Twin chain: A Blockchain based Federated Learning Intrusion Detection System using Optimized Backpropagation based Neural Network for Edge Assisted IoT Networks

Uma Narayanan (uman@rajagiritech.edu.in)  
Rajagiri School of Engineering and Technology

Varghese Paul  
Rajagiri School of Engineering and Technology

Research Article

**Keywords:** Intrusion Detection System (IDS), Federated Learning (FL), Internet of Things (IoT), blockchain, Edge Computing, Security

**Posted Date:** August 4th, 2023

**DOI:** https://doi.org/10.21203/rs.3.rs-3214924/v1

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

**Additional Declarations:** No competing interests reported.
Twin chain: A Blockchain based Federated Learning Intrusion Detection System using Optimized Backpropagation based Neural Network for Edge Assisted IoT Networks

Dr. Uma Narayanan  
Department. of Computer Science and Engineering  
Rajagiri School of Engineering and Technology  
Kochi, India  
{uman@rajagiritech.edu.in}

Dr. Varghese Paul  
Department. of Computer Science and Engineering  
Rajagiri School of Engineering and Technology  
Kochi, India  
{varghesep@rajagiritech.edu.in}

Abstract – Ensuring security and privacy in IoT environments is a critical concern due to the prevalence of intrusions. Federated learning (FL) has emerged as a prominent technology for intrusion detection without compromising data privacy. This study proposes a novel model called BlockFL-IDS (Blockchain-based Federated Learning for Intrusion Detection System) that combines blockchain and deep learning approaches for effective intrusion detection. The BlockFL-IDS model consists of three key processes: efficient client selection, secure channel selection, and federated learning-based IDS. To streamline the complexity of federated learning, we employ Auction game theory to select efficient clients based on metrics such as trust, energy, bandwidth, and network conditions. Furthermore, we employ the Base Criterion Method (BCM), a multicriteria decision-making algorithm, for secure channel selection. BCM evaluates multiple criteria, including noise, path loss, channel quality, stability, trust, and fading, resulting in improved accuracy and reduced data loss in intrusion detection. For federated learning, we utilize the Optimized Back Propagation-based Deep Belief Network (OB-DBN), enabling the generation of both local and global models. The edge server generates local models, extracting packet-based features from client data for intrusion detection. Cloud servers aggregate these local models to create global models stored in a circular-based regression tree structure to enhance scalability and reduce retrieval time. The proposed OB-DBN algorithm calculates backpropagation error, facilitating loss reduction and weight updates. To evaluate the performance of the BlockFL-IDS model, we implement it using the NS-3.26 network simulator and assess its effectiveness using various performance metrics. Through our research, we aim to address security and privacy concerns in IoT environments, providing an innovative solution that enhances intrusion detection while preserving data privacy.

Index Terms- Intrusion Detection System (IDS), Federated Learning (FL), Internet of Things (IoT), blockchain, Edge Computing, Security

I. INTRODUCTION

Internet of Things (IoT) is a growing paradigm that is experiencing sharp growth with fifth-generation (5G) communication which supports the heterogeneity of IoT devices with highly reliable communication [1]. However, the 5G IoT lacks transmission reliability and increased latency. The issue faced by the 5G IoT is addressed by sixth-generation (6G) communication which supports high transmission reliability, low latency, and IoT heterogeneity when compared to 5G communication. The main issue in IoT networks is susceptibility to security threats. The poor security trials in the IoT devices make the device vulnerable to several malicious actions thereby leading to data leakage and security breaches. Another problem in IoT is latency due to its limited resource constraint, hence it takes much time to transfer the data from users to servers. To overcome this issue mobile edge computing (MEC) is introduced in IoT environment which provides the services faster due to its shortest distance [2].

One of the crucial frameworks in IoT for ensuring security is Intrusion Detection System (IDS) [3]. The IDS can split the IoT intrusions (i.e., various attacks) into known and unknown attacks. The known attacks are pre-definably trained in an IDS which can be mitigated easily while the unknown attacks are detected through the development of intelligent and self-learning machine learning and deep learning algorithms [2]. The existing centralized approach for IDS always faces less scalability, security, and privacy problems. Many machine learning algorithms were proposed for intrusion detection such as Support Vector Machine (SVM), Random Forest (RF), Gradient Boosting Machine (GBM), K-Nearest Neighbor (KNN), etc [4]-[6]. The existing work used many deep learning algorithms for intrusion detection...
such as Convolutional Neural Network (CNN), Long Short Term Memory (LSTM), Generative Adversarial Network (GAN), etc [7]. The existing machine learning and deep learning approach limits with high time consuming and less attack detection accuracy respectively. In addition, the parameters of the machine learning and deep learning models are sensitive to IDS which lacks the IDS with high time consumption and poor attack detection.

The problems in the IDS in 6G-IoT are addressed by introducing Federated Learning (FL) approach. The FL approach could maintain the particular device's privacy and support a decentralized framework [8]. The existing research works regarding FL are employed of two stages, (i) train the local model within the different IoT devices itself and (ii) aggregating the local model to the central server updating their local models [9]. However, these approaches were limited by latency and scalability issues. Edge computing in the FL is introduced to alleviate the problem of centralized servers in terms of latency and scalability, reducing the centralized servers’ workload. In addition, security aspects also need to be improved. The existing works utilize machine learning models for local and global model training; however, they are limited with high time consumption and require large amounts of data thus facing security threats. Some of work aims to mitigate poison attacks because federated learning is highly vulnerable to poison attacks. The existing work utilizes trust-based methods for client selection for mitigating poison attacks however they are limited by considering only trust metrics [10]-[13]. The blockchain-based FL method is introduced to improve the overall security in blockchain in terms of local and model storing however, the precise solutions were left as a gap in 6G-IoT-blockchain-FL area [14],[15].

A. Aim & Objectives

This research aims to provide security to the IoT environment using federated learning and blockchain. In addition, this research provides secure local and global model training for enhancing security and privacy in the IoT environment. The main objective of this research is to perform federated learning-based IDS in IoT environment with high privacy and security. The remaining objectives of this research are described as follows,

- To increase the security and reduce the latency of federated learning model by performing selection of clients by considering various parameters.
- To enhance the channel security between entities by performing a selection of secure channel that increases the security and transmission efficiency.
- To improve the security against various attacks validation and investigation of local model that detects and classifies the intrusions that provide accurate results with high security.

B. Research Motivations

The IoT-based federated learning in 6G faces many challenges in terms of security and privacy. The existing works address some specific problems in 5G environment, however the problems faced by the IoT 6G environment were yet addressed. We are motivated to solve the following problems which are existed in the previous research,

- Lack of Client Selection Metrics: The client selection in the federated learning reduces the malicious users in the network and less scalability. The existing works lack client selection, leading to decreased time consumption performance and security threats. While some of the works perform client selection by considering only limited metrics (i.e., trust), which is insufficient for efficient client selection.
- Poor security: The existing works are limited with poor security as they did not consider the poisoning attacks in model rather considered several attacks whereas the federated learning is mainly vulnerable to poisoning attacks. The lack of selection of optimal communication channels also lacks them with poor security. Using machine learning models for model creation also leads to high time consumption, thereby causing data leakage and security breaches.
- Improper Local and Global Training Model: The existing works utilize machine learning and deep learning model for model training however which leads to high false alarm rate as the parameters in the machine learning and deep learning model is sensitive to intrusion detection system which makes high time to detect an intrusion.

C. Research Contributions

In this paper, we proposed a BlockFL-IDS model for detecting intrusion in IoT networks. The research contributions are listed as follows,
In first, we perform efficient client selection using numerous parameters such as trust, bandwidth, energy, etc., using auction game theory which efficiently increases the security and performance in federated learning.

In second, we perform secure channel selection using BCM by considering both efficiency and security-related parameters such as channel quality, stability, trust, etc. which improves the channel efficiency and security.

Finally, we store the sensitive information in the sub-chain and other transactions are stored in the main-chain to increase the clients’ privacy. In addition, improved security is achieved by blacklisting the malicious model, and IDS is performed using investigator by OB-DBN algorithm.

The performance of this research is evaluated based on accuracy, delay, F1 score, loss, and security strength, proving that the proposed work achieved superior performance compared to existing approaches.

D. Paper Organization

This paper is further organized into various sections which are listed as follows, Section II describes the existing research works and its research gaps. Section III illustrates the important problems which are faced on IDS in IoT. Section IV presents the research methodology of the proposed BlockFL-IDS model which includes algorithms, pseudocodes and mathematical derivations. Section V represents the simulation results which describes the simulation setup, comparison results, and research summary of the proposed work. Section VI concludes the BlockFL-IDS model with future work in a detailed manner.

II. Literature Survey

The Internet of Things (IoT) has witnessed a significant proliferation of connected devices, operating in diverse environments, with limited human intervention. IoT devices' increasing number and mobility have made them an attractive target for potential attackers. As a result, various techniques, including authentication, availability, encryption, and data integrity, have been integrated to secure IoT systems. Intrusion Detection Systems (IDSs) have proven to be an effective security tool, which can be further enhanced through the application of machine learning (ML) and deep learning (DL) algorithms. The paper [16] introduces an improved IDS leveraging Gradient Boosting (GB) and Decision Tree (DT) algorithms implemented through the open-source Catboost framework for IoT security. The proposed model is evaluated using the improved NSL-KDD, IoT-23, BoT-IoT, and Edge-IIoT datasets, with the experimental setting enhanced by utilizing GPUs.

In paper[17] a two-factor authentication scheme based on elliptic curve cryptosystem to overcome weaknesses like off-line password guessing attacks, impersonation attacks, and failed to achieve perfect forward secrecy, user anonymity, and unlinkability. Paper provide security proofs for scheme using the formal verification tool ProVerif. Compared to related schemes, proposed scheme achieves a higher level of security while maintaining acceptable computational efficiency. To the best of our knowledge, this is the first scheme that satisfies both two-factor security and user anonymity under sensor node captured attacks.

Smart home applications leveraging IoT technologies have improved convenience, efficiency and security, but existing solutions lack interoperability, data independence, privacy and optimization. Edge AI-enabled systems offer a solution by shifting computation to client-side devices reducing energy costs and enhancing security while enabling remote applications. Anna et.al [18] propose a comprehensive system for smart homes based on IoT and edge computing incorporating fog computing techniques and a case study on human fall detection using a lightweight deep neural network architecture on edge devices validated with the Le2i dataset.

The widespread use of Industrial Internet of Things(IIoT) has enabled large-scale, reliable, and secure industrial environments, but existing deployments often fall short in meeting security standards and have limited resources leading to security breaches and potential critical outcomes. To address the concerns, a secure architecture is proposed [19] that combines blockchain-based solutions with IIoT environments, utilizing a structured asynchronous blockchain Directed Acyclic Graph(DAG) for improved security and transaction efficiency. The proposed solution incorporates detailed use cases, sequence diagrams, and a treat model created using the STRIDE approach for comprehensive security testing.
The flexible architecture significantly reduces attack vectors in IIoT environments and can be customized and extended for various industrial scenarios.

Blockchain technology has emerged as an advanced solution for securing sensitive data, and its application in various sectors, including healthcare, has gained significant attention. Integrating blockchain with IoT devices in the healthcare sector can improve security, privacy, transparency and efficiency, offering valuable business opportunities. The paper[20] presents a secure blockchain-based Proposed Application (PA) that generates, maintains and validates healthcare certificates. Acting as a communication medium between the backend blockchain network and application entities, the PA ensures confidentiality, authentication and access control through smart contracts. Comparative and performance analysis demonstrate the effectiveness of the proposed solution over schemes.

In paper [21], authors proposed an approach to perform bandwidth allocation and client selection in FL networks. Long-term perspective was implemented to resource allocation in the wireless FL networks. Initially, OCEAN algorithm was developed to perform both client selection and bandwidth allocation in which client selection was performed by considering the virtual energy constraints of the clients. Bandwidth allocation was performed by considering the long-term constraints regarding energy. Both bandwidth allocation and client selection were performed using Lyapunov technique. Finally, per-round problem was solved using SEA algorithm by adding the clients in selection set based on priority and according to this selection set, computation of specific bandwidth allocation for solving the problems regarding optimization. MNIST dataset was used to perform experimental analysis. However, client selection is performed in ascending pattern. However, not considering clients' privacy leads to high risk of privacy leakage.

In paper [22], authors proposed an approach to perform client selection in FL system based on adaptive manner using DRL approach. Initially, Mobile-Edge Computing (MEC) was implemented in FL which adaptive selection of client devices for participating in FL at each round using Markov-decision process. Deep Q learning was implemented to select the devices’ subset to reduce each rounds’ training delay, bandwidth, and energy consumption for increasing the scalability. After selecting the adaptive client, efficient clients were selected using reinforcement learning for performing each round. Fashion-MNIST and MNIST datasets were used to perform the performance analysis of this work. In this work, adaptive client selection is performed by considering the delay, bandwidth, and energy. However, lack of security in the network leads to high-security threats.

In this paper, authors proposed an approach to detect the malware IoT devices using federated learning [23]. Initially, data acquisition was performed from the IoT devices by considering the data traffic and preprocessing was performed by normalizing the data samples. Two machine learning approaches (i.e., both unsupervised and supervised) were introduced in the federated learning (FL) model such as auto-encoder and Multi-Layer Perceptron to detect and classify the IoT devices into benign and malicious in which selection of collaborative threshold was performed in the unsupervised approach to detect the anomalies. This FL models also protect clients' privacy and the FL approach's robustness is measured by implementing malicious client setup. Finally, respective action was performed based on adversary robustness. N-BaIoT dataset was used in this work to perform experimental analysis. However, malware detection and classification were performed using two machine learning approaches. However, lack of considering the channel security that decreases the security against various attacks.

In paper [24], proposed intrusion detection for industrial IoT using federated learning approach. Initially, clients performed local model training which was responsible for training global model updated by the local model. During federated learning training and aggregation differential, privacy was applied to ensure privacy ad accuracy. For model training, this paper used supervised learning method which classified the dataset into normal or malicious. Finally, the performance of the proposed work is evaluated based on ToN-IoT dataset.

Alcazar et al. [25] proposed federated learning-based intrusion detection using ensemble approaches for IoT environments. The proposed work includes four processes: data preprocessing, dimensionality reduction, model validation, and intrusion detection. Initially, data preprocessing and feature extraction were performed to clean and obtain high accuracy respectively. After that, dimensionality reduction was performed from the extracted features by using a principal component analysis algorithm. Finally, classification was performed based on two machine learning algorithms: k-nearest neighbor and random forest. Here, federated learning was performed by using multi-layer perceptron algorithm. The result demonstrates the proposed work achieved better performance in terms of true positive rate and false-positive rates. Here, machine learning algorithm was proposed for intrusion detection in IoT which takes much time for training that increases the training time of local and global models results in high latency during intrusion detection.
Chatterjee et al. [26] proposed federated learning-based intrusion detection in an IoT environment. Intrusion detection was performed based on a federated learning-based convolutional neural network. The federated learning model integrates a stochastic gradient descent algorithm for updating the model average which also processes the non-IID data. The proposed federated learning model computes the weights values of the client to aggregate the local models. Finally, the server aggregated the weighted values for optimizing global model dynamically. The performance of the proposed work was evaluated by NSL-KDD dataset. Here, intrusion detection was performed based on federated learning, however, it leads to poor security because this work does not consider any security during training which leads to high poisoning attacks in the network.

This paper proposed anomaly detection using federated learning in IoT environment [27]. Here, federated learning was performed based on Gated Recurrent Unit algorithm. Initially, preprocessing was performed to increase the accuracy of model training. After that, federated learning was performed for detecting anomalies in IoT. Finally, machine learning-based ensemble learning was performed to increase the accuracy of model training. The experimental results show that the proposed work performed better than machine learning.

• Here, federated learning is performed for anomaly detection, however, the trained models are transmitted through public channels without any security that leads to high data leakage.

Authors in [28], proposed blockchain-assisted intrusion detection system for IoT cloud environment. The proposed work includes four components: vendor, blockchain, smart contract, and central coordinator unit. This work used privacy-preserving blockchain to ensure smart security, reducing poisoning attacks in IoT environment. Here, intrusion detection was performed by using a bidirectional long short-term memory algorithm by extracting the features from the user data. The performance of the proposed work was evaluated by two datasets namely UNSW-NB15 and BoT-IoT. The experimental results demonstrate the proposed work achieved better performance in terms of detection rate, and false alarm rate compared to existing works.

In paper [29], authors proposed federated learning-based intrusion detection using blockchain in IoT healthcare environment. In this research, sensors monitored the health condition and room conditions of the patients. The edge server has the responsibilities of identifying the attacks using Artificial Neural Network (ANN) model. The local model values were updated in the blockchain during federated learning to provide security. After completed local model training, global aggregation was performed in cloud assisted blockchain layer. Finally, the proposed work's performance was evaluated using the BoT-IoT dataset, proving that the proposed work achieved good performance compared to existing works.

Authors in [30] proposed client selection by considering multiple criteria for IoT based federated learning. Initially, the request messages were collected from the IoT devices, and then perform global model generation for communication. Here, filtering engine was proposed for filtering the random number of clients. The random clients were selected based on time, energy, memory, and CPU. The aggregation has the responsibility of updating the federated average function. Finally, machine learning engine was utilized for local data training which were stored in the devices. However, this research takes much time for selecting groups of clients that leads to high latency during the training process of federated learning.

In paper [31], authors performed optimal client selection in federated learning. Here, the reserved number of clients were selected using the heuristic method, which selects the best clients for federated learning. The test accuracy of the clients was evaluated by considering the predefined threshold. After selecting the candidates, the proposed work initiated the global model generation. This research evaluated the performance of the proposed work for worst case scenario. Finally, the experimental results show that the proposed work achieved superior performance in terms accuracy.

In paper [32], authors proposed anomaly detection for Edge assisted IoT environment. Initially, network traffic was captured for extracting the network traffic flows. From the network traffic, passban IDS extract the features for detecting the intrusions. Based on the extracted features random forest classified the traffic was normal or intrusion. If it is detected as intrusions, it will send to the action manager to take corresponding actions. This research addressed various types of attacks with less false positive rate and high accuracy. Here, intrusions were identified in a centralized manner which leads to high security threats.
III. Problem Statement

Blockchain-based security was provided to IoT devices via federated learning was introduced in this work [33]. Here, Q learning algorithm was proposed for performing federated learning. Client selection was performed based on trust assessment. This research includes some major research problems which are listed as follows,

- Here, the edge server is responsible for client selection and forward the trained model to blockchain-connected cloud however, the security of the edge server is not considered leads to security and privacy threats.
- This work selects optimal clients by using adaptive threshold method based on pre-defined trust value however, the selection of optimal clients was not efficient by considering only with trust value which leads to high malicious traffic and less scalability.
- Here, Q learning is adopted for supporting federated learning for training the local models however, the usage of Q learning limits with less convergence which leads to decaying of learning rate.

The attack detection in the decentralized IoT-edge environment was introduced in this work [34]. Here, virtual worker is employed in each local model (i.e., autoencoder and decoder model) who is responsible to improve the training local model. The improvised training model is fed to global federated learning server for model aggregation. The main research problems of this research are listed as follows,

- Here, the virtual worker is employed to analyze the traffic in the network for botnet attacks and is also responsible for improvising the training model however, the federated learning method is highly vulnerable to poisoning attacks which are not considered by not validating the local models which leads to security threats.
- The communication between the entities and IoT devices is held over a public channel, leading to less transmission efficiency and security as the sensitive information is vulnerable to being breached.
- This work adopts autoencoder and decoder for local model training however, the autoencoder model suffers from high complexity as it has many layers, and also the parameters are susceptible to imperfection and losses and IDS which causes high false alarm rate.

The privacy of the IoT devices was ensured by blockchain federated learning was introduced in this work [35]. The problems of this research are defined as below,

- This work allows the desirable IoT devices that want can join in the federated learning however, it leads to high network traffic which leads to scalability issues in federated learning approach.
- The machine learning model is utilized for training the local model however it leads to increased time consumption as it needs large amount of time for training that leads to improper local model training which causes high data leakage and security breaching problems.
- This work adopts convolutional neural network for global model training however the convolutional neural network is limited with slower training process and high complexity as it has many convolutional layers.

This work adopts federated learning-based intrusion detection for IoT devices which improves the efficiency of attack classification [31]. This work includes some research problems which are explained as below,

- This work effectively detects the malicious attacks by ensemble mechanism however the local model privacy is affected by poisoning attacks which may lead to manipulating the whole network and performing malicious actions.
- Here, the global server is responsible for global model aggregation and sharing however, the security of both global server and communication channel between entities was not considered which leads to severe security threats.

Research Solutions: This section provides the solutions for the existing problems. (1) Initially, efficient client selection is performed by considering several parameters including security-related parameters such as trust which ensures the security of the edge server that reduces the FL vulnerability against poisoning attacks. Network traffic in federated learning is reduced by performing efficient client selection using auction game theory and scalability is improved by implementing edge servers and circular based tree structure storage of global model. In addition, privacy is preserved by storing sensitive (i.e., private) information in the twin-chain. (2) In the edge server, the generator constructs the local model. The investigator validates the constructed local model using smart contract and blacklist the malicious model which increases the security of global server. In addition, secure channel selection is performed using BCM method which increases the models’ security. (3) Here, selection of secure channels is performed using BCM considering numerous parameters such as stability, trust, channel quality, etc., which provides optimal channel selection with enough
security. The deep learning parameters are optimally selected using POA which has high convergence that increases the learning rate. Here, global model is stored in circular based tree structure, reducing complexity. In addition, both local and global models are trained using OB-DBN algorithm which reduces the loss function by periodically updating the weight values.

IV. PROPOSED WORK

In this research, we mainly focus on ensuring the privacy and security of the IoT environment by performing federated learning-based intrusion detection using blockchain technology. This work consists of three entities such as IoT devices (i.e., clients), edge servers, global server (aggregator), and twin-chain in which the twin-chain includes both main-chain and sub-chain that increase security and federated learning is implemented in this work to increase the scalability. In addition, 6G is introduced to achieve high data transmission rate in the IoT environment, providing high reliability and network coverage with low latency. Fig 1 represent the architecture of the proposed BlockFL-IDS model. This proposed work includes three sequential phases which are described as follows,

- Efficient Client Selection
- Secure Channel Selection
- Federated Learning based IDS

A. Efficient Client Selection

Initially, effective clients are selected for performing federated learning which increases the security and achieves high performance in terms of achieving low time consumption and number of rounds in FL to attain the target for intrusion detection. For selecting the clients, we consider trust \((T)\), energy \((\mathcal{E})\), bandwidth \((b)\), and network conditions \((n_c)\) \((i.e., \text{RSSI and CSI})\) using Auction Game Theory algorithm. Here, client selection is performed by edge server for effective federated learning. For client selection, we perform games between clients and edge server. The edge server selects the optimal clients by conducting the game between clients. The winning clients are selected for performing federated learning. In auction game, edge acts as a buyer which conduct the game, and clients acts as a select which participate in the game. All the clients are submitter their bidding ranges based on \(T, \mathcal{E}, b, \text{and } n_c\). In this research, we used \(B = \{b_i\}, i = 1,2,3,...,n\) denotes the bidding policies of clients and \(b_i\) represent the bidding value of clients. The highest bidding values of client is selected by the edge server as an optimal client, which is defined as follows,

\[
O_c = \sum_{i=1}^{n} b_i
\]

\[
b_i = \sum_{i=1}^{n} T_i, \mathcal{E}_i, b_i, n_{c_i}
\]

After collecting the bidder values from the clients, winners are determined by the Edge server which ranks the received bids based on descending order. The approximate values of the received bid is determined as follows,

\[
Ab_i = \frac{C_v}{\sqrt{|B_s|}}
\]

Where \(Ab_i\) represent the approximate value of the received bid, \(C_v\) represent the valuation of the clients, and \(B_s\) represent the bid size which is submitted by the clients. Here, size represent the availability of \(\mathcal{E}\), and \(b\), and quality of \(T, n_c\).
The edge server lists the approximate value of the received bids in a descending order \(D(n)\) to announce the winners, where \(n\) represent the count of received bid which takes \(n * \log(n)\) for sorting which is defined as follows,

\[
\begin{align*}
D^m(n^m) &= \{d^m(1), d^m(2), \ldots d^m(n), \ldots d^m(n^m)\} \\
D^1(n^1) &= \{d^1(1), d^1(2), \ldots d^1(n), \ldots d^1(n^1)\} \\
D^2(n^2) &= \{d^2(1), d^2(2), \ldots d^2(n), \ldots d^2(n^2)\}
\end{align*}
\]

Where \(D^m(n^m)\) is sort list of approximate values of the bids submitted by the clients, similarly \(D^1(n^1), D^2(n^2)\) represent the values of the bids submitted by the client 1, client 2, etc. The client with the first value in the sort list as
considered as the winner in first round. This algorithm provides optimal decision making by playing games between all the clients which reduces the latency and performs accurate client selection that also increases the security. Fig 2 represents the process of client section using Auction Game theory.

**Fig. 2 Auction based Client Selection Process**

**B. Secure Channel Selection**

After successfully selecting the efficient clients, optimal channel selection is performed to increase the security and transmission efficiency. Selection of optimal channel is performed by Base Criterion Method (BCM) considering several metrics such as noise ($n$), path loss ($P_l$), channel quality ($Q_c$), stability ($S$), trust ($T$), and fading ($f$). The criterion for channel selection is defined as follows,

$$C = \{n, P_l, Q_c, S, T, f\}$$  \hspace{1cm} (5)

For every channel we consider these criteria for selecting optimal channel. Initially, we consider the set of criteria for decision making which is defined as below,

$$(C_1, C_2, C_3, \ldots, C_n)$$  \hspace{1cm} (6)

After that, specified the base criterion which identifies the worst and best criteria for channel selection. The relative importance of the criteria is defined as follows,

$$R = \begin{bmatrix}
        r_{11} & r_{12} & \cdots & r_{1n} \\
        r_{21} & r_{22} & \cdots & r_{2n} \\
      \vdots  & \vdots  & \ddots & \vdots \\
        r_{n1} & r_{n2} & \cdots & r_{nn}
\end{bmatrix}$$  \hspace{1cm} (7)

where $r_{ij}$ represent the relative importance of criterion $i$ and criterion $j$, and the pairwise comparison of relative importance is shown with mathematical scale of $1/9$ to $9$. The base comparison of criteria as defined as follows,

$$r_{base,j} = (r_{b1}, r_{b2}, r_{b3}, \ldots, r_{bn})$$  \hspace{1cm} (8)

where $r_{bij}$ represent the performance of base criterion to relative criterion $j$. Here, we explained the relative importance of every single criterion to other criteria which is shown as below,

$$r_{base,i} \times r_{ij} = r_{base,j}$$  \hspace{1cm} (9)
Finally, weight value of the criteria is obtained for decision making. The optimal weight value of \( w_b/w_j \) will be equal to \( r_{bj} \). For all \( j \), we defined a way to get the maximum absolute difference value \( |w_b/w_j - r_{bj}| \). Then the criteria value is non-negative, the problem can be defined as below,

\[
\min \max |\frac{w_b}{w_j} - r_{bj}| \quad (10)
\]

where

\[
\begin{align*}
\sum_{j=1}^{n} A(w_j) &= 1 \\
w_j &\geq 0 \ \forall j
\end{align*}
\]  

(11)

Rewritten equation () is shown as below,

\[
\min \alpha \quad (12)
\]

where

\[
\begin{align*}
\left|\frac{w_b}{w_j} - r_{bj}\right| &\leq \alpha \\
\sum_{j=1}^{n} A(w_j) &= 1 \\
w_j &\geq 0 \ \forall j
\end{align*}
\]  

(13)

Finally, the consistency ration is determined for evaluating the comparison matching degree. In which all the pairwise comparisons are fully constant that is explained as below,

\[
C_R = \frac{\alpha}{C_i} \quad (14)
\]

where, \( C_R \) represent the ratio of consistency and \( C_i \) represents the index of consistency. Based on the weight values decision making is performed which selects an optimal and secure channel for communication. This method performs decision making to select the secure channel with better consistency and high accuracy that increase the security against various attacks, especially man-in-the-middle attacks.

---

**Pseudocode for secure channel selection**

**Input:** Channel criteria \( C = \{n, P_l, Q_c, S, T, f\} \)

**Output:** Optimal channel selection

**Begin**

**For all channel** \( C \) do

- Initialize set of criteria using eqn (5)
- Assign weight values for every \( C \) based on pairwise comparison
- Relative importance of each criterion is defined by using eqn (9)
- Obtain the weight values for each criteria using eqn (10)

  **if** (criteria == non negative)**

  - Finish and take a decision based on current rank
  
  **Else**

  - Gather more information and rewritten eqn (10) as eqn (13)
  - Compute consistency ratio for evaluating comparison matching degree using eqn (14)

**End For**

**End**
C. Federated Learning based IDS

After selecting optimal clients and channels, IDS is performed based on federated learning by generating both local and global models. This section is further divided into two subsections which are described as follows,

(i) Local Model Generation

The gathered data from the clients are transmitted to the edge server to train the data for creating local model. Edge server is mainly implemented to reduce the complexity and increase scalability. It consists of two entities such as generator and an investigator in which the local models are generated by the generator. The investigator investigates the local model by considering packet features (src IP, dest IP, src Port, dest Port, packet size, payload, etc), based on the extracted packet features the investigator classified the packets into two classes such as normal and malicious using Optimized Back Propagation based Deep Belief Network (OB-DBN) algorithm. If the local model is valid, it allows the client to aggregate the global model otherwise, ignores the client and is added to the blacklist.

![Diagram of the Proposed Twin Chain](image)

The twin-chain consists of two types of chains such as main-chain and sub-chain in which the sensitive information of the clients is stored in sub-chain and all other transactions are stored in main-chain that increases both privacy and security. Here, main chain includes public chain which is arranged in a linear structure which is used to validate the accuracy of the sidechain. Fig 3 represents the block diagram of the proposed twin chain. The main chain block includes block header, block body, in which the block header includes the hash values of the current and previous block, signature, timestamp and merkle tree root. In which the block body record the transactions of all clients participate in the federated learning, and maintains sub chain block summary for ensuring the trust.

The sub chain includes private chain for storing sensitive information which is verified and constructed based on main chain. The verification block saved the summary information of sub chain data. The private blockchain provides high security than public blockchain. The main purpose of sub chain is construction of sub chain for communicating the main chain which ensures the
communication reliability between main and sub chain. The proposed twin-chain increases the reliability with low latency which increases the performance.

(ii) Global Model Generation

After generating the local model generation, it is transferred to the global server to aggregate the local model for generating global model in which the global model is stored in the form of Circular based Regression Tree Structure that increases the scalability and reduces the complexity in generating global model. Initially, root node is defined to start tree construction. The tree structure observes the terminal node from root node where parameters are assessed for the learning observations. Here, learning observations are expressed by evaluating the weight values that designate whether the observation of \( i \)th learning and observation of \( z \) fit to the same terminal node.

\[
W_i^t(z) = \sum_{c=1}^{C} 1\{(z_i \in C_c)^{\cap}(z \in C_c)\}. \quad (15)
\]

Where \( 1(.) \) represent the function of indicator and \( C_c \) is the \( c \)th out of \( C \) segments which segmented the covariate space in separate subsections. Since, the evaluated parameter pair \((l, \rho)(z)\) requiring the estimated von Mises distribution for \( z \) is obtained by evaluating the weighted maximum likelihood which is defined as follows,

\[
(l, \rho)(z) = \underset{l, \rho}{\operatorname{Arg Max}} \sum_{i=1}^{n} W_i^t(z)q(l, \rho; x_i). \quad (16)
\]

Therefore, the similar parameter pair estimation is performed for all the observations fitting to the similar terminal node that increases the computation speed, then the parameter evaluation does not recalculate for new observation that can be mined directly from the observation learnings. In our work, global models are stored in a circular tree-based structure. In real time many circular trees are formed to store the data, hence we combine all the trees and formed a circular regression forest for improving the stability. For every new observation \( z \) is a set of nearest neighbors and weight value of the observations are obtained based on the count of trees. Here, \( z \) values is assigned to similar terminal node as every learning observations \( x_i \), where \( i \in 1 \ldots, n \}. \) The weight values of the circular regression forest is calculated as below,

\[
W_i^t(z) = \frac{1}{t} \sum_{T=1}^{n} \sum_{c=1}^{C} \frac{1\{(z_i \in C_c)^{\cap}(z \in C_c^T)\}}{|C_c^T|}. \quad (17)
\]

Where \( |C_c^T| \) represent the observation count in the \( c \)th partition of \( T \)th tree. Hence, the specific weight values are calculated for every observation, and specific parameter evaluated for every von Mises distribution which is defined as follows,

\[
(l, \rho)(z) = \underset{l, \rho}{\operatorname{Arg Max}} \sum_{i=1}^{n} W_i^t(z)q(l, \rho; x_i). \quad (18)
\]

Hence, the resulting parameter can easily adopt the covariates \( z \), where \( W_i^t(z)=1 \) will be agreed to the unweighted sample evaluations and \( W_i(z) \in \{0,1\} \) agreed to the subcategory selection from the circular regression tree. The proposed tree structure can easily capture smoothness and changes automatically.
The proposed OB-DBN algorithm is used to train both local and global models in which the backpropagation updates the weight values periodically that effectively reducing the loss function. The architecture of the proposed OB-DBN is shown in fig 4. The understanding of the DBN training process is based upon the algorithm or error backpropagation, which can be obtain the error through the forward transmission of input and backward transmission of obtained error. The proposed DBN structure includes stacked of three Restricted Boltzmann Machine (RBM) structure for training both local and global model. Hence, the proposed DBN works without supervision which provides better results. In first, we train the initial RBM structure. The output of first RBM as the input of second RBM. Similarly, the output of second RBM as the input of third RBM. Finally, we got the output of DBN which provides local models. The input of softmax classifier of neural network is defined as follows,

\[ I = \{(u^{(1)}, v^{(1)}), \ldots, (u^{(n)}, v^{(n)}), v^{(n)} \in \{1, 2, \ldots, k\} \} \tag{19} \]

For every input \( u \) we used classifier for estimating the probability of posterior \( p(v = i/u) \), it is the probability that \( u \) is the sample input of \( i \). The hidden layer activation function is defined as follows,

\[
H_\theta(u) = \begin{bmatrix}
p(v = 1/u, \theta) \\
p(v = 2/u, \theta) \\
\vdots \\
p(v = k/u, \theta)
\end{bmatrix} = \frac{1}{n_f} \begin{bmatrix}
E^\theta 1, u \\
E^\theta 2, u \\
\vdots \\
E^\theta k, u
\end{bmatrix} \tag{20}
\]

\[
P(H_i = 1|V) = f(\varepsilon_i + \delta_{i,j}V)p(V_i = 1|H) = f(\sigma_i + \delta_{i,j}H) \tag{21}
\]
Where $V$ represent the visible layer, $\sigma_i$ represent the visible layer bias vector, and $\epsilon_i$ represent the bias values of the hidden layer, $\delta_i$ represent the weight values, and $n_f = \sum E^\theta_i u$ represent the factor of normalization function. Here, softmax classifier provides the output with higher accuracy.

To reduce error rate of the proposed DBN, the parameters of the neural networks are optimally selected or fine-tuned by utilizing backpropagation strategy. Here gradient descent algorithm is proposed to revise the weight matrix of the network. Hence, the propagation errors are changed in opposite direction. The cost function is defined as follows,

$$J(\theta) = -\frac{1}{\eta} \left[ \sum_{i=1}^{n} \sum_{j=1}^{m} 1\{v(i) = j\} \log \frac{E^\theta_j u(i)}{\sum_{k=1}^{k} E^\theta_k u(i)} \right]$$  \hspace{1cm} (22)

Where $1\{v(i) = j\}$ represent the indicative function, when the value is 1 then $v(i) = j$ and 0 when not. Every time we perform the parameter tuning for making the smaller value of $J(\theta)$ by using gradient descent method which is defined as follows,

$$\nabla_\theta J(\theta) = -\frac{1}{\eta} \sum_{i=1}^{n} \left[ u(i)(1\{v(i) = j\} - p(1\{v(i) = j|u(i); \theta)) \right] \theta_j(n + 1)\theta_j(n) + g \nabla_\theta$$  \hspace{1cm} (23)

Where $g$ represent the factor of convergence which helps to control the velocity of convergence. After completed local model generation, global model generation is performed by aggregating the local models for performing intrusion detection. The deep learning parameters are optimally selected using Pelican Optimization Algorithm (POA) in which the POA algorithm has high convergence rate that provides rapid performance. Initially, population of pelicans are initialized based on upper bound and lower bound. The population matrix is defined as follows,

$$D = \begin{bmatrix} D_1 \\ \vdots \\ D_i \\ \vdots \\ D_n \end{bmatrix}_{n \times m} = \begin{bmatrix} D_{1,1} & \ldots & D_{1,j} & \ldots & D_{1,m} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ D_{i,1} & \ldots & D_{i,j} & \ldots & D_{i,m} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ D_{n,1} & \ldots & D_{n,j} & \ldots & D_{n,m} \end{bmatrix}_{n \times m}$$  \hspace{1cm} (24)

Where $D$ represent the pelicans population matrix. The objective function of pelican optimization is defined as follows,

$$S = \begin{bmatrix} S_1 \\ \vdots \\ S_i \\ \vdots \\ S_n \end{bmatrix}_{n \times 1} = \begin{bmatrix} S(D_1) \\ \vdots \\ S(D_i) \\ \vdots \\ S(D_n) \end{bmatrix}_{m \times 1}$$  \hspace{1cm} (25)

Where $S$ represent the vector of objective function, the proposed pelicans include two phases such as exploration phase (moving towards to prey), and exploitation phase (flying on water surface). The mathematical expression of exploration phase is defined as follows,

$$D_{i,p}^{1p} = \begin{cases} D_{i,j} + \text{Rand.}(l_p - \gamma. D_{i,j}), & S_{i,p} < S_i \\ D_{i,j} + \text{Rand.}(D_{i,j} - l_p), & else \end{cases}$$  \hspace{1cm} (26)

Where $D_{i,p}^{1p}$ represent the current status of the pelican based on phase 1, $\gamma$ is a random number that is equal to one or two, $l_p$ indicates the prey location in $j$th dimension, and $S_{i,p}$ is a value of objective function. The updation of objective function is defined as follows,

$$D_i = \begin{cases} D_{i,j}^{1p}, & S_{i}^{1p} < S_i \\ D_i, & \text{Else} \end{cases}$$  \hspace{1cm} (27)
Where $D_{i,j}^{lp1}$ represent the current new status of the pelican with objective function $S_i^{lp1}$. The mathematical representation of hunting behavior of pelican on water surface is defined as below,

$$D_{i,j}^{lp2} = D_{i,j} + \gamma \cdot (1 - \frac{t}{T}) \cdot (2 \cdot \text{Rand} - 1) \cdot D_{i,j} \quad (28)$$

Where $D_{i,j}^{lp2}$ represent the new status of the pelican on phase 2, and $\gamma$ represent the constant value which is equal to 0.2, and $\gamma \cdot (1 - \frac{t}{T})$ indicates the neighborhood radius of the pelican, $t$ is the iteration count, and $T$ represent maximum count of iterations. The updation of pelican on phase 2 is defined as follows,

$$D_t = \begin{cases} D_{i,j}^{lp2}, & S_i^{lp2} < S_t \\ D_t, & \text{Else} \end{cases} \quad (29)$$

Where $D_{i,j}^{lp2}$ represent the updated status of the pelican phase 2 with objective function $S_i^{lp2}$. In this way, the parameters of neural network are optimized in this research. Finally, the global aggregator converts the global model to anonymity global model for updating the clients through edge server that increases the security against attacks. From the global model all the clients know the intrusions in the environment without knowing their identity which leads to high security.

---

**Pseudocode for OB-DBN based federated learning**

1. **Input:** local dataset of users, global parameters
2. **Output:** Global model generation
3. **Begin**
4. **While** initialize global parameters in cloud server **do**
5. Global parameter aggregation
6. **While** users obtain local model by training local parameters **do**
7. Obtain the local model by edge server using OB-DBN
8. Generate local model using eqn (19)-(21)
9. Calculate and obtain backpropagation error using eqn (22),(23)
10. Optimized the neural network parameters using eqn (24)-(29)
11. Store the generated local model into sub chain for security
12. **End**
13. **While** cloud server aggregates local model **do**
14. Update existing global parameters
15. Aggregate new parameters and obtain global model
16. Repeat step (10) from (12)
17. Construct circular based regression tree using eqn (15)-(18)
18. Store the global model into circular regression tree
19. **End**
20. **End**
21. **End**
V. EXPERIMENTAL RESULTS

In this section, we illustrate the proposed BlockFL-IDS model in IoT networks. The experimental results section includes three sub-sections: simulation setup, comparison analysis, and research summary. The numerical results demonstrate that the proposed work achieved better performance than previous research.

A. Simulation Setup

This section describes the simulation setup of the proposed BlockFL-IDS model which is implemented based on NS-3.26 network simulator. Table 1 represents the configuration of the simulation setup, and table 2 represents the configuration of the network parameters.

<table>
<thead>
<tr>
<th>Configurations of Hardware</th>
<th>RAM</th>
<th>2GB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hard disk</td>
<td>60 GB</td>
</tr>
<tr>
<td></td>
<td>Processor</td>
<td>Pentium dual core and above</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configurations of Software</th>
<th>Network Simulator</th>
<th>NS3.26</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operating System</td>
<td>Ubuntu 14.04 LTS</td>
</tr>
</tbody>
</table>

Table 2 Configuration of Network Parameters

<table>
<thead>
<tr>
<th>Network Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of IoT devices</td>
<td>100</td>
</tr>
<tr>
<td>No. of Edge servers</td>
<td>4</td>
</tr>
<tr>
<td>No. of Global server</td>
<td>1</td>
</tr>
<tr>
<td>Twin chain</td>
<td>1</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>1400m×1500m</td>
</tr>
<tr>
<td>Modules</td>
<td>Wi-Fi, Internet, Ipv4</td>
</tr>
<tr>
<td>Initial Energy</td>
<td>100J</td>
</tr>
<tr>
<td>Simulation time</td>
<td>300s</td>
</tr>
<tr>
<td>Node mobility</td>
<td>10 m/s</td>
</tr>
<tr>
<td>Mobility type</td>
<td>Random waypoint</td>
</tr>
<tr>
<td>Transmission range</td>
<td>150m</td>
</tr>
<tr>
<td>Number of packets</td>
<td>1000</td>
</tr>
<tr>
<td>Channel bandwidth</td>
<td>100 MHz</td>
</tr>
<tr>
<td>Packet data rate</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Interval of packets</td>
<td>1s</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>UDP, TCP/IP</td>
</tr>
<tr>
<td>No. of retransmission</td>
<td>7</td>
</tr>
<tr>
<td>Size of packets</td>
<td>64, 128, 256, 512, 1024 bytes</td>
</tr>
</tbody>
</table>
B. Comparative analysis

In this section, we illustrated the comparison between the proposed BlockFL-IDS model and exiting methods namely PPB-FL [30], SFL [28]. The main objective of this work is to identify the intrusion detection by utilizing federated learning approach. The proposed work achieved superior performance in terms of accuracy, delay, loss, F1-Score, and security strength with respect to number of epochs and number of devices.

a. Impact of Accuracy

This metric is used to evaluate the accuracy of the proposed BlockFL-IDS model. The highest accuracy indicates the system detects intrusions accurately. Accuracy is defined as that the proportions of true negative and true positive in total samples. The mathematical representation of the accuracy is defined as follows,

\[
Ac = \frac{TP + TN}{TP + TN + FP + FN}
\]  

Where \( Ac \) represent the accuracy, and TP is true positive, FP represent false positive, TN is true negative, and FN indicates false negative. Fig 5 represent the comparison of accuracy with respect to number of epochs. Similarly, and fig 6 represent the comparison of accuracy with respect to number of devices. The comparison result shows that the proposed BlockFL-IDS achieved high accuracy compared to other two existing works such as PPB-FL, and SFL. In our work, we perform efficient client selection using game theory which eliminates the unwanted clients during federated learning that increases the performance of federated learning, in addition secure channels are selected to reduce data loss and increases security. To identify the intrusions accurately we extract the packet based features from the user data using OB-DBN algorithm which classifies the data into normal or malicious. The back propagation strategy also improves the accuracy of intrusion detection by updating the weight values based on the propagation error. The accuracy is increased with the increasing count of epochs. The highest accuracy is achieved by performing efficient training. The best training process also increased the accuracy. In existing, does not focus on secure channel selection, rather than they send their data to the public and random channel which increase high data loss. Additionally, packet based features are not consider to generate local models which leads to misclassification or poor accuracy. The proposed BlockFL-IDS achieves 7% highest accuracy compared to SFL and 14% higher than PPB-FL model.

![Accuracy vs. Number of Epochs](image-url)

Fig.5 Accuracy vs. Number of Epochs
b. Impact of Delay

This metric used to evaluate the delay of the proposed BlockFL-IDS model, in which the delay represents the additional time taken by the network to complete the task. Delay is used to defined the performance of the proposed work. If the work has less delay, then it will achieve good performance. Delay means that the difference between expected completed time and current completion time. The mathematical representation of the delay is defined as follows,

$$\mu = \£ - \€$$  \hspace{1cm} (31)

where $\mu$ represent the delay, and $\£$ the current completion time and $\€$ represent the expected completion time. Fig 7 represents the comparison of delay for both proposed and existing works. The comparison result shows that the proposed work achieved less delay compared to existing approaches. The delay increased with the increasing number of devices, because many devices participate in federated learning for intrusion detection, hence it takes much time to identify the intrusions. In our work, we have detected the intrusions with minimum amount of time due to select clients optimally, and extract the packet based features from the user data. Additionally, we have used OB-DBN algorithm for federated learning which provides a result in a faster manner with less error. The propagation errors are calculated and weight values are updated based on the errors which increases the prediction accuracy and reduces the delay for intrusion detection. The existing works does not extract the packet features from the input data which takes some additional time to identified the intrusions. Additionally, existing SFL works used Q-learning algorithm which takes much time to update the Q values which leads to high delay. The existing PPB-FL algorithm used CNN for federated learning based intrusion detection which leads to high delay due to generate unwanted convolutional layers during execution. The proposed BlockFL-IDS achieves 25ms less delay compared to SFL model and 43ms less than PPB-FL model.
c. Impact of Loss

This metric used to evaluate the loss value of the proposed BlockFL-IDS method. If the system works with less loss, then it improves the accuracy and performance during intrusion detection. The mathematical representation of the loss function is defined as follows,

\[ L = C_O - E_O \]  \hspace{1cm} (32)

Where \( L \) represent the loss function and \( C_O \) represent the current output and \( E_O \) represent the expected output. The difference between current and expected output is known as loss. Fig 8 represents the comparison of loss with respect to number of epochs. The comparison result shows that the proposed BlockFL-IDS achieved less loss value compared to other two existing works. In this research, we applied backpropagation strategy to the OB-DBN method for reducing the loss values, because it calculates the backpropagation error and update the weight values based on the error function which reduces the loss functions. The existing PPB-FL model used convolutional neural network and SFL model used Q learning algorithm which leads to high loss compared to our proposed method due to lack of fine tuning of weight values and reward functions. The loss values are increased with the increasing number of epochs. The proposed BlockFL-IDS model reduces 0.5 loss compared to PPB-FL model and reduces 0.4 loss compared to SFL model.
This metric is used to calculate the accuracy of the work. F1-score is calculated from the harmonic mean of the precision and recall. Here, precision represents the positive sample prediction value, and recall represents the negative sample prediction value from total samples. The mathematical representation of the F1-Score is defined as follows,

\[
F = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}
\]

(Figure 8: Loss vs. Number of Epochs)

Fig 9 represent the comparison of proposed and existing F1-score values with respect to number of epochs. The F1-score is increased with the increasing number of epochs. The comparison results demonstrate the proposed BlockFL-IDS achieved high F1-score compared to other two existing works. The increasing count of F1-score also represent the accuracy of the work. If the work has high F1-score then it has high accuracy. The proposed BlockFL-IDS performed optimal client
selection, reducing the complexity during intrusion detection and increasing the accuracy by eliminating unwanted clients in an initial stage. The local and global models are generated based on OB-DBN, providing accurate intrusion detection results by performing packet-based feature extraction and optimal weight value updation. The proposed BlockFL-IDS achieved 0.11 higher than compared to SFL model, and achieved 0.19 higher than PPB-FL model.

e. Impact of Security Strength

This metric is used to evaluate the security level during data transmission. The highest security strength indicates the efficient security during data transmission without any data loss. Fig 10 represents the comparison of security strength with respect to number of epochs. The security strength is increased with the increasing number of epochs. The comparison results shows that the proposed work achieved highest security strength compared to existing works. The reasons of highest security in secure channel selection and blockchain based data storage. Here, communication channels are selected based on channel criterions with high security that reduces the data loss and increases the security. We consider the trust values for optimal client selection that reduces illegitimate clients participating in federated learning. Finally, we have stored the sensitive transactions into the sub chain and non-sensitive transactions are stored in the main chain, increasing security and scalability. In this way, the legitimate users also have restrictions to store and retrieve the data, leading to high security and less data loss due to attackers. But the existing works store all the data into the same blockchain which can easily know and access by the clients, reducing the security strength. The proposed BlockFL-IDS achieved 10% higher than SFL and 15% higher than PPB-FL methods.

\[ \text{Fig.10 F1-Score vs. Number of Epochs} \]

C. Research Summary

In this section, we explain the summary of the experimental results which also proved that the proposed BlockFL-IDS model achieves better performance via numerical analysis. The performance of the proposed work is evaluated in terms of accuracy, delay, loss, f1-score, and security strength which are shown in fig 5 from fig 10. Table 3 illustrates the average numerical values of the proposed and existing work performance metrics. The highlights of the proposed work is listed as follows,

- For increasing the security with high performance in federated learning, we perform efficient client selection using numerous parameters such as trust, bandwidth, energy, etc., using auction game theory which efficiently increases the security.
For improving the channel efficiency and security, we perform secure channel selection using BCM by considering both efficiency and security-related parameters such as channel quality, stability, trust, etc.

To increase the clients' privacy, we store the sensitive information in the sub-chain and other transactions in the main-chain. In addition, improved security is achieved by blacklisting the malicious model, and IDS is performed using investigator by OB-DBN algorithm.

<table>
<thead>
<tr>
<th>Performance metrics</th>
<th>Scenario</th>
<th>Proposed vs. Existing Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PPB-FL</td>
<td>SFL</td>
</tr>
<tr>
<td>Accuracy (%)</td>
<td>No. of devices</td>
<td>78.2</td>
</tr>
<tr>
<td></td>
<td>No. of Epochs</td>
<td>79.4</td>
</tr>
<tr>
<td>Delay (ms)</td>
<td>No. of devices</td>
<td>68.6</td>
</tr>
<tr>
<td>Loss</td>
<td>No. of Epochs</td>
<td>0.7</td>
</tr>
<tr>
<td>F1-score</td>
<td>No. of Epochs</td>
<td>0.74</td>
</tr>
<tr>
<td>Security Strength (%)</td>
<td>No. of Epochs</td>
<td>78</td>
</tr>
</tbody>
</table>

**VI. CONCLUSION AND FUTURE WORK**

In the IoT environment security is an important issue to reduce data loss. This research proposes the BlockFL-IDS model for identifying intrusions by performing federated learning using blockchain and deep learning approaches. Initially, optimal clients are selected based on auction game theory, reducing the complexity during federated learning that increases the performance of proposed work. After that, a secure channel is selected to send the user data, which improves the security and privacy of the data and is performed based on a multicriteria-based decision making algorithm, namely BCM. Finally, federated learning is performed to identify the intrusion in the network, which is identified by extracting the packet based information during local model in which the data packets are classified into normal and malicious. The normal local models are sent to global model for aggregation, providing accurate intrusion detection results. For improving privacy and security issues, we used a twin chain that includes both private and public blockchain, improving the scalability of blockchain. Finally, the proposed BlockFL-IDS achieves superior performance in terms of accuracy, delay, loss, security strength, and f1-score. In future, we planned to implement Anarchic Federated Learning (AFL) for satisfying the need of the clients. Here, the clients have the freedom to define the number of local steps in each round based on its energy, privacy and communication channels.
REFERENCES


[18] Mansoor Nasir, Khan Muhammad, Amin Ullah, Jamil Ahmad, Sung Wook Baik, Muhammad Sajjad, Enabling automation and edge intelligence over resource constraint IoT devices for smart home, Neurocomputing, Volume 491, 2022, Pages 494-506, ISSN 0925-2312.


