follows a Poisson distribution with an arrival rate of $\lambda\lambda$. This property is applicable for each DAG in the Multizone-DAG-Blockchain. With the increase in tt, the GG grows exponentially but still at a lower rate than the linear blockchain. The main differences between conventional blockchain and the proposed Multizone-DAG-Blockchain are given in Table 1.

Table 1. proposed Multizone-DAG-Blockchain compassion analysis

Parameter	Conventional Blockchain	Multizone-DAG-Blockchain
Scalability	Limited	High
Complexity	High	Lower
Growth Rate	Exponential	Sub-exponential
Transaction Addition	Added as new blocks	Added as vertices in multiple DAGs
Graph Structure	Linear chain	Directed Acyclic Graph (DAG)
Genesis Block	Single genesis block	Single genesis block per DAG
Transaction Handling	All nodes validate	Specific zones handle transactions
Consensus Mechanism	PoW (Proof of Work)	PoAh (Proof of Authentication)
Consensus Complexity	High	Lower (using BoSo algorithm)
Node Selection	Random/Election based	Optimal node selection (BoSo algorithm)
Redundancy Handling	No specific mechanism	Jaccard similarity-based analysis
Sensitivity Analysis	Not specified	Neutral Neural Intelligent Network (N2IN)
Encryption	SHA-2, ECDSA	CubeHash, Four-Q Curve
Energy Consumption	High	Lower
Data Storage	All data stored in chain	Redundant data minimized
Network Suitability	Not optimized for IoT	Optimized for IoT environment

This table provides a concise comparison of the key parameters and benefits of the proposed Multizone-DAG-Blockchain against the conventional blockchain approach. In our proposed design, a proposed PoAh consensus algorithm is applied to validate the transactions. The IoT nodes create the data in the form of transactions as T1,T2,T3…Tn$T1,T2,T3\ldots Tn$ in a period. These transactions are bundled into a block, and respectively block is updated with each new transaction. Before this happens, the consensus node validates the transaction to update the block. Here, the trusted nodes are considered the consensus nodes. As explained earlier, we apply the Four-Q-Curve algorithm to

perform the cryptographic functions. First, the IoT generates data and signs it before spreading it on the network. Then, a node is selected from the trusted network to be part of the PoAh. If the node's trust value is greater than the threshold value, the block is assigned as part of the chain after authenticating the block.

Algorithm POAH Based Validation with DPUF-VM Auth

Init Block (T_1,T_2…T_n) Blocks
Auth [DPUF-VM]
If Auth== True && Verify Sign (Block)==True
Block|| POAh Broadcast
Hash (Block) - Add to blocks
End If
End

PoAh is performed entirely by the consortium node selected from the ABNs. This PoAh implementation is energy-consuming due to a large number of calculations. Thus, the IoT nodes are unable to perform PoAh. We perform a process of selecting the optimal consensus node (OCN) For this purpose, we propose the BoSo algorithm. In the BoSo algorithm, two objective functions are designed to select the OCN among the ABNs. The spiral optimization algorithm is a heuristic algorithm that solves complex problems. The spiral optimization algorithm determines the optimal solution by searching for the solution over multiple spiral models, which overcomes the optimum local problem.

In the end, all the other search points update the position to the optimal position. Thus, the optimal ABN is selected as OCN, which ensures the consensus algorithm. Since the ABNs execute the consensus algorithm, the load and complexity on the IoT nodes are significantly reduced.

The generic processing flow of the proposed approach as illustrated in Fig. 4. The proposed work achieves scalability and efficiency through lightweight authentication, lightweight encryption, and lightweight consensus algorithm in its design.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

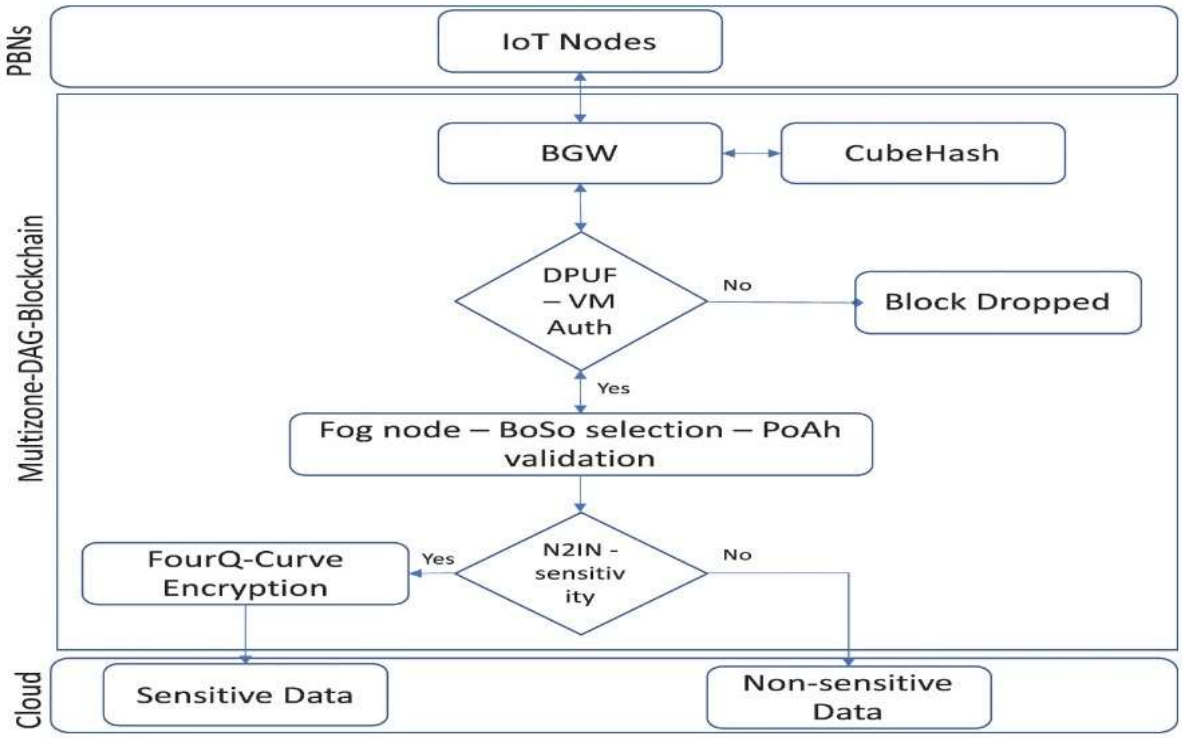

Figure 4: Multizone-DAG-blockchain flow design

4. Performance Evaluation

Through the use of a comparison analysis, the purpose of this part is to analyse the performance of the Multizone DAG Blockchain that has been proposed. Our examination of the outcomes is taking place in a setting that is as similar to the real world as is conceivable. We are going to focus on the most important aspects of benchmarking in the Internet of Things environment, including energy usage, response time, and any other relevant factors.

4.1 Simulation Environment

The Multizone DAG Blockchain that we have presented was simulated using Network Simulator NS three. In particular, it offers appropriate support for the protocols and activities of the Internet of Things. According to the Internet of Things (IoT) that we require in our everyday lives, the field of application for our suggested system is large. As shown in Table 5, we differentiate between applications that are industrial, smart cities, smart homes, transportation, and a great number of other applications. For each of these applications, the Internet of Things primarily consists of environmental sensors. The next step in our simulation study will involve taking into consideration, as an illustration, sensors that are utilized in our everyday lives. As a result, we are able to observe that every sensor is able to detect sensitive data that is associated with a particular private area. The motion detector is regarded as a sensitive technology due to the fact that it is typically utilized as a virtual guardian that monitors the entire area during its operation. When it comes to the classification of sensors, the geographical context is taken into consideration. The temperature sensor that is installed adjacent to the kitchen is therefore more sensitive than the other devices that are available. At each and every data transmission, each of these Internet of Things nodes is validated. Data

encryption is performed in this manner to any and all sensitive data that is discovered by the Internet of Things nodes. The blockchain is responsible for validating the transactions, which results in an environment that is more safe and confidential.

4.2 Analysis of Power Consumption

The amount of energy that is consumed by Internet of Things nodes while they are transmitting data is referred to as energy consumption. As a result of detecting, transferring, and receiving data, the energy that is consumed by the Internet of Things nodes. Both the number of nodes and the number of transactions were taken into consideration when doing our analysis of the energy consumption. An examination of the comparison of energy consumption is presented in Figure 5, with the goal of increasing the value of n. Given that the suggested task has a suitable energy consumption ranging from 100 to 120 watts, we have seen that the n value does not have any effect on the job proposition. On the other hand, the ELIB mode brings about a rise in the amount of energy that is consumed whenever the value of n is raised. The work that is being presented is, in fact, scalable because the amount of energy that is consumed does not change even if the number of nodes is increased. On the other hand, when there are a large number of nodes, the job that is now being done is unable to function well. The computations are offloaded to the fog nodes in our proposal, and the ELIB model executes all of the calculations on the IoT nodes. This allows for a reduction in the amount of energy that is consumed without sacrificing efficiency. However, the computations are carried out in the IoT nodes, despite the fact that fog nodes are utilized in BFAN. An examination of the relationship between the number of transactions and the amount of energy consumed is presented in Figure 6. Due to the fact that each transaction requires the construction and validation of a block, the difficulty of the process of reaching consensus is increased when the number of transactions increases.

Table 2: Energy Consumption vs. Number of Nodes

Number of Nodes (n)	Energy Consumption (Proposed MG-DAG) [W]	Energy Consumption (BFAN) [W]	Energy Consumption (ELIB) [W]
10	105	110	115
20	107	130	140
30	110	150	165
40	113	170	190
50	115	190	215
60	118	210	240
70	120	230	265
80	122	250	290
90	123	270	315
100	125	290	340

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

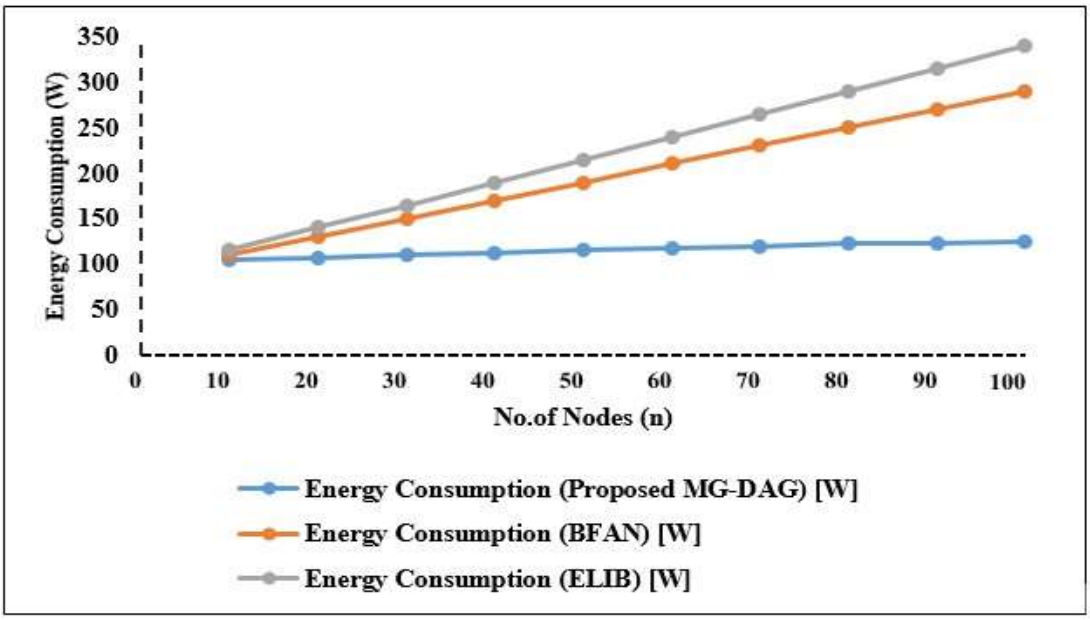

Figure 5 (a). Performance Analysis of Energy Consumption and Number of Nodes

Table 3: Energy Consumption vs. Number of Transactions

Number of Transactions (t)	Energy Consumption (Proposed MG-DAG) [W]	Energy Consumption (BFAN) [W]	Energy Consumption (ELIB) [W]
100	100	110	120
200	105	130	140
300	110	15	160
400	115	170	180
500	120	190	200
600	125	210	220
700	130	230	240
800	135	250	260
900	140	270	280
1000	145	290	300

The energy efficiency of the suggested system in relation to the current ELIB model will be amply illustrated by these tables and graphs. The transaction cost, then, is the measure of energy use. As such, the ELIB model uses between 650 and 1200 watts of electricity. One hundred transactions of the BFAN type use one hundred thirty watts of electricity. The proposed work uses 140 watts of electricity for precisely the same amount of transactions. The consensus procedure in the proposed work is carried out by an optimal ABN (fog node) chosen by the BoSo algorithm, which is the main cause of this significant increase. Furthermore, employed is a lightweight PoAh that outperforms PoW. Thus, the proposed work reduces the power consumption up to 1000 watts.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

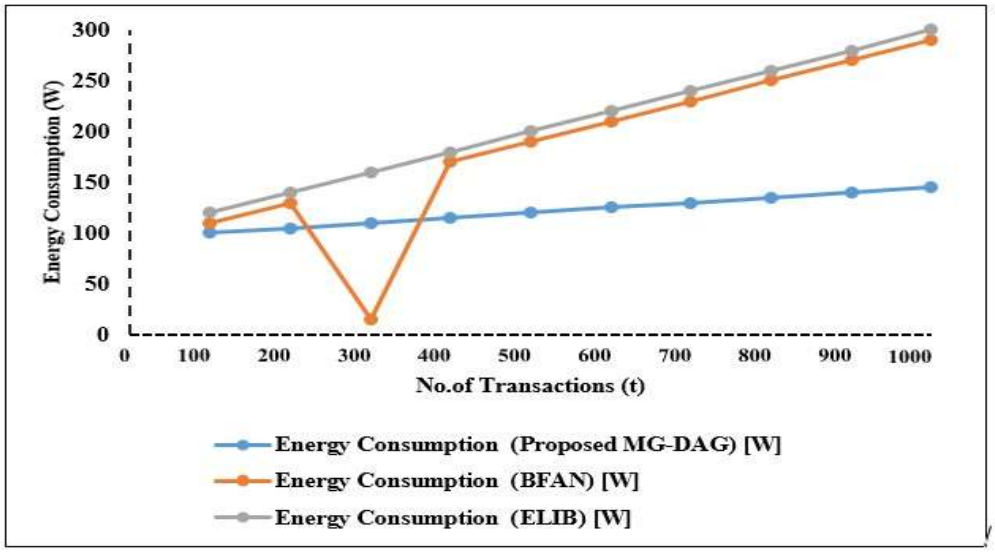

Figure 5(b). Performance Analysis of Energy Consumption - Number of Transactions

5.3. Analysing Storage Efficiency

The amount of storage needed for the Internet of Things data produced by the IoT nodes dictates storage costs. We compare this measure with the quantity of transactions and nodes. Figure 6 (a) and (b) shows the analysis of storage cost in relation to the quantity of Internet of Things nodes. The storage cost increases as the number of nodes does. It is shown by this analysis that block size and storage cost rise with node count. The storage efficiency is increased four times over the current BFAN & ELIB works by the proposed (MZ-DAG) effort. The primary disadvantage is that these works make the blockchain larger, which raises the cost of storage. The linear blockchain paradigm thus raises storage costs as well, which is inappropriate for the resource-constrained IoT setting.

Table 4: Storage Cost vs. Number of Nodes

Number of Nodes (n)	Storage Cost (Proposed MZ-DAG) [MB]	Storage Cost (BFAN) [MB]	Storage Cost (ELIB) [MB]
10	40	160	160
20	80	310	320
30	120	450	480
40	160	600	640
50	200	750	800
60	240	900	960
70	280	1100	1120
80	320	1200	1280
90	360	1410	1440
100	400	1500	1600

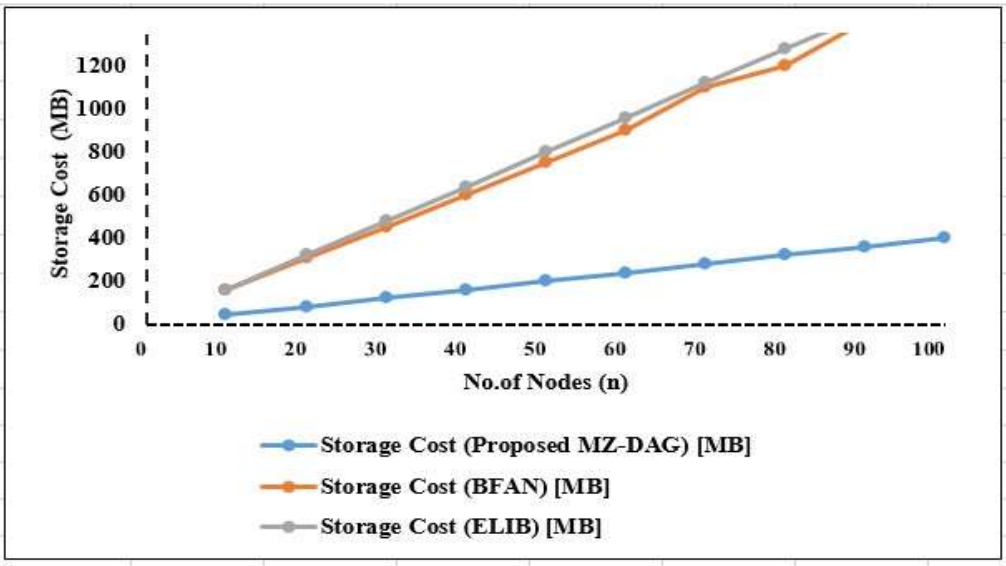

Figure 6(a). Performance Analysis of Storage Cost and Number of Nodes

Table 5. Storage Cost vs. Number of Transactions

Number of Transactions (t)	Storage Cost (Proposed MZ-DAG) [MB]	Storage Cost (BFAN) [MB]	Storage Cost (ELIB) [MB]
100	4	14	16
200	8	30	32
300	12	45	48
400	16	60	64
500	20	75	80
600	24	90	96
700	28	110	112
800	32	122	128
900	36	130	144
1000	40	150	160

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

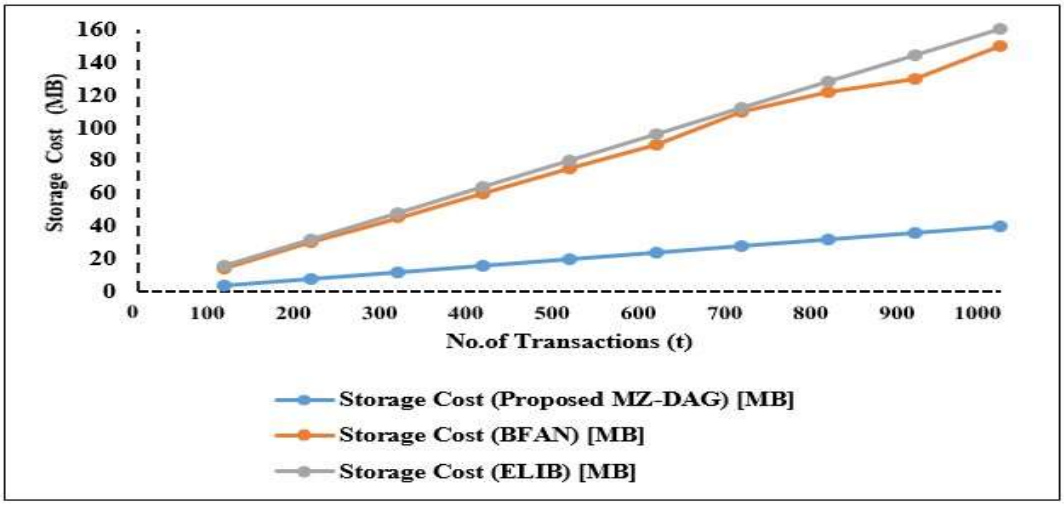

Figure 6(b): Performance Analysis of Storage Cost and Number of Transactions

Figure 6(b) analyses the storage cost according to the quantity of transactions. The storage cost is just 30 MB even for 100 transactions. Still, the BFAN model costs 135 MB for storage for 100 transactions, compared to the ELIB model's 124 MB. The blockchain gets bigger and longer linearly as the number of transactions does. A higher cost of storage follows from this rise. Data from Internet of Things devices is gathered and kept in cloud servers in ELIB and BFAN modes without any redundancy control. Repetitive data results in more expensive storage. But the suggested technique removes superfluous data via JS analysis of the data gathered from IoT nodes. Moreover, we just encrypt data that the N2IN algorithm identifies as sensitive. Overall, by incorporating fog computing with the Multizone-DAG-Blockchain framework, the suggested work reduces the storage cost.

5.2.3. *Analyzing Response Times*

Response time is the duration that requests are handled by the system. It is decided in this instance by how long it takes the blockchain to verify the transaction and produce the block with fresh input data. Figure 8 shows the reaction time with respect to the quantity of transactions. The study shows that the response time of the suggested Multizone-DAG-Blockchain is slower than that of the BFAN approach and the ELIB model. Figure 8. It is demonstrated that the reaction time in both current works increases exponentially with the amount of transactions since, with a large number of transactions, the blockchain becomes enormous and stops responding to new ones. Multizone-DAG-Blockchain responds in 12 ms even for about 100 transactions, whereas the ELIB models take 45 ms and the BFAN takes 75 ms. New transactions are not validated and added as new blocks because to this prolonged reaction time. In this situation, the Internet of Things environment offers a tremendous volume of data every millisecond that is inconclusive with the two previous works.

Table 6. Response Time vs. Number of Transactions

Number of Transactions (t)	Response Time (Proposed MZ-DAG) [ms]	Response Time (BFAN) [ms]	Response Time (ELIB) [ms]
100	12	75	45
200	14	90	60
300	18	105	75
400	25	120	90

500	30	135	105
600	40	150	120
700	55	165	135
800	70	180	150
900	90	195	165
1000	120	210	180

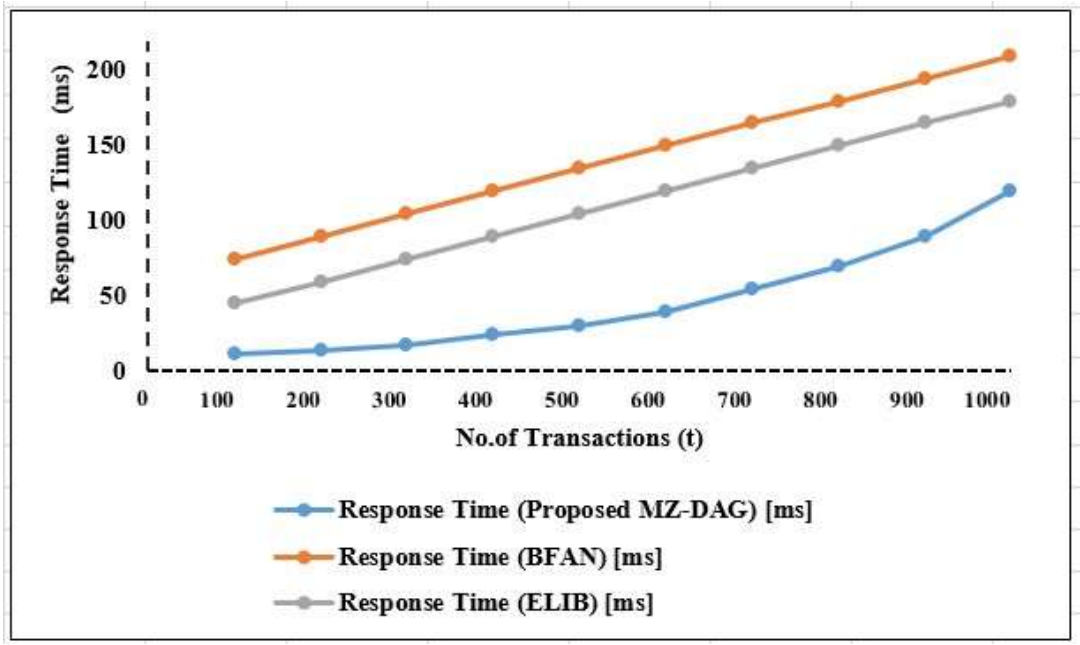

Figure 8. Performance Analysis of Response Time and Number of Transactions

5.2.4 Analysis of the Throughput

The amount of transactions processed and kept in the blockchain during the designated time frame is the system's throughput. Figure 9. uses transaction analysis to assess throughput. The throughput rises concurrently with the amount of transactions. Particularly, the 135 kbps throughput of the suggested Multi-Zones-DAG-Blockchain with 100 transactions. Compared to the BFAN technique and the ELIB model, this is rather higher. 95 kbps is the throughput of the ELIB model and 85 kbps for 100 transactions of BFAN. The blockchain structure is enlarged linearly for new transactions in both of the current works. Conversely, the proposed effort disperses the blockchain structure. As so, the suggested approach outperforms the current ELIB model and BFAN approach in terms of throughput.

Table 7. Throughput vs. Number of Transactions

Number of Transactions (t)	Throughput (Proposed MZ-DAG) [kbps]	Throughput (BFAN) [kbps]	Throughput (ELIB) [kbps]
100	135	85	95
200	270	170	190
300	405	255	285
400	540	340	380
500	675	425	475
600	810	510	570

700	945	595	665
800	1080	680	760
900	1215	765	855
1000	1350	850	950

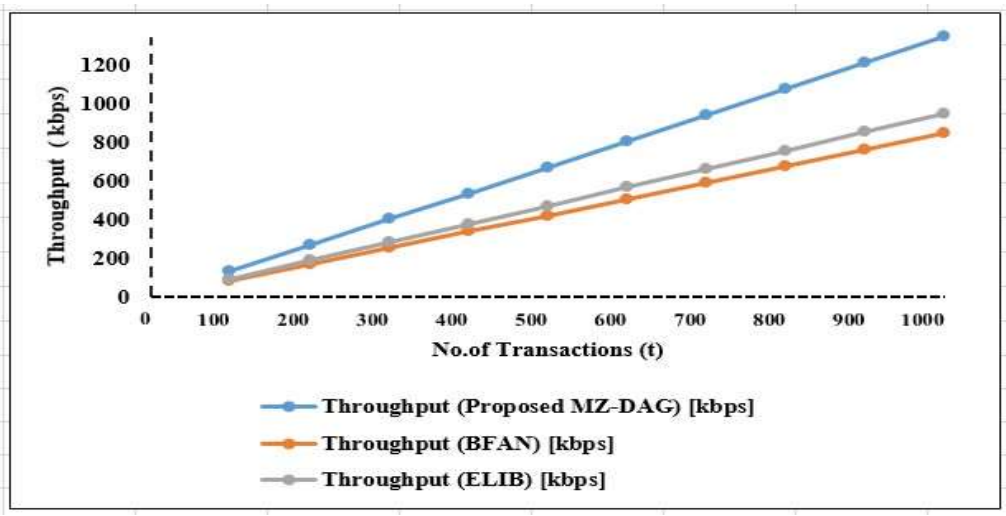

Figure 9. Performance Analysis of Throughput and Number of Transactions

6.Conclusion

In this work, we propose a new framework, Multizone DAG blockchain, adapted to the resource constraints of the IoT environment. The proposed scheme ensures high-level medical data security through lightweight computation. Initially, a lightweight authentication mechanism (DPUF-VM) is proposed to authenticate the legitimacy of every IoT node and fog node. The collected information from fog nodes is further analyzed for redundancy and sensitivity. For redundant data removal, the JS measure is presented, and the N2IN algorithm for sensitivity analysis is also proposed. Each transaction is validated in the Multizone-DAG-Blockchain using the PoAh lightweight consensus algorithm. In Multizone-DAG-Blockchain, the CubeHash lightweight hash algorithm is used, and the Four-Q-Curve algorithm performs the digital signature. The optimal fog node is selected by the BoSo algorithm and respected as the consensus node. The extensive evaluation in ns-3.26 shows promising results in energy consumption, storage cost, response time, and throughput. In the future, we plan to extend Multizone-DAG-Blockchain for real-world use with a lightweight intrusion detection system (IDS) to analyze security threats in detail.

Reference

[1] El Majdoubi, Driss, Hanan El Bakkali, and Souad Sadki. "SmartMedChain: a blockchain-based privacy-preserving smart healthcare framework." *Journal of Healthcare Engineering* 2021 (2021).

[2] El Majdoubi, Driss, Hanan El Bakkali, and Souad Sadki. "SmartMedChain: a blockchain-based privacy-preserving smart healthcare framework." *Journal of Healthcare Engineering* 2021 (2021).

[3] Miyachi, Ken, and Tim K. Mackey. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." *Information processing & management* 58, no. 3 (2021): 102535.

[4] Makhdoom, Imran, Ian Zhou, Mehran Abolhasan, Justin Lipman, and Wei Ni. "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." *Computers & Security* 88 (2020): 101653.

[5] Alzubi, Omar A., Jafar A. Alzubi, K. Shankar, and Deepak Gupta. "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things." *Transactions on Emerging Telecommunications Technologies* 32, no. 12 (2021): e4360.
[6] Stamatellis, Charalampos, Pavlos Papadopoulos, Nikolaos Pitropakis, Sokratis Katsikas, and William J. Buchanan. "A privacy-preserving healthcare framework using hyper ledger fabric." *Sensors* 20, no. 22 (2020): 6587.
[7] Fu, Junsong, Na Wang, and Yuanyuan Cai. "Privacy-preserving in healthcare blockchain systems based on lightweight message sharing." *Sensors* 20, no. 7 (2020): 1898.
[8] Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management." *IEEE Transactions on Computational Social Systems* (2022).
[9] Elhoseny, Mohamed, Khalid Haseeb, Asghar Ali Shah, Irshad Ahmad, Zahoor Jan, and Mohammed I. Alghamdi. "IoT solution for AI-enabled PRIVACY-Preserving with big data transferring: an application for healthcare using blockchain." *Energies* 14, no. 17 (2021): 5364.
[10] Pal, Kamalendu. "A Decentralized Privacy Preserving Healthcare Blockchain for IoT, Challenges, and Solutions." In *Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare*, pp. 158-188. IGI Global, 2022.
[11] Lakhan, Abdullah, Mazin Abed Mohammed, Jan Nedoma, Radek Martinek, Prayag Tiwari, Ankit Vidyarthi, Ahmed Alkhayyat, and Weiyu Wang. "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare." *IEEE Journal of Biomedical and Health Informatics* (2022).
[12] Alzubi, Omar A., Jafar A. Alzubi, K. Shankar, and Deepak Gupta. "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things." *Transactions on Emerging Telecommunications Technologies* 32, no. 12 (2021): e4360.
[13] Sharma, Pratima, Suyel Namasudra, Naveen Chilamkurti, Byung-Gyu Kim, and Ruben Gonzalez Crespo. "Blockchain-based privacy preservation for IoT-enabled healthcare system." *ACM Transactions on Sensor Networks* 19, no. 3 (2023): 1-17.
[14] Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "Access control and privacy-preserving blockchain-based system for diseases management." *IEEE Transactions on Computational Social Systems* (2022).
[15] Luong, Duc Anh, and Jong Hwan Park. "Privacy-preserving blockchain-based healthcare system for IoT devices using zk-SNARK." *IEEE Access* 10 (2022): 55739-55752.
[16] Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions." *Future Generation Computer Systems* 97 (2019): 512-529.
[17] Kumar, Prabhat, Randhir Kumar, Gautam Srivastava, Govind P. Gupta, Rakesh Tripathi, Thippa Reddy Gadekallu, and Neal N. Xiong. "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities." *IEEE Transactions on Network Science and Engineering* 8, no. 3 (2021): 2326-2341.
[18] Tran, Quang Nhat, Benjamin P. Turnbull, Hao-Tian Wu, A. J. S. De Silva, Katerina Kormusheva, and Jiankun Hu. "A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture." *IEEE Open Journal of the Computer Society* 2 (2021): 72-84.
[19] Sharma, Prakash Chandra, Md Rashid Mahmood, Hiral Raja, Narendra Singh Yadav, Brij B. Gupta, and Varsha Arya. "Secure authentication and privacy-preserving blockchain for industrial internet of things." *Computers and Electrical Engineering* 108 (2023): 108703.

[20] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq et al., "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Cluster Computing, vol. 23, no. 3, pp. 2067–2087, 2020.
[21] H. A. Khattak, M. A. Shah, S. Khan, I. Ali and M. Imran, "Perception layer security in Internet of Things," Future Generation Computer Systems, vol. 100, pp. 144–164, 2019.
[22] . Z. Li, Z. Yang, P. Szalachowski and J. Zhou, "Building low-interactivity multifactor authenticated key exchange for industrial Internet of Things," IEEE Internet Things Journal, vol. 8, no. 2, pp. 844–859, 2021.
[23] B. Mbarek, N. Jabeur, T. Pitner and A. U. H. Yasar, "MBS: Multilevel blockchain system for IoT," Personal and Ubiquitous Computing, vol. 25, pp. 247–254, 2019.
[24] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty et al., "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," IEEE Internet Things Journal, vol. 7, no. 3, pp. 2343–2355, 2020.
[25] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," Sensors (Switzerland), vol. 19, no. 2, pp. 1–17, 2019.
[26] A. Gauhar, A. Naveed, C. Yue, K. Shahzad, H. Cruickshank et al., "XDBAuth: Blockchain based cross domain authentication and authorization framework for internet of things," IEEE Access, vol. 8, pp. 58800–58816, 2020.
[27] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao et al., "A hybrid Block Chain-based identity authentication scheme for multi-WSN," IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241–251, 2020.
[28] S. Kudva, S. Badsha, S. Sengupta, I. Khalil and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," Information Sciences, vol. 545, no. August, pp. 170–187, 2021.
[29] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," Journal of Parallel and Distributed Computing, vol. 134, pp. 180–197, 2019.
[30] S. Mohanty, K. Ramya, S. Rani, D. Gupta, K. Shankar et al., "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," Future Generation Computer Systems, vol. 102, pp. 1027–1037, 2020.
[31] K. Tamura and K. Yasuda, "The spiral optimization algorithm: Convergence conditions and settings," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 360–375, 2020.