Journal of Theoretical and Applied Information Technology

30th September 2023. Vol.101. No 18

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

DETECTION OF ANOMALIES IN BLOCKCHAIN USING FEDERATED LEARNING IN IOT DEVICES

SWAPNA SIDDAMSETTI[1], DR. MUKTEVI SRIVENKATESH [2]

[1]Research scholar, Department of Computer Science, GITAM Institute of Science, GITAM deemed to be University, Visakhapatnam and Assistant Professor, Department of Computer Science and Engineering, Neil Gogte Institute of Technology, Hyderabad, Telangana, India.

[2]Associate Professor, Department of Computer Science, GITAM Institute of science, GITAM deemed to be University, Visakhapatnam, Andhra Pradesh, India .

E-mail: [1]swapnangit2021@gmail.com

ABSTRACT

Botnet attacks now pose a substantial cyber security threat to the Internet of Things (IoT). Botnet classification systems that depend on these methodologies, like ordinary machine learning and deep learning, cannot be scaled. Based on federated learning (FL), researchers have created a classification approach for botnet attacks. This paper aims to solve the challenges of safeguarding user privacy while attaining acceptable classification performance. However, even a single, underperforming local model is included in each round's global model. In that case, the traditional FedAvg may produce an underperforming global model. FedAvg assigns equal weight to all local models when determining the average. This study develops dynamic weighted updating federated averaging (DWU-FedAvg) to overcome this problem. A system that dynamically modifies local model weights depending on client performance is needed to accomplish this goal. When the DWU-FedAvg is tested, it is compared to two well-known benchmark datasets, BotIoT and N-BaIoT. Both of these datasets are used in botnet attack classification studies. According to the results, our proposed model is scalable and capable of protecting user privacy while beating the classical FedAvg in terms of accuracy, with 98.4% for 15 rounds and 98.9% for 20 rounds for Botnet attack classification.

Keywords: *Privacy preservation, FedAvg, DWU-FesAvg, Federated Learning, Blockchain*

1.INTRODUCTION

Over the last ten years, internet users have been subjected to a barrage of attacks, the majority of which have taken the form of widespread email viruses and worms. Cybercriminals will become increasingly aware of its potential applications as more people get interested in machine learning and utilize it for security [1-3]. Among them botnet attack is very serious problem in Internet of Things (IoT) applications. Malicious adversaries can intentionally insert false training data into a machine learning model when constantly modified to account for new threats. This type of attack is known as a causal or data poisoning attack. This makes a machine learning (ML) model useless and exposes it to other attacks, leaving it vulnerable. Earlier works have revealed that Deep neural networks (DNN models can practice network traffic data to detect botnet attacks in IoT networks [4]. Data from each blockchain block must be sent to a centralized server to identify anomalies. This data must be collected and trained manually, which is time-consuming and labor-intensive. Furthermore, the model required new block data throughout the testing phase, which was challenging. As previously stated, hostile actors would intentionally input their data into a system incapable of detecting unexpected occurrences. Federated learning refers to a centralized education and training system. According to [5], federated learning is a centralized training approach that secures user privacy by using the user's unique data distribution features. Clients, also known as FL program participants, give the FL server training data based on their unique, locally stored datasets. This data might then be utilized to improve existing models. The FL server will then assemble all the updated local models and generate the global model for clients to download as shown in Figure 1.

In addition, FL is widely employed in real-world sectors [6-10]. However, FL excels and

demonstrates its efficacy in privacy preservation via design, optimal bandwidth, and reduced latency. On the other hand, FL is subject to several confidentiality and security constraints.

Fig. 1 Federated Learning Architecture

The FL model parameters aggregation approach makes the whole model dependent on the central FL server. When a central server fails, a distributed denial of service (DDoS) assault and a single point of failure (SPoF) occur. Furthermore, a visible method in the existing FL system for recording local model adjustments must be visual. As a result, to identify and prevent rogue updates, an effective decentralized system is necessary. As mentioned above, the threats may be mitigated by incorporating blockchain technology into FL platforms.

Blockchain and federated deep learning solves the potential poisoning and attack time-scale. This proposed model's most significant benefit is that training data can be decentralized. This increases training efficiency and overall performance. With the distributed ledger, we can securely, reliably, and transparently record machine learning model changes. Federated learning and blockchain technologies can help to identify trained collaborative machine learning models. Since blockchains prevent retractions, the federated learning system's high trustworthiness is increased. This research examines blockchain-based federated deep learning audibility. In classic FL, Federated Averaging (FedAvg) is used to build the global model at each round by combining all the local models received from all the FL participants. Since FedAvg equally benefits all local models when averaging. The classic FedAvg, on the other hand, has a drawback: if one poor-performing local model is considered in global model building for each round, it results in an underperforming global model. To address the concerns raised above, we present a dynamic weighted updating federated averaging (DWU-FedAvg) technique in which we dynamically change the weights for each local model depending on their performance at the client to classify attacks.

The following describe how the paper is structured: In part 2, we discuss the associated effort of detecting anomalies in blockchain models based on Federated Learning. Work proposed in Section 3. The results and discussion are covered in section 4. The paper is concluded in Section 5.

2.BACKGROUND AND RELATED WORK

The author of [11] suggested creating a trust-building system that could be used between the edge server and IoT devices, contending that trust should be taken into account at every stage of the decision-making process. This was done to ensure that the two could speak privately. While the local training is being provided, the trust mechanism will try to identify any Internet of Things devices that misuse or waste the available resources. As a next step in the development of this topic, the DDQN-Trust method, a selection technique based on double deep Q learning, was developed and introduced. When deciding how to schedule jobs, it takes into account both the current battery life and the reliability ratings of the various Internet of Things devices. In the end, they combined their method into four approaches to federated learning aggregation. FedAvg, FedProx, FedShare, and FedSGD are the names given to these methods. Our DDQN-Trust method consistently outperforms the DQN and random scheduling methods, which are acknowledged to be the two benchmarks that are the most important. This was demonstrated in

experiments using a real-world dataset.

However, this does not include supervision of the Federated Learning model or the computing process, as stated by the author of [12], who claims that the solution uses blockchain technology to monitor the original data and the outcomes of computations. Consequently, they proposed the ideas of a sandbox and a state channel to develop a new model for sharing private data that incorporates both Blockchain and Federated Learning. They linked Blockchain with Federated Learning to use state channels in their conceptualization. Additionally, the state channel is utilized in constructing a "trusted sandbox" to instantiate Federated Learning tasks within an environment devoid of trust. The simulation findings show that the presented approach is superior in terms of efficacy and efficiency to the one currently used to exchange data. In the meantime, their primary issue is the sharing of data in Federated Learning, particularly regarding its privacy, as well as the decline in system performance induced by poor data quality.

According to the author of [13], the Federated Learning Method is a game-changing technique that can enhance accuracy and precision compared to the previous method, which could not locate the best possible answers. This study offers Elliptical Curve Cryptography with Blockchain-based Federated Learning (ECC-BFL) to safeguard users' local gradients during federated learning. Blockchain is BFL, and Elliptical Curve Cryptography is ECC. Many factors must be considered, including transaction processing speed, classification precision, operation time, communication overhead, and computing overhead. ECC-BFL is compared to HC for Homomorphic Cryptosystems and MA-ABS for Multiple Authorities with Attribute-Based Signatures. These differences are shown in the table below.

In [14], the authors intended to fulfill the requirement of "running on untrusted domains" using blockchain technology as a reliable federated learning platform. The creator designed for this to be the outcome. They started by investigating issues that arise with vanilla federate learning. These issues include poor client motivation, clients quitting the project, model poisoning, model theft, and unauthorized access. As a result of these challenges, we were compelled to devise solutions in the form of building blocks, which included incentive mechanisms, reputation systems, peer-reviewed models, commitment hashes, and model encryptions. This was accomplished by using blockchain technology. Following the assessment findings, the recommended improvements contributed to an increase in the credibility of federated learning. In addition, the system that has been developed can motivate individuals to behave honestly and work hard to increase their chances of receiving higher rewards and penalize fraudulent activity. As a direct consequence, federated learning may now occur in settings where trust cannot be built initially.

In [15], the authors proposed a top-down blockchain-based federated learning architecture for collaborative IoT intrusion detection that is safe and privacy-preserving. They proved the need to exchange cyber threat knowledge across inter-organizational IoT networks to increase the detecting features of the model. The proposed ML-based intrusion detection system adheres to a hierarchical federated learning framework to secure the privacy of the learning process and organizational data. The transactions (model changes) and procedures will occur on a secure blockchain, and the smart contract will validate the completion of duties. They evaluated the practicality of the concept by building it and testing its attack detection efficiency using a critical IoT data set. The result is a securely constructed ML-based IDS that detects various suspicious practices while securing data privacy.

In[16] ,the authors proposed a federated learning method for IoT device anomaly detection. According on data from a collection of IoT devices, the author provided the FedGroup model and algorithms that would train and validate local models. Additionally, FedGroup calculates the average learning of each device rather than updating the learning of the central model based on the learning changes brought about by each group of IoT devices. Our empirical analysis of the actual IoT dataset shows that our FedGroup model has the same or superior capability and anomaly detection accuracy than federated and non-federated learning methods. Given that all of the IoT data are utilized to train and update the models locally, FedGroup is also more secure and works well.

To detect log data anomalies, suggested a model in [17]. Artificial intelligence learning is employed in sensitive information because it ensures the anonymity of the user data gathered and only gathers weights learned from each local server in the central server. In this paper, an

experiment on system log anomaly detection was carried out using federated learning. The results demonstrated the potential of using federated learning in deep learning-based system-log anomaly detection in contrast to the existing centralized learning approach. Additionally, the author offered a potent federated learning-based deep learning model for system log anomaly identification.

According to the author of [18], a high-accuracy algorithm for finding anomalies of power consumption data in distributed power systems has been developed using an Auto Encoder-based Federated Learning method that integrates the Auto Encoder and Federated Learning networks. The suggested approach enables decentralized training of anomaly detection models across IoT devices, speeding up response times and ultimately resolving the problem of data leaking. The experimental findings show how well the FLAE method works to identify abnormalities without the requirement for data transfer.

In[19], the authors developed a threat hunting system called Block Hunter using Federated Learning (FL) to automatically search for attacks in blockchain-based IIoT networks. In a federated context, Block Hunter uses a cluster-based architecture for anomaly detection together with a number of machine learning models. In IIoT networks, Block Hunter is the first federated threat hunting model that can spot unusual behavior while still protecting privacy. The outcomes demonstrated the effectiveness of the Block Hunter in identifying abnormal activities with high precision and minimal bandwidth used.

The authors[20] addressed the problem of anomaly detection in vehicle trajectories, and investigate the benefits of using federated learning. The author applied several state-of-the-art learning algorithms like one-class support vector machine (OCSVM) and isolation forest, thus solving a one-class classification problem. Based on these learning mechanisms, they successfully proposed and verified a federated architecture for the collaborative identification of anomalous trajectories at several intersections. Demonstrated that the federated approach is beneficial not only to improve the overall anomaly detection accuracy, but also for each individual data owner. The experiments show that federated learning allows to increase the anomaly detection accuracy from in average AUC-ROC scores of 97% by individual intersections up to 99% using cooperation.

In[21] the authors proposed a block-chain based federated learning algorithm for secured knowledge sharing with IP and privacy protection. Finally, depicted a complete design for a use case of this algorithm called Knowledge capital bank is demonstrated.

A trust-based Federated learning anomaly detection system was put forth by authors in [22]. The local data model was trained by the author using the edge nodes, and the machine learning parameters were uploaded to the central node. While this is going on, we establish various weights to correspond with each terminal's processing power based on the performance of edge nodes during training, which will result in a faster convergence rate and more accurate attack categorization. The risk of information disclosure can be decreased because the user's private information will only be processed locally and won't be uploaded to the main server. Finally, using the KDD Cup 99 dataset and the MNIST dataset, the author contrasted the fundamental federated learning model with the TFCNN method. The TFCNN algorithm can increase accuracy and communication efficiency, according to the testing results.

3. PROPOSED WORK: DYNAMIC WEIGHTED UPDATING FEDERATED AVERAGING (DWU-FEDAVG)

In the existing body of research, several studies have focused on the utilization of federated learning in various contexts and its applications in conjunction with blockchain. Yet, there remains a noticeable gap in the literature surrounding the optimal aggregation of local models in federated learning to enhance performance, especially in the context of botnet attack classification in IoT.

3.1. Gaps in Existing Literature:

The aggregation process in classic FL is often based on a simple average (FedAvg). Most existing models do not consider the quality or accuracy of individual local models during aggregation.Many studies have pointed towards the issue of single underperforming models degrading the performance of the global model. However, none have introduced a robust system to dynamically adjust the weightage of local models based on their performance.While a few studies have touched upon the trustworthiness of

nodes or devices in federated learning, there is limited exploration on integrating this trust factor directly into the model aggregation process.

3.2. Contribution of DWU-FedAvg:

To address these gaps, we introduce the DWU-FedAvg methodology. Our primary contributions are:

Dynamic Weight Assignment: Instead of treating all local models equally during the aggregation, our system dynamically assigns weights to each local model based on its individual performance. This ensures that higher-performing models have a larger influence on the global model, optimizing the model's accuracy.

Integration with Blockchain: We leverage the transparency and security features of blockchain to securely record the performance metrics of each local model. This ensures that the dynamic weighting process is tamper-proof and auditable.

Enhanced Botnet Attack Classification: Our system, when tested against established benchmarks, showcases superior performance in botnet attack classification in IoT systems, confirming its applicability in real-world scenarios.

3.3. Justification of Novelty:

The novelty of our approach lies in the dynamic weighting mechanism, which, to the best of our knowledge, has not been implemented in this context before. By effectively mitigating the influence of underperforming local models, we are able to produce a global model with enhanced accuracy. This addresses a significant challenge in federated learning and paves the way for more reliable IoT systems.

4.1. PROBLEM STATEMENT:

The exponential growth of the Internet of Things (IoT) devices has brought with it an equally substantial increase in botnet attacks, threatening the security of numerous interconnected devices and their associated networks. Existing research underscores the potential of Federated Learning (FL) as a viable solution for botnet attack classification in IoT. However, a salient challenge identified in the literature is the suboptimal aggregation of local models in FL, often culminating in compromised global model performance due to single or few underperforming local models. A closer examination of the existing literature reveals the conspicuous absence of methodologies that dynamically consider the quality or accuracy of individual local models during aggregation, especially in the context of botnet attack classification in IoT. Therefore, there is an impending need to design an efficient aggregation mechanism that dynamically adjusts weightage based on local model performances, ensuring improved accuracy of the global model for botnet attack classification.

4.2. Research Questions:

To address the gaps identified in the problem statement, this research seeks to answer the following pivotal questions:

RQ1: How can the accuracy of local models be effectively incorporated into the aggregation process in FL, ensuring that high-performing models significantly influence the global model?

RQ2: What are the potential benefits and implications of integrating blockchain with the federated learning model aggregation process, especially concerning the security, transparency, and accountability of dynamic weighting?

RQ3: How does the proposed Dynamic Weighted Updating Federated Averaging (DWU-FedAvg) methodology improve botnet attack classification in IoT systems in comparison to traditional Federated Averaging (FedAvg) methods?

RQ4: To what extent can DWU-FedAvg mitigate the impact of underperforming local models on the global model, and how does this influence the overall robustness and reliability of federated learning systems in IoT?

By elucidating answers to these research questions, we aim to develop a holistic understanding of the potential of DWU-FedAvg in enhancing the performance of federated learning systems, especially in the realm of botnet attack classification for IoT.

5. PROPOSED MODEL

In this section, we go through the characteristics of IoT network traffic, the Federated deep learning with blockchain architecture, and the DWU-FedAvg algorithm that has been suggested for IoT device botnet attack detection.

By averaging (Federated Averaging, or FedAvg) all local models from participating clients, FL creates a global model for every round. The traditional FedAvg has a flaw: the global model may perform poorly if a local model with poor performance is used to create the global model for each round. FedAvg averages all local models alike, for this reason. We might use weighted averaging in this situation, which gives local models weights. Applying weights to local models necessitates a trial-and-error procedure, which has an impact on efficiency.

This study develops a dynamic weighted updating federated averaging (DWU-FedAvg) technique that dynamically adjusts local model weights depending on client performance to overcome this challenge. The global server calculates FedAvg using eq. (1).

$$w_u^g = \frac{1}{M_c}\sum_{1}^{M_c} w_{u-1,j}^k \qquad (1)$$

Later, the DWU-FedAvg is executed grounded on the eq. (2) at global server:

$$w_u^g = \frac{1}{M_c}\sum_{1}^{M_c} \alpha_j w_{u-1,j}^k \qquad (2)$$

Where w_u^g denotes the global model generated at time u, M_c is the total number of local models received at the global server, which also indicates the number of clients participating in the FL, $w_{u-1,j}^k$ is the local model received from all clients at time $u-1$, and α is the dynamic weights associated with each local model accepted. This article considers complete FedAvg and DWU-FedAvg customer involvement. The client's local model performance automatically adjusts the dynamic weight β. The global server assumes each local model has the same authority and precedence.

The global server generates the global precedence score matrix with local model weights. Based on local model performance, weights are updated dynamically. This condition governs dynamic weight alters:

Journal of Theoretical and Applied Information Technology
30th September 2023. Vol.101. No 18

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

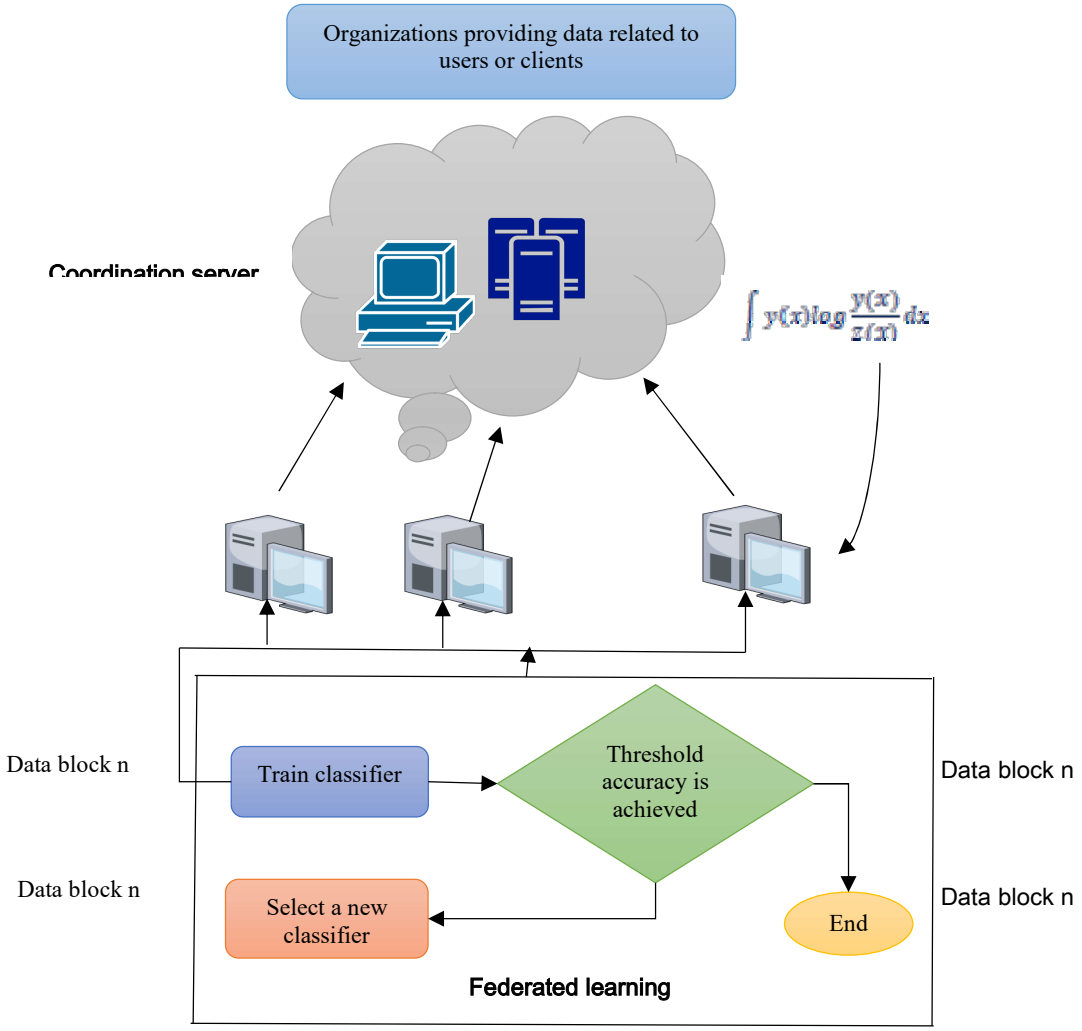

Figure 2: Working procedure Central FL framework

Initialize $\beta_{i,t} = \frac{1}{N_t}$
α= 0.2 (penalty factor)
$Acc_{pi} \leftarrow 0$ and $Acc_{pi} \leftarrow$ all local models test accuracy
If round ==1 then $Acc_{pi} = Acc_{ti}$
Else
If $Acc_{ti} \geq Acc_{pi}$ then $\beta_{t,i} = \beta_{t,i} + \beta_{t,i} * \alpha$
Else
If $Acc_{ti} < Acc_{pi}$ then $\beta_{t,i} = \beta_{t,i} - \beta_{t,i} * \alpha$
Else do nothing
Weight rescaling $\beta_{t,i} = \frac{\beta_{t,i}}{sum(\beta_{t,i})}$
Repeat until all rounds

We present the analysis results in two folds. The results of locally and globally conducted training are gathered and kept on the blockchain. After completing the pre-learning process and data collection in the local learning centers federated learning system, we added the data to the blockchain in fragmented blocks for local and global learning processes. Data is held in fragmented blocks on the blockchain and, if required, may be reconstructed into its original form to be available for use. The learning procedures that are either active or passive are used in this condition. A method known as differential entropy (DE) is applied to prepare the data stored in the central federated learning framework for usage in the global storage as shown in Figure 2.

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

Argument and proof: Data can be saved piecemeal using the DE technique, and ML algorithms can be applied to this data at the same time.

Consider $y(x)$ to be density sufficient $\int y(x)_{xx} dx = \sum_{xy}$
Also consider $y = M(0, \Sigma)$ (3)

$$0 \leq KI(y|z) = \int y(x) log \frac{y(x)}{z(x)} dx \quad (4)$$

$$= -l(y) - \int y(x) log z(x) = -l(y) - \int z(x) log z(x)$$

$$= -l(y) + l(z) \quad (5)$$

$$\int y(x) log \frac{y(x)}{z(x)} dx \quad (6)$$

To ensure long-term sustainability, we must address two significant issues: data security and the societal acceptability of the deep learning technique.

Step 1: The data obtained for the local client is verified before it is put into the relevant blockchain for the global model.

Step 2: This server's responsibilities include data collection, local learning algorithm execution, global learning data maintenance, data transmission to the general learning algorithm, and acting as a link between new and old client data local models.

Step 3: This process accesses the data generated by global learning in federated learning, also considered a type of local learning. This process occurs throughout the operation. In addition, a range of data privacy and security measures and powerful key encryption will be used.

Step 4: Phase 3 of the Global Model Update: The update method employs global learning while considering the previous phase's data structures and data gathered. Once the updating method has been completed, the information collected is distributed to all participants.

Description of the dataset:

Bot-IoT Data Set: This is a publicly available data collection [23] for cyber security research. It secures against four different botnet attack scenarios: reconnaissance, data theft, denial of service, and other potential threats and innocuous Internet of Things network traffic. A smart thermostat, a motion-activated lighting system, a remote-controlled garage door, a weather station, and an intelligent refrigerator were among the testbed components that generated the secure Internet of Things network traffic data.

N-BaIoT Data Set: This data collection [24] is available to the general public and used to assist with cyber security investigations. This data was gathered using an Internet of Things (IoT) test that includes a webcam, two doorbells, a thermostat, a baby monitor, and four security cameras. After the data collecting and feature extraction stages, it delves deeper into the approach and provides more details on these operations. This data collection includes the network behavior of trustworthy and malicious Internet of Things devices. Attacks such as ACK, Scan, and SYN attacks, as well as UDPP flooding assaults, may all be classified as examples of malicious traffic. We analyzed the activities of botnets that targeted industrial IoT devices using these statistical features.

6. RESULTS AND DISCUSSION

In this section, for experimental part PyTorch was used to develop my machine-learning model. PySyft is a Python package that allows for private and secure deep learning. PySyft was produced by the Syft development team. During our investigation, we used the Jupiter notebook. Scikit Learn was utilized in the evaluation of the classifiers. This evaluation evaluates the models' efficacy. The qualitative model's efficiency in true positives, false positives, and false negatives is evaluated. Precision, recall, and f1-score scores were computed. The "Accuracy" multi-class performance measure is used in this experiment to determine how well the real models are performed in terms of overall performance.

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \quad (7)$$

$$Re = \frac{TP}{TP + FN} \times 100\% \quad (8)$$

$$Pr = \frac{TP}{TP + FP} \times 100\% \quad (9)$$

$$F1 = \frac{2 \times (Pr \times Re)}{Pr + Re} \times 100\% \quad (10)$$

Effect of DL nodes with FL model

We take the distributed deep learning process that is taking place inside of a federated learning system and increase the number of nodes that are participating in it from two to twelve, and we continue the training for a total of fifty epochs. Since the effort will be shared, we anticipate that the total training time will be lowered. The neural network will also have less weight. The united effort should provide both outcomes. To get the same loss value on the test and train data will take more epochs. Fedlocal models will average weight changes. Figure 3 shows execution time and convergence epochs.

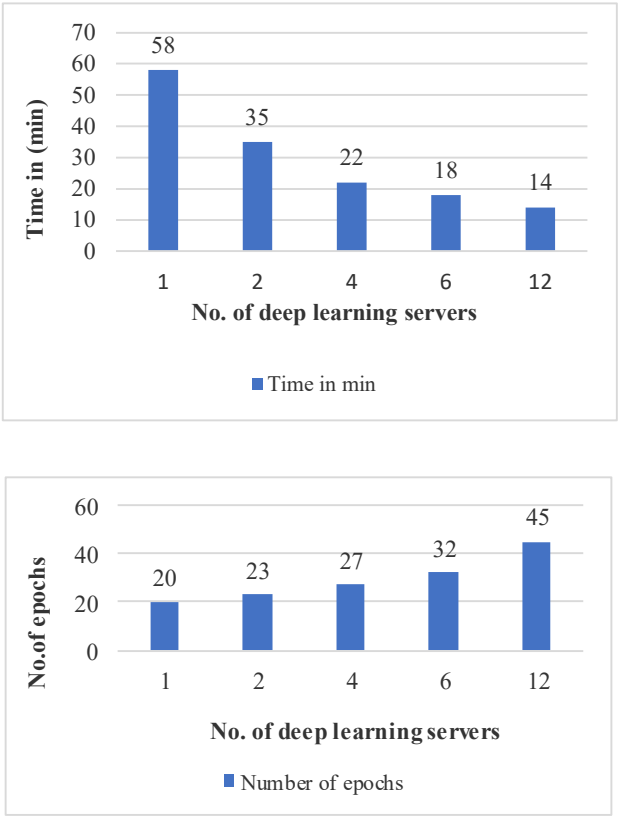

Figure 3: Federated Training On Botnet Data For Testing.

FL model with Blockchain Maintenance

The MultiChain blockchain not only stores the latest weight changes but so are the modified models. Blockchain technology can now be profited in two ways:

1. Weight updates are sent immediately from deep learning servers to parameter servers, which are processed as soon as they arrive.
2. A parameter server will execute only weight modifications that have been properly stored and confirmed on the blockchain.

In either case, clients who have acquired access to the deep learning system will deposit the most recent version of their weights on the blockchain. In the second case, however, the federated model averaging may face a substantial delay, especially if the parameter server waits for numerous block confirmations. This is true regardless of the time it takes to create a block, which in MultiChain is set to 15 seconds by default. The block building and confirmation delay are proportional to the true epoch time, which is over one minute for a deep-learning client.

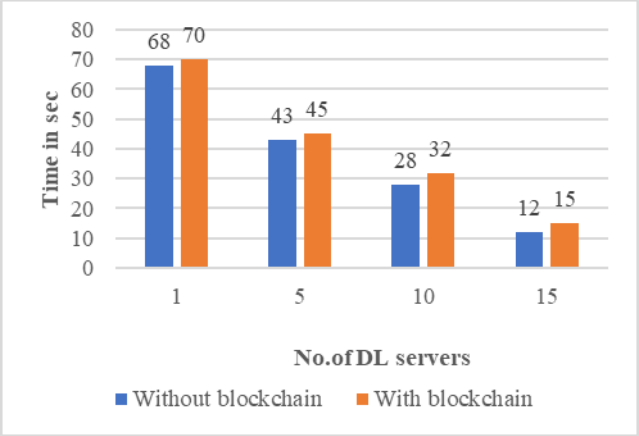

Figure 4: Comparison Of DL Server Performance With And Without Blockchain W.R.T Time

Table 1: Performance metrics of the global model for 15 rounds

Dataset	No.of clients	FedAvg				DWU-FedAvg			
		Accuracy	Precision	Recall	F1-score	Accuracy	Precision	Recall	F1-score
Bot-IoT	5	0.986	0.987	0.977	0.987	0.990	0.989	0.981	0.989
	10	0.978	0.974	0.968	0.974	0.985	0.979	0.974	0.982
N-BaIoT	5	0.987	0.987	0.965	0.968	0.989	0.990	0.975	0.978
	10	0.978	0.974	0.974	0.974	0.984	0.981	0.976	0.977

Table 2: Performance metrics of the global model for 25 rounds

Dataset	No.of clients	FedAvg				DWU-FedAvg			
		Accuracy	Precision	Recall	F1-score	Accuracy	Precision	Recall	F1-score
Bot-IoT	5	0.988	0.989	0.988	0.989	0.992	0.990	0.985	0.991
	10	0.981	0.977	0.971	0.976	0.988	0.983	0.977	0.985
N-BaIoT	5	0.989	0.989	0.969	0.972	0.991	0.992	0.978	0.981
	10	0.981	0.978	0.978	0.977	0.989	0.985	0.979	0.981

The delay has an impact. MultiChain's block confirmation time may be decreased to 2 seconds, and if no new weight updates are received, block formation can be postponed to minimize the chain's total number of blocks. Both of these features can reduce chain blocks. Reducing a chain's blocks is possible using one of these two methods.

1) In the first hypothetical circumstance, Figure 4 shows probable occurrences. The blockchain must be synced more frequently as nodes increase, but the rate must also increase proportionally. Therefore, the blockchain delays the operation very slightly. This delay will incur a processing penalty of 5% to 15% and considerable wait time. The parameter server will also update the distributed ledger model to reflect recent changes. The network will see little disruption as a consequence.

2) In the second situation, just one block confirmation is needed, but because blocks take so long to build and verify, delays are more evident due to increased block production time. When the target block duration was 15 seconds, it took 43 seconds to update a model. This happened with a 15-second goal block time. By decreasing the goal-blocking time to five seconds, we reduced this statistic to 13 seconds.

Analysis on global model

We summarize the experimental results for our proposed DWU-FedAvg in this section and contrast it with the traditional FedAvg [25] over a range of client numbers and round counts. For our investigation, we looked into a total of 2 distinct

client scenarios (5 and 10) with varied rounds. All of the performance indicators for the global model are shown in Tables 1 and 2. Tables 1 and 2 demonstrate that, for 15 rounds and 20 rounds, respectively, the proposed DWU-FedAvg model can beat the established FedAvg model in the current situation in terms of Recall, Precision, Accuracy, and F1-score. This is because the suggested strategy tends to learn and store the most recent values in the local memory, thus minimizing the loss of information of data. Moreover, the identification of specific attacks further enhances the overall accuracy of the presented approach.

7. COMPARISON WITH RELEVANT WORK AND DETAILED ANALYSIS

7.1. Comparison with Relevant Work:
Traditional Federated Learning (FedAvg):
Similarity: Both the traditional FedAvg and our proposed DWU-FedAvg adopt a federated learning paradigm, enabling model training across multiple devices or nodes without centralized data storage.
Difference: The traditional method provides uniform weightage to all nodes during model aggregation, while DWU-FedAvg adjusts weightage based on individual node performance. Furthermore, our integration of blockchain ensures security and transparency, a feature absent in the conventional approach.
Blockchain in Cybersecurity (Non-FL Applications):
Similarity: Other works have explored the use of blockchain for securing data transactions, emphasizing its decentralized and immutable nature.
Difference: Our work is distinct in its application of blockchain for federated learning, specifically for securing model aggregations and ensuring traceability of model updates.
Dynamic Weighted Approaches in Non-FL Domains:
Similarity: Dynamic weighting has been employed in other computational realms to optimize performance.
Difference: Our approach contextualizes dynamic weighting within the federated learning environment, ensuring that it caters specifically to the nuances of decentralized model training.

7.2. Detailed Analysis of DWU-FedAvg's Pros and Cons:
Pros:
Adaptive Model Aggregation: DWU-FedAvg's dynamic weighting allows for a more adaptive and performance-oriented model aggregation. This ensures that better-performing local models have a more significant influence on the global model, potentially improving global model accuracy.
Enhanced Security and Transparency: By integrating blockchain, every model update is recorded, ensuring traceability, transparency, and security against malicious actors.
Reduced Central Dependency: With weights being adjusted locally based on local performance, there is reduced dependency on a central entity for model optimization, promoting genuine decentralization.
Flexibility: The proposed method is flexible enough to be adapted to various IoT environments, with minor adjustments, making it versatile across different domains and applications.
Cons:
Computational Overhead: The dynamic weight calculation and the addition of blockchain can introduce computational overhead, potentially slowing down the training process.
Complexity in Implementation: Compared to traditional FedAvg, the DWU-FedAvg approach requires sophisticated mechanisms to evaluate local model performance and adjust weights dynamically.
Scalability Concerns: With the introduction of blockchain, scaling up to a massive number of nodes may introduce latency, especially if every model update is to be recorded as a separate transaction.
Risk of Over-reliance on Local Models: If a local model performs exceptionally well due to data peculiarities (and not genuine robustness), it might unduly influence the global model, leading to potential biases.

In summary, while our research introduces innovative methods to optimize federated learning's aggregation process and secure it using blockchain, there are challenges that warrant further investigation and optimization. The balance between the advantages and potential pitfalls emphasizes the need for continuous refinement and adaptation in real-world scenarios.

8.NOVELTY,PROFOUND INFORMATION AND BEST PRACTICES VERSUS INCREMENTAL KNOWLEDGE CREATION

8.1 Novelty and Profound Information:

The proposed DWU-FedAvg approach not only introduces a methodological innovation to federated learning but also sheds light on a profound understanding of its practical implications. Unlike traditional federated learning techniques which adopt a uniform approach towards model aggregation, DWU-FedAvg introduces a dynamic paradigm where the weightage of each local model is influenced by its individual performance.

Additionally, our exploration of blockchain's integration with federated learning offers profound insights into leveraging decentralized ledgers for security, transparency, and accountability in the model aggregation process. This novel proposition has potential ramifications beyond just botnet attack classification, laying the groundwork for a secure and trustable FL framework.

8.2. Best Practices:

Throughout our research, we have identified and incorporated several best practices:

Continuous Monitoring of Local Models: Regular evaluation of local model performances ensures timely adjustments in their respective weightage during aggregation, promoting a more robust global model.

Secure Transactions: Using blockchain technology, every model update is recorded as a transaction, ensuring complete transparency and tamper-proof records.

Validation and Verification: To avoid overfitting and ensure model generalizability, we propose periodic validation using diverse datasets and rigorous verification procedures.

8.3. Incremental Knowledge Creation:

While the primary focus of our research is on profound innovations, we recognize the importance of incremental knowledge contributions that can be significant in the broader context:

Fine-tuning of DWU-FedAvg: Our research contributes incremental insights into optimizing the weighting parameters, ensuring better performance consistency across diverse IoT setups.

Comparison Benchmarks: By juxtaposing DWU-FedAvg with traditional FedAvg methodologies, we offer incremental improvements in botnet attack classification rates.

Enhanced Security Protocols: Building upon existing blockchain mechanisms, we present iterative enhancements that better align with the peculiarities of federated learning environments.

In conclusion, while our research champions profound knowledge creation in federated learning's aggregation methodologies and the introduction of blockchain, it also acknowledges the value of smaller, incremental steps that build upon existing knowledge. Both these aspects combined foster a comprehensive, multi-dimensional contribution to the realm of IoT security and federated learning.

9. CONCLUSIONS AND FUTURE RESEARCH AVENUES

This paper applied federated deep learning to permissioned blockchains to see how it might work. It examined deep learning. During our work on federated learning, we utilized a DWU-FedAvg model for anomaly-based botnet detection, a dataset based on real-world intrusion detection, and MultiChain to build an immutable audit trail. Partly attributed, this methodology was developed as a result of this study to detect damaging activity in edge devices of the Internet of Things. It was evident that the proposed DWU-FedAvg model outperformed the classical FedAvg model in terms of recall of 97.6%, precision of 98.1%, accuracy of 98.4%, and f1-score of 97.7% for 15 rounds and recall of 97.9%, precision of 98.5%, accuracy of 98.9%, and f1-score of 98.1% 20 rounds respectively. The result may be partly attributed to each of the three major factors. The proposed model made use of data from both Bot-IoT and N-BaIoT. The classification was done with the help of this model, which considers all the data.Our study presented a pioneering approach to federated learning, DWU-FedAvg, that capitalizes on dynamic weighting for model aggregation and integrates blockchain for enhanced security and traceability. The findings have emphasized both the promise and the challenges inherent in our method, offering a nuanced understanding of its applicability and implications in decentralized learning environments.

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

10. GAPS AND UNATTENDED ISSUES IN THE STUDY:

10.1Granularity of Dynamic Weighting: While our method takes into account the performance of local models, the exact metrics and thresholds for weight adjustments weren't deeply explored. How granular should these adjustments be? And what performance metrics beyond accuracy might be relevant?

Blockchain Efficiency: Our incorporation of blockchain for security, while innovative, didn't deeply explore the scalability and efficiency issues that might arise in massive-scale federated environments.

Heterogeneity of Local Models: The study was based on the assumption of moderate heterogeneity among local models. However, in extremely diverse environments, the dynamics of weight adjustments might be different.

Real-world Application Scenarios: Our research was largely experimental and may not account for the complexities of real-world data distributions and IoT environments.

10.2. Open Research Issues:

Advanced Dynamic Weighting Mechanisms: There's a need to investigate more sophisticated mechanisms for dynamic weighting that consider various parameters beyond just model performance, such as the age of the data, volume of data, etc.

Blockchain Alternatives: Are there more efficient alternatives to blockchain that can offer similar levels of security and traceability, especially in scenarios where rapid model updates are needed?

Bias and Fairness in Federated Learning: As dynamic weighting gives more influence to certain local models, how does this impact the fairness of the global model? Is there a risk of systematic biases, and how can they be mitigated?

Robustness against Adversarial Attacks: With the decentralized nature of federated learning, the system is open to adversarial attacks on local models. Investigating the robustness of DWU-FedAvg against such attacks is crucial.

Incorporating Domain Knowledge: Future research can explore how domain-specific knowledge can be integrated into the weight adjustment process, making the aggregation more context-aware.

To conclude, while DWU-FedAvg stands as a promising step forward in optimizing federated learning, there remain uncharted territories and unattended gaps that offer fertile ground for future research. Addressing these will pave the way for more efficient, fair, and robust decentralized learning systems.

11. CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

REFERENCES

[1] Zhang, Tingqi & Sun, Mingyang & Cremer, Jochen & Zhang, Ning & Strbac, G. & Kang, Chongqing,(2021). A Confidence-Aware Machine Learning Framework for Dynamic Security Assessment. IEEE Transactions on Power Systems. 10.1109/TPWRS.2021.3059197.

[2] Nadeem, Azqa & Vos, Daniël & Cao, Clinton & Pajola, Luca & Dieck, Simon & Baumgartner, Robert & Verwer, Sicco. (2022). SoK: Explainable Machine Learning for Computer Security Applications. 10.48550/arXiv.2208.10605.

[3] Zhang, L. & Cui, Y. & Liu, J. & Jiang, Y. & Wu, J.-P. (2018). Application of Machine Learning in Cyberspace Security Research. Jisuanji Xuebao/Chinese Journal of Computers. 41. 1943-1975. 10.11897/SP.J.1016.2018.01943.

[4] Popoola, Segun & Adebisi, Bamidele & Gui, Guan & Hammoudeh, Mohammad & Gacanin, Haris & Dancey, Darren. (2022). Optimizing Deep Learning Model Hyperparameters for Botnet Attack Detection in IoT Networks. 10.36227/techrxiv.19501885.

[5] McMahan B, Moore E, Ramage D, Hampson S, Arcas BAy (2017) Communication-efficient learning of deep networks from decentralized data. In: Singh A, Zhu J (eds) Proceedings of the 20th international conference on artificial intelligence and statistics, vol 54 of Proceedings of machine learning research, pp 1273–1282. PMLR, 20–22 Apr 2017. https://proceedings.mlr.press/v54/mcmahan17a.html.

[6] Zheng Z, Zhou Y, Sun Y, Wang Z, Liu B, Li K (2021) Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges. Connect Sci. https://doi.org/10.1080/09540091.2021.1936455.

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

[7] Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F (2020) Federated learning for healthcare informatics. J Healthc Inform Res 5(1):1–19.

[8] Chen Y, Qin X, Wang J, Yu C, Gao W (2020) FedHealth: a federated transfer learning framework for wearable healthcare. IEEE Intell Syst 35(4):83–93. https://doi.org/10.1109/mis.2020.2988604.

[9] Long G, Tan Y, Jiang J, Zhang C (2020) Federated learning for open banking. In: Lecture Notes in Computer Science. Springer International Publishing, New York, pp 240–254. https://doi.org/10.1007/ 978-3-030-63076-8_17.

[10] Tan K, Bremner D, Kernec JL, Imran M (2020) Federated machine learning in vehicular networks: a summary of recent applications. In: 2020 international conference on UK-China Emerging Technologies (UCET). IEEE. https://doi.org/10.1109/ucet51115.2020.9205482.

[11] Rjoub, Gaith & Wahab, Omar & Bentahar, Jamal & Batineh, Ahmed. (2022). Trust-driven Reinforcement Selection Strategy for Federated Learning on IoT Devices. Computing. 10.1007/s00607-022-01078-1.

[12] Guo, Shaoyong & Zhang, Keqin & Gong, Bei & Chen, Liandong & Ren, Yinlin & Xuesong, Qiu. (2022). Sandbox Computing: A Data Privacy Trusted Sharing Paradigm via Blockchain and Federated Learning. IEEE Transactions on Computers. PP. 1-12. 10.1109/TC.2022.3180968.

[13] Arumugam, Sampathkumar & Shandilya, Shishir K & Bacanin, Nebojsa. (2022). Federated Learning-Based Privacy Preservation with Blockchain Assistance in IoT 5G Heterogeneous Networks. Journal of Web Engineering. 10.13052/jwe1540-9589.21414.

[14] Oktian, Yustus & Stanley, Brian & Lee, Sanggon. (2022). Building Trusted Federated Learning on Blockchain. Symmetry. 14. 1407. 10.3390/sym14071407.

[15] Sarhan, Mohanad & Lo, Wai Weng & Layeghy, Siamak & Portmann, Marius. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers and Electrical Engineering. 103. 108379. 10.1016/j.compeleceng.2022.108379.

[16] Yixuan Zhang, Basem Suleiman, Muhammad Johan Alibasa:FedGroup: A Federated Learning Approach for Anomaly Detection in IoT Environments(2023).

[17] Tae-Ho Shin and Soo-Hyung Kim :Utility Analysis about Log Data Anomaly Detection Based on Federated Learning(2023), https://doi.org/ 10.3390/app13074495.

[18] Kimleang KeaID, Youngsun Han, Tae-Kyung KimID:Enhancing anomaly detection in distributed power systems using autoencoder-based federated learning(2023), https://doi.org/10.1371/ journal.pone.0290337.

[19] Abbas Yazdinejad, Ali Dehghantanha, S,Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-based IIoT Networks(2022).

[20] Christian Koetsier , Jelena Fiosina , Jan N. Gremmel , Jörg P. Müller , David M. Woisetschläger , Monika Sester ¨Detection of anomalous vehicle trajectories using federated learning (2022), https://doi.org/10.1016/j.ophoto.2022.100013.

[21] Xi Chen , Bin Xiao , Qingzhen Xu , Chengyin g He , Jianwu Lin,:Block-chain based federated learning for knowledge capital(2021), https://doi.org/10.1016/j.procs.2021.04.080.

[22] Chen, Naiyuea , Jin, Yib, Li, Yinglongc , Cai, Luxina,:Trust-based federated learning for network anomaly detection(2021), 10.3233/WEB-210475.

[23] Koroniotis, Nickolaos & Moustafa, Nour & Sitnikova, Elena & Turnbull, Benjamin. (2019). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. Future Generation Computer Systems. 100. 779-796.

[24] Meidan, Yair & Bohadana, Michael & Mathov, Yael & Mirsky, Yisroel & Shabtai, Asaf & Breitenbacher, Dominik & Elovici, Yuval. (2018). N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing. 17. 12-22. 10.1109/MPRV.2018.03367731.

[25] Kone˘cn´y, J., McMahan, H.B., Yu, F.X., Richtarik, P., Suresh, A.T., Bacon, D.: Federated learning: Strategies for improving communication efficiency. In: NIPS Workshop on Private Multi-Party Machine Learning (2016), https://arxiv.org/abs/1610.05492