Computers, Materials & Continua
DOI:10.32604/cmc.2022.020833
Article

Tech Science Press

Lightweight Direct Acyclic Graph Blockchain for Enhancing Resource-Constrained IoT Environment

Salaheddine Kably[1,2,*], Mounir Arioua[1] and Nabih Alaoui[2]

[1]Laboratory of Information and Communication Technologies, National School of Applied Abdelmalek Saadi University, Tanger, Morocco
[2]Ecole Supérieure d'informatique et du Numérique, TICLab Université Internationale de Rabat Sala, El Jadida, Morocco
*Corresponding Author: Salaheddine Kably. Email: salaheddine.kably@gmail.com
Received: 10 June 2021; Accepted: 08 November 2021

Abstract: Blockchain technology is regarded as the emergent security solution for many applications related to the Internet of Things (*IoT*). In concept, blockchain has a linear structure that grows with the number of transactions entered. This growth in size is the main obstacle to the blockchain, which makes it unsuitable for resource-constrained IoT environments. Moreover, conventional consensus algorithms such as PoW, PoS are very computationally heavy. This paper solves these problems by introducing a new lightweight blockchain structure and lightweight consensus algorithm. The Multi-Zone Direct Acyclic Graph (DAG) Blockchain (*Multizone-DAG-Blockchain*) framework is proposed for the fog-based IoT environment. In this context, fog computing technology is integrated with the IoT to offload IoT tasks to the fog nodes, thus preserving the energy consumption of the IoT devices. Both IoT and fog nodes are initially authenticated using a non-cloneable physical function- based validation mechanism (*DPUF-VM*) in which multiple authentication certificates are verified in the blockchain. Each transaction is stored in a hash function in the blockchain using the lightweight CubeHash algorithm and signed by the Four-Q- Curve algorithm. In the cloud, sensitive data is stored as ciphertext. Fog nodes provide data security to avoid the energy consumption and complexity of IoT nodes. The fog node first performs a redundancy analysis using the Jaccard Similarity (JS) measure and sensitivity analysis using the Neutrosophic Neural Intelligent Network (*N2IN*) algorithm. A lightweight proof-of-authentication (*PoAh*) algorithm is presented and executed by the optimal consensus node selected by the bi- objective spiral optimization (*BoSo*) algorithm for transaction validation. The proposed work is modeled in Network Simulator 3.26 (ns-3.26), and the performance is evaluated in terms of energy consumption, storage cost, response time, and throughput.

Keywords: Multi zone DAG blockchain; dynamic PUF; lightweight PoAh consensus; BoSo node selection; four-q-curve encryption; IoT environment

1 Introduction

The Internet of Things (IoT) is an emerging technology with wide-ranging applications [1], including the Smart City [2], Smart healthcare [3], and more. However, security is a significant issue in the IoT environment. In IoT, a large amount of heterogeneous data is generated every second and stored in a remote server for other purposes [4,5]. As the data is accessed remotely, security is the critical challenge. Security is by cryptographic functions, multi-factor authentication, key distribution, and moreover [6,7]. Recently, blockchain technology is the optimal solution to IoT security challenges [8]. The blockchain is the distributed ledger that validates every transaction performed by IoT nodes in a decentralized and secure manner. The validation uses a consensus algorithm. This decentralized nature of the blockchain plays a vital role in ensuring high-level security [9]. Although blockchain proves its effectiveness in security, it still has some computational complexity challenges [10]. The main challenges in using blockchain for IoT are the complexity of the traditional consensus algorithms. Firstly, the nodes running the consensus algorithm have higher resource consumption. Secondly, the involvement of redundant data in the IoT network increases the size of the blockchain exponentially. Finally, the conventional linear structure of the blockchain is not suitable for the IoT environment is not scalable [11].

In order to address these challenges, lightweight blockchain structures are being studied in recent times [8]. Although the blockchain infrastructure reduces complexity, the consensus algorithm used in the blockchain is also crucial in deciding the complexity of the blockchain technology [12]. The conventional proof-of-work (PoW) consensus algorithm consumes more complexity than others [13]. Moreover, the consensus algorithm running by the consensus node, which is also an IoT node. Since IoT nodes are resource-constrained, they do not have enough resources to execute the complex consensus algorithms. Therefore, the consensus algorithm and the selection of the consensus node also play a critical role.

On the other hand, fog computing is an emerging technology that brings network services closer to the edge [14]. It provides better resources to resource-constrained IoT nodes and also minimizes the response time for requested services. IoT-Fog integration brings efficiency to the IoT environment in scalability, energy efficiency, and response time [15]. Besides, authentication of IoT nodes [16] ensures that data is not accessible to any unauthorized nodes [17]. In general, identification, password, MAC address, and IP address are mainly used to validate IoT nodes [18]. However, these credentials can be easily hacked by attackers. On the other hand, the physically tilting function 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 [5]. Due to this complexity, these algorithms are not suitable for the IoT environment because devices have limited resources. Due to this nature, highly complex algorithms are not suitable for the IoT environment. Therefore, lightweight encryption algorithms become an essential solution for securing the IoT [21]. However, the following research questions are still unsolved in IoT and need to be addressed: How to authenticate IoT nodes with lightweight and dynamic credentials? How to secure transactions performed by IoT nodes with cryptographic functions? How to 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 of 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.

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 CubeHash 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.

2 Related Works

Multi-level blockchain system (MBS) [22] 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) [23], The proposed consensus algorithm minimizes IoT nodes' time waste and memory. The PoBT consensus algorithm is integrated into the Hyperledger fabric framework. However, the consensus algorithm is still executed by a random IoT node, which increases the complexity [11].

Distributed blockchain is employed to authenticate IoT devices [24]. For this purpose, a cross-domain authentication scheme (xDBAuth) [25], 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 [17]. 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 composes an IoT environment. To avoid the single point of failure, this work [26] 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 [16] proposes a blockchain-based security scheme for secure data transmission [27]. 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 [8].

In Tab. 1, the main research limitations as identified. Firstly, the blockchain's linear growth decreases its scalability; Secondly, computationally intensive consensus algorithms are not suitable for the resource-constrained IoT environment, and last but not least, the level of security is low due to the involvement of inefficient credentials.

Table 1: Related works summary

Related works	Objectives	Limitations
LSB [28]	Scalable blockchain by overlay network	Uses PoW consensus not suitable for IoT Environment.
SVM-Blockchain [16]	Preserve privacy using support vector machine	Homomorphic operations increase complexity.
PoBT [23]	Lightweight consensus algorithm IoT friendly	The random node selection increase complexity.
MBS [22]	Scalable and flexible Blockchain for IoT environment	Mobile agents increase the deployment complexity.
xDBAuth [25]	Blockchain to authenticate IoTs using cross-domain server	Unreliable authentication.
SDN-Fog Blockchain [17]	Fog access secured with low latency	Heavy computational power.
Hybrid blockchain [26]	Identity authentication	High computational complexity.
Blockchain for secure data transmission [27]	Use of a symmetric encryption	Linear blockchain decreases scalability.

3 Problem Definition

A proposed distributed authentication device in a Fog- IoT environment based on distributed blockchain technology [26]. The significant issues with the above approach are many; firstly, the access of non-authorized users is minimized, the proposed approach is furthermore complex due to ECDSA and SHA-1, as these two algorithms are 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, which increases the public address's vulnerability. Thirdly, The PoW (proof of work) consensus algorithm is used in this work, which is more 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 lower resources, then that node will have a higher resource consumption. A lightweight blockchain uses a lightweight consensus algorithm, the so-called synergistic multiple proofs [12]. Here, 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 blockchain's unlimited growth. This work also stores the redundant data in the blockchain, which increases 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. Thus, the IoT nodes' surcharging is at a high level. An Efficient Lightweight Integrated Blockchain (ELIB) design has been proposed [29]; 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 is applied 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 the main 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 [14]. Although, PoW consensus provides security to validate transactions through complex and heavy computation. Although the deployment of fog nodes are deployed, the IoT nodes 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. This increases the size of the data, and the complexity of the network is also high. These mentioned research problems are still not solved in the IoT environment. Our work focuses on these problems.

4 Proposed Framework

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. The first tier includes n a number of IoT sensors $(S_1, S_2, S_3 \ldots S_n)$. 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 $(F_1, F_2, F_3 \ldots F_m)$. 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.

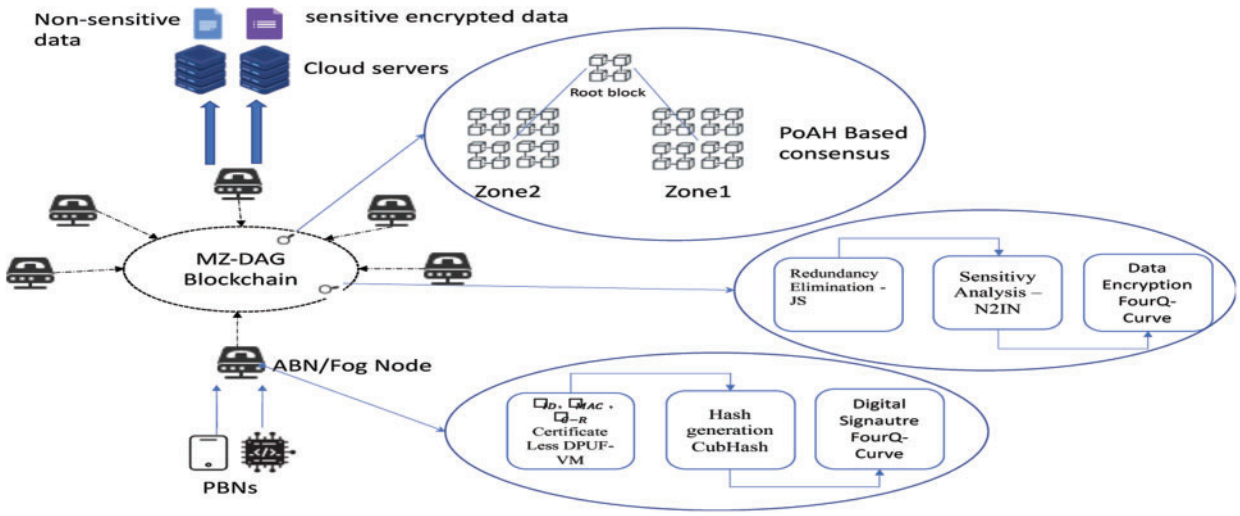

Figure 1: Proposed tri-level multizone-DAG-blockchain architecture

The proposal provides efficiency through the following processes:

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

4.1 Light Weight 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:

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 $S_{ID}(i)$, MAC address $S_{MAC}(i)$, PUF($S_{C-R}(i)$), and the sensor's last detected value ρ_i. The random ID's generated as follow:

$$R_{ID}(i) = S_{ID}(i) \oplus \rho_i \tag{1}$$

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

The second step is device registration. The credentials are stored in the blockchain as hash values at this step. Furthermore, the CubeHash algorithm is proposed for hash generation. The operation of CubeHash involves five major parameters listed in Tab. 2.

Table 2: CubeHash algorithm parameters

Parameter	Description
R_{Ini}	Number of initial rounds
R_{fin}	Number of final rounds
r	Number of rounds per block
bs	Block size (128 bytes max)
hs	Hash output size (512 bytes max)
H	Hash output

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

$$H(x) = R_{Ini} + \frac{r}{bs} + R_{fin} - hs(x) \tag{2}$$

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

CubeHash generation algorithm

Init

Add x_i *into* $x_{i\oplus16}$ *for* $0 \leq R_{Ini} \leq 15$

Rotate x_i *on left by seven bits or* $0 \leq R_{Ini} \leq 15$

Swap x_i *and* $x_{i\oplus8}$ *for* $R_{Ini} \subset [1,2,3,4,5,6,7]$

XOR $x_{i\oplus16}$ *and* x_i *for* $0 \leq R_{Ini} \leq 15$

Swap x_i *and* $x_{i\oplus2}$ *for* $i \subset [16,7,20,21,24,25,28,29]$

Add x_i *into* $x_{i\oplus16}$ *for* $0 \leq R_{Ini} \leq 15$

Rotate x_i *on left by eleven bits*

Swap x_i *and* $x_{i\oplus8}$ *for* $R_{Ini} \subset [0,1,2,3,8,9,10,11]$

XOR $x_{i\oplus16}$ *and* x_i

Swap x_i and $x_{i\oplus1}$ *for* $i \subset [16,18,20,22,24,26,28,30]$

End

The third step is device authentication. The S_i triggers authentication with the sending of an authentication request to the BGW. Then the BGW requests a random certificate with a digital signature. The R_{CER} is generated based on the R_{ID} and S_{MAC} as follows,

$$R_{CER} = H(R_{ID} \oplus S_{MAC}) \tag{3}$$

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

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

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

$$\varepsilon(\mathcal{F}_{p^2}) : -x^2 + y^2 = 1 + gx^2y^2 \tag{5}$$

where p is a prime number, and is a non-square in $\mathcal{F}_{p^2}$. This curve, dubbed "FourQ". p is defined to generate digital signature. First, the hash is generated for PUF by using CubeHash algorithm. In the order of l, the random selected i is from [1, $l-1$], the curve point computed as follow,

$$(x_1, y_1) = lxG \tag{6}$$

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

$$r = x_1 \ mod \ l \tag{7}$$

$$s = l^1(z + rSK) mod \ l \tag{8}$$

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 (R_{CER}, $Sign(R_{C-R})$)

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.

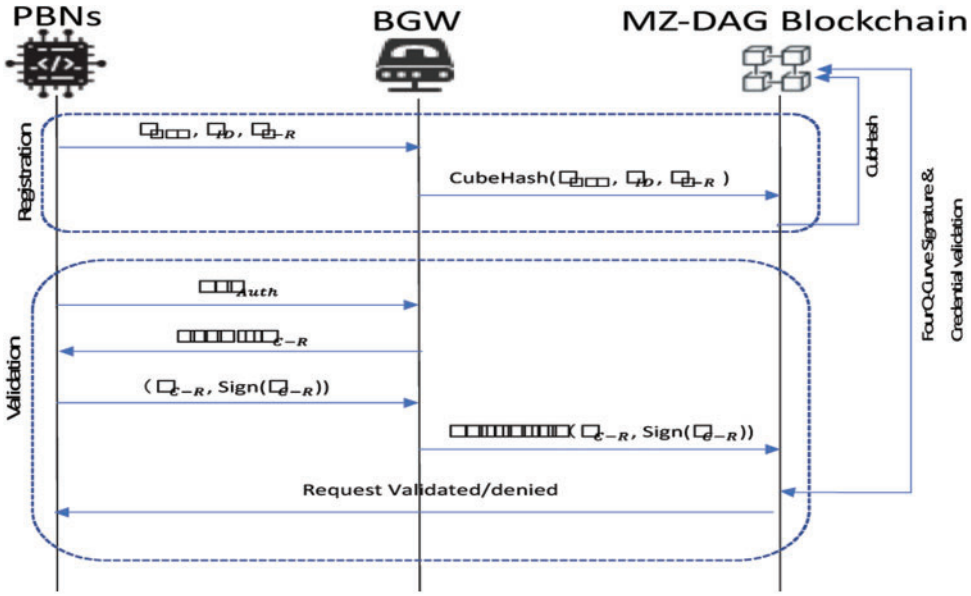

Figure 2: Proposed DPUF-VM authentication

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

4.2 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,

$$JS(SD_u,\ SD_v) = \frac{|SD_u\ \cap SD_v|}{|SD_u\ \cap SD_v|} \tag{9}$$

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 (S_T), and the sensor location (S_L) 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.

In the hidden layer, the membership function is initialized as truth set *Ti*, indeterminate set *Ii*, and false set *Fi*. The objective function of N2IN is the following representation:

$$L(T,I,F) = \sum_{i=1}^{u} (\sigma_1 + T_{ij})^M .||F_i - \varphi_j||^2 + (\sigma_2 I_{ij})^M .||F_i - \varphi_j||^2 + \alpha^2(\sigma_3 F_{ij})^M .||F_i - \varphi_j||^2 \tag{10}$$

Here, $\sigma_1,\ \sigma_2, \sigma_3$ are the weight vectors, and φ_j is estimated based on the indexes of *Tij*. All three membership functions are given as follows:

$$T_{ij} = \frac{\beta}{\sigma_1}(F_i - \varphi_j)^{\frac{2}{M-1}} \tag{11}$$

$$I_{ij} = \frac{\beta}{\sigma_2}(F_i - \varphi_j)^{\frac{2}{M-1}} \tag{12}$$

$$F_{ij} = \frac{\beta}{\sigma_3}(\alpha)^{\frac{2}{M-1}} \tag{13}$$

And $\beta = \left(\frac{\rho}{M}\right)^{\frac{1}{M-1}}$ where p is the constant parameter.

The algorithm logic of N2IN

If ρ is abnormal && S_T is sensitive && S_L is sensitive.

Then SD_i is sensitive

Apply Encryption

Send $SD_i - encrypted$ to the cloud level

Else,

SD_i is non-sensitive

Send SD_i To the cloud level

End If

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 SD_i, the fog node applies encryption. Then, the encrypted data ($Encrypted[SD_i]$) is stored as a new transaction in the blockchain.

4.3 Lightweight Consensus Algorithm

The consensus algorithm is the primary mechanism for the validation of all transactions processed through the blockchain. The existing consensus algorithm has high complexity and computational overhead that needs an adjustment. In the same way, the existing traditional linear structure of the blockchain presents many problems in terms of scalability and complexity. Therefore, we propose a new Multizone-DAG-Blockchain structure. In the proposed structure, the IoT perception layer is segmented into multiple zones, and the transactions in each zone are managed in the corresponding zone. The model of Multizone-DAG-Blockchain is shown in Fig. 3.

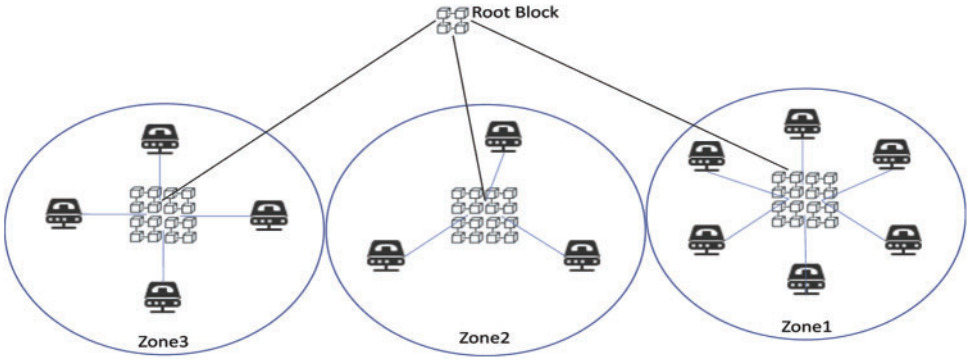

Figure 3: Multizone DAG blockchain design

In a fundamental sense, the DAG blockchain promotes scalability and minimizes complexity compared to the regular blockchain [4]. As each transaction is added in the form of new blocks in the regular blockchain, the blockchain grows exponentially. This sum mentioned phenomenon is addressed in the DAG-based blockchain, in which the graph G is composed over transactions. In the proposed Multizone-DAG-Blockchain model, a number v of direct acyclic graphs are constructed as $G1, G2, \ldots, Gv$ for Gv number of zones. That is, we obtain multiple DAGs with corresponding transactions for multiple zones. The graph i^{th} is defined as $G = \{S_j, E, W\}$ with $S_j \in Z_i$.

S_j is the set of IoT sensors located in zone i (Z_i), E is the set of edges between S_j, and W is the weight function presented as $E \subseteq (S_j \times S_j)$ and $W \subseteq (S_j \times S_j) \rightarrow R$. The G is entirely undirected so that there are no cycles in the graph. In the Multizone-DAG-Blockchain, the transactions are the vertexes (V), and the blocks have all transactions. The root block of the Multizone-DAG-Blockchain is the genesis block, and the Gj is a finite graph of $\{V, E\}$. The arrival of each transaction at each time t follows Poisson operation at the arrival rate of λ. This property is applicable for each DAG in the Multizone-DAG-Blockchain. With the increase in t, the G grows exponentially still lower than the linear blockchain. The main differences between conventional blockchain and the proposed Multizone-DAG-Blockchain are given in Tab. 3.

Table 3: Linear & multizone-DAG-blockchain comparison

Axes	Linear blockchain	Multizone-DAG-blockchain
Consensus	PoW	PoAh
Transaction speed	Depends on hash speed (minutes, hours or days)	3 to 5 milliseconds
Mining time	Slow mining	Fast mining
Transaction validation	Hash verification	Hash verification
Chaining	Single and slow chaining	Fast chaining
Blockchain growth	exponential growth	Linear growth

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 $T_1, T_2, T_3 \ldots T_n$ 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 $Block(T_1 \ldots T_n) \rightarrow Blocks$
  Sign(Block) → Broadcast
  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 [30]. 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 [30]. The spiral optimization algorithm determines the optimal solution by searching for the solution over multiple spiral models, which overcomes the optimum local problem. In BoSo, the search points are defined on the spiral path as follows,

$$y(t+1) = y^* + r \times R(\theta) \times (y(t) - y^*) \tag{14}$$

y(t), is the initial position of search points n at t iteration, and y^* is the best position learned, and $R(\theta)$ is the composite random matrix. The rotation angle $\theta \in \left[-\frac{\pi}{2}, +\frac{\pi}{2}\right]$ and the random number r. The BoSo process performs according to the steps described further below:

- BoSo initializes the number of search points which is $n \geq 2$, r, θ, scaling factor (SF), objective function $\mathcal{F}(g)$, and maximum iteration
- The initial position of the search point is defined randomly. Furthermore, For every search point, the relevance is calculated for each ABNs, for The j^{th} ABN, The $\mathcal{F}(g_j)$ is calculated based on two objectives: trust value $\mathcal{T}_j$, and load status $\mathcal{L}_j$. The trust value defines the number of transactions adequately validated by the ABN, and the load status defines the number of tasks running by the ABN. The $\mathcal{F}(g_j)$ is formulated as following,

$$\mathcal{F}(g_j) = \frac{\mathcal{T}_j}{\mathcal{L}_j} \tag{15}$$

- Based on the output of relevance function value $\mathcal{F}(g_j)$, the search point is selected properly. Based on the most suitable solution, the search position is updated as follows,

$$y(t+1) = x + r \times R(\theta) \times (y(t) - y^*) \tag{16}$$

$$y^* = \begin{cases} y^*_2, & r \leq \wp \\ y^*_1, & else \end{cases} \tag{17}$$

- y^*_1 and y^*_2 Zare respectively the first and second center points, $\wp$ is the probability index which lies between [0,1].
- All the search points are evaluated based on the relevance function, and the new position is updated as follows,

$$y^* = \arg\max\{\mathcal{F}(g_j)(y_i(t))\}, \text{with } i \in [1, SP] \tag{18}$$

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.

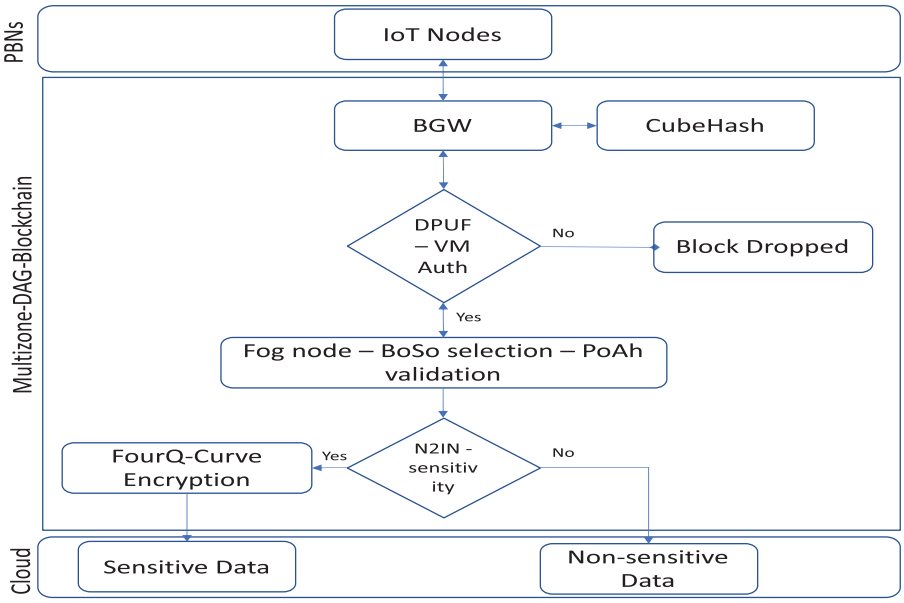

Figure 4: Multizone-DAG-blockchain flow design

5 Performance Evaluation

This section aims to evaluate the performance of the proposed Multizone DAG Blockchain through a comparative analysis. We are examining the results in an environment as close to reality as possible. We will highlight the significant areas of benchmarking in the IoT environment, such as energy consumption, response time, and moreover.

5.1 Simulation Environment

Our proposed Multizone DAG Blockchain simulated in Network Simulator NS-3. In particular, it provides proper support for IoT protocols and operations. Therefore, we chose ns-3 as the simulation tool as shown in Tab. 4.

Table 4: Parameters list used for the simulation purpose

Parameter	Value
Simulator version	3.26
OS	Ubuntu 14.04
RAM	4 GB
Number of IoT nodes	50
Number of fog nodes	10
Number of BGW	1
Number of cloud servers	3
Communication standard	Wi-Fi
Initial energy of IoT nodes	5 j to 10 j

(Continued)

Table 4: Continued

Parameter		Value
Packet generation rate		10 packets/sec
Packet size		512 bytes
Number of packets		100
Packet interval		0.1 s
Number of zones		5
CubeHash parameters	R_{Ini}	100
	R_{fin}	100
	r	36
Four-Q-curve parameters	Key size	512 bytes
	Number of rounds	10
N2IN	Hidden layers	10
	Activation function	sigmoid
	Learning rate	0.2
BoSo	Initial population	100
	ran	0.2
	Maximum iteration	100
Simulation time		100 s

The field of application of our proposed system is enormous according to our need for IoT in daily life; as shown in Tab. 5, we distinguish among applications industrial, smart cities, smart home, transport, and many others. In all these applications, the IoTs are mainly environmental sensors. we will continue our simulation analysis by considering as an example of sensors that we use in the daily life.

Table 5: Sensor deployed for simulation purpose

IoT sensor	Characteristic
Fire detector	Detects level of Carbon Monoxide (CO) in the air
	Follows split spectrum for transmission
	Operates in Wi-Fi band
Leak detector	Detects leakage and water level through the level of moisture content
	Operates in Z-wave and Wi-Fi band
Motion detector	Detects movement in the particular area
	Can adjust the delay demands from 10 s to 7 min
	Detects motions based on temperature variations (by infrared radiation)

Thus, we can notice that all sensors detect sensitive data related to a different private area. The motion detector is considered a sensitive device since it is usually used as a virtual guardian that

monitors the entire environment. All other sensors are classified according to the geographical context. Therefore, a temperature sensor set up next to the kitchen is more sensitive than the other devices. All of these IoT nodes are validated with each data transmission. In this way, data encryption is applied for all sensitive data detected by the IoT nodes. Since the blockchain validates the transactions, the environment is more secure and confidential.

5.2 Comparative Analysis

The proposed work is evaluated in terms of key performance metrics such as energy consumption, storage cost, response time, and throughput. The main differences between the proposed work and the existing works are shown in Tab. 6.

Table 6: Comparative analysis summary

Characteristics	Multizone-DAG-blockchain	ELIB	BFAN
Aim	Secure and lightweight blockchain based solution for IoT environment	Lightweight blockchain for Smart Home environment	Blockchain security for IoE environment
Network design	Blockchain Fog IoT	Blockchain IoT	Blockchain Fog IoT
Blockchain model	Multi-zones-DAG	Linear	Linear
Consensus	Lightweight-enhanced PoAh	Lightweight consensus by DTM	PoW
Node selection	Optimal node selection by BoSo algorithm	IoT node from overlay network	Random selection
Redundancy check	Performed by JS	Not performed	Not performed
Encryption	Four-Q-Curve	ECDSA	ECDSA
Hash algorithm	CubeHash	SHA-256	SHA-256
Blockchain characteristics remarks	Minimize complexity	Minimize consensus complexity	High complexity
	Improve scalability	Encryption and hashing complexity are high	Not scalable
	Minimize power consumption	Power consumption increased	High power consumption
	Increase storage capability	Poor storage efficiency	Poor storage efficiency
	Fast process & response time minimized	response time is large	Reasonable response time

The analysis shows that there are many research problems with the ELIB model theoretically, which can also be confirmed experimentally.

5.2.1 Power Consumption Analysis

Energy consumption is the quantity of energy consumed by the IoT nodes during data transmission. The energy consumed by the IoT nodes for sensing, transmitting, and receiving data. We analyzed the energy consumption as a function of the number of nodes and the number of transactions. In Fig. 5, the comparison of energy consumption is analyzed to increase the value of n. We notice that the n value has no impact on the proposed job since it has a reasonable energy consumption from 100 to 120 watts. At the same time, the ELIB mode increases the energy consumption with the increase of n value. Indeed, the proposed work is scalable since even increasing the number of nodes does not affect energy consumption. In contrast, existing work is unable to perform well when the number of nodes is high. In our proposal, energy consumption is minimized since the computations are offloaded to the fog nodes while the ELIB model performs all calculations on the IoT nodes. Although fog nodes are used in BFAN, the computations are performed in the IoT nodes.

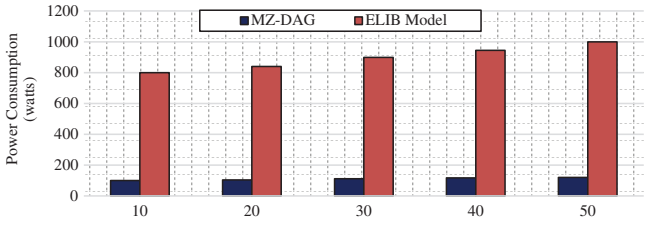

Figure 5: Power consumption analysis based on number of nodes

In Fig. 6, the energy consumption is analyzed as a function of the number of transactions. The increase in the number of transactions raises the complexity of the consensus validation process, as each transaction involves the creation and validation of a block.

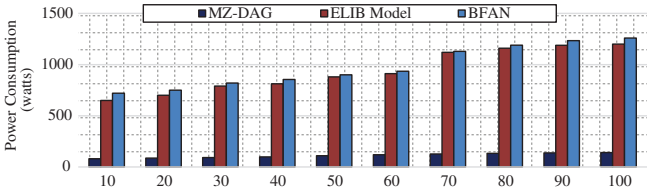

Figure 6: Power consumption analysis based on number of nodes

Thus, energy consumption is measured by the transaction cost. Therefore, the ELIB model has a power consumption of 650 to 1200 watts. The BFAN model has a power consumption of 1300 watts for 100 transactions. For the exact same number of transactions, the proposed job has a power consumption of 140 watts. The primary reason for this enormous improvement is the fact that the consensus algorithm is executed by an optimal ABN (fog node) selected by the BoSo algorithm in the proposed work. In addition, a lightweight PoAh is used which performs better than PoW. Thus, the power consumption is minimized up to 1000 watts in the proposed work.

5.2.2 Storage Efficiency Analysis

Storage cost is determined by the storage required for the IoT data generated by the IoT nodes. This metric is compared in terms of the number of nodes and the number of transactions.

In Fig. 7, the storage cost is analysed as a function of the number of IoT nodes. When nodes number increased, then the storage cost raises. This analysis shows that increasing the number of

nodes increases the block size and storage cost. The proposed work increases the storage efficiency, and It's four times higher than the existing BFAN & ELIB works. The main drawback is that these works increase the blockchain's size, which results in a higher storage cost. As a result, the linear blockchain model also increases the storage cost, which is not suitable for the resource-constrained IoT environment.

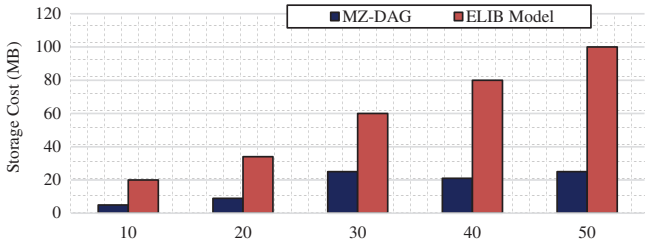

Figure 7: Storage cost analysis per number of IoT nodes

In Fig. 8, the storage cost is analysed based on the number of transactions. Even for 100 transactions, the storage cost is only 30 MB. However, for 100 transactions, the ELIB model has a storage cost of 124 MB, and the BFAN model has a storage cost of 135 MB. As the number of transactions increases, the size and length of the blockchain increase linearly.

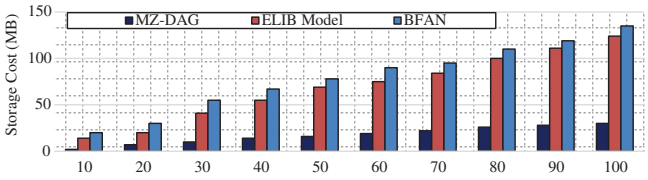

Figure 8: Storage cost analysis per number of IoT nodes

This increase results in a higher storage cost. In ELIB and BFAN mode, data from IoT nodes is collected and stored in cloud servers without any redundancy control. They are keeping repeated data results in a higher storage cost. However, the proposed work analyses the redundancy by JS among the data collected from IoT nodes and eliminates the redundant data. Furthermore, we apply data encryption only for sensitive data identified by the N2IN algorithm. Overall, the proposed work minimizes the storage cost with the Multizone-DAG-Blockchain framework and fog computing involvement.

5.2.3 Response Time Analysis

Response time is the time it takes the system to respond to requests. In this case, it is determined according to the time needed for the blockchain to validate the transaction and create the block for new input data. In Fig. 9, the response time is examined as a function of the number of transactions.

The analysis proves that the proposed Multizone-DAG-Blockchain has a slower response time than the ELIB model and the BFAN method. It is shown that the increase in the number of transactions exponentially increases the response time in both existing works since, with a high number of transactions, the blockchain becomes massive and fails to respond to new transactions. Even for some 100 transactions, the response time of Multizone-DAG-Blockchain is 12 ms, while the ELIB models are 45 ms and BFAN is 75 ms. Due to this long response time, new transactions fail to be

validated and added as new blocks. In this context, the IoT environment provides a massive amount of data every millisecond, which cannot be validated with both existing works.

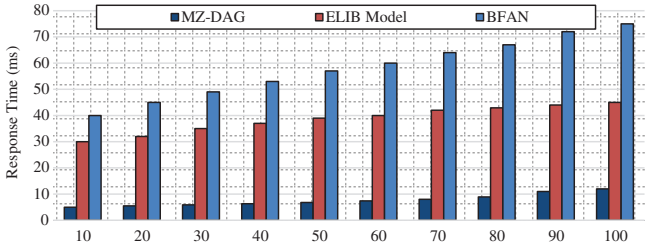

Figure 9: Response time analysis per number of IoT nodes

5.2.4 Throughput Analysis

The throughput of the system is the number of transactions processed and stored in the blockchain during the specified period.

In Fig. 10, the throughput is evaluated by analyzing the number of transactions. With an increase in the number of transactions, the throughput increases in parallel. In particular, the proposed Multi-Zones-DAG-Blockchain has a throughput of 135 kbps with 100 transactions. This is relatively higher than the ELIB model and the BFAN method. The ELIB model has a throughput of 95 kbps and BFAN has 85 kbps for 100 transactions. In both existing works, the blockchain structure is increased linearly for new transactions. On the other hand, the proposed work distributes the blockchain structure. Consequently, the proposed work achieves better throughput than the existing ELIB model and BFAN method.

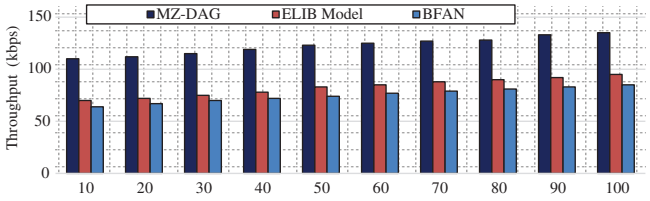

Figure 10: Response time analysis per number of IoT nodes

5.2.5 Results Analysis

Tab. 7 summarizes the average numerical results obtained for the proposed work and the existing works. The analysis shows that the proposed work achieves better performance in each performance metric.

This study shows that the proposed work is well adapted to the IoT network. This is mainly by minimizing energy consumption even with many nodes and transactions, which is vital for the IoT network. The main aspects of the research work are summed up as follows,

- The complexity and overhead are reduced in all aspects, including lightweight authentication, encryption, hash generation, and consensus algorithm.
- For the authentication, a random identifier is dynamically generated every time, and the unique MAC address is taken into account with physically tilted functions (PUF) to make the authentication as strong.

Table 7: Results summary

Metrics		ELIB	BFAN	MZ-DAG
Powers consumption (watts)	Based on transactions	941 ± 3	979 ± 4	112 ± 2
	Based on nodes number	896 ± 8	998	110 ± 6
Storage cost (MB)	Based on transactions	69 ± 4	79 ± 9	17 ± 4
	Based on nodes number	58 ± 8	73 ± 8	17
Response time (ms)		38 ± 0.69	58 ± 0.2	7 ± 0.78
Throughput (kbps)		82 ± 8	75 ± 2	122 ± 7

- Resource-constrained IoT nodes are considered passive nodes, and fog nodes are used to validate transactions.
- A lightweight consensus algorithm is presented with an optimal consensus node selection procedure.

Altogether, the proposed work minimizes the energy consumption of IoT nodes. As the proposed work is improved in the above aspects, this work achieves better efficiency.

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 security through lightweight computation. For starters, 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.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. M. Ogonji, G. Okeyo and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38, pp. 100312, 2020.

[2] J. Ahamed, M. Zahid, M. Omar and K. Ahmad, "AES and MQTT based security system in the internet of things," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 8, pp. 1589–1598, 2019.

[3] M. Abdel-Basset and M. Mohamed, "A novel and powerful framework based on neutrosophic sets to aid patients with cancer," *Future Generation Computer Systems*, vol. 98, pp. 144–153, 2019.

[4] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[5] 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.

[6] S. Görmüş, H. Aydın and G. Ulutaş, "Security for the internet of things: A survey of existing mechanisms, protocols and open research issues," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 33, no. 4, pp. 1247–1272, 2018.

[7] A. P. Bhatt and A. Sharma, "Quantum cryptography for internet of things security," *Journal of Electronic Science and Technology*, vol. 17, no. 3, pp. 213–220, 2019.

[8] S. Kably, M. Arioua and N. Alaoui "Lightweight blockchain network architecture for IoT devices," in *the 3rd Int. Symp. on Advanced Electrical and Communication Technologies (ISAECT2020)*, Kenitra, Morocco, vol. 978-0–7381, 2020.

[9] B. Mackenzie, R. I. Ferguson and X. Bellekens, "An assessment of blockchain consensus protocols for the internet of things," in *Int. Conf. on Internet of Things, Embedded Systems and Communications, IINTEC 2018*, Hamammet, Tunisia, pp. 183–190, 2018.

[10] A. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," in *2019 Int. Conf. on Electronics, Information, and Communication*, Auckland, New Zealand, pp. 1–2, 2016.

[11] D. Zakariae, E. Abdellah and B. A. Saïd, "A lightweight blockchain framework for IoT integration in smart cities," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 5, pp. 889–894, 2021.

[12] Y. Liu, K. Wang, Y. Lin and W. Xu, "Lightchain: A lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, 2019.

[13] D. Dasgupta, J. M. Shrein and K. D. Gupta, "A survey of blockchain from security perspective," *Journal of Banking and Financial Technology*, vol. 3, no. 1, pp. 1–17, 2019.

[14] P. Singh, A. Nayyar, A. Kaur and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, pp. 1–12, 2020.

[15] A. K. Das, S. Kalam, N. Sahar and D. Sinha, "UCFL: User categorization using fuzzy logic towards PUF based two-phase authentication of Fog assisted IoT devices," *Computers and Security*, vol. 97, pp. 101938, 2020.

[16] M. Shen, X. Tang, L. Zhu, X. Du and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, 2019.

[17] S. Rathore, B. Wook Kwon and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *IEEE Internet of Things Journal*, vol. 143, no. December 2018, pp. 167–177, 2019.

[18] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb and A. Refoufi, "A review of security in Internet of Things," *Wireless Personal Communications*, vol. 108, no. 1, pp. 325–344, 2019.

[19] A. Braeken, "PUF-based authentication and key exchange for Internet of Things," *IoT Security*, pp. 185–204, 2020, https://doi.org/10.1002/9781119527978.ch10.

[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] 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.

[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao *et al.,* "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.
[27] 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.
[28] 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.
[29] 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.
[30] 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.