Scientific Research Publishing

Journal of Computer and Communications, 2024, 12, 78-102
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Privacy Preserving Federated Learning System for IoT Devices Using Blockchain and Optimization

Yang Han

School of Computing, Nanjing University of Information Science & Technology, Nanjing, China
Email: yang18han@gmail.com

How to cite this paper: Han, Y. (2024) A Privacy Preserving Federated Learning System for IoT Devices Using Blockchain and Optimization. *Journal of Computer and Communications*, **12**, 78-102.
https://doi.org/10.4236/jcc.2024.129005

Received: August 10, 2024
Accepted: September 11, 2024
Published: September 14, 2024

Abstract

In this study, a blockchain based federated learning system using an enhanced weighted mean vector optimization algorithm, known as EINFO, is proposed. The proposed EINFO addresses the limitations of federated averaging during global update and model training, where data is unevenly distributed among devices and there are variations in the number of data samples. Using a well-defined structure and updating the vector positions by local searching, vector combining, and updating rules, the EINFO algorithm maximizes the shared model parameters. In order to increase the exploration and exploitation capabilities, the model convergence rate is improved and new vectors are generated through the use of a weighted mean vector based on the inverse square law. To choose validators, miners, and to propagate new blocks, a delegated proof of stake based on the reliability of blockchain nodes is suggested. Federated learning is included into the blockchain to protect nodes from both external and internal threats. To determine how well the suggested system performs in relation to current models in the literature, extensive simulations are run. The simulation results show that the proposed system outperforms existing schemes in terms of accuracy, sensitivity and specificity.

Keywords

Blockchain, Credibility Status, Federated Learning, IoT, Privacy, Weighted Mean of Vectors

1. Introduction

The integration of the Internet of things (IoT) has provided technological advancements in most sectors of human endeavors, such as healthcare [1], power

[2], agriculture [3], manufacturing [4], entertainment [5] [6], etc. The IoT facilitates autonomous sensor or device communication and real-time decision-making based on the vast computational power of cloud and edge computing infrastructures [7]. The sensors generate a massive amount of data, which is paramount in IoT applications. Moreover, conventional methods have been employed to share the data, and they have centralized storage systems and management, which are prone to threats and data leakage. Additionally, centralized systems have been known to face single points of attack or failure [8]. Furthermore, data privacy concerns cannot be ruled out when dealing with data sharing using conventional data sharing methods. Since data owners have distinct or unreliable behaviors and uneven data distribution, there is a likelihood that shared models will be compromised. Therefore, the federated learning approach provides secured shared models where training and model updating are performed without sharing the actual data. Federated learning provides an enabling environment where a distributed machine-learning approach is created without the need to share data samples. Moreover, problems of data heterogeneity, privacy preservation, and data availability are resolved in federated systems while minimizing model bias, which makes it a better machine learning paradigm for IoT [7]. However, federated learning has encountered several challenges, making it not suitable for real-world IoT applications. The challenges are resource management problems, especially for resource-constrained IoT devices or sensors when they become central servers; single points of failure for central servers as any disruption can make collaborative learning inefficient; and federated learning is not scalable when the number of participating devices increases. Federated averaging is a popular method for updating the global model during global model training. Devices receive the updated global model when the global model has been updated through the averaging of local models [9]. However, in real-world situations, federated averaging could not agree, especially if the data is not evenly distributed among devices and there are appreciable variations in the number of data samples. The reason for this is that in the early phases of training, local models may not always outperform the average-based global model. To this end, there is a need to provide efficient methods for updating the global models. Additionally, more robust decentralized systems need to be provided in the context of federated learning.

Nowadays, blockchain technology acts as one of the security providers in IoT applications, and data can be shared in a decentralized and distributed fashion. Federated learning incorporated into blockchain protects participants from intrusion attacks using advanced machine learning algorithms [10]. Blockchain improves transparency and trust in IoT systems, while federated learning facilitates speedy distribution and model training across multiple IoT devices. **Table 1** provides the list of abbreviations and their meaning. Motivated by the limitations of [9], this study proposes a blockchain-based federated learning system using an enhanced weighted mean of vectors optimization algorithm for IoT environment. The specific contributions of this study are as follows:

Table 1. The list of abbreviations used in this paper.

Abbreviation	Full name
AI	Artificial intelligence
IoT	Internet of things
IoMT	Internet of medical things
QoS	Quality of service
PPFLEC	Privacy protection federated learning under edge computing
FedMSQE	Federated learning with minimum quantification square error
FL-PMT	Federated learning-based person movement identification
BiLSTM	Bidirectional long-short term memory
SCALT	Scalable and transferable classification system
MI	Mutual Information
QTA	Quality-oriented task allocation
TCL	Trust-based collaborative learning approach
EMT	Encrypted model training scheme
DPoS	Delegated proof of stake
CNN	Convolutional neural network
CHCT	Chameleon hash scheme with a changeable trapdoor
RMB	Redactable medical blockchain
RSA	Rivest-Shamir-Adleman
DES	Data encryption standard
AES	Advanced encryption standard
ODMS-FL	Optimal data management and secured federated learning
MODE	Multi-objective differential evolution
IMOAO	Improved multi-objective Aquila optimizer
OBL	Opposition-based learning
MACSA	Multi-objective cuckoo search algorithm
PMQoSR	Priority-based multi-objective quality of service routing
WLFA	Whale lion fireworks optimization
MOEA/D	Multi-object evolutionary algorithm based on decomposition
NSGA-III/OBL	Non-dominated sorting-based genetic algorithm incorporated with opposition-based learning
ODNN	Optimized deep neural network
IoTFECNN	Internet of things feature selection convolutional neural network
CSA	Capuchin search algorithm
FedAvg	Federated averaging
EINFO	Enhanced weIghted MeaN oF vectOrs

1) To propose a security and privacy preservation system for IoT using blockchain-based federated learning.

2) To improve federated learning using an enhanced weighted mean of vectors optimization algorithm.

3) To enhance a delegated proof of stake (DPoS) consensus protocol using credibility status method for the selection of delegates.

This rest of this paper is organized as follows: Section 2 discusses literature review in three subsections: federated learning systems for IoT, federated learning based on blockchain technology for IoT and multi-objective optimization problems for IoT. Section 3 provides the proposed system model and problem formulation while Section 4 discusses the simulations results. Section 5 concludes the paper with future recommendations.

2. Literature Review

This section discusses the literature review in three subsections as follows:

2.1. Federated Learning for Internet of Things

Today, the Internet based on 5G and 6G has enabled the deployment of billions of IoT devices [11]. It implies that a massive amount of data will be generated from IoT devices, creating room for big data. Unfortunately, most IoT devices are controlled by central systems, which are prone to high costs of communication, storage, security, and privacy concerns. Additionally, robust algorithms are required for aggregating data on IoT platforms. To this end, federated learning provides a promising way to solve the limitations mentioned above. Federated learning is a data-driven machine learning paradigm that ensures collaborative learning between different participants without disclosing sensitive information about them. Thus, it minimizes the costs of storage, communication, and maintaining privacy. Federated learning has certain advantages for the IoT, such as scalability, improved model performance, and privacy preservation. Scalability is achieved via federated learning, where multiple IoT devices can leverage limited computation resources, including hardware, storage, etc., in a parallel manner, especially for low-bandwidth IoT devices. Due to the distributive nature of federated learning, more devices can join the network without incurring extra costs on a centralized server. Since a single IoT device may be resource-constrained, it is possible to have insufficient data to train a high-quality model. With federated learning, a single IoT device can collaborate with other devices to train high-quality models without exposing privacy. It means that raw data cannot leave devices during the model training process while model update parameters are shared between participants and the server. A review in [12] suggested systems heterogeneity and statistical heterogeneity to be challenges associated with federated learning for the Internet of medical things (IoMT). The system heterogeneity challenge occurs when each device in federated learning has distinct hardware, processing, communication, and storage capabilities. It limits the maximum efficiency when

deploying federated learning and may increase laggard mitigation and fault tolerance. Statistical heterogeneity occurs when the number of data points on different devices absolutely differs, which may increase model complexity in analysis and evaluation and laggard risk. The authors in [13] presented a framework based on federated learning for healthcare IoT. The proposed framework is suitable for decentralized databases while achieving quality of service (QoS) and privacy. However, issues of scheduling and coordination in federated learning are not addressed. To this end, the authors in [14] proposed a privacy protection scheme for federated learning under edge computing (PPFLEC). The scheme preserves privacy using shared secrets and weight masks. Also, it protects devices against collusion attacks and equipment dropping while ensuring consistency and integrity using digital signatures. However, the deployment of neural network models is expensive and challenging. To resolve the challenge, a fixed-point quantizer with stochastic rounding is adopted, but how to achieve the minimum square quantization error is not resolved. The work in [15] proposed federated learning with minimum square quantization error (FedMSQE) to minimize quantization error for every participant in the federated learning. However, how to resolve the problem of malicious participants degrading the model's quality by sharing low-quality data is not addressed. Therefore, the work in [16] addressed the problem by proposing an approach-based clustering to utilize social content data for selecting participants. Here, different groups of edge participants were established using group-specific federated learning. Aggregation is performed using models of different edge groups to achieve the robustness of the global model. However, intrusion attacks from different edge groups are not addressed. To this end, the authors in [17] proposed a method based on federated learning to detect unwanted intrusions among participants. This method guarantees the privacy and security of the local training models while sharing gradient parameters with the central global server. Afterwards, the server aggregates and shares the improved detection algorithm with the participants. However, the memory and computational costs of training unlabeled data on a cloud server are not addressed. The limitation was tackled by [18] via the federated learning-based person movement identification (FL-PMT) system. Deep reinforcement learning is used in the system to auto-label the unlabeled data, which is then used to train the model. In this case, the edge server allows parameters to travel via the cloud instead of the sensor data. In addition, bidirectional long short-term memory (BiLSTM) is employed in a number of smart healthcare system operations to categorize data. However, how to determine the contribution rate of each participant is not considered. The authors in [19] presented IoT for the healthcare system based on federated learning. Instead of using dataset size to estimate the contribution rate, the method uses the qualities of each participant's datasets. Furthermore, the dropout-tolerable strategy is used to stop the federated learning process, particularly if the number of online participants is equal to or greater than the predetermined threshold. Furthermore, the proposed method is impervious to attacks, including model inversion and

reconstruction. However, how to improve latency is not considered. The study in [20] makes use of clustered federated learning and edge computing to diagnose COVID19. The proposed method trains a multi-modal machine learning model that can diagnose COVID-19 in both X-ray and ultrasound images, enabling intelligent processing of visual input at the edge. However, the distribution and appearance of health data have unknown classes. Therefore, the authors in [21] proposed a scalable and transferable classification system, known as SCALT. The system is a one-classifier-per-class-based federated learning system that consists of a one-dimensional convolutional network used for feature extraction and an individual mini-classifier for every class. When a new class emerges, scaling is simple because only a mini-classifier needs to be trained. Only when it is moved to a new task does the feature extractor get updated. Another work in [22] combined deep neural networks, federated learning, and mutual information (MI) for effective feature selection and extraction. The proposed method can be used for anomaly detection of intrusions in the IoT network. Besides, IoT devices store information locally for model training, while models' weights are modified and shared with a centralized server. However, none of the authors in [11]-[22] solved the problem of global model aggregates in a synchronous and asynchronous federated learning context.

2.2. Federated Learning Based on Blockchain Technology for Internet of Things

The IoT paradigm allows a significant number of physical devices to be connected to the Internet, where massive amounts of data are generated. The data generated from IoT devices is useful for training high-quality machine learning models, more specifically deep learning models. It means that patterns can be easily inferred and appropriate intelligent decisions can be derived from data via learning models. Unfortunately, the IoT paradigm is centralized, which makes it vulnerable to privacy leakage, issues of scalability, security threats, etc. Federated learning, among many solutions, reduces privacy leakages through collaborative training without disclosing sensitive information, but it is still prone to security threats, trust issues, and single points of failure or attack. By integrating blockchain technology, federated learning for IoT systems can be holistically se-cure, and problems of trust and single points of attack can be resolved [23]. A survey in [24] discussed the current challenges of blockchain-based federated learning for IoT applications, which include privacy leakage; lightweight blockchain for federated learning and IoT that should balance between privacy and security, storage and communication cost, and scalability and power consumption; lazy clients; stragglers; statistical heterogeneity; system heterogeneity; unsupervised federated learning; and artificial intelligence (AI)-enabled smart contracts. Additionally, an efficient real-time privacy policy is required to secure participants' data in healthcare IoT applications. Therefore, the authors in [25] presented a blockchain and federated learning-empowered secure architecture for privacy preservation in

smart healthcare. Also, blockchain-based cloud platforms are employed for privacy and security. However, personalized healthcare demands cannot be met by a one-size-fits-all model due to the diversity of health problems among patients. A blockchain-enabled personalized federated learning system that enables users to train personalized models without directly uploading sensitive data was proposed in [26] as a solution to this issue. However, only a subset of IoT devices with limited training data are selected to perform federated learning tasks due to their low budget. The problem was overcome by the authors in [27], who presented a blockchain-based federated learning market to decentralize federated learning via blockchain, maximize the amount of training data to maximize budget, and provide data for devices with limited resources. They proposed the quality-oriented task allocation algorithm (QTA) to assign suitable devices to complete federated learning tasks while optimizing training quality under a set budget and the trust-based collaborative learning approach (TCL) for data sharing among trusted devices. In order to fend off attacks from malevolent devices, an encrypted model training scheme (EMT) employs countervailable differential privacy technology. Furthermore, a fair reward distribution is guaranteed using the proposed contribution-driven DPoS consensus mechanism.

However, the heterogeneity problem is not resolved. The work in [28] addressed the het-erogeneity problem in federated learning by designing systems, model tiers, and data to reduce heterogeneity and propagate high-quality models for each federated client. Be-sides, blockchain-enabled federated learning lowers latency and consumption while pre-serving privacy. Two technological challenges, namely how to provide correct global model aggregation via a centralized federated learning server and how to develop techniques that encourage federated learning clients to donate their computer resources and time, were not solved. The authors of [29] addressed the issues by putting forth a decentralized solution based on federated learning and blockchain. They also proposed a trust-decentralized loop federated learning consensus protocol to manage resources within IoMT. During the aggregation process, suitable features are chosen using a hybrid weighted-leader exponential distribution optimization algorithm, which suggests that multiple features exhibit different degrees of variation across each feature. These chosen features are then sent to the training phase through the proposed pyramid squeeze attention generative adversarial networks in order to categorize the data as positive and negative. To achieve more efficiency in blockchain-based federated learning, the authors in [30] integrate blockchain and federated learning in a fog-IoT network. The proposed approach utilizes the distributive structure of the fog-IoT network to produce an adaptive network for IoT devices while preserving privacy. However, the problems of latency, da-ta sufficiency, traceability, and privacy concerns due to the increasing number of heterogeneous data are not solved. The authors in [31] proposed a federated learning-enabled blockchain-based framework, known as PPFchain, to guarantee the security and privacy preservation of IoT devices. In PPFchain, cryptographic primitives and a federated learning model

are employed to ensure privacy in off-chain fog nodes, while blockchain is used to achieve low-cost and high performance in the network. Another work in [32] presented a technique based on blockchain and deep learning to preserve the privacy of electronic health records. In this technique, a convolutional neural network (CNN) is employed to distinguish between normal and abnormal users, while blockchain-based federated learning processes abnormal users and removes them from the database along with their accessibility of the health records. But because unscrupulous individuals can readily tamper with model updates, federated learning is susceptible to this kind of attack. The authors of [33] created a chameleon hash scheme with a changeable trapdoor (CHCT) for secure federated learning in industrial IoT environments in order to solve this limitation. The use of trapdoors was subject to a number of restrictions under the planned plan. Furthermore, a redactable medical blockchain (RMB) is an implementation of the CHCT system. However, a blockchain-based federated learning approach may not be the most plausible solution, as it is easy for models to be manipulated and intercepted during transmission between users and servers. Therefore, the authors in [34] proposed a system that ensures the security of the transmitted model between every component in the federated learning. Besides, the model is encrypted with Rivest-Shamir-Adleman (RSA), data encryption standard (DES), and advanced encryption standard (AES) algorithms, while the checksum is determined using a hash function, which is stored along with a private key in the blockchain. However, there are needs to improve existing solutions for safeguarding and effective administration of sensitive data generated by IoT devices. The authors in [35] designed an optimized data management and secured federated learning (ODMSMFL) system while integrating blockchain. The proposed system is capable of addressing unique requirements of IoMT, such as decentralized data administration, federated learning, and security. Besides, data management is enhanced using blockchain, which facilitates retrieval, adequate storage, and exchange of data without disclosing privacy.

2.3. Multi-Objective Optimization Problems for the Internet of Things

The IoT paradigm allows interactions among systems, processes, software, and technology over the Internet. It provides room for achieving the system's efficiency but increases factors such as time of operation, energy consumption, delay, and workload, which may lead to conflict among them. To mitigate this problem, the factors can be formulated as a single or multi-objective optimization problem. In [36], the authors provided a multi-objective-based evolutionary algorithm where rapid mutation operators and multi-objective differential evolution (MODE) are employed to address the problem of stagnation of the local optimum. They considered the objectives of IoT services, such as load, energy consumption, delay, and service cost, as the basis for the multi-objective optimization problem. Pareto front in the local space provides sufficient diversity and accelerates the rate of

convergence. However, because of the resource constraints of IoT devices, task completion increases along with delay. Therefore, the authors in [37] presented an improved multi-objective Aquila optimizer (IMOAO) with Pareto front to offload tasks from devices to fog nodes while minimizing delay. Opposition based learning (OBL) is used to improve the IMOAO algorithm and achieve sufficient diversity. How-ever, improper deployment of IoT devices on either a federated learning system or fog computing can lead to resource and bandwidth waste, a rise in energy consumption, and a poor QoS level. Thus, in [38], the authors proposed a mechanism to reduce bandwidth wastage, energy consumption, and single points of failure. Also, a multi-objective is formulated to minimize both energy consumption and delay between each component of the IoT network. Besides, a combinatorial optimization problem is solved using the multi-objective cuckoo search algorithm (MOCSA). However, an improper estimation model for control and monitoring of end-to-end communication and sensing is caused by the energy constraints of IoT devices. Also, it is challenging to achieve QoS requirements in IoT networks. Therefore, in [39], multi-objective optimization for QoS routing method is proposed to distinguish traffics while deriving better data communication. Also, a mechanism based on energy-efficient priority-based multi-objective QoS routing (PMQoSR) is designed to ensure QoS and energy in the IoT networks. The whale lion fireworks optimization method with fitness function routing (WLFA) mechanisms is an optimization technique with three hybrid algorithms that the proposed system uses to control the routing performance based on QoS criteria. The WLFA uses priority label and time delay patterns while transferring data to the destination in order to minimize localization errors, prevent congestion, and choose the shortest way via the network. However, IoT device selection, which is an NP-hard problem, needs to be solved. The authors in [40] formulated the IoT device selection problem as a multi-objective problem and incorporated OBL in the general framework of a multi-objective evolutionary algorithm-based on decomposition (MOEA/D). Also, convergence and diversity are enhanced using the many-objective algorithm, known as the non-dominated sorting-based genetic algorithm incorporated with OBL (NSGA-III/OBL). However, there is a challenge with IoT service placement in fog. Therefore, in [41], the authors provided a conceptual framework based on fog-cloud control to optimize IoT service placement. An automated planning model is formulated to manage service requests because of the heterogeneity of IoT resources and applications. Besides, automated evolutionary-based particle swarm optimization was employed to solve the IoT service placement problem while maximizing resources and improving the QoS of fog. However, achieving optimal security is challenging in the IoT network. To this end, the authors in [42] improved a meta-heuristic-based clustering protocol to achieve optimal communication. Here, an optimized deep neural network (ODNN) is used to detect malicious IoT devices based on their energy characteristics. Energy characteristics are determined using optimal cluster head selection, optimal routing, and neighborhood-based spider monkey

optimization. However, due to the dynamic nature of the IoT environment, intrusion detection systems are paramount. In [43], the authors presented a multi-objective evolutionary CNN to detect intrusion. In the proposed approach, CNN is a classifier to detect intrusions, while MOEA/D is used to simplify the parameter tuning process of CNN. Specifically, MOEA/D simultaneously optimizes the two competing goals of the CNN model, such as detection performance and model complexity. It is achieved through a novel encoding scheme that converts CNN's topological architecture into a chromosome. It allows MOEA/D to produce a variety of intrusions with different CNN model detection performances and complexities. Similar work in [44] designed an IoT feature extraction CNN (IoT-FECNN) to detect anomalies in the IoT network. Besides, a binary multi-objective enhanced Capuchin search algorithm (CSA) called BMECapSA is proposed to efficiently select features. However, there is a lack of collaboration between application containers and resource allocation problems in the IoT-based cloud. The work in [45] presented a container model named Band-area application container to express in reality the variety of things. Also, an artificial fish swarm algorithm is proposed for optimizing container-enabled task scheduling. Another work in [46] presented multi-objective combinatorial convex optimization to minimize execution cost while blockchain-enabled cost-efficient scheduling algorithm framework to address deadlines and security challenges in IoMT. However, it is more challenging to satisfy the requirements of industrial IoT systems. Therefore, the authors in [47] presented a multi-agent deep reinforcement learning-based offloading method to satisfy the various requirements of different tasks in cloud-edge device computing.

3. The Proposed System Model

The proposed system model is presented in **Figure 1**. In the figure, the proposed system model comprises three layers: federated learning, an optimization algorithm, and a blockchain network. IoT device security and privacy can be achieved through the use of federated learning and blockchain technology. In this research, we adopt Paillier encryption for security and privacy instead of differential privacy or anonymization techniques, which could lead to more difficulties when it comes to training data and auditing. According to this study, IoT devices have limited resources and are unable to transmit data and conduct both local and global training at the same time. However, by lowering the overall computation cost and transmission delay of the proposed system through the use of robust machine learning and game theoretical methodologies, this work expects to provide answers to the limitations in the future. During local and global model training, blockchain enables federated clients, *i.e.*, IoT devices, to exchange model parameters through uploading and downloading. Additionally, every aspect of IoT device operation is protected against both internal and external threats. The IoT devices in this study are in charge of local task initialization and model bootstrapping [48]. IoT devices can create new blocks on the blockchain by acting as

Algorithm 1. The proposed blockchain-based federated learning with enhanced weighted mean vector optimization algorithm.

1: **Parameter:** $n>0, n\in Z^{+}, 0\le\theta\le 1$

2: **Initialization:** $x_0 =, N_p, max_y$

3: Generate Initial population using Equation (15)

4: Determine best vector xb_s

5: **for** $t=1$ to T **do**

6: **for** $n=1$ to N **do**

7: Client n performs local training using Equation (1)

$$x^t(n+1)=x^t(n)-ng^t(n)+\theta\left(x^t(n)-x^t(n-1)\right) \tag{1}$$

8: Client n updates Equation (2)

$$x^{t+1}=\sum_{n=1}^{N} w_n x^t(n) \tag{2}$$

9: **end for**

10: **if** $r<0.5$, **then**

$$x_{n\in w}^1 = x+\sigma MR+r\frac{\left(x_{bs}-x_{a1}\right)}{f\left(x_{bs}\right)-f\left(x_{a1}\right)+1} \tag{3}$$

$$x_{n\in w}^2 = x_{bs}+\sigma MR+r\frac{\left(x_{bs}-x_{a1}\right)}{f\left(x_{bs}\right)-f\left(x_{a1}\right)+1} \tag{4}$$

11: **else**

$$x_{n\in w}^1 = x_{a1}+\sigma MR+r\frac{\left(x_{a2}-x_{a3}\right)}{f\left(x_{a2}\right)-f\left(x_{a3}\right)+1} \tag{5}$$

$$x_{n\in w}^2 = x_{bt}+\sigma MR+r\frac{\left(x_{a1}-x_{a2}\right)}{f\left(x_{a1}\right)-f\left(x_{a2}\right)+1} \tag{6}$$

12: **end if**

13: **if** $r<0.5$, **then**

$$u_1 = x_{n\in w}^1+\mu\left|x_{n\in w}^1-x_{n\in w}^2\right| \tag{7}$$

14: **else if** $r>0.5$, **then**

$$u_2 = x_{n\in w}^2+\mu\left|x_{n\in w}^1-x_{n\in w}^2\right| \tag{8}$$

15: **else**

$$x_{n\in w}^1 = x_{n\in w}^2 \tag{9}$$

16: **end if**

17: **if** $r<0.5$, **then**

18: $x_{n\in w} = x_{bs}+rMR+r\left(x_{bs}-x_{a1}\right)$ (10)

19: **else**

$$x_{n\in w} = x_{md}+rMR+r\left(x_{bs}-x_{md}\right)$$

20: **end if**

21: $x_{md}=\phi x_{avg}+\left(1-\phi\right)\left(\phi x_{bt}+\left(1-\phi\right)x_{bs}\right)$

22: $x_{avg}=a_1+a_2+a_3$ ▷ where $\phi\in(0,1)$ is a random number

23: **if** $f\left(x_{n\in w}^1\right)=f\left(x_{n\in w}^2\right)$ **then**

24: $x=x_{n\in w}$

25: Update x_{bs}

26: **end if**

27: **end for**

validators and initiators. In a specific case, the validator turns into a miner based on how many stakes it has. Therefore, the DPoS consensus protocol is adopted in this work [49]. Miners hash all of the recently generated blocks and digitally sign them. In the blockchain, the signed block is contained as a transaction. Over the network, the validators disseminate confirmation messages for blocks. Prior to the creation of any block in the blockchain, the miners are in charge of making this determination. Upon receiving the blocks from a miner, validators have to confirm their authenticity by contrasting the signatures on each block with those that have previously been stored in the blockchain. A new block is formed when the miner obtains a sufficient number of confirmation messages from the validators, provided that the number of valid messages exceeds the number of invalid messages. The most recent block is also appended to the end of the blockchain in chronological order. The nonce, the previous hash value, the current hash value, and the address of the data block make up each blockchain's block, as shown in Figure 1. The data block, nonce, and hash value from the previous block are used by the IoT devices create a new hash value of the cur-rent block. Each IoT device has a memory address to store all blockchain transactions and a wallet address to store cryptocurrency. In our proposed system, DPoS overcome the activities of malicious nodes by maintaining network security and integrity via frequent voting of delegate and delegation change. This help to checkmate the activities of malicious node in the system. Furthermore, In DPoS consensus protocol, IoT devices select delegate to vote on behalf of those who chosen them and the delegate is dismissed if it under-performed. The delegate is given the opportunity to elect validators to propagate new blocks. It means that computational power required to mine or create new blocks is drastically minimized [49]. In the process of selecting delegates, reputation of delegates is considered rather than depending on their stakes alone. Note that every IoT device is assigned a node in the blockchain, which implies that each node has distinct reputation status. To this end, the number of nodes that vote changes accordingly. At the start of each election, the credibility status of node is calculated as follows:

$$S = \frac{NV}{RS}\alpha, \tag{11}$$

where NV is the number of votes, $RS \in Z^+$ is the reputation score, which can be calculated using page ranking [50], direct or indirect trust computation, etc., and $\alpha \in [0,1]$ is the degree of honesty. If $\alpha \geq 0.5$, then node behaves honestly and can be selected as delegate provided it has more stakes; otherwise, the node is dishonest. Equation (11) is sorted in ascending order to determine whose node will be selected first as delegate.

The federated learning layer consists of central server and federated clients. Federated learning is designed based on the principle of training machine learning models over a decentralized servers or devices holding local data without disclosing sensitive information. This addresses the concerns of security and privacy. In Figure 1, federated clients (*i.e.*, IoT devices) train local data using the consensus

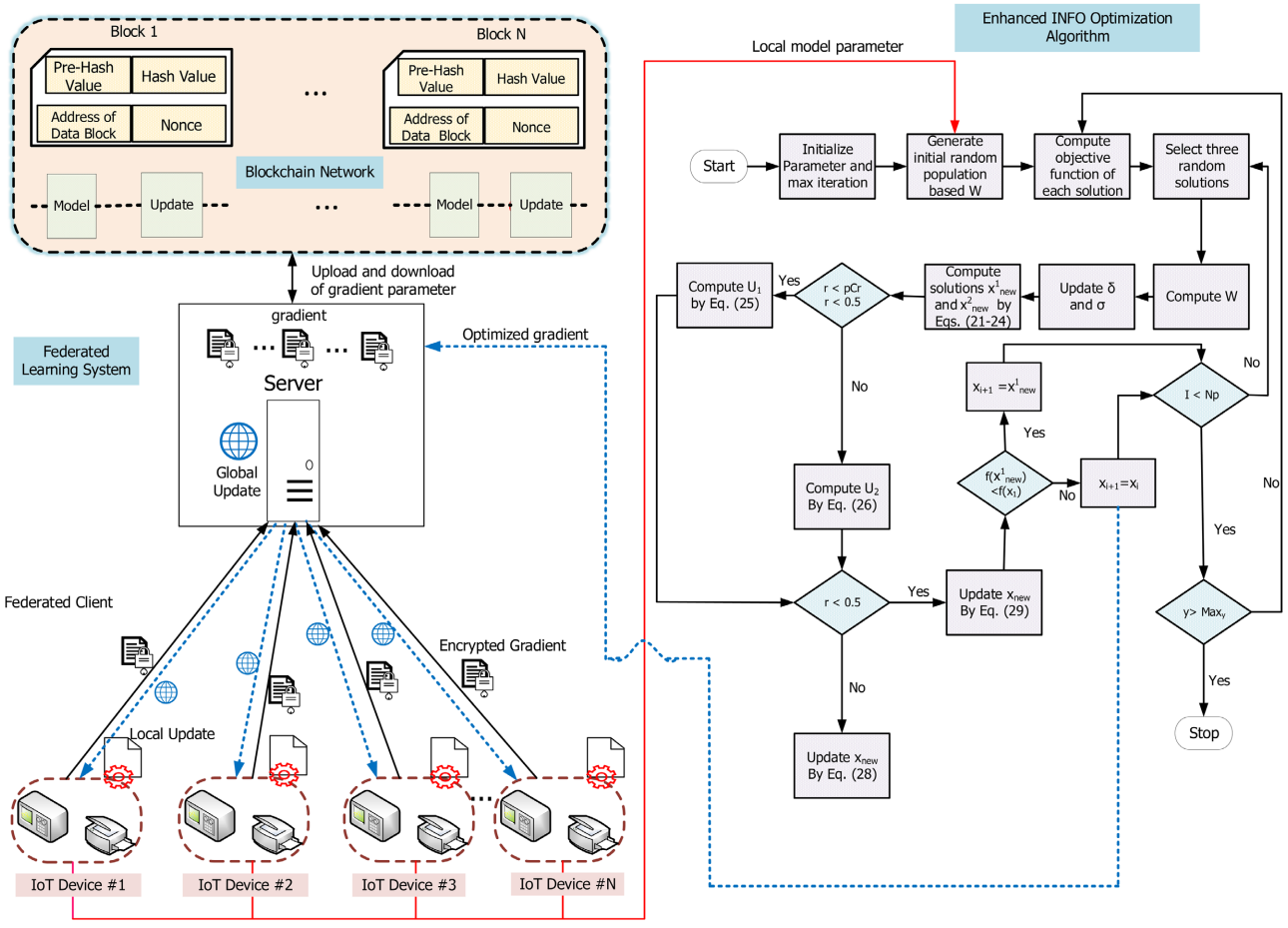

Figure 1. The proposed blockchain-based federated learning for IoT environment.

machine learning model, e.g., CNN, to train local data. Local model training and updates are carried out in the federate client, and the local model is transmitted to the server while the proposed optimization algorithm is used to optimize the global gradient parameter. Using the Paillier encryption, encrypted model and gradient parameters are uploaded and downloaded to the block-chain by the server. The server receives the model parameters and processes them further. Global gradient updates and aggregate model parameters are sent to the federated clients from the federated server side. In a federated learning system, federated averaging, named FedAvg, is a common strategy that sends the updated global model to devices for their local model update after updating the global model by averaging local models [9] [51]. However, FedAvg may diverge in real-world scenarios, particularly when the data is not uniformly distributed across devices and the quantity of data samples differs noticeably between devices. It is because the average-based global model is not always superior to local models in the early stages of the training process. Moreover, there are variants of FedAvg such as theoretical guarantee, momentum method for clients, adaptive FedAvg, lazy and quantized gradient, etc. [52]. Unlike the work in [53] that excludes the central server from federated learning in a peer-to-peer environment, this study solves

the problem of FedAvg by proposing an enhanced weIghted meaN oF vectOrs, named EINFO, for optimizing gradients collected from devices during local model training. Note that EINFO is derived from the study in [54] [55]. The proposed EINFO optimization algorithm addresses the problems of balancing exploration and exploitation found in most optimization algorithms. Let the vector $x=\{x_1,x_2,\cdots,x_N\}$, and we consider the case of decentralized federated learning with momentum where client $n\in N$ holds the appropriate copy of parameters $x_n\in R^d$ and compute the unbiased estimate of $f(x)$, which is defined as [52]

$$f(x)=\min_{x\in R^d}\frac{1}{n}\sum_{n=1}^{N}f_n(x);\ f_n(x)=E_{\xi\sim D_n}F_n(x,\xi), \tag{12}$$

where D_n is the data distribution of the n^{th} client and $F_n(x,\xi)$ is the loss function associated with the training data ξ. The client n updates its local parameters $x(n)$ as the weighted average of its neighbors: $\tilde{x}(n)=\sum_{l=1}^{N}w_l x(l)$ where N is the number of clients. The client updates its parameters as $x(n)=\tilde{x}-\eta g(n)$, where learning rate $\eta>0$ and $g(n)$ is the global gradient vector. For simplicity, at every $t\in Z^+$ iteration, each client computes

$$x^{t+1}(n)=\sum_{n=1}^{N}w_n\left[x^t(n)-\eta g^t(n)\right], \tag{13}$$

where $\sum_{n=1}^{N}w_n=1$. We optimize Equation (13) using the proposed EINFO optimization algorithm, and the weighted mean WM is calculated as [54].

$$WM=\frac{\sum_{n=1}^{N}\left(x_n-x_{n+1}\right)^2 w_n}{4\pi\left(x_{ws}-x_{bs}\right)^2\sum_{n=1}^{N}w_n}, \tag{14}$$

where $w=\cos\left(f(x_n)+f(x_{n+1})\pi\right)\exp\left(-\frac{x^2}{\omega}\right)$, which is calculated based on wavelet function, and during the optimization process, wavelet function is used to produce noticeable fluctuations. ω is a constant number called the dilation parameter, and $f(x)$ is the fitness function. In the proposed EINFO algorithm, the weighted mean vector for the search space is calculated while the population is generated based on a set of vectors that describe the possible solutions. Besides, the proposed EINFO is described in the following stages:

3.1. Population Initialization Stage

The proposed EINFO optimization algorithm consists of a population of x vectors in N dimensional search space and a k number of decision variables, which corresponds to the number of clients in the federated learning. The random population is defined as follows:

$$x=\min(x)+\left(\max(x)-\min(x)\right)\times r, \tag{15}$$

where $\min(x)$ and $\max(x)$ are the lower and upper bounds of the population, $r\in[0,1]$ is a random number, and there are two control parameters: weighted mean factor $\delta=(2\beta r-\beta)$ where $\beta=c\exp\left(-d\frac{y}{max_y}\right)$, r is a random value,

max_y is the maximum number of generations, and scaling factor σ. The control parameters are employed to amplify the obtained vector through an updating rule that depends on the size of the search space. Moreover, the control parameters can be tuned dynamically on the basis of population generation.

3.2. Updating Rule Stage

In this stage, a new vector is created using the updating rules. The updating rules increase population diversity during the search procedure. We modified the mean-based rule of [54] using the inverse square law. The mean-based rule is derived from the weighted mean of the random vectors, where it begins with the initial population and moves to the next solution using the weighted mean information. Moreover, the updating rule accelerates the convergence rate, which helps reach the optimum solution and improves the algorithm's performance. The mean-based rule is designed on the basis of the best x_{bs}, better x_{bt}, and worst x_{ws} solutions. The mean-based rule is defined as follows:

$$MR = rWM_1 + (1-r)WM_2, \tag{16}$$

where $r \in [0, 0.5]$ is a random value.

$$WM_1 = \delta \frac{w_1 (x_{a1} - x_{a2})^2 + w_2 (x_{a1} - x_{a3})^2 + w_3 (x_{a2} - x_{a3})^2}{\left(4\pi (x_{ws} - x)^2\right)(w_1 + w_2 + w_3) + \epsilon} + \epsilon r, \tag{17}$$

where ϵ is a constant with small values and $f(x)$ is the fitness function such that $a_1 \neq a_2 \neq a_3$

$$w_1 = \cos\left(\left(f(x_{a1}) - f(x_{a2})\right) + \pi\right) \exp\left(-\frac{f(x_{a1}) - f(x_{a2})}{\omega}\right) \tag{18}$$

$$w_2 = \cos\left(\left(f(x_{a1}) - f(x_{a3})\right) + \pi\right) \exp\left(-\frac{f(x_{a1}) - f(x_{a3})}{\omega}\right) \tag{19}$$

$$w_3 = \cos\left(\left(f(x_{a2}) - f(x_{a3})\right) + \pi\right) \exp\left(-\frac{f(x_{a2}) - f(x_{a3})}{\omega}\right) \tag{20}$$

$$\omega = \max\left(f(x_{a1}), f(x_{a2}), f(x_{a3})\right). \tag{21}$$

$$WM_2 = \delta \frac{w_1 (x_{bs} - x_{bt})^2 + w_2 (x_{bs} - x_{ws})^2 + w_3 (x_{bt} - x_{ws})^2}{\left(4\pi (x_{ws} - x)^2\right)(w_1 + w_2 + w_3) + \epsilon} + \epsilon r, \tag{22}$$

where

$$w_1 = \cos\left(\left(f(x_{bs}) - f(x_{bt})\right) + \pi\right) \exp\left(-\frac{f(x_{bs}) - f(x_{bt})}{\omega}\right) \tag{23}$$

$$w_2 = \cos\left(\left(f(x_{bs}) - f(x_{ws})\right) + \pi\right) \exp\left(-\frac{f(x_{bs}) - f(x_{ws})}{\omega}\right) \tag{24}$$

$$w_3 = \cos\left(\left(f(x_{bt}) - f(x_{ws})\right) + \pi\right) \exp\left(-\frac{f(x_{bt}) - f(x_{ws})}{\omega}\right) \tag{25}$$

$$\omega = \max\left(f\left(x_{bs}\right), f\left(x_{bt}\right), f\left(x_{ws}\right)\right). \tag{26}$$

This study adds convergence acceleration to the updating rules of the proposed EINFO optimization algorithm to enhance global search capability via the best solutions. The convergence acceleration is defined as follows:

$$CA = r\frac{x_{bs} - x_{a1}}{\left(f\left(x_{bs}\right) - f\left(x_{a1}\right)\right) + \epsilon} \tag{27}$$

Therefore, the new vector $x_{n\in w}$ is defined as:

$$x_{n\in w} = g\left(x\right) + \sigma MR + CA. \tag{28}$$

4. Simulation Result

This section evaluates the performance of the proposed EINFO optimization algorithm and compares its performance with the existing INFO algorithm [54]. We consider the population size N_p of 30 and the maximum iteration max_y of 500. The values of other parameters used in this study are given in Table 2. Initially, the study explores Griewank's function as an optimization to evaluate the algorithms. Moreover, other optimization objective functions are considered in the evaluations. The proposed system is implemented using Python 3.10 with 8 GB RAM and processor capacity of 1.60 GH.

Table 2. The list of parameters and variables used in this paper.

Variable/parameter	Meaning	Value
NV	Number of voters	30
RS	Reputation score	[0, 1]
a	Degree of honesty	[0, 1]
c	Constant number	2
d	Constant number	4
N_p	Maximum population	30
Max_y	Number of iterations	500
N	Number of clients	1000

4.1. Evaluation of the Objective Function

Table 3 shows the performance of the proposed EINFO. The table shows that the best cost and execution time of the algorithm are used to evaluate performance. After around 30 iterations, the proposed EINFO exhibits the smallest optimal cost and surpasses the current approach in terms of average objective function values. The proposed EINFO's performance shows that the algorithm is capable of doing appropriate exploration and search. Additionally, as Figure 2 illustrates, there is a suitable balance between exploration and exploitation, preventing early convergence. By utilizing the inverse square law of Equation (14), an improvement over

the work in [54], the updating rule enhances both local and global search. However, there is a tradeoff between best cost and execution, as presented in Table 3.

Table 3. Comparison of the proposed in terms of best cost and execution time.

Model	Best cost	Execution time (s)
INFO	7.8744e−54	3.1160
Proposed EINFO	4.3501e−05E	3.3649

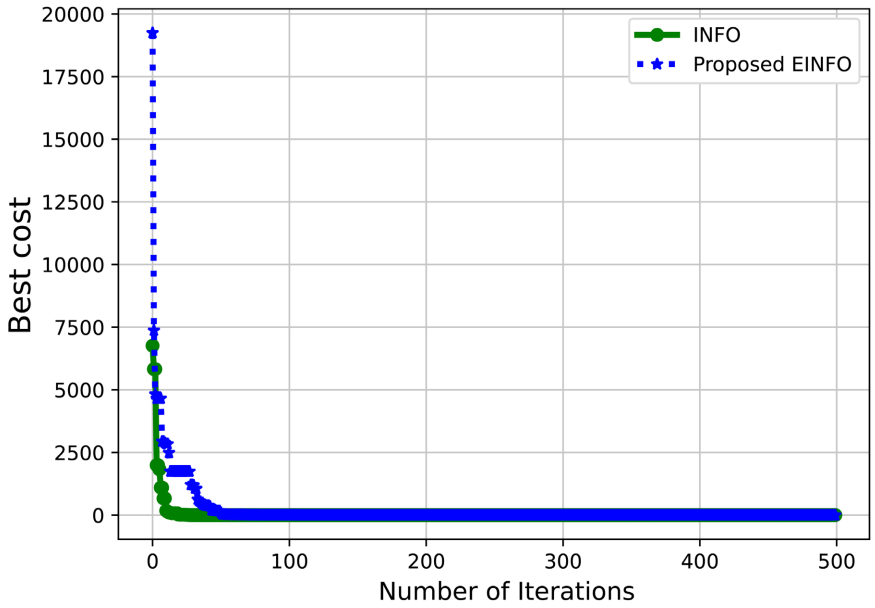

Figure 2. Evaluation based on convergence.

The convergence analysis presented in Figure 2 indicates that the proposed EINFO avoids premature convergence because it can search both locally and globally in solution space, finding solutions with a high density in the vicinity of the global optimal and a low density in the vicinity of the global optimal. It indicates that the proposed EINFO can effectively discover the optimal solutions by examining interesting regions in the search space that have the best cost.

4.2. Evaluation of the Proposed Federated Learning

Table 4 shows the performance of the proposed system in terms of accuracy, sensitivity, and specificity metrics. Specificity has a true negative rate and reveals more about the model than the accuracy metric, especially if the number of true positive and true negative instances is imbalanced. It is also similar to specificity [56]. This study compares the proposed model with multi-layer perception (MLP) [57], radial basis function neural network (RBFNN) [58], and extreme learning machine (ELM) [59].

In the table, it is observed that the proposed system model outperforms existing models in terms of accuracy, specificity, and sensitivity with higher values. The performance is achieved because of the optimized gradient parameter of the

model using the proposed EINFO optimization algorithm. Moreover, the binary classification of the model is enhanced.

Table 4. Comparison with other models.

Model	Accuracy	Sensitivity	Specificity
MLP	0.95	0.94	0.95
RBFNN	0.90	0.90	0.91
ELM	0.82	0.80	0.86
Proposed system (CNN)	0.96	0.97	0.96

4.3. Evaluation of Proposed Blockchain-based Federated Learning System

In the proposed system, there is a tendency that blockchain can be split into different states, which creates rooms for compromise, known as forks. It implies that there are disagreements among delegates. This type of scenario allows two or more delegates to solve a nonce of blockchain simultaneously [60]. The probability that a fork will happen follows a Poisson, which is as follows:

$$P_f = \alpha\left(\exp -\lambda\left(L-1\right)\gamma\right)+\left(1-\alpha\right)\exp\left(-\lambda\left(L-1\right)\right)\gamma, \tag{29}$$

where γ is block propagation delay and $L=\left[10,20,30\right]$ is the delegate; $\lambda=\left[0.01,0.1\right]$ is the expected time to generate blockchain, and α is the degree of honesty. The block propagation delay of the proposed blockchain-based federated learning is defined as:

$$\gamma = \frac{b_h + t_r bs}{\aleph}, \tag{30}$$

where $b_h = 200$ Kbits is the block header size, $t_r = 5$ Kbits is the transaction size, $b_s = 1000$ is the block height, and $\aleph = \left[1,5,20\right]$ Mbits is the capacity of the transmission link. As shown in **Figure 3**, we assume different values of $\lambda, \aleph$ and L. It is observed that the probability of fork creation slowly approaches zero for each value of λ and $\aleph$. It implies that a new block can be propagated if the value of $\alpha \geq 0$. Furthermore, only delegates with high reputation scores can mine and propagate new blocks. As the number of delegates increases, the probability of having a fork approaches zero, irrespective of the client's capacity for transmission

Using Equation (11), it is observed in **Figure 4** that the credibility status approaches one as the number of clients increases along with α. It implies that delegates have a high level of reputation. Furthermore, credibility status is directly proportional to reputation scores. Hence, the proposed DPoS consensus protocol is efficient in resolving the problem of in-discriminate propagation of new blocks.

In **Figure 5**, the evaluation of the proposed system model in terms of communication latency is shown for different numbers of clients. It is observed from the figure that P_f and γ are considered in computing the communication delay.

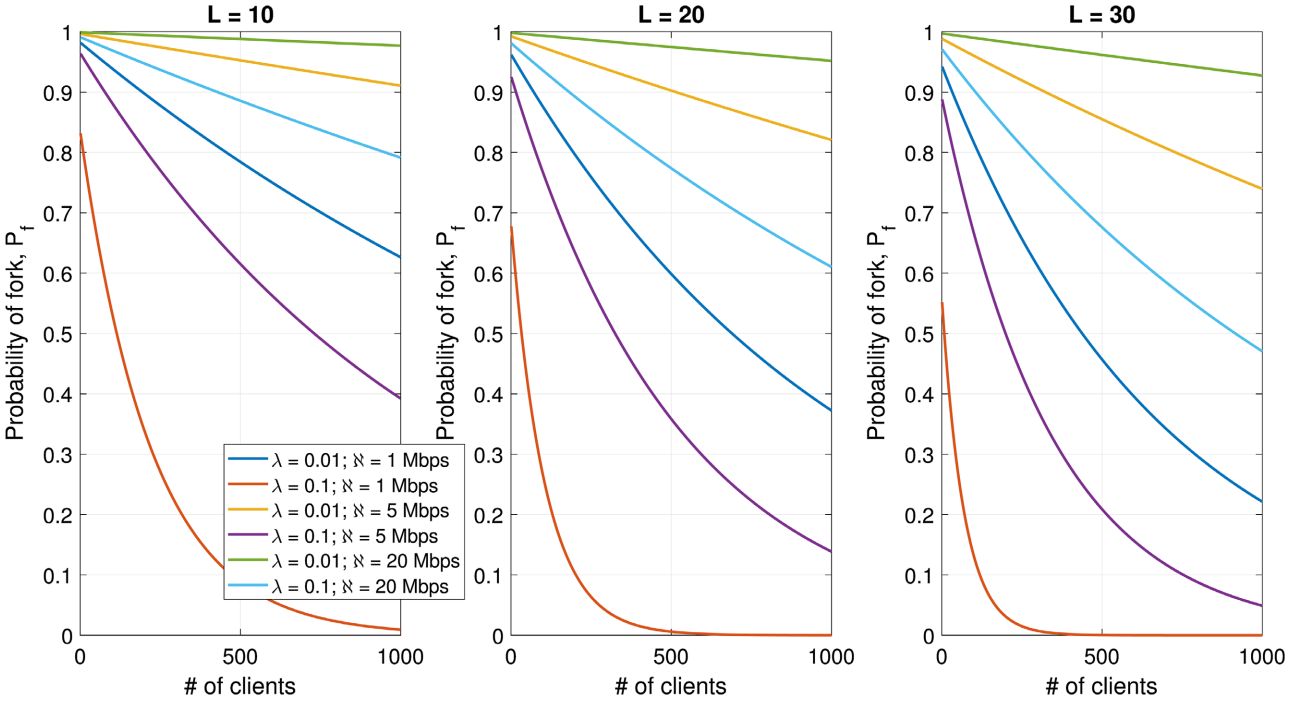

Figure 3. Evaluation of blockchain-based federated learning.

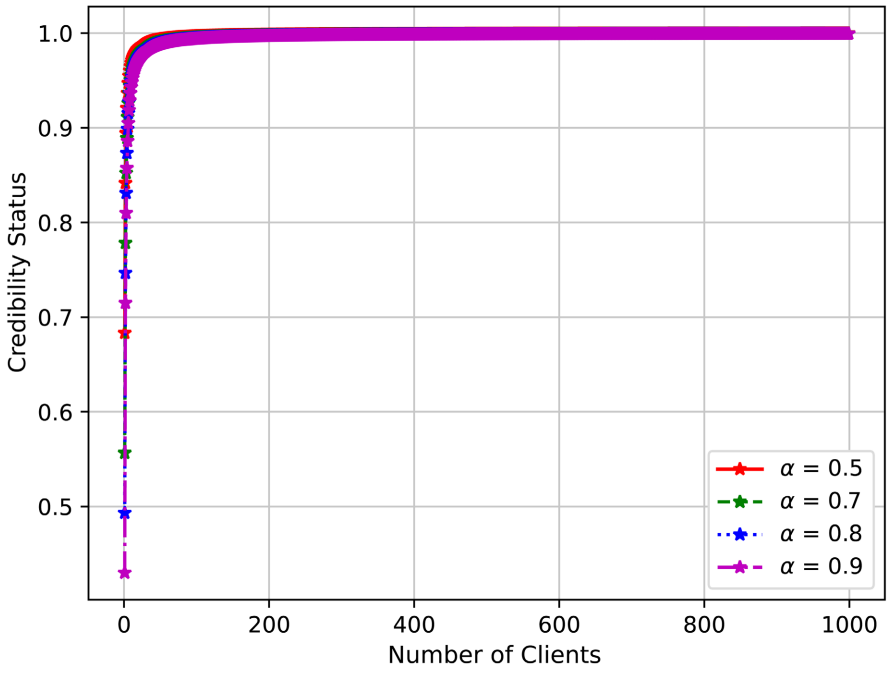

Figure 4. Evaluation of proposed delegated proof of stake.

We consider different communication delays (in percent) to analyze the proposed system. Besides, when the $N = 10$ and communication delay is 10% and above, the communication response time is minimal because fewer clients are used for both validators and delegates. It implies that communication delays among clients are minimized. Also, as N continues to increase, the proposed system achieves

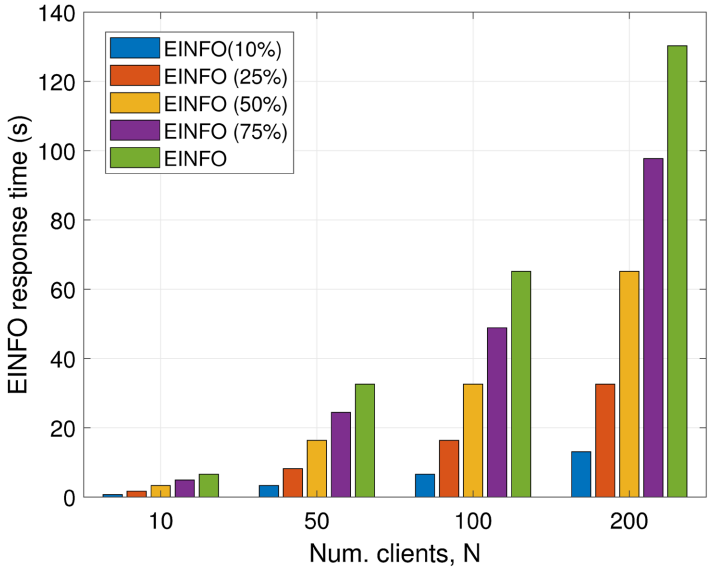

Figure 5. Evaluation of response time.

better response times for different values of communication delay. It shows the efficacy of the proposed system in terms of communication delay.

5. Conclusion

The paper proposes an enhanced weighted mean vector optimization algorithm, EINFO, in a blockchain-based federated learning system. The drawbacks of federated averaging during global update and model training—where data is not uniformly disseminated across devices and there are differences in the quantity of data samples—are tackled by the proposed EINFO. The EINFO algorithm maximizes the shared model parameters by employing a well-defined structure and updating the vector positions through local searching, vector combining, and updating rules. The weighted mean vector based on the inverse square law is used to create new vectors and enhance the model convergence rate to expand the exploration and exploitation capabilities. To choose validators, miners, and to propagate new blocks, a delegated proof of stake based on the reliability of blockchain nodes is suggested. Federated learning is included into the blockchain to protect nodes from both external and internal threats. To determine how well the suggested system performs in relation to current models in the literature, extensive simulations are run. The simulation results show that the proposed system outperforms existing schemes in terms of accuracy, sensitivity and specificity. In future, this study hopes to collaborate with relevant stakeholders for the real-time implementation of the proposed system model. Moreover, the proposed system did not discuss the communication model between the IoT devices as they exchange model update with the server, and also, privacy and security analysis will be carried out in future work to ascertain the proposed system model robustness against security and privacy related threats and attacks such as 51% attack, impersonation attack and transaction hacking. Similarly, as the blockchain became

incapacitated, we hope to use off-chain storage system such as IPFS to store data address instead of the real data; furthermore, convergence speed and computational complexity will be conducted in the future work.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Krishnamoorthy, S., Dua, A. and Gupta, S. (2021) Role of Emerging Technologies in Future IoT-Driven Healthcare 4.0 Technologies: A Survey, Current Challenges and Future Directions. *Journal of Ambient Intelligence and Humanized Computing*, **14**, 361-407. https://doi.org/10.1007/s12652-021-03302-w

[2] Fazel, E., Najafabadi, H.E., Rezaei, M. and Leung, H. (2023) Unlocking the Power of Mist Computing through Clustering Techniques in IoT Networks. *Internet of Things*, **22**, Article 100710. https://doi.org/10.1016/j.iot.2023.100710

[3] Rudrakar, S. and Rughani, P. (2023) IoT Based Agriculture (Ag-IoT): A Detailed Study on Architecture, Security and Forensics. *Information Processing in Agriculture*, In Press. https://doi.org/10.1016/j.inpa.2023.09.002

[4] Bi, Z., Jin, Y., Maropoulos, P., Zhang, W. and Wang, L. (2021) Internet of Things (IoT) and Big Data Analytics (BDA) for Digital Manufacturing (DM). *International Journal of Production Research*, **61**, 4004-4021. https://doi.org/10.1080/00207543.2021.1953181

[5] Shome, P.P., Khan, T., Kishk, A.A. and Antar, Y.M.M. (2023) Quad-Element MIMO Antenna System Using Half-Cut Miniaturized UWB Antenna for IoT-Based Smart Home Digital Entertainment Network. *IEEE Internet of Things Journal*, **10**, 17964-17976. https://doi.org/10.1109/jiot.2023.3280628

[6] Kumar, S.M., Selvi, J., Madhavan, B., Rajarajan, S. and Babu, C.N.K. (2023) Emotion-Enhanced Content Recommendation in IoT-Connected Entertainment Environments for Personalized Streaming Experiences. 2023 *Second International Conference on Smart Technologies for Smart Nation* (*SmartTechCon*), Singapore, 18-19 August 2023, 1244-1248. https://doi.org/10.1109/SmartTechCon57526.2023.10391471

[7] Ali, S., Li, Q. and Yousafzai, A. (2024) Blockchain and Federated Learning-Based Intrusion Detection Approaches for Edge-Enabled Industrial IoT Networks: A Survey. *Ad Hoc Networks*, **152**, Article 103320. https://doi.org/10.1016/j.adhoc.2023.103320

[8] Feng, Z. (2024) IoT Data Sharing Technology Based on Blockchain and Federated Learning Algorithms. *Intelligent Systems with Applications*, **22**, Article 200359. https://doi.org/10.1016/j.iswa.2024.200359

[9] Zhang, H., Wu, T., Cheng, S. and Liu, J. (2024) CC-FedAvg: Computationally Customized Federated Averaging. *IEEE Internet of Things Journal*, **11**, 4826-4841. https://doi.org/10.1109/jiot.2023.3300080

[10] Sun, N., Wang, W., Tong, Y. and Liu, K. (2023) Blockchain Based Federated Learning for Intrusion Detection for Internet of Things. *Frontiers of Computer Science*, **18**, Article No. 185328. https://doi.org/10.1007/s11704-023-3026-8

[11] Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B. and Avestimehr, A.S. (2022) Federated Learning for the Internet of Things: Applications, Challenges, and Opportunities. *IEEE Internet of Things Magazine*, **5**, 24-29.

https://doi.org/10.1109/iotm.004.2100182

[12] Neranjan Thilakarathne, N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Kumar Mahendran, R., *et al.* (2022) Federated Learning for Privacy-Preserved Medical Internet of Things. *Intelligent Automation & Soft Computing*, **33**, 157-172. https://doi.org/10.32604/iasc.2022.023763

[13] Huang, C., Xu, G., Chen, S., Zhou, W., Ng, E.Y.K. and de Albuquerque, V.H.C. (2022) An Improved Federated Learning Approach Enhanced Internet of Health Things Framework for Private Decentralized Distributed Data. *Information Sciences*, **614**, 138-152. https://doi.org/10.1016/j.ins.2022.10.011

[14] Wang, R., Lai, J., Zhang, Z., Li, X., Vijayakumar, P. and Karuppiah, M. (2023) Privacy-Preserving Federated Learning for Internet of Medical Things under Edge Computing. *IEEE Journal of Biomedical and Health Informatics*, **27**, 854-865. https://doi.org/10.1109/jbhi.2022.3157725

[15] Xu, Z., Guo, Y., Chakraborty, C., Hua, Q., Chen, S. and Yu, K. (2023) A Simple Federated Learning-Based Scheme for Security Enhancement over Internet of Medical Things. *IEEE Journal of Biomedical and Health Informatics*, **27**, 652-663. https://doi.org/10.1109/jbhi.2022.3187471

[16] Zhou, X., Ye, X., Wang, K.I., Liang, W., Nair, N.K.C., Shimizu, S., *et al.* (2023) Hierarchical Federated Learning with Social Context Clustering-Based Participant Selection for Internet of Medical Things Applications. *IEEE Transactions on Computational Social Systems*, **10**, 1742-1751. https://doi.org/10.1109/tcss.2023.3259431

[17] Rashid, M.M., Khan, S.U., Eusufzai, F., Redwan, M.A., Sabuj, S.R. and Elsharief, M. (2023) A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. *Network*, **3**, 158-179. https://doi.org/10.3390/network3010008

[18] Arikumar, K.S., Prathiba, S.B., Alazab, M., Gadekallu, T.R., Pandya, S., Khan, J.M., *et al.* (2022) FL-PMI: Federated Learning-Based Person Movement Identification through Wearable Devices in Smart Healthcare Systems. *Sensors*, **22**, Article 1377. https://doi.org/10.3390/s22041377

[19] Zhang, L., Xu, J., Vijayakumar, P., Sharma, P.K. and Ghosh, U. (2023) Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System. *IEEE Transactions on Network Science and Engineering*, **10**, 2864-2880. https://doi.org/10.1109/tnse.2022.3185327

[20] Qayyum, A., Ahmad, K., Ahsan, M.A., Al-Fuqaha, A. and Qadir, J. (2022) Collaborative Federated Learning for Healthcare: Multi-Modal COVID-19 Diagnosis at the Edge. *IEEE Open Journal of the Computer Society*, **3**, 172-184. https://doi.org/10.1109/ojcs.2022.3206407

[21] Sun, L. and Wu, J. (2023) A Scalable and Transferable Federated Learning System for Classifying Healthcare Sensor Data. *IEEE Journal of Biomedical and Health Informatics*, **27**, 866-877. https://doi.org/10.1109/jbhi.2022.3171402

[22] Wang, X., Wang, Y., Javaheri, Z., Almutairi, L., Moghadamnejad, N. and Younes, O.S. (2023) Federated Deep Learning for Anomaly Detection in the Internet of Things. *Computers and Electrical Engineering*, **108**, Article 108651. https://doi.org/10.1016/j.compeleceng.2023.108651

[23] Wahrstätter, A., Khan, S. and Svetinovic, D. (2024) OpenFL: A Scalable and Secure Decentralized Federated Learning System on the Ethereum Blockchain. *Internet of Things*, **26**, Article 101174. https://doi.org/10.1016/j.iot.2024.101174

[24] Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N. and Tari, Z. (2023) Blockchain-Based

Federated Learning for Securing Internet of Things: A Comprehensive Survey. *ACM Computing Surveys*, **55**, 1-43. https://doi.org/10.1145/3560816

[25] Singh, S., Rathore, S., Alfarraj, O., Tolba, A. and Yoon, B. (2022) A Framework for Privacy-Preservation of IoT Healthcare Data Using Federated Learning and Blockchain Technology. *Future Generation Computer Systems*, **129**, 380-388. https://doi.org/10.1016/j.future.2021.11.028

[26] Lian, Z., Wang, W., Han, Z. and Su, C. (2023) Blockchain-Based Personalized Federated Learning for Internet of Medical Things. *IEEE Transactions on Sustainable Computing*, **8**, 694-702. https://doi.org/10.1109/tsusc.2023.3279111

[27] Wang, P., Zhao, Y., Obaidat, M.S., Wei, Z., Qi, H., Lin, C., *et al.* (2022) Blockchain-Enhanced Federated Learning Market with Social Internet of Things. *IEEE Journal on Selected Areas in Communications*, **40**, 3405-3421. https://doi.org/10.1109/jsac.2022.3213314

[28] Farooq, K., Syed, H.J., Alqahtani, S.O., Nagmeldin, W., Ibrahim, A.O. and Gani, A. (2022) Blockchain Federated Learning for in-Home Health Monitoring. *Electronics*, **12**, Article 136. https://doi.org/10.3390/electronics12010136

[29] Kuliha, M. and Verma, S. (2024) Secure Internet of Medical Things Based Electronic Health Records Scheme in Trust Decentralized Loop Federated Learning Consensus Blockchain. *International Journal of Intelligent Networks*, **5**, 161-174. https://doi.org/10.1016/j.ijin.2024.03.001

[30] Baucas, M.J., Spachos, P. and Plataniotis, K.N. (2023) Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare. *IEEE Transactions on Computational Social Systems*, **10**, 1732-1741. https://doi.org/10.1109/tcss.2023.3235950

[31] Sezer, B.B., Turkmen, H. and Nuriyev, U. (2023) PPFchain: A Novel Framework Privacy-Preserving Blockchain-Based Federated Learning Method for Sensor Networks. *Internet of Things*, **22**, Article 100781. https://doi.org/10.1016/j.iot.2023.100781

[32] Alzubi, J.A., Alzubi, O.A., Singh, A. and Ramachandran, M. (2023) Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning. *IEEE Transactions on Industrial Informatics*, **19**, 1080-1087. https://doi.org/10.1109/tii.2022.3189170

[33] Wei, J., Zhu, Q., Li, Q., Nie, L., Shen, Z., Choo, K.R., *et al.* (2022) A Redactable Blockchain Framework for Secure Federated Learning in Industrial Internet of Things. *IEEE Internet of Things Journal*, **9**, 17901-17911. https://doi.org/10.1109/jiot.2022.3162499

[34] Prokop, K., Połap, D., Srivastava, G. and Lin, J.C. (2022) Blockchain-Based Federated Learning with Checksums to Increase Security in Internet of Things Solutions. *Journal of Ambient Intelligence and Humanized Computing*, **14**, 4685-4694. https://doi.org/10.1007/s12652-022-04372-0

[35] Ramani, R., Rosline Mary, A., Edwin Raja, S. and Arun Shunmugam, D. (2024) Optimized Data Management and Secured Federated Learning in the Internet of Medical Things (IoMT) with Blockchain Technology. *Biomedical Signal Processing and Control*, **93**, Article 106213. https://doi.org/10.1016/j.bspc.2024.106213

[36] Singh, S.P., Dhiman, G., Viriyasitavat, W. and Kautish, S. (2022) A Novel Multi-Objective Optimization Based Evolutionary Algorithm for Optimize the Services of Internet of Everything. *IEEE Access*, **10**, 106798-106811. https://doi.org/10.1109/access.2022.3209389

[37] Nematollahi, M., Ghaffari, A. and Mirzaei, A. (2023) Task Offloading in Internet of

Things Based on the Improved Multi-Objective Aquila Optimizer. *Signal, Image and Video Processing*, **18**, 545-552. https://doi.org/10.1007/s11760-023-02761-2

[38] Ramzanpoor, Y., Hosseini Shirvani, M. and Golsorkhtabaramiri, M. (2021) Multi-Objective Fault-Tolerant Optimization Algorithm for Deployment of IoT Applications on Fog Computing Infrastructure. *Complex & Intelligent Systems*, **8**, 361-392. https://doi.org/10.1007/s40747-021-00368-z

[39] Thenmozhi, R., Sakthivel, P. and Kulothungan, K. (2022) Hybrid Multi-Objective-Optimization Algorithm for Energy Efficient Priority-Based QoS Routing in IoT Networks. *Wireless Networks*. https://doi.org/10.1007/s11276-021-02848-z

[40] Younas, I. and Naeem, A. (2022) Optimization of Sensor Selection Problem in IoT Systems Using Opposition-Based Learning in Many-Objective Evolutionary Algorithms. *Computers & Electrical Engineering*, **97**, Article 107625. https://doi.org/10.1016/j.compeleceng.2021.107625

[41] Salimian, M., Ghobaei-Arani, M. and Shahidinejad, A. (2022) An Evolutionary Multi-Objective Optimization Technique to Deploy the IoT Services in Fog-Enabled Networks: An Autonomous Approach. *Applied Artificial Intelligence*, **36**, Article 2008149. https://doi.org/10.1080/08839514.2021.2008149

[42] Manocha, P.S. and Kumar, R. (2022) Improved Spider Monkey Optimization-Based Multi-Objective Software-Defined Networking Routing with Block Chain Technology for Internet of Things Security. *Concurrency and Computation: Practice and Experience*, **34**, e6861. https://doi.org/10.1002/cpe.6861

[43] Chen, Y., Lin, Q., Wei, W., Ji, J., Wong, K. and Coello, C.A.C. (2022) Intrusion Detection Using Multi-Objective Evolutionary Convolutional Neural Network for Internet of Things in Fog Computing. *Knowledge-Based Systems*, **244**, Article 108505. https://doi.org/10.1016/j.knosys.2022.108505

[44] Asgharzadeh, H., Ghaffari, A., Masdari, M. and Soleimanian Gharehchopogh, F. (2023) Anomaly-Based Intrusion Detection System in the Internet of Things Using a Convolutional Neural Network and Multi-Objective Enhanced Capuchin Search Algorithm. *Journal of Parallel and Distributed Computing*, **175**, 1-21. https://doi.org/10.1016/j.jpdc.2022.12.009

[45] Ouyang, M., Xi, J., Bai, W. and Li, K. (2022) Band-Area Application Container and Artificial Fish Swarm Algorithm for Multi-Objective Optimization in Internet-of-Things Cloud. *IEEE Access*, **10**, 16408-16423. https://doi.org/10.1109/access.2022.3150326

[46] Lakhan, A., Mohammed, M.A., Elhoseny, M., Alshehri, M.D. and Abdulkareem, K.H. (2022) Blockchain Multi-Objective Optimization Approach-Enabled Secure and Cost-Efficient Scheduling for the Internet of Medical Things (IoMT) in Fog-Cloud System. *Soft Computing*, **26**, 6429-6442. https://doi.org/10.1007/s00500-022-07167-9

[47] Cai, J., Fu, H. and Liu, Y. (2023) Multitask Multiobjective Deep Reinforcement Learning-Based Computation Offloading Method for Industrial Internet of Things. *IEEE Internet of Things Journal*, **10**, 1848-1859. https://doi.org/10.1109/jiot.2022.3209987

[48] Muazu, T., Yingchi, M., Muhammad, A.U., Ibrahim, M., Samuel, O. and Tiwari, P. (2024) IoMT: A Medical Resource Management System Using Edge Empowered Blockchain Federated Learning. *IEEE Transactions on Network and Service Management*, **21**, 517-534. https://doi.org/10.1109/tnsm.2023.3308331

[49] Hu, Q., Yan, B., Han, Y. and Yu, J. (2021) An Improved Delegated Proof of Stake Consensus Algorithm. *Procedia Computer Science*, **187**, 341-346. https://doi.org/10.1016/j.procs.2021.04.109

[50] Samuel, O., Javaid, N., Awais, M., Ahmed, Z., Imran, M. and Guizani, M. (2019) A Blockchain Model for Fair Data Sharing in Deregulated Smart Grids. 2019 *IEEE Global Communications Conference* (*GLOBECOM*), Waikoloa, 9-13 December 2019, 1-7. https://doi.org/10.1109/globecom38437.2019.9013372

[51] Nilsson, A., Smith, S., Ulm, G., Gustavsson, E. and Jirstrand, M. (2018) A Performance Evaluation of Federated Learning Algorithms. *Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning*, Rennes, 10-11 December 2018, 1-8. https://doi.org/10.1145/3286490.3286559

[52] Sun, T., Li, D. and Wang, B. (2023) Decentralized Federated Averaging. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **45**, 4289-4301. https://doi.org/10.1109/tpami.2022.3196503

[53] Xing, H., Simeone, O. and Bi, S. (2020) Decentralized Federated Learning via SGD over Wireless D2D Networks. 2020 *IEEE* 21*st International Workshop on Signal Processing Advances in Wireless Communications* (*SPAWC*), Atlanta, 26-29 May 2020, 1-5. https://doi.org/10.1109/spawc48557.2020.9154332

[54] Ahmadianfar, I., Heidari, A.A., Noshadian, S., Chen, H. and Gandomi, A.H. (2022) INFO: An Efficient Optimization Algorithm Based on Weighted Mean of Vectors. *Expert Systems with Applications*, **195**, Article 116516. https://doi.org/10.1016/j.eswa.2022.116516

[55] Merrouche, W., Lekouaghet, B., Bouguenna, E. and Himeur, Y. (2024) Parameter Estimation of ECM Model for Li-Ion Battery Using the Weighted Mean of Vectors Algorithm. *Journal of Energy Storage*, **76**, Article 109891. https://doi.org/10.1016/j.est.2023.109891

[56] Rainio, O., Teuho, J. and Klén, R. (2024) Evaluation Metrics and Statistical Tests for Machine Learning. *Scientific Reports*, **14**, Article No. 6086. https://doi.org/10.1038/s41598-024-56706-x

[57] Zhang, F., Zhang, Y., Ji, S. and Han, Z. (2024) Secure and Decentralized Federated Learning Framework with Non-IID Data Based on Blockchain. *Heliyon*, **10**, e27176. https://doi.org/10.1016/j.heliyon.2024.e27176

[58] Mostajeran, F. and Hosseini, S.M. (2023) Radial Basis Function Neural Network (RBFNN) Approximation of Cauchy Inverse Problems of the Laplace Equation. *Computers & Mathematics with Applications*, **141**, 129-144. https://doi.org/10.1016/j.camwa.2023.04.026

[59] Yu, Z., Liu, J., Yang, M., Cheng, Y., Hu, J. and Li, X. (2022) An Elderly Fall Detection Method Based on Federated Learning and Extreme Learning Machine (Fed-ELM). *IEEE Access*, **10**, 130816-130824. https://doi.org/10.1109/access.2022.3229044

[60] Wilhelmi, F., Giupponi, L. and Dini, P. (2021) Blockchain-Enabled Server-Less Federated Learning. arXiv:2112.07938.