SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I12P106

Volume 10 Issue 12, 54-64, December 2023
© 2023 Seventh Sense Research Group®

Original Article

Secured Federated Learning for DDoS Detection in Heterogenous Telecom Cloud Networks Using Recurrent Neural Networks

Abdoul-Aziz Maiga[1], Edwin Ataro[2], Stanley Githinji[3]

[1]*Pan African University, Institute for Basic Sciences Technology and Innovation (PAUSTI), Nairobi, Kenya.*
[2]*The Technical University of Kenya/Electrical and Information Engineering, Nairobi, Kenya.*
[3]*United States International University - Africa (USIU-A), Nairobi, Kenya.*

[1]*Corresponding Author : abdoul.maiga@students.jkuat.ac.ke*

Received: 12 October 2023 Revised: 14 November 2023 Accepted: 12 December 2023 Published: 23 December 2023

Abstract *- The recent evolution of cloud computing has enabled the cloudification of Telecommunication (Telecom) network functions. The cloud-based Telecom infrastructure is more scalable, flexible, and cost-efficient for service providers. However, a significant security challenge for Telecom cloud providers is ensuring the availability of services provided to users by mitigating Distributed Denial of Service (DDoS) attacks. The fact that Virtual Network Functions (VNF) in the Telecom cloud are hosted on the Internet makes them easy targets for large-scale DDoS attacks. This study proposes the use of secured supervised Federated Learning (FL) with an efficient Hybrid Recurrent Neural Network (H-RNN) for DDOS attack mitigation in the Telecom cloud. The proposed H-RNN model combines LSTM, a Bidirectional GRU (BiGRU), and a Bidirectional LSTM (BiLSTM) to obtain a state-of-the-art LSTM+BiGRU+BiLSTM model. FL is used with Secure Sockets Layer (SSL) encryption, which supports data privacy and integrity in heterogeneous Telecom cloud networks. The simulation results using the CICDDOS2019 benchmark dataset displayed a detection accuracy of 99.59%, a False Positive Rate (FPR) of 0.042%, and an average detection time of 0.062 ms. A novel H-RNN model and secured FL are proposed to enable deep-learning-based anti-DDoS technology building and deployment in cloud-based Telecom networks.*

Keywords *- DDoS attack mitigation, Deep Learning, Federated Learning, SSL, Telecom cloud.*

1. Introduction

Telecom cloud is the next generation of telecommunication (Telecom) networks that combine Software-Defined Network (SDN), Network Function Virtualization (NFV), and cloud native technologies [1, 2] to enable Telecommunication Service Providers (TSPs) to offer customized services to users with flexibility [3], speed, and cost-effectiveness. The main challenge for TSPs is always to meet Service-Level Agreements (SLA) with customers [4]. SLA is a formal contract between a TSP and a customer that defines the services that will be provided, the quality of the services, and the remedies provided if telecommunication service providers fail to meet the SLA contract [5].

Cloud-based telecommunication network services have many advantages; however, Distributed Denial of Service (DDoS) attacks are part of the most evolving and impacting cyber-attacks that can compromise SLA because of their capability to compromise the availability of TSPs for end users [6]. Telecommunication Virtual Network Functions (VNFs) are easy targets for cyber criminals because of their hosting on the Internet. Deep Learning (DL)--based anti-DDoS systems have surpassed traditional systems in the literature owing to their capability to detect both known and unknown types of DDoS attacks [7]. The use of deep learning models requires a significant amount of data during training, and cloud-based Telecom network functions can be hosted by cloud providers in various geographical regions.

To train a deep learning model, raw data must be sent to a centralized server if a centralized learning method is adopted. This can cause data privacy violation risks or tempering during data transport. There is a deficiency in developing a high-performance system that combats DDoS attacks while ensuring data integrity and safeguarding privacy.

This study addresses this gap by proposing secured federated learning with a high-performing Hydride deep Recurrent Neural Network (H-RNN) for DDoS attack detection in the Telecom cloud. The use of federated learning addresses data privacy concerns by enabling the training of a DL model from different sources in the cloud without sharing raw data. The sources (clients) that participate in the training can use their local data to train the model locally and only share the locally trained model parameters with a centralized server, which aggregates all the local models to build an enhanced global model that will be used in production. However, sharing local model parameters with the server can be tempered if they are not protected.

A Secure Sockets Layer (SSL) with Rivest-Shamir-Adleman (RSA) encryption technology is proposed to encrypt the parameters sent between the server and the clients. The proposed H-RNN is designed by combining three different Recurrent Neural Network (RNN) layers. The input layer is a Long Short-Term Memory (LSTM) layer followed by a Bidirectional Gated Recurrent Unit (BiGRU) and a Bidirectional LSTM (BiLSTM) layer. It is designed for the deep inspection of network traffic and identification of traffic dependencies to detect DDoS attacks accurately. The system proposed in this study is more comprehensive. It has a higher level of security and privacy preservation, designed explicitly for heterogeneous Telecom cloud applications, with enhanced performance compared to previous related works. The contribution of this study to the telecommunications field can be summarized as follows:

1. A state-of-the-art high-performance deep recurrent neural network model is proposed for DDoS attack detection.
2. Secured federated learning using SSL and RSA encryption technology is proposed for data privacy preservation and data integrity assurance in a heterogeneous Telecom cloud network.
3. The proposed framework is evaluated, and the outcomes are compared with the literature and presented to the readers.

The remaining sections are organized as follows. Section 2 discusses previous studies that used deep-learning-based FL against DDOS attacks. In Section 3, the proposed methodology is presented. Section 4 describes the proposed system performance evaluation. The results are discussed in Section 5, and the paper is concluded in Section 6.

2. Previous Works

Federated Learning (FL) has been applied in many areas to address privacy concerns [8]. Its application to cybersecurity has also been observed. In contrast to centralized machine learning, FL does not require centralization of data for model training, which can improve data privacy preservation. This section discusses only the latest studies that have used Federated Learning and Deep Learning (DL) for DDoS attack detection and mitigation. Some researchers have explored the use of deep learning combined with FL for DDoS attack detection and mitigation in various network types.

For the purpose of detecting and mitigating DDoS attacks while aligning with data privacy, Dingyang et al. [9] proposed FLDDoS in their study. They constructed an FL-based CNN model for DDoS attack detection and mitigation. The accuracy of the proposed model for DDoS attack detection was as high as 99%, which is 20% higher than that of the traditional model, as claimed by the authors.

The authors of [10] proposed FLAD, an adaptive federated learning method for DDoS attack detection. FLAD addresses the limitations of traditional FL by mitigating the dependencies on fixed computation allocation and weighted averaging methods. It employs an adaptive mechanism that dynamically assigns computational resources to clients based on their profiles, thereby improving their learning experience. When evaluated using a fully connected neural network model with the CICDDoS2019 dataset, it exhibited superior performance over state-of-the-art FL algorithms.

With the development of enhanced 4G and 5G networks, Internet of Things (IoT) networks have been deployed in many application domains. However, they also suffer from various types of DDoS attacks. Researchers have proposed DL-based FL solutions to mitigate these attacks. In [11], Caldas Filho et al. developed a botnet detection and mitigation model for IoT using deep learning under federated learning training. They proposed the mitigation of DDoS attacks from the source in local networks by implementing both a host IDS and a network IDS.

The main idea is to allow IoT devices to participate locally in DDoS attack detection through traffic inspections. The proposed model achieved an accuracy of 89.753%. Always for IoT network protection against DDoS attacks, Zainudin et al. [12] proposed FedDDoS, a deep learning-based FL for efficient DDoS attack detection. The authors used an efficient feature selection technique, a filter-based Pearson Correlation Coefficient (PCC) feature selection technique for selecting potential features, and a deep-federated learning framework for local data privacy with deep inspection of network traffic. The DL model evaluated using the CICDDoS2019 dataset achieved an accuracy of 98.37% with a detection time of 3.917 ms.

The authors in [13] focused their study on Low-rate DDoS (LDDoS) attack detection. LDDoS attacks are difficult to detect owing to their periodic characteristics, behaving like regular traffic while degrading network quality. The authors proposed an asynchronous federated learning framework based on BiLSTM and an attention mechanism for LDDoS detection and mitigation. The suggested model outperformed state-of-the-art models in terms of accuracy and number of communication rounds.

Some authors have explored the application of federated learning to DDoS attack detection in 5G networks and beyond. This is the case of Sheikhi and Kostakos [14], who proposed unsupervised federated learning for DDoS detection in a 5G core targeting the GTP protocol. The authors implemented a 5G testbed, simulating a real public network for the study. The proposed model was deployed on a testbed and evaluated in real-time. The authors expressed the effectiveness of the proposed method.

As can be observed, federated learning has been applied in various areas for DDoS attack detection and mitigation. However, most researchers have not considered the possibility of data tempering when clients are located in different and distant networks during the federated training process. The system proposed in this study addresses this issue and proposes a secure federated learning framework based on SSL encryption.

3. Proposed Methodology

The proposed methodology is an all-in-one solution that addresses DDoS attack detection using an efficient hybrid RNN model, data privacy through federated learning, and data integrity preservation using SSL encryption. The techniques are described in the following subsections.

3.1. The Proposed Model: LSTM+BiGRU+BiLSTM

The proposed model is the core of the proposed system, with the role of processing network input traffic for DDoS attack detection and mitigation. Three different RNN models were combined with two dense layers for deep inspection of network traffic for DDoS traffic detection. The composition is simple, with a single layer for each RNN. The first layer is the LSTM layer. It was designed to address the limitations of traditional RNNs in capturing the long-range dependencies in sequential data. It was chosen in this study for its advantage over traditional RNNs. The following two layers are BiGRU and BiLSTM, both of which are modified and simplified versions of the LSTM.

The BiGRU, which is based on the GRU, has fewer gates than LSTM, making it less complex and more computationally efficient. BiGRU can process input data in both the forward and backward directions. This is the second choice for the design of the proposed model, owing to this particular advantage. The third layer, BiLSTM, has the advantage of processing input data in both the forward and backward directions compared to LSTM.

The three neural networks combined have the capacity for deep inspection of network traffic and traffic-dependency identification. For binary classification, two dense layers were added for greater accuracy, and the classification output was either regular traffic or a DDoS attack. BiLSTM and BiGRU are combinations of two LSTM and GRU layers in the forward and backward directions, respectively, which are standard RNN models in the literature.

To avoid repetition, the reader can explore the articles [15] and [16] for basic architectures and mathematical understanding of LSTM and GRU. The proposed hybrid model architecture is illustrated in Figure 1. It presents the characteristics of the model, such as the Activation Functions (AF) used for each layer, dropout size between the layers, and number of neurons or units for each layer.

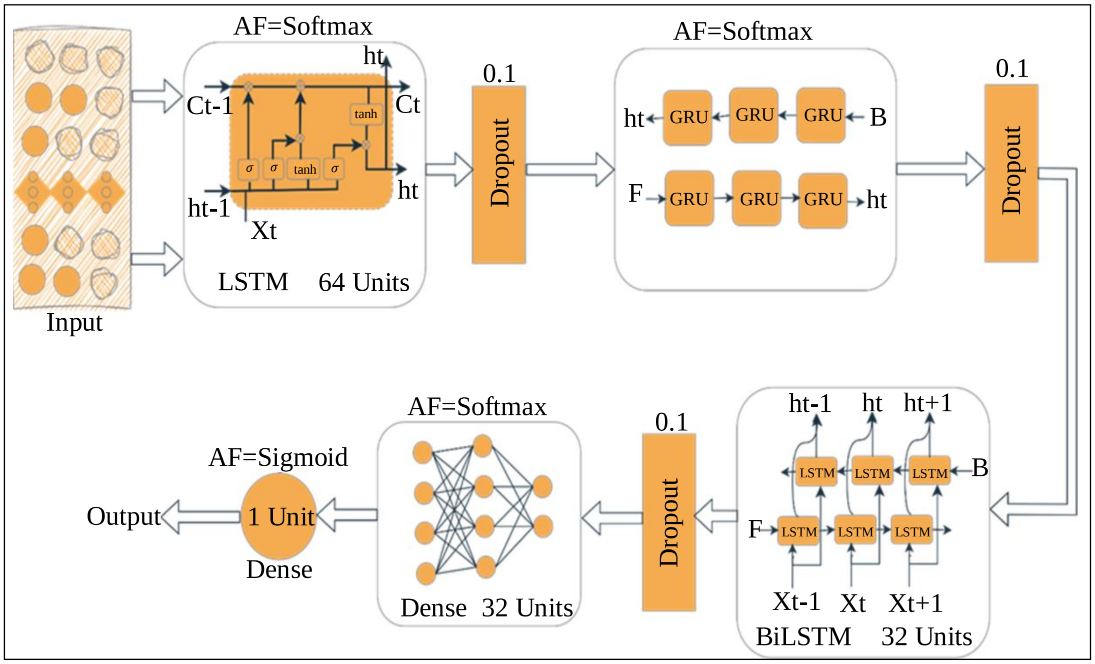


Fig. 1 The proposed model architecture overview

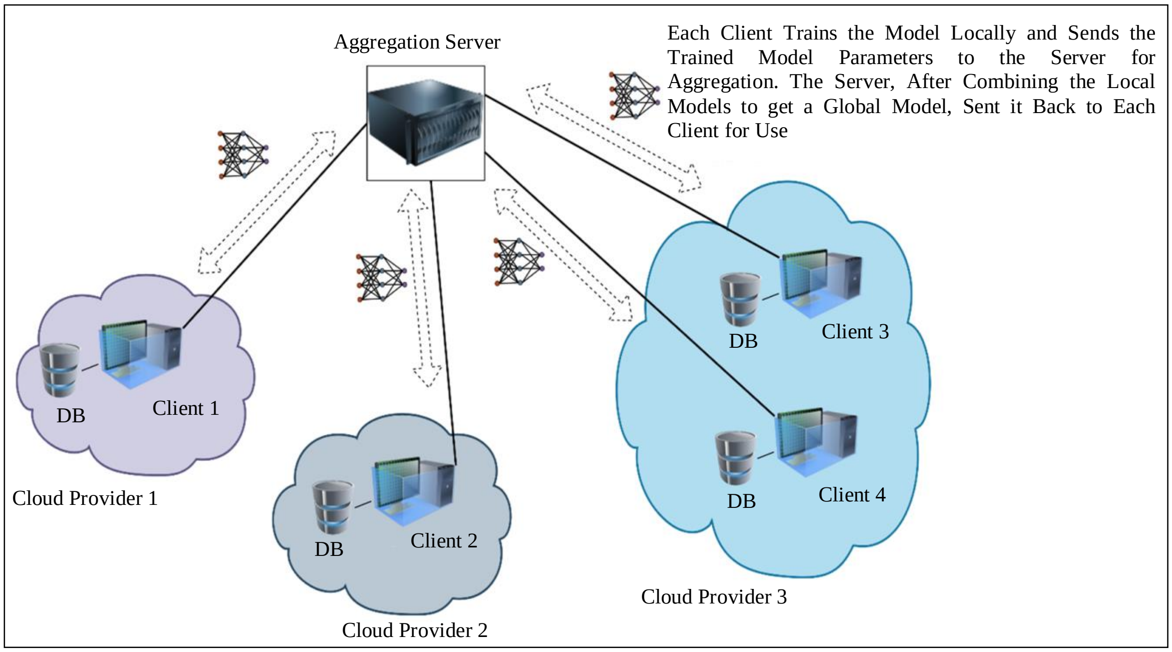

Aggregation Server
Each Client Trains the Model Locally and Sends the Trained Model Parameters to the Server for Aggregation. The Server, After Combining the Local Models to get a Global Model, Sent it Back to Each Client for Use
DB
Client 1
Cloud Provider 1
DB
Client 2
Cloud Provider 2
DB
Client 3
DB
Client 4
Cloud Provider 3

Fig. 2 Federated learning process (case of multi-cloud clients)

3.2. Federated Learning

In this study, federated learning was used as the primary technique to train the proposed model. This machine learning method enables models to be trained in a decentralized manner involving numerous participants known as clients. Each client uses its local data to train the model independently. Subsequently, they shared the trained specifications of the model with the central server. The server then merges all these local models to create a comprehensive global model, which is then sent back to each client.

The advantage of this approach is its ability to maintain data privacy for each client while allowing them to work together while training the same machine learning model. In the context of this study, federated learning is applied to facilitate collaboration among Telecom cloud Network Functions (NF) hosted in different clouds to train the proposed model without sharing raw data, mitigating the risk of data privacy violations.

In this study, the Flower Federated open-access framework [17] was used for the simulation. The Federated Average (FedAvg) method was used to aggregate the local models. FedAvg computes the average version of all local models to obtain a global model. The model training process using federated learning is depicted in Figure 2.

3.3. SSL Encryption

Federated learning, by default, does not encrypt the parameters sent between the server and clients. Hackers can intercept the parameters and temper them if they are not encrypted, which can compromise learning authenticity and accuracy. SSL was used in this study with Rivest-Shamir-Adleman (RSA) encryption technology to encrypt the parameters sent between the server and clients during the proposed model training to ensure data integrity. This was possible using OpenSSL version 1.1.1t to generate local self-signed certificates and private and public keys for simulation purposes. The step-by-step workflow of the encryption layer is as follows:

- Step 1: OpenSSL is used to generate the local certificate and the private and public RSA keys
- Step 2: The server shares the certificate and the public key with the clients but keeps the private key secret (for itself).
- Step 3: After training the model locally, the clients encrypt the parameters using the public key and send them to the server (only the corresponding private key can decrypt them).
- Step 4: The server decrypts the parameters using the corresponding private key and computes the local models' parameters to build a single global model.
- Step 5: The server encrypts the global model using the private key and sends the encrypted global model to clients. The clients can then use their public keys to decrypt the global model.

By adopting this encryption scheme, the proposed framework is secure and authentic, tailored for real-world applications, especially in the context of Telecom cloud where clients are hosted on the Internet, making them easy targets for man-in-the-middle attacks.

4. Performance Evaluation

In this section, the simulation dataset and the evaluation metrics are described.

4.1. Dataset Used Preprocessing

The simulation dataset used was the benchmark open-access CICDDoS2019 dataset [18]. Made public by the Canadian Institute for Cybersecurity (CIC), it contains various old and modern types of DDoS attacks, such as the Lightweight Directory Access Protocol amplification attack, Microsoft SQL Server amplification attack, NetBIOS amplification attack, Simple Network Management Protocol amplification attack, Simple Service Discovery Protocol amplification attack, User Datagram Protocol flood attack, UDP Lag flood attack, Web application layer DDoS attack, SYN flood attack, Trivial File Transfer Protocol amplification attack, Port scanning activity, and many others that can be explored from the official source. Before training, the dataset was preprocessed and normalized to satisfy the characteristics of the proposed model. The steps are described as follows:

- Step 1: The dataset initially multi-class labelled has been binary-encoded with the value 0 for standard samples and 1 for DDoS samples.
- Step 2: All integer-type features were normalized to int32, and all float-type features were normalized to Float32.
- Step 3: Some useless features were eliminated by applying a correlation function with a threshold of 80%. Features with a correlation value greater than 80% were excluded and the rest were retained. In this process, 55 features are selected for training and testing.
- Step 4: In the last step, the data are scaled to have zero mean and unit variance using the function.

$$Z = (X - \mu)/ \sigma \qquad (1)$$

Where Z is the Z-score, X is the corresponding data point, µ is the mean of the data, and σ is the standard deviation. The final dataset used in the simulation is presented in Table 1.

4.2. Simulation Process

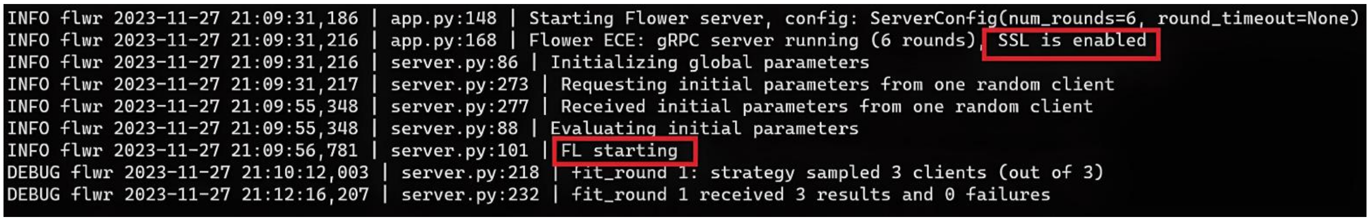
The experiments were performed on a Windows 11 platform running on an AMD Ryzen 7 4800H processor capable of reaching speeds of up to 4 GHz. This system was equipped with 24GB of RAM and 512GB SSD for local storage. In addition, it incorporates a Radeon graphics card with a capacity of 6GB.

For federated learning purposes, three virtual machines as clients and one virtual machine as the server were created using Python, Tensorflow, and the Flower federated learning framework [17]. The training dataset was equally shared with the clients for the FL purpose. SSL encryption technology has been configured for each client and for the server such that federated learning can start only if the SSL is enabled between entities.

Figure 3 and Figure 4 show the SSL connection status on the server and the connection handshake process for a given client, respectively. The proposed LSTM+BiGRU+BiLSTM was iteratively fine-tuned to obtain the best training hyperparameters, which are listed in Table 2.

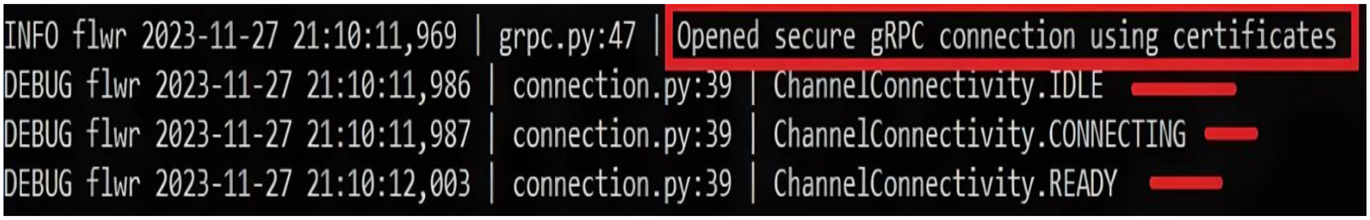
Table 1. CICDDoS2019 dataset distribution used for training and testing

Dataset	Total Samples	Selected Features	Training Samples	Testing Samples
CICDDoS2019	431,371	55	125,170	306,201



```
INFO flwr 2023-11-27 21:09:31,186 | app.py:148 | Starting Flower server, config: ServerConfig(num_rounds=6, round_timeout=None)
INFO flwr 2023-11-27 21:09:31,216 | app.py:168 | Flower ECE: gRPC server running (6 rounds), SSL is enabled
INFO flwr 2023-11-27 21:09:31,216 | server.py:86 | Initializing global parameters
INFO flwr 2023-11-27 21:09:31,217 | server.py:273 | Requesting initial parameters from one random client
INFO flwr 2023-11-27 21:09:55,348 | server.py:277 | Received initial parameters from one random client
INFO flwr 2023-11-27 21:09:55,348 | server.py:88 | Evaluating initial parameters
INFO flwr 2023-11-27 21:09:56,781 | server.py:101 | FL starting
DEBUG flwr 2023-11-27 21:10:12,003 | server.py:218 | fit_round 1: strategy sampled 3 clients (out of 3)
DEBUG flwr 2023-11-27 21:12:16,207 | server.py:232 | fit_round 1 received 3 results and 0 failures
```

Fig. 3 The server enabled SSL encryption before starting the training



```
INFO flwr 2023-11-27 21:10:11,969 | grpc.py:47 | Opened secure gRPC connection using certificates
DEBUG flwr 2023-11-27 21:10:11,986 | connection.py:39 | ChannelConnectivity.IDLE
DEBUG flwr 2023-11-27 21:10:11,987 | connection.py:39 | ChannelConnectivity.CONNECTING
DEBUG flwr 2023-11-27 21:10:12,003 | connection.py:39 | ChannelConnectivity.READY
```

Fig. 4 A client establishing a secured connection with the server before participating in the FL

Table 2. The best hyperparameters for the proposed model training

Hyperparameter	Value
Learning Rate	0.02
Number of Rounds	6
Number of Local Epochs	30
Batch Size	42
Drop Out	0.1
Loss Function	Binary_Crossentropy

4.3. Evaluation Metrics

The evaluation metrics adopted to assess the proposed model are the common metrics used to evaluate all types of machine learning models. Metrics such as model accuracy, precision, False Positive Rate (FPR), False Negative Rate (FNR), model recall, F1_score, and model detection time were used. The following equations describe each metric.

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)} \tag{2}$$

$$Precision = \frac{TP}{(TP+FP)} \tag{3}$$

$$FPR = \frac{FP}{(FP+TN)} \tag{4}$$

$$FNR = \frac{FN}{(FN+TP)} \tag{5}$$

$$Recall = \frac{TP}{(TP+FN)} \tag{6}$$

$$F1\_score = 2 \times \frac{Precision \times Recall}{(Precision + Recall)} \tag{7}$$

Where TP is the abbreviation for True Positive; TN is True Negative; FP is False Positive; and FN for False Negative.

5. Results and Discussions

In this section, the simulation results are presented and analyzed. All performances presented were obtained using the CICDDoS2019 testing set, which was solely employed to evaluate the ability of the designed model to differentiate between DDoS attacks and regular traffic. Finally, the model's performance was compared with that of previous studies.

5.1. Main Results

The prediction results of the proposed model on the CICDDoS2019 testing set are presented in Table 3. It achieved a classification accuracy of 99.59% with a precision of 99.99%, which is an exciting performance. Another high performance was an FPR of 0.042% achieved by the model. The smaller the FPR, the better the model. An FNR of 0.48% was another excellent performance indicator of the proposed model. With such a low FPR and FNR, the model proved effective in detecting DDoS attacks in regular network traffic. In terms of computation time, the model presented an average detection time of 0.062ms, which is acceptable. In addition to its high performance, the model is simple and computationally efficient, with a low average detection time. The training and validation graphs are presented in Figure 5 for accuracy, Figure 6 for loss, and Figure 7 for the model's Receiver Operating Characteristic (ROC) graph. They support the model's learning capability and justify its prediction efficiency.

5.2. Proposed Model Compared with Centralized Learning

In this subsection, the performance of the proposed model based on federated learning is compared with previous studies that used traditional or centralized deep learning methods in the context of DDoS attack detection using the CICDDoS2019 dataset. This assessment will allow readers to understand how well the proposed federated learning method can be compared with traditional learning methods in terms of performance.

As stated in the previous subsection, the proposed model evaluated using the CICDDoS2019 testing set achieved an accuracy of 99.59% in a federated learning setup. In this subsection, readers must note that all the previous works highlighted used the traditional learning method except for the proposed method, which uses FL. The purpose is to compare the proposed method with traditional methods.

Sbai and Elboukhari [19] developed a Deep Neural Network (DNN) model for DDoS attacks. The simulation results using the CICDDoS2019 dataset showed an accuracy of 99.94%. Compared to the proposed model (99.59% accuracy), their model performs slightly better. This is because, in traditional learning, all datasets are trained in a single machine compared to FL, where the dataset is distributed among the clients, and the model is trained by each client independently with its local data.

The final model of FL is an average model of all clients, which can present degradation in terms of accuracy compared to when the entire dataset is used to train the model at once. However, the advantage of using FL is finding a tradeoff between data privacy and high performance. By comparing the proposed model based on this criterion, the proposed system is more tailored for real-world applications (especially in the context of heterogeneous Telecom cloud networks) than the traditional method.

Amaizu et al. [20] developed a high-performing DNN model. Evaluated using the CICDDoS2019 dataset, it achieved an accuracy of 99.66%, which is also slightly more significant than that of the proposed FL model but lacks data privacy risk mitigation compared to the current model. The accuracy of the proposed model is also very close to that of centralized learning.

Cil et al. [21] also designed a DNN model against DDoS attacks using the CICDDoS2019 dataset. Their model showed an accuracy of 99.99% for binary classification and 94.57% for multi-class classification. Their model outperformed the one proposed in this study.

Kumar et al. [22] used the LSTM model on the CICDDoS2019 dataset. It displayed an accuracy of 98%. Compared with the accuracy of the proposed model (99.59%), their model is less accurate.

Subramanian et al. [23] proposed LSTM and GRU models for DDoS mitigation. When evaluated using the CICDDoS2019 dataset, they achieved an accuracy of 99.4% and 92.5%, respectively. Both of their models underperformed the proposed model in this study.

Canola Garcia and Blandon [24] built a DNN model against DDoS attacks. It showed an accuracy of 99.4% when evaluated using the CICDDoS2019 Dataset. The proposed model (99.59% accuracy) slightly outperformed their model. Centralized learning can be very effective in terms of performance when it comes to deep learning model training.

However, the data privacy requirements of authorities are a challenge that limits their applications in real-world scenarios. The proposed FL model showed limitations in terms of accuracy compared to some previous studies using centralized learning models, but it still outperformed some other centralized models. The comparison results are shown in Figure 8.

Despite the limitations compared with centralized learning in terms of performance, the proposed model in FL aligns with data privacy. The proposed system also integrates SSL encryption to enhance the security of FL by mitigating all types of man-in-the-middle attacks, making it an optimal solution for real-world applications.

5.3. Results Comparison with Previous Works: FL

Deep Learning-based anti-DDoS systems using Federated Learning (FL) are a recent concept, but previous researchers have proposed many models. In this section, the performance of the proposed system is compared with those of previous studies. Table 4 compares the proposed model with previous studies that employed federated learning with a focus on accuracy, FPR, and security. The current model achieved a higher accuracy of 99.59% than previous models for the same dataset and other datasets mentioned in the table. A similar superiority was observed for FPR.

In contrast to the proposed framework, most previous studies did not explore the importance of data encryption during federated learning in their study to avoid data tempering or man-in-the-middle attacks. Using SSL with RSA encryption technology, a secured federated learning framework tailored to cloud-based network applications is proposed in this study.

The proposed model is also simple and computationally efficient, with a detection time of 0.062 ms compared to [12] (with a detection time of 3.917 ms). For visual comparison, Figure 9 shows a comparison of the accuracies.

Table 3. Prediction results using the CICDDoS2019 testing data

Proposed Model	**Metric**	**Value**
LSTM+BiGRU+BiLSTM	**Accuracy**	**99.59%**
	FPR	**0.042%**
	FNR	**0.48%**
	Recall	99.52%
	Precision	99.99%
	F1-Score	99.75%
	Detection-Time	**0.062 ms**

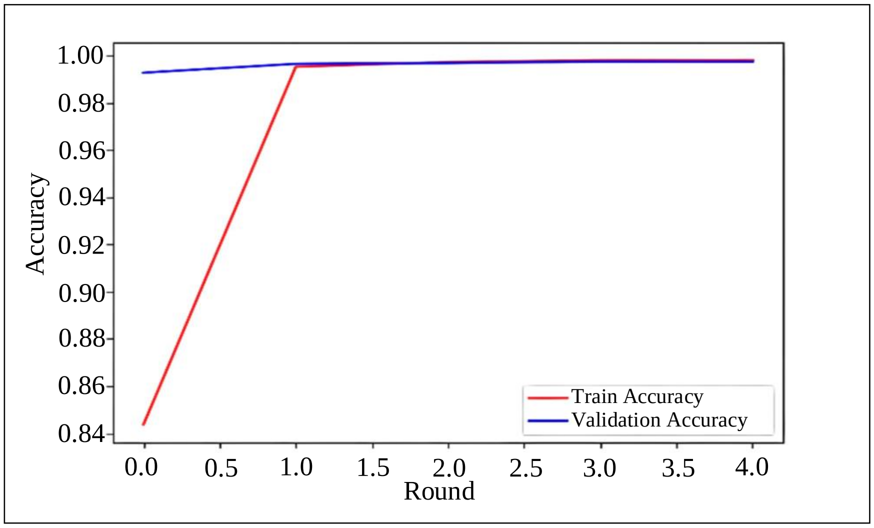


Fig. 5 Proposed model training and validation accuracy graphs

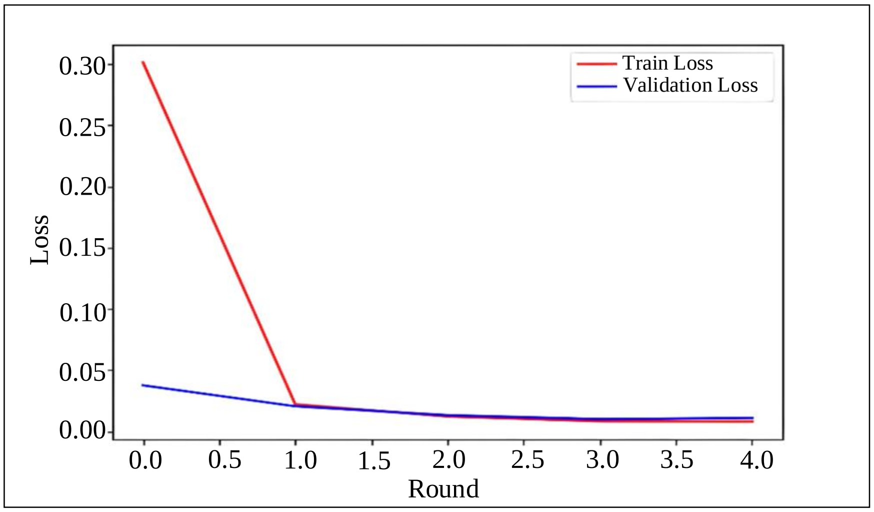


Fig. 6 Proposed model training and validation loss graphs

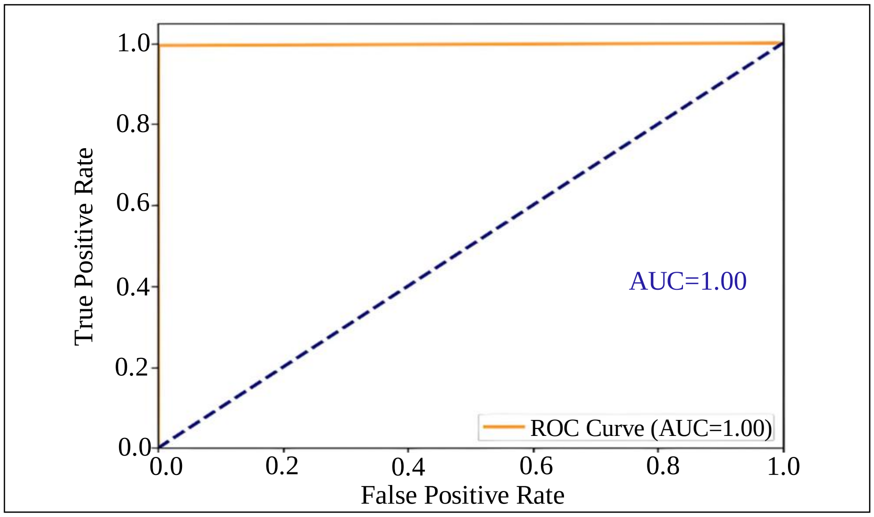


Fig. 7 Proposed model ROC curve graph

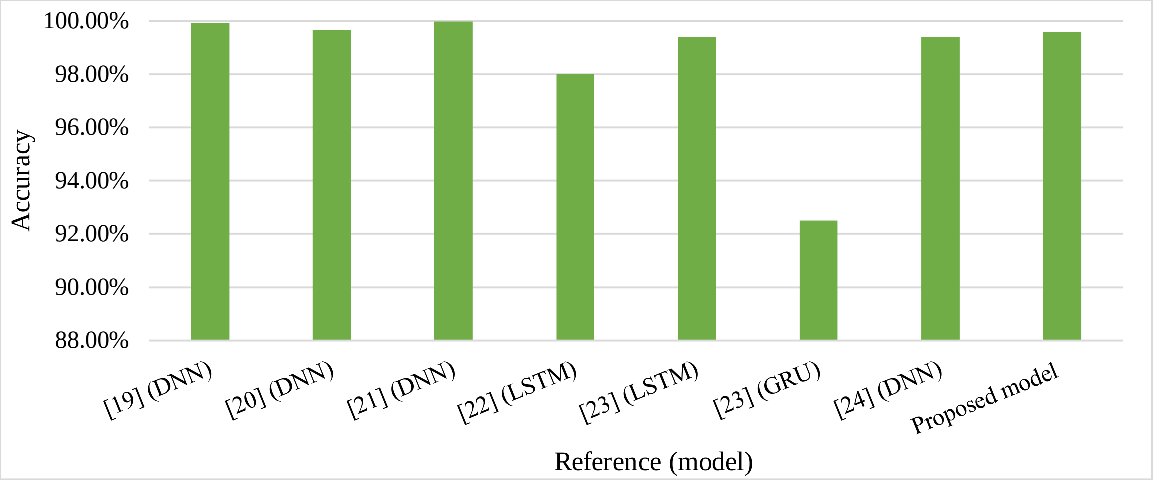


Fig. 8 Proposed model's accuracy comparison with previous centralized learning DL models

Table 4. The proposed model compared with the previous works that used Federated Learning

Reference (Year)	Model Used	Dataset Utilized	Accuracy	FPR	FL Encryption Technique
Proposed Model	**LSTM+BiGRU+BiLSTM**	**CICDDoS2019**	**99.59%**	**0.042%**	**SSL (RSA)**
[25] (2022)	Feedforward Neural Network (FNN)	CICDDoS2019	84.2%	-	No encryption used
[12] (2022)	Deep Neural Network (DNN)	CICDDoS2019	98.37%	-	No Encryption Used
[26] (2022)	Fully Connected ANN	CICDDoS2019	96%	-	No Encryption Used
[13] (2023)	BiLSTM and Attention Mechanism	DARPA, and ISCX-2016-SlowDos	98.80%	0.65%	No Encryption Used
[27] (2023)	Deep Neural Network (DNN)	CAIDA	98.85%	2.215%	No Encryption Used
[11] (2023)	1D-CNN	Private Dataset	89.753%	-	No Encryption Used
[28] (2022)	GRU	Real Network Simulated	98%	-	No Encryption Used

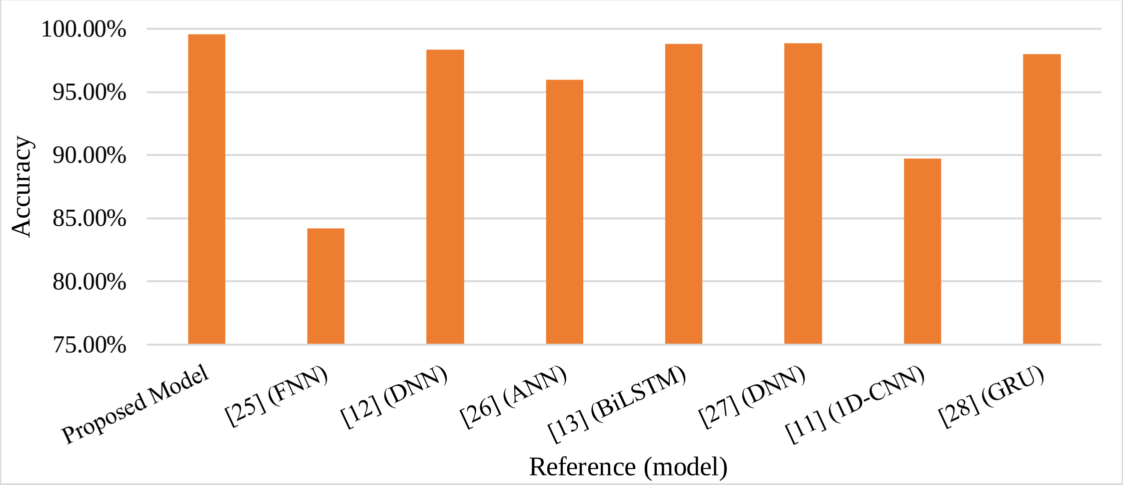


Fig. 9 Proposed model's accuracy comparison with previous studies that used DL with FL

5.4. Discussion and Limitation

The anti-DDoS system presented in this study was carefully designed to be deployable in real-world networks, particularly Telecom cloud networks. To achieve optimal performance, the proposed model was designed using different RNN technologies that are capable of profoundly capturing dependencies among network traffic, giving it an advantage over previously proposed models. The findings from the experiments show that the new model performs better than previous models in terms of both accuracy and speed in a federated learning environment.

A shorter detection time indicates the simplicity and computational efficiency of the proposed model. During the experiments, it was found that despite the SSL (RSA) encryption, the proposed model maintained an average performance that was similar to that observed without encryption during federated learning. This consistency might be attributed to the simplicity of the model, which is characterized by relatively few parameters.

Consequently, the encryption and decryption times have an imperceptible impact on the overall training duration of the model. Compared with the proposed system, previous studies did not consider the importance of data encryption during FL training. By using SSL encryption, the proposed system is more tailored for Telecom cloud network protection, which is heterogeneous in some cases.

The assessment of the proposed FL model compared to traditional models on the same dataset demonstrated some limitations in terms of performance. In fact, many traditional models outperform the proposed model, which the training process can explain. Centralized learning uses unified data, enabling a better understanding of attack patterns than FL.

However, the proposed models outperformed other traditional models. In real-world applications, data privacy preservation is very important, and FL provides this advantage compared to centralized learning. The proposed system presents a tradeoff between data privacy preservation and high performance, giving it more credit for Telecom cloud applications.

Despite the security and good performance of the proposed system for application to Telecom cloud, the study was limited by the size of the dataset, which did not allow for extensive exploration in larger network simulations, such as involving more than 100 clients in the federated learning process to mirror real-world Telecom cloud networks. Given the scope of the dataset, the simulation involved only three clients to maintain fairness and ensure efficient evaluation.

6. Conclusion

This study proposes the use of federated learning and a novel hybrid RNN model to combat DDoS attacks in a heterogeneous Telecom cloud environment, where network functions are hosted across different cloud provider networks. To enhance the security of federated learning, SSL with RSA encryption has been proposed to prevent data tampering or man-in-the-middle attacks during the FL process.

The outcomes of the simulation showed that the proposed model surpassed previous research in terms of accuracy, with lower false positive rates and quicker detection times. Unlike previous studies, the current approach is more secure and tailored to detect and mitigate DDoS attacks on heterogeneous, cloud-based Telecom networks. In the future, the focus will be on exploring large-scale simulations involving more clients using more extensive datasets.

Funding Statement

This study was also supported by the African Union (AU).

References

[1] Kasim Oztoprak, Yusuf Kursat Tuncel, and Ismail Butun, “Technological Transformation of Telco Operators towards Seamless IoT Edge-Cloud Continuum,” *Sensors*, vol. 23, no. 2, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] QingYun Meng et al., “An Automatic Integration Deployment Framework for Telecom Cloud Network,” *2022 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Beijing, China, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Anil Kumar Rangsietti, and Siva Sairam Prasad Kodali, “SDN-Enabled Network Virtualization and Its Applications,” *Software Defined Networks: Architecture and Applications*, John Wiley & Sons, Ltd, pp. 231–277, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] A.L. Zubilevich, S.A. Sidnev, and V.A. Tsarenko, “Service Level Agreement with Differentiated Reliability Requirements : Efficiency of Application in Communication Networks and On-Board Systems,” *2022 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russian Federation, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Kibeom Park et al., “Technology Trends and Challenges in SDN and Service Assurance for End-to-End Network Slicing,” *Computer Networks*, vol. 234, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Céline Gicquel, Sonia Vanier, and Alexandros Papadimitriou, “Optimal Deployment of Virtual Network Functions for Securing Telecommunication Networks against Distributed Denial of Service Attacks: A Robust Optimization Approach,” *Computers and Operations Research*, vol. 146, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Meenakshi Mittal, Krishan Kumar, and Sunny Behal, “Deep Learning Approaches for Detecting DDoS Attacks: A Systematic Review,” *Soft Computing*, vol. 27, no. 18, pp. 13039-13075, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Jie Wen et al., “A Survey on Federated Learning: Challenges and Applications,” *International Journal of Machine Learning and Cybernetics*, vol. 14, no. 2, pp. 513-535, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Dingyang Lv et al., “DDoS Attack Detection Based on CNN and Federated Learning,” *2021 Ninth International Conference on Advanced Cloud and Big Data (CBD)*, Xi'an, China, pp. 236-241, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Roberto Doriguzzi-Corin, and Domenico Siracusa, “FLAD: Adaptive Federated Learning for DDoS Attack Detection,” *Computers & Security*, vol. 137, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Francisco Lopes de Caldas Filho et al., “Botnet Detection and Mitigation Model for IoT Networks Using Federated Learning,” *Sensors*, vol. 23, no. 14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Ahmad Zainudin et al., “FedDDoS: An Efficient Federated Learning-Based DDoS Attacks Classification in SDN-Enabled IIoT Networks,” *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, pp. 1279-1283, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zengguang Liu et al., “An Asynchronous Federated Learning Arbitration Model for Low-Rate DDoS Attack Detection,” *IEEE Access*, vol. 11, pp. 18448-18460, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Saeid Sheikhi, and Panos Kostakos, “DDoS Attack Detection Using Unsupervised Federated Learning for 5G Networks and Beyond,” *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Gothenburg, Sweden, pp. 442-447, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Krzysztof Zarzycki, and Maciej Ławryńczuk, “Advanced Predictive Control for GRU and LSTM Networks,” *Information Sciences*, vol. 616, pp. 229-254, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kamil Masalimov, Tagir Muslimov, and Rustem Munasypov, “Real-Time Monitoring of Parameters and Diagnostics of the Technical Condition of Small Unmanned Aerial Vehicle’s (UAV) Units Based on Deep BiGRU-CNN Models,” *Drones*, vol. 6, no. 11, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Daniel J. Beutel et al., “Flower: A Friendly Federated Learning Research Framework,” *arXiv*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “A Detailed Analysis of the CICIDS2017 Data Set,” *Information Systems Security and Privacy*, pp. 172-188, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Oussama Sbai, and Mohamed Elboukhari, “Deep Learning Intrusion Detection System for Mobile Ad Hoc Networks against Flooding Attacks,” *IAES International Journal of Artificial Intelligence*, vol. 11, no. 3, pp. 878-885, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] G.C. Amaizu et al., “Composite and Efficient DDoS Attack Detection Framework for B5G Networks,” *Computer Networks*, vol. 188, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Abdullah Emir Cil, Kazim Yildiz, and Ali Buldu, “Detection of DDoS Attacks with Feed Forward Based Deep Neural Network Model,” *Expert Systems with Applications*, vol. 169, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Deepak Kumar et al., “DDoS Detection Using Deep Learning,” *Procedia Computer Science*, vol. 218, pp. 2420-2429, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Malliga Subrmanian et al., “Evaluating the Performance of LSTM and GRU in Detection of Distributed Denial of Service Attacks Using CICDDoS2019 Dataset,” *Proceedings of 7th International Conference on Harmony Search, Soft Computing and Applications*, pp. 395-406, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Juan Fernando Cañola Garcia, and Gabriel Enrique Taborda Blandon, “A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks,” *IEEE Access*, vol. 10, pp. 83043-83060, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Euclides Carlos Pinto Neto, Sajjad Dadkhah, and Ali A. Ghorbani, “Collaborative DDoS Detection in Distributed Multi-Tenant IoT Using Federated Learning,” *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, Fredericton, Canada, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Roberto Doriguzzi-Corin, and Domenico Siracusa, “FLAD: Adaptive Federated Learning for DDoS Attack Detection,” *Computers & Security*, vol. 137, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Muhammad Nadeem Ali et al., “Low Rate DDoS Detection Using Weighted Federated Learning in SDN Control Plane in IoT Network,” *Applied Sciences*, vol. 13, no. 3, pp. 1-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Jianhua Li et al., “FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4059-4068, 2022. [CrossRef] [Google Scholar] [Publisher Link]