Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.025219
Article

Tech Science Press

Design of Clustering Enabled Intrusion Detection with Blockchain Technology

S. Vimal[1], S. Nalini[2,*], K. Anguraj[3] and T. Chelladurai[4]

[1]Department of Computational Intelligence, SRM Institute of Science and Technology, Kattankulathur, 603203, Tamilnadu, India
[2]Department of Computer Science &Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, 620024, Tamilnadu, India
[3]Department of Electronics and Communication Engineering, Sona College of Technology, Salem, 636005, Tamilnadu, India
[4]Department of Electronics and Communication Engineering, PSNA College of Engineering and Technology, Dindigul, 624622, Tamilnadu, India
*Corresponding Author: S. Nalini. Email: autnalini@gmail.com

Received: 16 November 2021; Accepted: 24 December 2021

Abstract: Recent advancements in hardware and networking technologies have resulted in a large growth in the number of Internet of Things (IoT) devices connected to the Internet, which is likely to continue growing in the coming years. Traditional security solutions are insufficiently suited to the IoT context due to the restrictions and diversity of the resources available to objects. Security techniques such as intrusion detection and authentication are considered to be effective. Additionally, the decentralised and distributed nature of Blockchain technology makes it an excellent solution for overcoming the security issue. This paper proposes a chaotic bird swarm algorithm (CBSA)-based clustering technique based on an optimum deep belief network (ODBN) and Blockchain technology for secure authentication in an IoT setting. The CBSA-ODBN technique creates a clustering algorithm that utilises CBSA to pick cluster heads (CHs). The ODBN model is then utilised to identify the network, and the learning rate of the Deep Belief Network (DBN) model is optimally adjusted using the flower pollination technique (FPA). The suggested concept creates a layered security network paradigm for the Internet of Things using blockchain technology. Numerous simulations are run, with the outcomes analysed using a variety of measures, including detection rate, packet delivery ratio, energy usage, end-to-end latency, and processing cost. A careful comparison of the suggested model's performance to recently developed methodologies demonstrated the proposed model's superior performance.

Keywords: Authentication; distributed ledger technology; clustering; internet of things; intrusion detection; security; metaheuristics

1 Introduction

The Internet of Things (IoT) has gained popularity, and numerous IoT applications have become ingrained in daily life. Numerous new studies have been aided by this observation. Indeed, a recent Gartner study [1] predicts that by 2020, 50 billion networked gadgets will be installed. Business Insider reports that it has grown to over 64 billion connected devices. According to McKinsey Global Institute, there are currently 127 new Internet of Things devices connected to the Internet. According to a similar source, 100% of the world's population is predicted to have access to low-power, wide-range network coverage by 2022. Additionally, by 2025, the Internet of Things has the potential to generate between $4 and $11 trillion in economic value. As a result, the Internet of Things allows novel capabilities such as decision-making and analysis, as well as remote management and monitoring of devices using data acquired from several real-time data streams. As a result of the development of smart city concepts, IoT products are transforming cities and habits by enhancing frameworks, establishing cost-effective and effective municipal services, enhancing transportation services by reducing road congestion, enhancing citizen safety, and providing smart healthcare services [2]. ItT was constructed from an enormous number of diverse networked objects. All items must be approachable and generate material that is readily available independent of the user's position. It is critical that IoT objects may be accessed by authorised and authenticated users (people/things). Otherwise, it would be susceptible to a variety of security issues, including identity theft and data theft. Indeed, security concerns continue to be important impediments to the global implementation and adoption of IoT. In other words, people would resist IoT adoption if it introduces privacy and security risks.

Several security methods have been created recently to protect IoT signals. The author of [3] analysed physical layer security solutions for the IoT and recommended a variety of approaches for protecting IoT applications. This physical layer security solution encrypts quantized IoT signals using channel-based bit flipping, optimal sensor censorship, noise signal transmission, and probabilistic ciphering. According to [4], security gaps in IoT devices can be bridged utilising data concepts and encryption at the IoT's physical layers. Reference [5] proposes an IoT authentication protocol with lightweight encryption approaches for handling restricted IoT devices. Additionally, the author presented a learning technique for validating fingerprints and Internet of Things settings and connected devices in [6]. Watermarking was examined as a means of enhancing the security of IoT devices such as Cyber-Physical Systems (CPS). Reference [7] described a method for watermarking preset signals onto CPS input signals that enables the identification of replay attacks in which attackers repeatedly perform a series of previous measurements. Reference [8] describes a dynamic watermarking technique for detecting integrity concerns in network CPS. In [9], the author developed a security system that uses a non-stationary watermarking method to detect assaults involving non-zero average power signals to sensor measurements. Finally, [10] investigated the optimality of Gaussian watermarked signals in linear time-variant IoT-like systems against cyberattacks. However, the approach remains extremely difficult to execute at the perceptual layers of the IoT and requires increased computational power. Additionally, this strategy precludes more advanced attacks such as eavesdropping, in which attackers collect data over an extended period of time and use it to launch a covert attack.

The proposed study examined the following authentication schemes: two-party authentication via a trusted party with key exchange, mutual authentication, group authentication, session key-based authentication, One-Time Password (OTP)–based authentication, SecureID–based authentication, and directed path–based authentication. The majority of systems are built on top of an IoT framework. Additionally, the majority of them require key storage infrastructure and local key management, exposing them to key theft. Finally, they are almost all dependent on a single-factor authentication scheme, which poses security concerns in certain circumstances. Fig. 1 depicts an overview of the authentication method used in the Internet of Things. Using an optimum deep belief network (ODBN) and Blockchain technology, this study offers a chaotic bird swarm algorithm (CBSA)-based clustering technique for secure authentication in an IoT scenario. Additionally, a novel CBSA technique for cluster formation and head selection is devised (CHs). Additionally, intrusion detection is performed using the ODBN model, with the learning rate of the DBN model ideally controlled via the flower pollination technique (FPA). Additionally, an IoT environment is structured around a blockchain-enabled multilayer security network paradigm. A thorough experimental inquiry is conducted, and the data is analysed from a variety of perspectives. Section 2 discusses the review of literature in the proposed research work in the past two decades. Section 3 briefs the proposed research methodology, Section 4 discusses performance evaluation and Section 5 ends with conlusion and future findings.

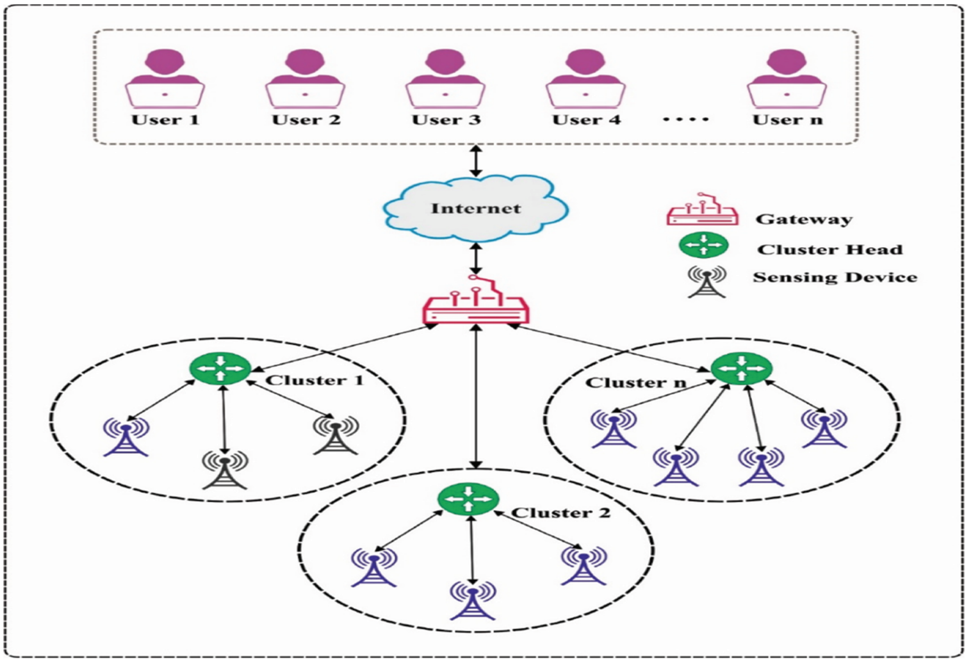


Figure 1: Overview of authentication process in IoT

2 Literature Review

In Li et al. [11], a lightweight blockchain should be developed to suit resource-constrained device scenarios. To attain a lightweight blockchain, an enhanced Practical Byzantine Fault Tolerance (PBFT) blockchain consensus mechanism is provided that is based on a reward and punishment strategy. Additionally, a blockchain storage optimization system based on RS erasure code is provided to reduce the storing overhead associated with ensuring the retrievability of blockchain. Tahir et al. [12] propose a novel authorization and authentication architecture based on a probabilistic approach for Blockchain-assisted IoT networks . The provided technique authenticates using arbitrary integers, which are also associated with joint condition probability. as a result, it establishes secure connections between IoT devices for gaining additional data.

Shen et al. [13] demonstrate an effective Blockchain-Added Secure device Authentication method BASA to cross-domain Industrial Internet of Things (IIoT). Particularly, consortium blockchains are presented for constructing a trust between distinct areas. Identity-based signature (IBS) is used at the time of authentication method. To ensure the device's anonymity, they created an identity management system capable of recognising that the device being certified unknown. Additionally, session keys among the two parties are negotiated that could secure the succeeding communication. Cui et al. [14], proposed blockchain-based solution for multi Wireless Sensor Networks (WSN) authentication system. The IoT node is classified as Base Station (BS), Cluster Head (CH), or normal nodes depending on their capacity to form hierarchical networks. Blockchain networks are created between various kinds of nodes to build hybrid blockchain models, which include public chains and local chains. These hybrid approaches provide node identity mutual authentication in variety of transmission circumstances, regular node identity authentication Via local blockchain, and CH node identity authentication Via public blockchain.

Sun et al. [15], proposed a clustering security management system of power distribution IoT that depends on trusted blockchain. Data transmission and clustering management for power distribution IoT were carried out using a trustworthy blockchain, which enhanced the data communication security. Searchable Symmetric Encryption (SSE) blockchain was proposed by Balaji et al. [16], presented for providing the best solution for the IoT environment by meeting the requirements of the IoT environment and ensuring end to end security. The offered blockchain implementations use overlay networks in order to provide a distributed environment in which the blockchains are governed by resource presents. On the one hand the new algorithm is presented to minimise the latency and irregularity; on the other hand, it is presented to maximise the scheme's throughputs. The Standard agreement method minimizes the irregularity in the latency and extraction operation. Chi et al. [17] propose secure data sharing frameworks are based on identity authentication and Hyperledger Fabric. Also, proposed a community detection method for dividing the client into distinct data distribution communities dependent upon the similarity of label data. The possibility of data distribution is chosen based on the results of the community detections determined Via the sharing amount, which effectively limits the possibilities of query data sharing and improves data distribution efficiency.

Zhang et al. [18], describe a lightweight data consensus approach for the IIoT that based on blockchain technology. This method enables safe data transfer from the IIoT to smart city applications. On a network of gateways, the algorithms make use of a common ledger. The two-path routing communication approach ensures data consistency throughout data transmission. The lightweight data block structures are an evolution of the more established blockchain technique. Revanesh et al. [19], proposed a trustworthy and dependable interconnected routing system based on deep learning, Blockchain technology, and Metaheuristics. The WSN's distributed routing data is handled using a Blockchain methodology, with the Shuffled Shepherd Optimization Algorithm (SSOA) algorithm determining the optimal routing. The routing data variants among the nodes are predicted and the optimum routing decision is made through the Deep convolutional Neural Network (DCNN) method. Algarni et al. [20] described a novel method for managing the supply of decentralized and lightweight secure access control for an IoT scheme using blockchain and multiagent schemes. The major objective is to develop a Block chain Management (BCM) that protects of IoT access control and enables secure communications among local IoT devices. Ourad et al. [21] demonstrated a blockchain-based solution for IoT devices connectivity and authentication. These solutions also benefit from the inherent properties of, depending on the current authentication mechanism. Particularly, blockchain-based design, solution, and architecture offered here enable traceability, accountability, and integrity by using tamper-proof records.

3 The Proposed Model

In this study, a new CBSA-ODBN model is derived for acheving security in an IoT context. The CBSA-ODBN paradigm is composed of three stages namely: CBSA based clustering, ODBN based intrusion detection, and blockchain-enabled authentication. Additionally, the optimal learning rate adjustment of the Deep Belief Network (DBN) model using Flexible Permission Ascription (FPA) aids in maximising the detection rate. Moreover, a local authentication scheme is applied by the CHs to perform the authentication process. Through the use of a local blockchain design, the blockchain technology ensures authentication for intercluster communication. The detailed working of these processes is given in the following.

3.1 Design of CBSA Technique

At the initial stage, the CBSA technique gets executed to select the CHs and construct clusters effectively. In this study, the CBSA technique is derived to construct clusters and choose CHs. The Basic Service Agreement (BSA) is a present optimization technique with features of easy procedure, optimum expansibility, and so on. Assume that N virtual birds fly and forage to food. Let $x_i^t(i \in [1,\ 2, \cdots,\ N])$ definite the place of *ith* bird at t. The bird's performance is explained as follows. The foraging performance was explained as:

$$x_{i,j}^{t+1} = x_{i,j}^t + (p_{i,j} - x_{i,j}^t) \times C \times rand(0,\ 1) + (g_{i,j} - x_{i,j}^t) \times S \times rand(0,\ 1) \tag{1}$$

Besides, the vigilance performance was explained in Eq. (2):

$$x_{i,j}^{t+1} = x_{i,j}^t + A_1(mean_j - x_{i,j}^t) \times rand(0,\ 1) + A_2(p_{i,j} - x_{i,j}^t) \times rand(-1,\ 1) \tag{2}$$

Where, A_1 and A_2 is explained mathematically as:

$$A_1 = a_1 \times \exp\left(-\frac{p_{Fit_i}}{sumFit + \varepsilon} \times N\right)$$

$$A_2 = a_2 \times \exp\left(\left(\frac{p_{Fit_i} - p_{Fit_k}}{|p_{Fit_k} - p_{Fit_i}| + \varepsilon}\right) \times \frac{N \times p_{Fit_k}}{sumFit + \varepsilon}\right)$$

a_1 and a_2 are constants from [0, 2]. ε have a smaller constant. Fig. 2 illustrates the flowchart of the CBSA technique.

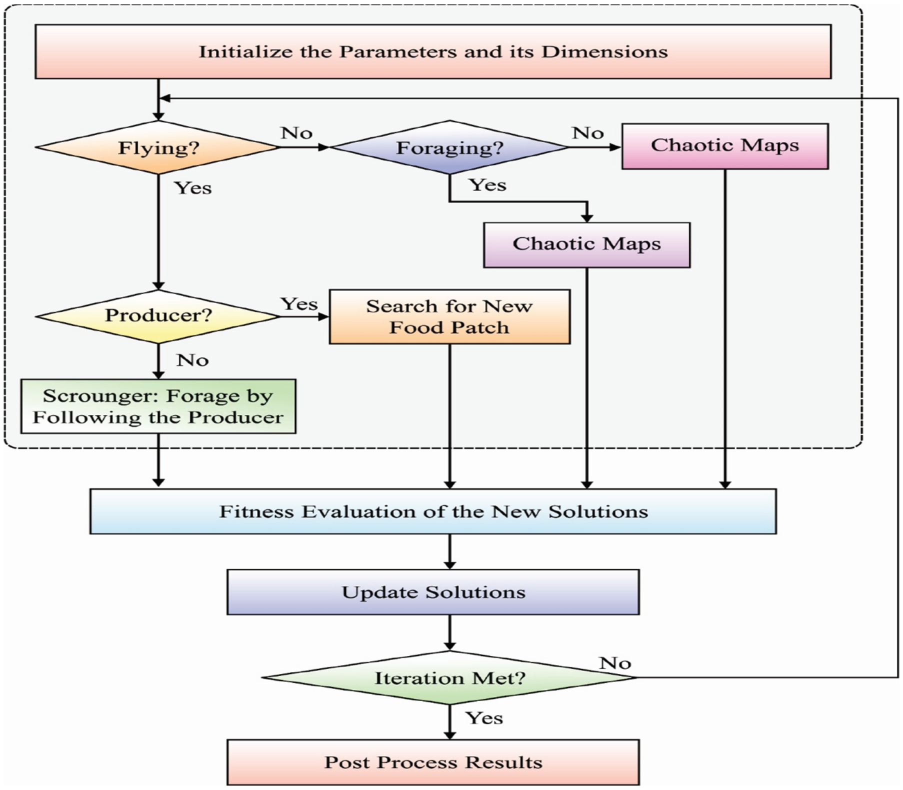

Initialize the Parameters and its Dimensions
Flying?
No
Foraging?
No
Chaotic Maps
Yes
Yes
Chaotic Maps
Producer?
Yes
Search for New Food Patch
No
Scrounger: Forage by Following the Producer
Fitness Evaluation of the New Solutions
Update Solutions
Iteration Met?
No
Yes
Post Process Results

Figure 2: Flowchart of CBSA technique

Then, the flight performance has been explained as follows.

$$x_{i,j}^{t+1} = x_{i,j}^{t} + randn(0,\ 1) \times x_{i,j}^{t} \tag{3}$$

$$x_{i,j}^{t+1} = x_{i,j}^{t} + (x_{k,j}^{t} - x_{i,j}^{t}) \times FL \times randn(0,\ 1) \tag{4}$$

Where FL is in [0, 2]. In the CBSA technique, the chaotic system is the property of sensitivity to primary conditions [22]. The chaotic signals created with deterministic models are the quality of genus-randomness. Its curve has defined as the primary value and chaos mapping parameter. Logistic mapping has been utilized extremely in practice. The Logistic chaotic model is difficult dynamical performances, it could be explained as variance Eq. (5).

$$\lambda_{i+1} = \mu \times \lambda_i \times (1 - \lambda_i) \tag{5}$$

$\lambda \in [0, 1]$, $i = 0, 1, 2, \cdots$, μ in [1,4]. Assume that μ has been nearby 4, λ refers the nearer to the average distribution amongst [0, 1]. In the meantime, the model has been finally chaotic if μ is 4. The primary population is a vital part of the intelligence optimization technique that controls the convergence rate and the last solution quality. During this case, the Logistic chaotic mapping has been utilized for initializing the population that creates full utilize of data solution space for improving the technical performance. In our presented technique, energy and distance are being regarded as 2 attributes to nodes clustering. The aim of the technique is to addressing further delay and difficulty and generate the technique appropriate to communication in the IoT environments.

3.2 Design of ODBN Technique

The ODBN model is used to identify intrusions in the IoT network. The DBN has been a generative method of the Deep Neural Network (DNN) technique. It can be structure as stacked Restricted Boltzmann Machines (RBM) and Sigmoid Belief Network (SBN). The projected DBN has three stacked RBM with three hidden layers $\{h1,\ h2,\ h3\}$. An input vector $\{X = h0\}$ and hidden layer $h1$ have been connected to the RBM procedure for generating stochastic Artificial Neural Network (ANNs). The 1st layer trained, the DBN assumes only one layer and so training the RBMI with constructive divergence technique. In the 2nd layer trained, the DBN involves two layers in which the upper layer has been assumed as RBM2 and the lower layer has been assumed as Sigmoid belief network and so freeze the weight $W1$. Likewise, in the 3rd layer trained, the top layer was regarded as RBM3 and another two are assumed as SBN so freeze the weight $W1$ and $W2$. The mathematical process of DBN has been projected in Eq. (6).

$$P(X,\ h^1,\ h^2,\ \ldots,\ h^n) = P(X|h^1)P(h^1|h^2)\ldots P(h^{(n-2)}|h^{(n-1)})P(h^{(n-1)},\ h^n) \tag{6}$$

The probability $P(h^{(n-1)}, h^n)$ of (1) is defined with RBM utilizing (7) and (8).

$$P(h^i|h^{i+1}) = \prod_j P(h_j^i|h^{(i+1)}) \tag{7}$$

$$P(h_j^i|h^{(i+1)}) = \sigma\left(b_j^i + \sum_k^{i+1} W_{kj}^i h_k^{i+1}\right) \tag{8}$$

The Greedy trained manner was utilized for training RBMs of DBN. The RBM is generating features and recreates inputs [23]. Thus, the contrastive divergence method has been utilized for training the RBM. The utilized Gibbs Sampling based contrastive divergence technique is as follows.

- Initiation of the parameters.
- Define the activation probability of hidden layers utilizing (9)

$$P(h_j|X) = \sigma\left(b_j + \sum_{i=1}^{m} W_{ij}X_i\right) \tag{9}$$

- Define the activation probability of input layer utilizing (10)

$$P(X_i|h) = \sigma\left(a_j + \sum_{j=1}^{n} W_{ij}h_j\right) \tag{10}$$

- Upgrade the edge weight utilizing (11)

$$Wij = Wij + \alpha(P(h_j|X) - P(X_i|h)) \tag{11}$$

At this point, α refers to the rate of learning. Afterwards, trained the initial RBM the edge weights are frozen. Then, it can be trained the succeeding RBM resulting the similar contrastive divergence phases. But, the resultant of preceding trained RBM was utilized as the input of succeeding RBM. Afterwards, the effective trained of stacked RBM, the DBN feature has been removed in the topmost hidden layers.

The FPA is used to optimise the learning rate of the DBN model. Yang [24] introduced a nature-inspired metaheuristic optimized technique called the FPA that is based on flower pollination. There are 2 types of pollination: self-pollination as well as cross-pollination. In self-pollination, the fertilization procedure has been carried out amongst the flowers of similar varieties, where the pollen in one flower drives for fertilizing another related one. Cross-pollination has been compared with transmitting the pollen to long distances amongst distinct plants, by insects namely birds, bees, and bats. It's worth noting that few insects tend to visit single flower without visiting others, a phenomenon known as flower constancy. typically, the flower pollination technique is stated as follows:

- Biotic and cross-pollination are defined as global pollination processes that are used to explore the region of the search space to identify a location. This phase has dependent upon levy distribution.
- The abiotic self-pollination defines the local pollination employed for exploiting the areas nearby the present solution to accelerate the convergence speed.
- The attribute of floral constancy is defined as a reproduction ratio that is proportionate to the degree of resemblance between two blooms.
- Due to physical closeness and wind, local pollination has a few advantages over global pollination. The local, as well as global pollinations, were composed by control variables P with values amongst [0, 1].

The mathematical formula of global pollination, as well as floral constancy, was contingent on combining the fittest bug with those capable of travelling long distances that were explained as follows:

$$\vec{x}_i^{t+1} = \vec{x}_i^t + \gamma l(\vec{x}_i^t - \vec{x}^*) \tag{12}$$

where t refers to the present iterations, x_i^t implies the existing place of ith solutions, x^* represents the better still solution, l defines the step created dependent upon levy distribution, γ signifies the step size scaling factors [25], and x_i^{t+1} denotes the next place. But the mathematical process of local pollination was explained as:

$$\vec{x}_i^{t+1} = \vec{x}_i^t + e(\vec{x}_k^t - \vec{x}_j^t) \quad (13)$$

Where e refers to the variable containing an arbitrary value created at the interval of [0, 1] dependent upon uniform distribution. x_k^t and x_j^t are 2 solutions elected arbitrarily in the present populations.

3.3 Blockchain-Enabled Authentication

The security framework consists of local authorization and authentication on edge computing device (Cluster head) layers that are determined by the clustering method and the fundamental network layers. These systems are related to the peer-to-peer nature of the multihop cellular networks. The registered IoT (entity) device is given by the local authorization and authentication services. The widely distributed system provides a service for establishing trust relationships with other CHs in the base station and network and computing edge node. The described technique for ensuring privacy and security of CH-CH transmission must address the resource-constrained and decentralized topology of the IoT networks. Additionally, the algorithms should conquer the key problems related to the blockchain include computation-intensive mining and time-consuming procedures. According to the distributed consensus a lightweight, decentralized blockchain-enabled data transport is provided. The presented blockchain-based frameworks also consider resource-constrained elements in the networks; therefore place a lightweight cryptographic hash function as an essential component. As previously stated, sophiscated security technique such as Asymmetric Cryptography may be implemented at the control layer level.

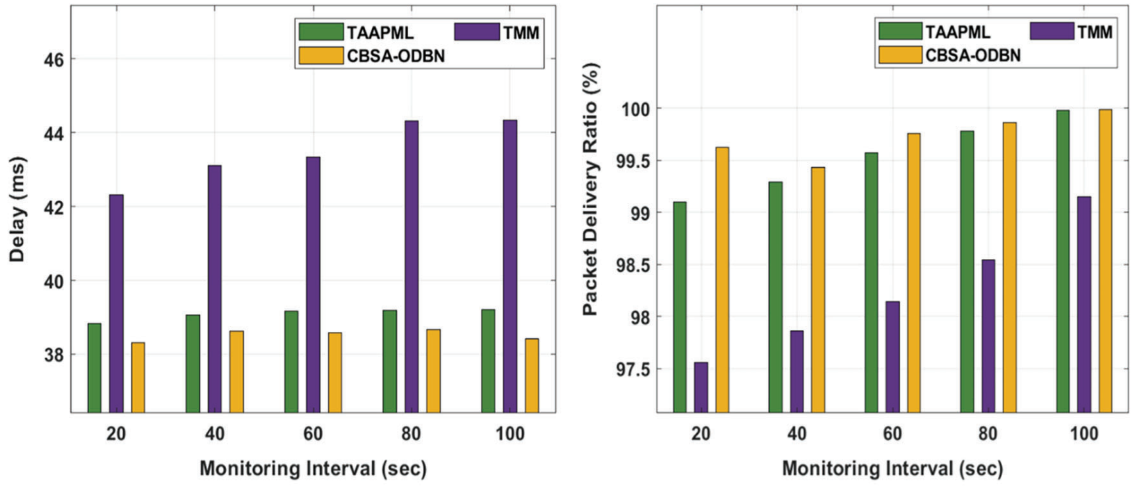
The blockchain security architecture depends on dispersed peer to peer networks. This model implementations deploy the Hyperledger Fabric framework [26] i.e., an opensource Blockchain environment. Hyperledger platforms would address certain issues associated with Blockchain implementations such as decentralization and latency. IoT devices communicate with blockchain by means of transactions. numerous tasks would be accomplished via a variety of transactions specified by smart contracts. The smart contract implementations enable connectivity between Blockchain networks and IoT nodes. numerous smart contracts are designed for the purpose of altering transactions. The IoT device/node sends distinct requests to the smart contracts for the purpose of carrying out various transactions within the Blockchain networks, including reading and writing. All the devices have a pair of keys; contain a public key and a private key. This set of keys is used to identity the device. Elliptic curve multiplications would be executed for producing public keys. The Blockchain is a distributed ledger technology that uses Merkle Tree (Hash Tree) for data integrity authentication. Hyperledger fabrics are open and allow for consensus modification in response to changing network requirements and application needs. In order to detect abnormal behaviour and perform synchronization of data, they adapt the PBFT (Practical Byzantine Fault Tolerance) as a consensus system that would lead to the consistency of blockchain networks. A collection of BSs from the higher-level layers serve as self-contained data miners with no central point. These layers comprise higher computer nodes that are distributedly coupled. A global blockchain architecture has been propsed for implementation in these levels, along with more robust security system. Asymmetric Cryptography like Elliptic Curve Cryptography (ECC) may be used. The data integrity was assured with a distributed blockchain-based network operation for improving the security levels.

4 Performance Validation

The CBSA-ODBN is compared to various approaches using monitoring periods in Tab. 1 and Fig. 3. The results ensured that the CBSA-ODBN technique has accomplished superior results over the other techniques. Based on delay, the CBSA-ODBN technique has demonstrated increased performance with least amount of delay across all monitoring periods. For example, with 20 s interval, the CBSA-ODBN technique has accomplished a lower delay of 38.32 ms whereas the Trust Aggregation Authentication Protocol based on the Machine Learning technique (TAAPML) and Trust Management Model (TMM) techniques have attained a higher delay of 38.84 and 42.32 ms respectively. Similarly, with 100 s interval, the CBSA-ODBN approach has accomplished a minimal delay of 38.42 ms whereas the TAAPML and TMM manners have reached a superior delay of 39.21 and 44.33 ms correspondingly.

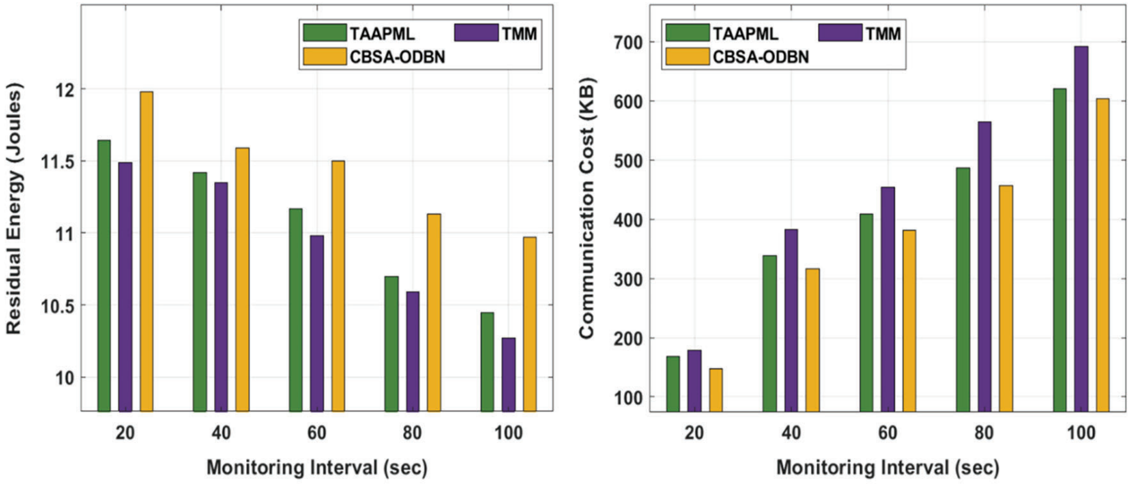
Table 1: Comparative results analysis of CBSA-ODBN technique under varying monitoring intervals

Monitoring interval (s)	Delay (ms)			Delivery ratio (%)		
	TAAPML	TMM	CBSA-ODBN	TAAPML	TMM	CBSA-ODBN
20	38.84	42.32	38.32	99.10	97.56	99.62
40	39.07	43.11	38.62	99.29	97.86	99.43
60	39.16	43.33	38.58	99.57	98.14	99.76
80	39.19	44.32	38.67	99.78	98.54	99.86
100	39.21	44.33	38.42	99.98	99.15	99.99
Monitoring interval (s)	Residual energy (Joules)			Communication cost (KB)		
	TAAPML	TMM	CBSA-ODBN	TAAPML	TMM	CBSA-ODBN
20	11.64	11.49	11.98	168	178	148
40	11.42	11.35	11.59	338	382	316
60	11.17	10.98	11.50	408	454	381
80	10.70	10.59	11.13	486	564	457
100	10.45	10.27	10.97	620	692	604



(a) (b)

Figure 3: (Continued)



(c) (d)

Figure 3: Result analysis of CBSA-ODBN model under different monitoring intervals

Next, with respect to Packet Delivery Ratio (PDR), a higher value is obtained by the CBSA-ODBN technique on all the applied monitoring intervals. For example, with 20 s interval, an increased PDR of 99.62% has been provided by the CBSA-ODBN technique whereas the TAAPML and TMM techniques have offered a reduced PDR of 99.10% and 97.56% respectively. Also, with 100 s interval, a maximum PDR of 99.99% has been offered by the CBSA-ODBN method whereas the TAAPML and TMM algorithms have existing a lower PDR of 99.98% and 99.15% correspondingly.

Afterwards, in terms of Residual Energy (RE), an increased value is attained by the CBSA-ODBN approach on all the applied monitoring intervals. For example, with 20 s interval, a higher RE of 11.98 Joules has been offered by the CBSA-ODBN method whereas the TAAPML and TMM techniques have obtainable a minimum RE of 11.64 and 11.49 Joules correspondingly. At the same time, with 100 s interval, an enhanced RE of 10.97Joules has been accessible by the CBSA-ODBN algorithm whereas the TAAPML and TMM methodologies have accessible a lower RE of 10.45 and 10.27 Joules correspondingly. According to Communication Cost (CC), the CBSA-ODBN approach has demonstrated higher efficiency with the least CC under all monitoring intervals. For the sample, with 20 s interval, the CBSA-ODBN manner has accomplished a reduced CC of 148 KB (Kilo Bytes) whereas the TAAPML and TMM techniques have attained a higher CC of 168 and 178 KB correspondingly. Eventually, with 100 s interval, the CBSA-ODBN manner has accomplished a minimum CC of 604 KB whereas the TAAPML and TMM algorithms have obtained a maximum CC of 620 and 692 KB correspondingly.

The comparison analysis of the CBSA-ODBN with other approaches takes place under different attack frequencies in Tab. 2 and Fig. 4. The outcomes make sure that the CBSA-ODBN algorithm has accomplished higher outcomes over the other techniques.

Table 2: Comparative results analysis of CBSA-ODBN technique under varying attack frequency

Attack frequency (Kb)	Delay (ms)			Delivery ratio (%)		
	TAAPML	TMM	CBSA-ODBN	TAAPML	TMM	CBSA-ODBN
20	38.76	44.28	38.02	99.82	98.96	99.92
40	38.87	44.3	38.37	99.43	98.27	99.56

(Continued)

Table 2 (continued)

Attack frequency (Kb)	Delay (ms)			Delivery ratio (%)		
	TAAPML	TMM	CBSA-ODBN	TAAPML	TMM	CBSA-ODBN
60	38.28	44.81	37.88	98.95	97.70	99.27
80	38.77	45.32	38.33	98.16	97.48	98.87
100	39.13	45.72	38.34	98.07	96.88	98.85
Attack frequency (Kb)	Residual energy (Joules)			Communication cost (KB)		
	TAAPML	TMM	CBSA-ODBN	TAAPML	TMM	CBSA-ODBN
20	10.99	10.66	11.21	92.03	142	81
40	11.10	10.87	11.25	138.01	242	128
60	11.15	10.98	11.51	184.06	342	165
80	11.19	11.05	11.47	230.01	382	210
100	11.21	11.09	11.39	275.99	452	253

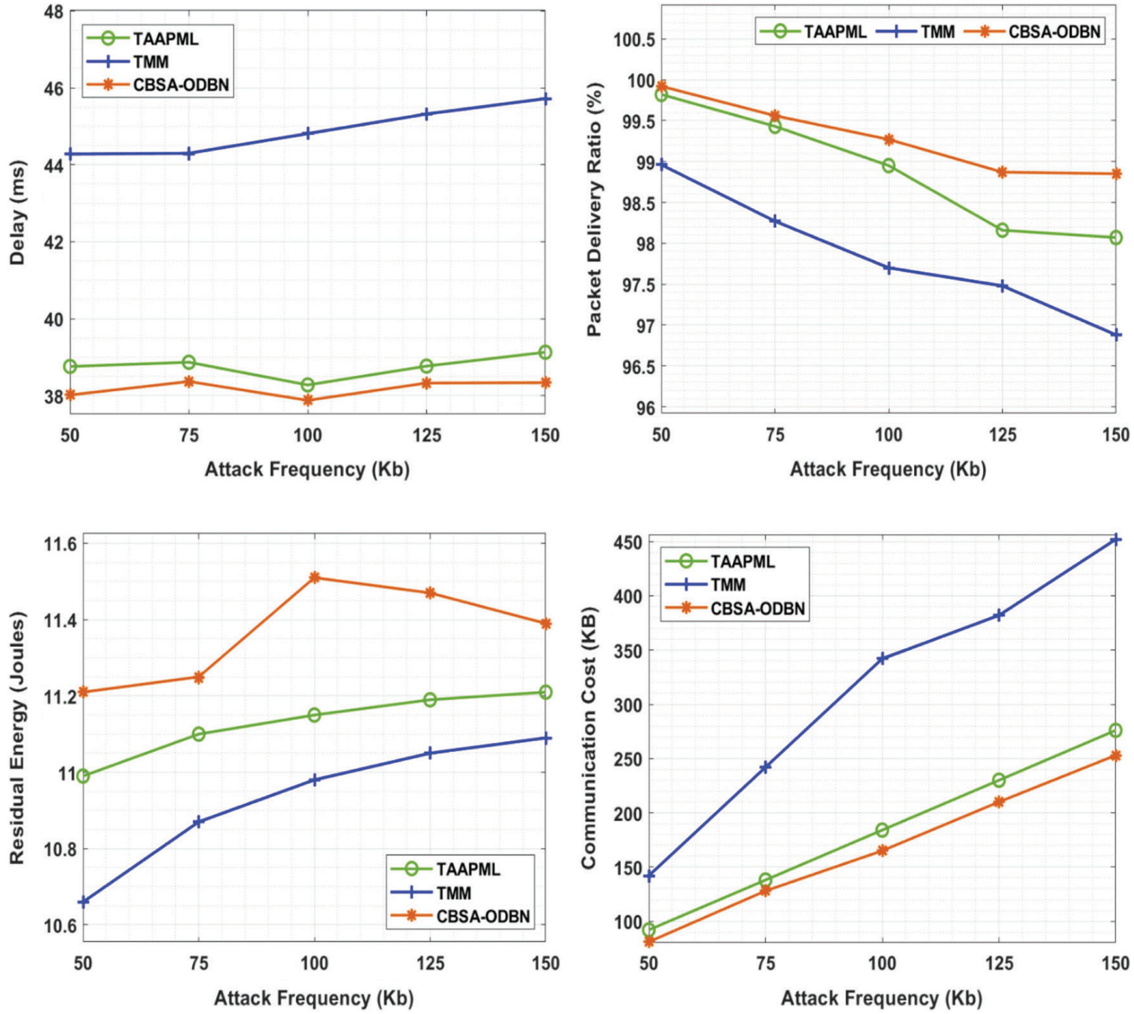


Figure 4: Result analysis of CBSA-ODBN model under different attack frequency

According to delay, the CBSA-ODBN technique outperformed enhanced performance at all attack frequencies with the least amount of delay. For example, with 20Kb frequency, the CBSA-ODBN methodology has accomplished a decreased delay of 38.02 ms whereas the TAAPML and TMM manners have gained a maximum delay of 38.76 and 44.28 ms correspondingly. Along with that, with 100Kb frequency, the CBSA-ODBN manner has accomplished the least delay of 38.34 ms whereas the TAAPML and TMM methods have reached a superior delay of 39.13 and 45.72 ms correspondingly. Then, in terms of PDR, a maximum value is reached by the CBSA-ODBN manner on all the applied attack frequencies. For the example, with 20Kb frequency, an enhanced PDR of 99.92% has been providing by the CBSA-ODBN method, whereas the TAAPML and TMM systems have accessible a minimum PDR of 99.82% and 98.96% respectively. additionally, with 100Kb frequency, a maximum PDR of 98.85% has been obtainable by the CBSA-ODBN manner whereas the TAAPML and TMM approaches have existing a lower PDR of 98.07% and 96.88% respectively.

Following that, the CBSA-ODBN approach obtains a higher value for RE for all the applied attack frequencies. For example, using 20Kb frequency, a higher RE of 11.21Joules has been given by the CBSA-ODBN technique whereas the TAAPML and TMM techniques have offered a reduced RE of 10.99Joules and 10.66Joules correspondingly. Additionally, with 100Kb frequency, a maximal RE of 11.39Joules has been offered by the CBSA-ODBN manner whereas the TAAPML and TMM algorithms have existed a lower RE of 11.21Joules and 11.09Joules respectively. According to CC, the CBSA-ODBN algorithm has demonstrated superior performance with the lower CC at all attack frequencies. For example, with 20Kb frequency, the CBSA-ODBN approach has accomplished a minimum CC of 81 KB whereas the TAAPML and TMM algorithms have gained a maximum CC of 92.03 and 142 KB correspondingly. In line with, with 100Kb frequency, the CBSA-ODBN approach has accomplished a reduced CC of 253KB whereas the TAAPML and TMM methodologies have attained an increased CC of 275.99 and 452KB respectively.

The intrusion detection performance of the CBSA-ODBN technique is examined using two benchmark datasets namely Network Socket Layer–Knowledge Discovery in Database (NSL-KDD) 2015 and Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS) 2017 dataset. The former dataset has 125973 samples with 41 features whereas the latter dataset has 2830743 samples with 80 features. A brief intrusion detection performance of the CBSA-ODBN technique on the applied datasets is given in Tab. 3 and Fig. 5.

Table 3: Performance analysis of intrusion detection dataset for proposed CBSA-ODBN method

Measures	NSL-KDD 2015	CICIDS 2017
Precision	99.99	99.97
Detection rate	99.98	99.98
Accuracy	99.98	99.97
F-score	99.98	99.98
Computation time (s)	56.89	89.64

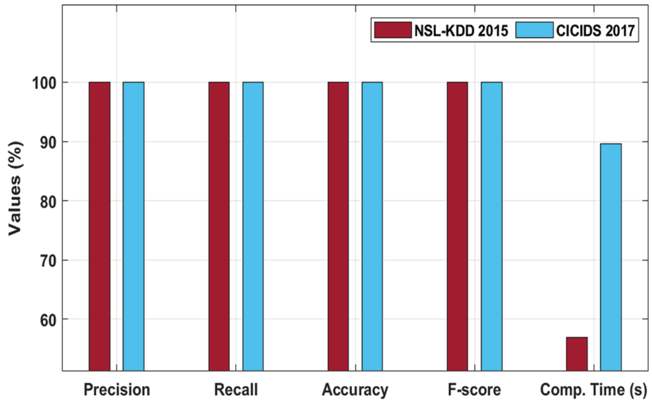


Figure 5: Intrusion detection analysis of CBSA-ODBN model with varying measures

The results showcased that the CBSA-ODBN technique has accomplished effective outcomes on the test datasets. With respect to precision, the CBSA-ODBN technique has attained 99.99% and 99.97% on the test NSL-KDD 2015 and CICIDS 2017 datasets. Followed by, in terms of detection rate, the CBSA-ODBN approach has gained 99.98% and 99.98% on the test NSL-KDD 2015 and CICIDS 2017 datasets. In line with, with respect to the accuracy, the CBSA-ODBN methodology has achieved 99.98% and 99.97% on the test NSL-KDD 2015 and CICIDS 2017 datasets. Along with that, in terms of F-score, the CBSA-ODBN approach has reached 99.98% and 99.98% on the test NSL-KDD 2015 and CICIDS 2017 datasets. At last, with respect to computation time, the CBSA-ODBN algorithm has obtained 56.89 and 89.64 s on the test NSL-KDD 2015 and CICIDS 2017 datasets.

Finally, a comparative detection accuracy analysis of the CBSA-ODBN technique with recent models shown in Fig. 6 [27]. The results demonstrated that the Cuckoo Search–Particle Swarm Optimization (CS-PSO) algorithm has accomplished worse outcomes with an accuracy of 0.7551. At the same time, the other Genetic+Fuzzy, DNN+SVM, and Behaviour-IDS techniques have offered moderate accuracy. Though the DBN and Machine Learning-Intrusion Detection System (ML-IDS) techniques have accomplished near optimal accuracy of 0.9996 and 0.9993, the CBSA-ODBN technique has outperformed the existing techniques with higher accuracy of 0.9998. From the above-mentioned tables and figures, it is apparent that the CBSA-ODBN technique has resulted in an effective tool for authentication and intrusion detection in the IoT environment.

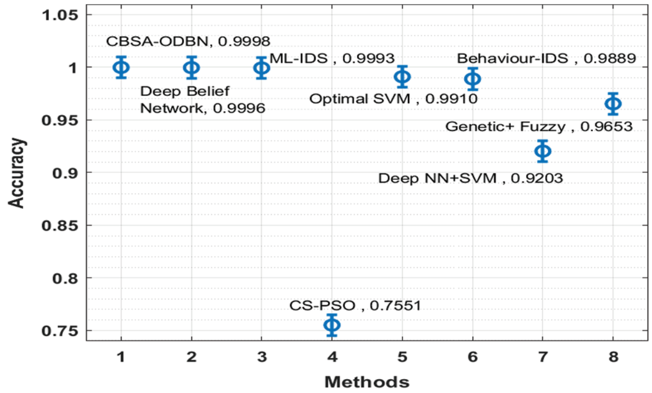


Figure 6: Accuracy analysis of CBSA-ODBN model with existing approaches

5 Conclusion

The purpose of this study is to develop a new CBSA-ODBN model for achieving security in IoT context. The CBSA-ODBN paradigm is composed of three-stages: clustering based on CBSA, intrusion detection based ODBN, and blockchain-enabled authentication. Additionally, the optimal learning rate adjustment of the DBN model using FPA aids in maximising the detection rate. Moreover, a local authentication scheme is applied by the CHs to perform the authentication process. A detailed experimental investigation is conducted, and the results are analysed from a variety of angles. A careful comparison of the suggested model's performance to previously established methodologies demonstrated the proposed model's superior performance. In future, lightweight cryptographic schemes can be developed to enhance security and data aggregation techniques can be integrated to significantly minimise the amount of data transmission across the IoT ecosystem.

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] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, "A lightweight ECC-based authentication scheme for internet of Things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, 2020.

[2] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad and L. Khoukhi, "IoT technologies for smart cities," *IET Network*, vol. 7, no. 1, pp. 1–13, 2017.

[3] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *IEEE Proceedings*, vol. 103, no. 10, pp. 1747–1761, 2015.

[4] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[5] J. Y. Lee, W. C. Lin and Y. H. Huang, "A lightweight authentication protocol for internet of things," in *Proc. Int. Symp. on Next-Generation Electronics (ISNE)*, Tao-Yuan, Taiwan, pp. 1–2, 2014.

[6] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of Things," in *IEEE 17th Int. Symp. on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Coimbra, Portugal, vol. 21, pp. 1–3, 2016.

[7] Y. Mo, S. Weerakkody and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems*, vol. 35, no. 1, pp. 93–109, 2015.

[8] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber-physical systems," *IEEE Proceedings*, vol. 105, no. 2, pp. 219–240, 2017.

[9] P. Hespanhol, M. Porter, R. Vasudevan and A. Aswani, "Dynamic watermarking for general LTI systems," in *2017 IEEE 56th Annual Conf. on Decision and Control (CDC)*, Melbourne, VIC, Australia, vol. 12, pp. 1834–1839, 2017.

[10] M. Hosseini, T. Tanaka and V. Gupta, "Designing optimal watermark signal for a stealthy attacker," in *Proc. of European Control Conf. (ECC)*, Aalborg, Denmark, vol. 1, pp. 2258–2262, 2016.

[11] C. Li, J. Zhang, X. Yang and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *Information Processing & Management*, vol. 58, no. 4, pp. 102602–102616, 2021.

[12] M. Tahir, M. Sardaraz, S. Muhammad and M. Saud Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability*, vol. 1, no. 17, pp. 6960–6978, 2020.

[13] M. Shen, H. Liu, L. Zhu, K. Xu and H. Yu, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[14] Z. Cui, X. U. E. Fei, 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.

[15] Y. Sun, W. Chen, L. Chenand, M. Li, "Research on clustering management of power distribution internet of things based on trusted blockchain," in *Journal of Physics: Conf. Series*, Shenyang, China, vol. 1748, no. 5, pp. 52064–52079, 2021.

[16] B. S. Balaji, P. V. Raja, A. Nayyar, P. Sanjeevikumar and S. Pandiyan, "Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain," *Energies*, vol. 13, no. 7, pp. 1795–1809, 2020.

[17] J. Chi, Y. Li, J. Huang, J. Liu, Y. Jin *et al.,* "A secure and efficient data sharing scheme based on blockchain in industrial internet of things," *Journal of Network and Computer Applications*, vol. 1, no. 167, pp. 102710–102726, 2020.

[18] W. Zhang, Z. Wu, G. Han, Y. Feng and L. Shu, "Ldc: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications," *Future Generation Computer Systems*, vol. 108, no. 4, pp. 574–582, 2020.

[19] M. Revanesh and V. Sridhar, "A trusted distributed routing scheme for wireless sensor networks using blockchain and meta-heuristics-based deep learning technique," *Transactions on Emerging Telecommunications Technologies*, vol. 7, no. 14, pp. 4259–4271, 2021.

[20] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassamet *et al.,* "Blockchain-based secured access control in an IoT system," *Applied Sciences*, vol. 11, no. 4, pp. 1772, 2021.

[21] A. Z. Ourad, S. Belgacem and D. Salah, "Using blockchain for IOT access control and authentication management," in *Int. Conf. on Internet of Things*, Honolulu, HI, USA, vol. 9, pp. 150–164, 2018.

[22] D. Zhang, J. Yang and P. Yang, "An improved chaos bird swarm optimization algorithm," in *Journal of Physics: Conference Series*, United Kingdom, vol. 1176, no. 2, pp. 22001–22016, 2019.

[23] M. M. Hassan, M. G. R. Alam, M. Z. Uddin, S. Huda, A. Almogren *et al.,* "Human emotion recognition using deep belief network architecture," *Information Fusion*, vol. 51, no. 15, pp. 10–18, 2019.

[24] X. S. Yang, "Flower pollination algorithm for global optimization," in *Proc. of the Transactions on Petri Nets and other Models of Concurrency XV; Springer Science and Business Media LLC*, Berlin/Heidelberg, Germany, vol. 8, pp. 240–249, 2021.

[25] M. Abdel-Basset, R. Mohamed, S. Saber, S. S. Askarand, M. Abouhawwash, "Modified flower pollination algorithm for global optimization," *Mathematics*, vol. 9, no. 14, pp. 1661–1678, 2021.

[26] M. A. Rashid and H. H. Pajooh, "A security framework for IoT authentication and authorization based on blockchain technology," in *2019 18th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications/13th IEEE Int. Conf. on Big Data Science and Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, vol. 5, pp. 264–271, 2019.

[27] M. Maheswari and R. A. Karthika, "A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks," *Wireless Personal Communications*, vol. 118, no. 2, pp. 1535–1557, 2021.