PSO-Enhanced Federated CNN-LSTM for Privacy-Preserving DDoS Detection in Multi-Tenant Clouds

Reena TG[1], Vasumathi AK[2], Bharath H C[3]

[1] Department of Computer Science and Engineering, Cambridge Institute of Technology, Bengaluru, India

[2] Department of Computer Science and Engineering, Cambridge Institute of Technology, Bengaluru, India

[3]Department of Computer Science and Engineering (Data Science), Bapuji Institute of Engineering and Technology, Davangere, India

HOW TO CITE:

Reena TG[1], Vasumathi AK[2], Bharath H C3 (2026). PSO-Enhanced Federated CNN-LSTM for Privacy-Preserving DDoS Detection in Multi-Tenant Clouds.

International Journal of Special Education, 41(19s),781 - 794

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks are a major security challenge in cloud computing because of their characteristic of depleting resources, thereby lowering availability of services. The centralized machine learning based detection of DDoS attack poses some major challenges related to privacy and scalability issues within multi-tenant cloud. This work introduces a PSO-Optimized Federated CNN-LSTM model for accurate and privacy-preserving DDoS detection. CNN used for extraction of spatial traffic features, LSTM is used for capturing sequential traffic behaviors. Federated learning permits collaborative training of the model without exposing raw traffic. Particle swarm optimization (PSO) is applied for hyper parameter optimization. Evaluation on DRDoS data-set consisting of 193,956 traffic records and 70 features provides a 98.62% detection accuracy. Our model provided the increase in scalability, privacy-preservation, and correct DDoS detection.

Keywords: DDoS Detection, Federated Learning, CNN-LSTM, Particle Swarm Optimization, Cloud Computing, Multi-Tenant Architecture, AWS

. Introduction

Cloud computing is one of the most rapid technologies to adapt itself within present computing scenarios. It benefits not only from elasticity, flexibility, but also from efficient and cost-effective resources. It allows computation services to be deployed over the internet and has been adapted by various modern applications such as healthcare systems, financial institutes, industrial automation, and education. Among different deployment models in cloud computing, multi-tenant cloud computing has received tremendous research interest as it permits various users or tenants to share one cloud environment while retaining an individual logical environment from each other's view.

Resource utilization is hence increased and operation cost for the cloud provider is decreased. However, security vulnerabilities have severely impacted the cloud computing environment in various ways, and Distributed Denial-of-Service (DDoS) is one of the most critical and damaging attack in cloud systems [1]. DDoS attack is an intrusion that seeks to

compromise the availability of a server, network resource or a service by flooding with a huge volume of traffic from botnets. This attack may lead to exhaustion of resources, degradation of performance, increased network congestion and hence deny access of services for normal users. The threats from DDoS attack become more serious in a multi-tenant cloud environment due to resource sharing. The performance and availability of a tenant may also be influenced by an attack aimed at another tenant in the same cloud infrastructure. Therefore, efficient and scalable DDoS detection mechanism becomes essential for providing the stable and reliable services in cloud computing systems [2]. Traditional detection techniques used are typically signature-based methods and centralized machine learning methods. Signature-based methods can detect known attack patterns effectively, but often fail in detecting novel attacks. Machine learning based intrusion detection systems can adapt themselves in detecting anomalous traffic behaviour patterns and new attacks better than signature-based detection techniques. However, a large portion of centralized machine learning algorithms require the collection of tremendous amount of data from a large number of users or devices to a central location. But centralized machine learning approaches raise issues on user privacy, high communication overhead, data leakage risk, and poor scalability in large distributed cloud environments [3]. More recently, deep learning methods have greatly enhanced the performance in network intrusion detection systems. CNNs can effectively extract the high level spatial features in network traffic data while LSTMs excel in capturing sequential behaviour and temporal traffic patterns [4], [5]. Combining both CNNs and LSTMs would help in learning both spatial and temporal features from network traffic, thus increasing detection accuracy.

To avoid centralized learning challenges, federated learning (FL) has been developed as a decentralized machine learning approach where numerous clients train a shared model collaboratively without sharing the actual raw data [6]. Each tenant trains the model in its own local environment using its private data. Only model parameters are shared with a centralized federated server. FL offers a way to preserve user data privacy, minimize communication costs, and achieve better scalability [7]. Although Federated Learning improves user privacy and distributed model training, performance of deep learning model is still affected by number of hyper-parameters such as learning rate, dropout rate, hidden layer number, etc. Fine-tuning of hyper parameters using manual search is generally inefficient and does not guarantee an optimal result. Optimization algorithms, such as Particle Swarm Optimization (PSO), may hence be used to find out the optimal values for hyper-parameters to increase the model performance [8].

In this research, a PSO-Optimized Federated CNN-LSTM framework is proposed for efficient DDoS detection in multi-tenant cloud computing environment. It combines the effectiveness of CNN feature extraction capability, LSTM's ability of sequential learning, FL's user data privacy preservation feature and PSO's optimization ability. The framework is tested in a simulated multi-tenant cloud computing environment using DRDoS dataset which contains

The main contributions of this work are summarized as below:

• A novel PSO-Optimized Federated CNN-LSTM framework is developed to implement efficient DDoS detection in multi-tenant cloud computing.

• Federated Learning technique is incorporated to preserve tenant's data privacy from being directly revealed.

• The spatial and sequential behavior patterns in the network traffic data are jointly captured using combined CNN and LSTM models.

• Particle Swarm Optimization is used to optimize hyper parameters to further enhance classification performance.

An extensive experimental study has been conducted on a real world dataset of 193,956

records and 70 features (DRDoS dataset) in a multi-tenant cloud scenario. The experimental results indicated that the proposed framework effectively detects DDoS attacks while ensuring scalability and user privacy for cloud computing environment.

2. Related Work

Various researches have been carried out for DDoS attack detection based on machine learning, deep learning, Federated learning and optimization techniques. Here in this section we will be discussing researches based on CNN-based detection models, LSTM-based intrusion detection systems, Federated Learning-based security frameworks and PSO-based optimization methods for better detection performance in the cloud.

2.1. CNN-Based DDoS Detection Studies

CNNs are well popular in network security due to their ability to automatically discover and learn high level features from enormous volumes of network traffic data without feature engineering. CNN based method is powerful and efficient for detecting the complex traffic patterns of DDoS attack.

Rethish Kumar S. And Vijayakumar R. Presented a hybrid CNN-LSTM model for DDoS detection in the cloud using the CICDDoS2019 dataset [4] that achieved 98.7% detection accuracy and low false positive rate. The system uses a centralized learning architecture and is unable to handle privacy in multi-tenant clouds. Navya Vattikonda et al. Compared CNN-LSTM models to the ID3 machine learning model to analyze the performance of the system for DDoS attack detection [1], reporting 98.5% classification accuracy and improved attack detection rates. They fail to address distributed learning or methods to optimize the model. Saswati Chatterjee et al. Proposed a PSO-CNN-LSTM-ANFIS model for DDoS detection which reached a 99.30% accuracy [9]. Their work was created with a centralized learning structure and has no approach for multi-tenant privacy or scalability.

Despite these highly accurate CNN-based DDoS detection systems, most of them have the fundamental issue of central data collection that can compromise privacy and leads to high communication and scalability costs in the cloud.

2.2. LSTM-Based Intrusion Detection Studies

Intrusion Detection System (IDS) employ Long Short-Term Memory (LSTM) networks because they have the ability to learn the time-based and sequence-based patterns of traffic data. Rethish Kumar S and Vijayakumar R, proposed a hybrid deep learning model based on LSTMs that used sequence learning of traffic for detection of DDoS attacks. The detection accuracy was also very high [4]. In [8] R. Diro and N. Chilamkurti developed a distributed deep learning-based intrusion detection framework for the IoT environment using deep neural network models. It achieved high detection performance for attack detection by learning traffic behavior from the distributed environment. In [10]

A. Javaid et al designed a deep learning-based intrusion detection system, it detects unusual network traffic behaviors and the classification performance was high. Even though the LSTM based models have efficient capability for sequential learning, stand-alone LSTM models is poor on extract spatial features of traffic from network traffic, while the CNN based models show excellent performance on this aspect. Therefore, hybrid deep learning architectures such as CNN-LSTM have gained significant attention because they combine the feature extraction capability of CNN with the sequential learning capability of LSTM, thereby improving overall DDoS detection performance [4], [5].

2.3. Federated Learning-Based Security Studies

Federated Learning (FL) is a distributed approach to machine learning, in which a number of clients/tenants together train an ML model without revealing any private data, thus also saving communication costs. Given these characteristics, Federated Learning has drawn a

lot of interest in the areas of cybersecurity and cloud-based intrusion detection systems.

The work by Yuxi Wang et al. Presented a Federated Learning-based anomaly detection framework for multi-tenant cloud platform by introducing personalization of the model so that robust detection results are achieved under heterogeneous cloud environments [3]. Although the proposed framework showed better detection performance it is intended for general anomaly detection rather than the specific problem of DDoS attack detection. Rahmati and Pagano provided a Federated Learning-based intrusion detection system for IoT security applications [4] which also provided stronger privacy protection. Their approach gained high detection accuracy while improving privacy preservation but is more suitable for IoT environments rather than multi-tenant cloud systems.

2.4 PSO-Based Optimization Studies

PSO (particle swarm optimization) is commonly utilized in the hyper-parameter tuning of machine and deep learning models since it is capable to find out appropriate parameters more effectively Sharma et al. implemented a PSO-based optimization approach for intrusion detection systems and achieved improved classification accuracy with reduced training time [14]. However the framework was evaluated only in single tenant environment. Saswati Chatterjee et al.Have incorporated PSO into CNN-LSTM frameworks for detecting DDos attacks and obtained high detection accuracy and convergence [9]. Although the framework works fine, the framework is proposed in a centralized learning manner, without the adoption of FL to protect the privacy in multi-tenant cloud.

2.5 Research Gap Analysis

Although the prior research work on the DDoS detection has achieved favorable performance through different techniques including CNN, LSTM, Federated Learning and PSO optimization, most of the existing systems depend on a centralized learning system and thus share the network traffic directly with other users, which may lead to privacy issues and large scalability in the cloud. While Federated learning ensures the privacy preservation in the cloud network, most existing work is on the general intrusion detection systems, and it doesn't consider the specific case of DDoS attack in multi-tenant cloud system.

Moreover, there is very little investigation that deals with integration of hybrid CNN-LSTM with Federated Learning and PSO for privacy-preserving detection of DDoS attacks. Hence, we propose a PSO-Optimized Federated CNN-LSTM model to effectively detect DDoS attack in simulated multi-tenant cloud system with data privacy and classification accuracy.

3. Dataset Description

The success of both deep learning and machine learning models depends on the quality, quantity and relevance of dataset used in training and testing of the models. In this research work, the DRDoS (Distributed Reflection Distributed Denial-of-Service) dataset acquired from the Canadian Institute for Cybersecurity (CIC) traffic collection framework was used to train and test the proposed PSO-Optimized Federated CNN-LSTM framework to detect DDoS attack in a simulated multi-tenant cloud environment. The dataset consists of normal network traffic and malicious network traffic from different DDoS attack type in a simulated real world environment. This dataset has several statistical flow-based network traffic features that can be effectively used for intrusion detection and traffic classification. Table 1 lists out the general description of the DRDoS dataset used for this research work.

Table 1.DRDoS Dataset Description

Parameter	Value
Dataset Name	DRDoS Dataset
Source	Canadian Institute for Cybersecurity (CIC)
Total records	193,956
Number of Features	70
Number of Classes	6
Classification Type	Multi-Class

The network traffic features of this dataset includes Source Port, Destination Port, Flow Duration, Packet Length Mean, Flow Bytes per Second, Flow Packets per Second, Average Packet Size and Inter-arrival Time. The set of these traffic features are important statistics that helps to distinguish normal traffic from DDoS malicious attack traffic pattern.

The DRDoS dataset comprises of six different traffic patterns which falls under normal network traffic behaviour and different types of DDoS attack behaviours. Then these classes are numerically labeled as 0-5 for the multi-class classification in pre-processing stage. Table 2 summarizes the class distribution on the numerically labeled traffic classes used in this study.

Table 2. Class Distribution of DRDoS Dataset

Label	Attack Type
0	Benign Traffic
1	DrDoS_DNS
2	DrDoS_LDAP
3	DrDoS_SNMP
4	DrDoS_UDP
5	SYN Flood

4. Proposed Methodology

This framework uses the CNN, LSTM, Federated Learning (FL) and Particle Swarm Optimization (PSO) model to perform DDoS detection efficiently with privacy-preservation over the simulated multi-tenant cloud environment. Firstly, the training dataset of DRDoS is individually kept within each tenant, such as in the cloud storage of Amazon S3, then

preprocesses the data by performing data cleaning, normalization, label encoding, train-test splitting, etc. Next, every tenant individually trains its CNN-LSTM model over the privately data locally and does not share any of raw traffic data.

Then sends the locally trained model weight to the Federated Aggregator, by utilizing FedAvg algorithm which aggregates all of model weights into one improved global model. Finally, it is sent to back to each tenant to update locally trained model. And also PSO module is used as a hyperparameter optimization layer that aims at optimizing learning rate, dropout rate, batch size and hyperlayer setting in CNN-LSTM, etc., At last, the well-trained global CNN-LSTM model will be used to detect and classify DDoS attacks. Lastly, the optimized CNN-LSTM model is kept in the cloud storage (Amazon S3).

4.1Global Framework Architecture

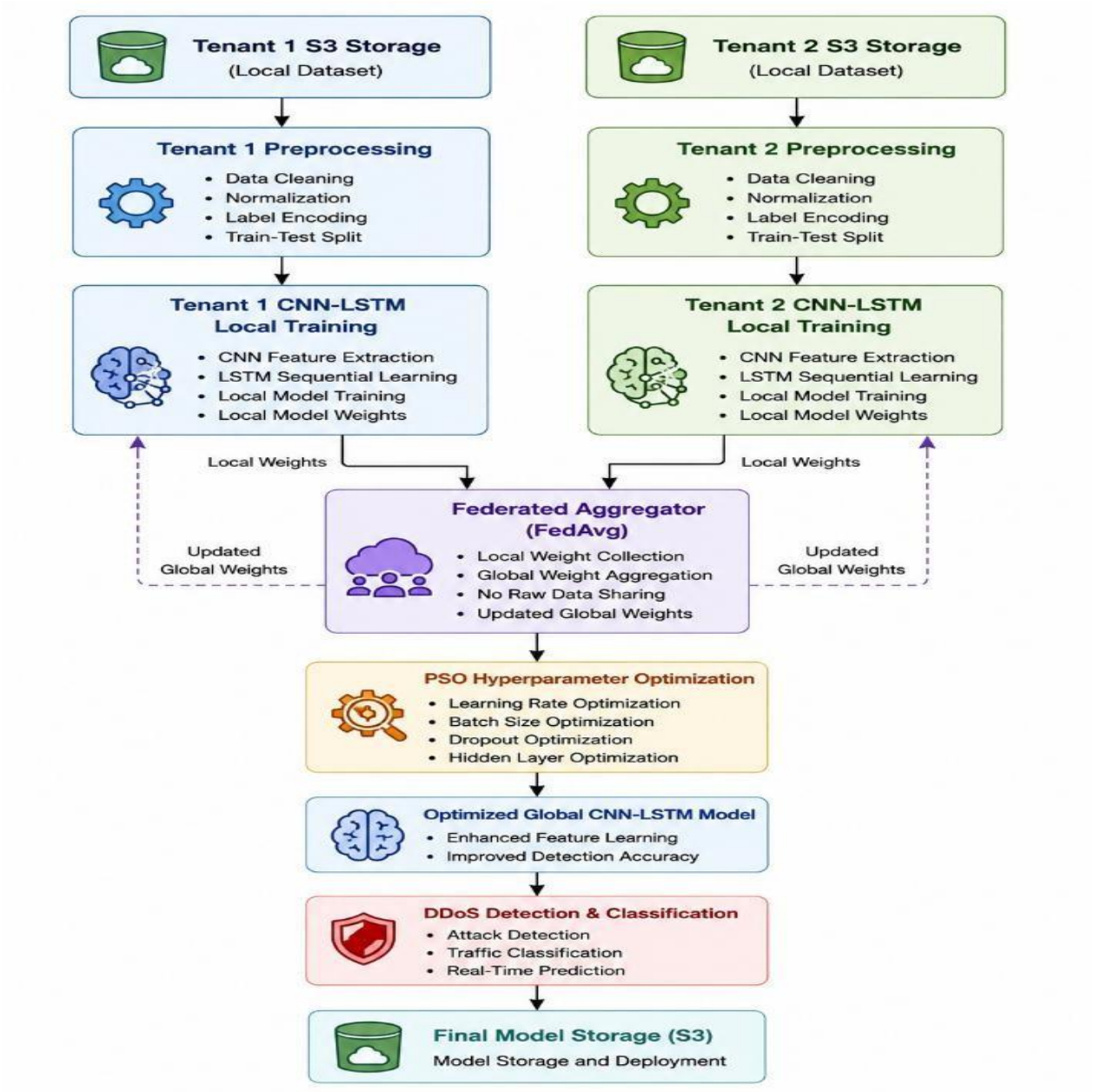

Figure 1 Proposed PSO-Optimized Federated CNN-LSTM Framework for DDoS

4.2 CNN-LSTM Architecture

A hybrid CNN-LSTM model as described below is used for detecting and classifying DDoS attacks on the basis of network traffic. The CNN portion helps to extract effective spatial traffic features from network records while the LSTM model helps to analyze temporal behavior and traffic pattern related to DDoS attacks. This combination significantly enhance learning ability and better results are achieved compared to normal ML based approaches. First, the processed network traffic data are input to the CNN layer. Convolution operation is used to extract meaningful traffic patterns and hidden attack features from the records using multiple filters, after which the Max-Pooling layer is used to reduce feature dimensionality and computational complexity of traffic features while keeping essential traffic patterns, the obtained feature map are fed into the LSTM layer and then effective analysis for sequential dependency and temporal attack features is carried out.

The dropout layer is also introduced into the model to mitigate over fitting and make it generalized, in the end these learned features are fed to multiple Dense layers and a Softmax layer to perform multiclass classification of different kinds of DDoS attack, the combined CNN-LSTM model can efficiently extract spatial and temporal traffic features thereby the DDoS detection effectiveness of the model could be boosted on the multi-tenant cloud platform. The components of proposed CNN-LSTM model is detailed below:

Table 3. CNN-LSTM Layer Configuration

Layer	Configuration	Layer
Conv1D	64 filters	Conv1D
MaxPooling1D	Pool size = 2	MaxPooling1D
LSTM	50 units	LSTM

4.3 Federated Learning Procedure

Federated Learning (FL) is a distributed machine learning method in which multiple tenants jointly train a global model while keeping their local raw data off the network, thereby mitigating the privacy issues of centralized training approach and decreasing the communication load in multi-tenancy cloud environment. In the described architecture, two tenants were set up by independently dividing the DRDoS data set, so as to emulate the multi-tenancy cloud environment. Each tenant has its own private network traffic data and trained a local CNN-LSTM model by using the data. After local model training, each tenant only sends the weights and parameters of the trained local models, instead of raw network traffic data, to the centralized FL server in order to preserve data privacy and facilitate distributed learning among tenants. The federated server is used to average the models of individual tenants and updates a global model parameter by using the Fed-Avg algorithm. Then, the weights of the global model are distributed to individual tenants, and this procedure is repeated for a certain number of iterations. The designed FL approach could enhance scalability, decrease the risk of sensitive data sharing, and accelerate the process of efficient privacy-preserved DDoS detection in multi-tenancy cloud.

4.3 Fed-Avg Aggregation

Fed-Avg Aggregation Fed-Avg or Federated Averaging is the aggregation mechanism adopted in the proposed federated learning

architecture. Each tenant sends their local CNN-LSTM model parameters to the federated server. In this process, raw network traffic data is not shared by each tenant to avoid data privacy issues and communication overhead, and only locally trained model weights are communicated. In the proposed approach, each tenant trains its local CNN-LSTM model based on its own data privately. After the local model training, local model parameters are sent to the federated server and fed-avg algorithm is used by the federated server to aggregate all the local model weights to get updated global model. Finally, the updated global model parameters are sent to the tenants. The mathematical representation of Federated Averaging is given by:

$$Wglobal = (W1 + W2 + \ldots + Wn) / n \quad (1)$$

Where, W

By applying the Fed-Avg aggregation mechanism, the collaborative learning performance can be enhanced while retaining the privacy protection mechanism for the multi-tenants cloud systems

4.4 PSO Hyper parameter Optimization

In order to enhance the efficiency of the CNN-LSTM model, the proposed framework makes use of Particle Swarm Optimization (PSO) as a hyper-parameter optimization algorithm. PSO is a population-based stochastic optimization technique that mimics the swarming behavior of birds or fish school. In the proposed work, the optimum hyper parameter configuration for the federated CNN-LSTM model is obtained using PSO to attain faster convergence of the model and enhance the detection accuracy for DDoS attacks. To begin with, an arbitrary set of particles are initialized that depict the potential hyper parameter solution for the CNN-LSTM model. As the optimization process progresses, every particle will adjust its own best solution along with the global best solution obtained by the swarm. The optimization will continue for multiple iterations until the optimal hyper parameter solution is obtained. In this framework, PSO is used to optimize important CNN-LSTM hyper parameters such as learning rate, batch size, dropout rate and hidden layer configurations. By selecting optimal hyper parameter values, the proposed framework improves classification performance, minimizes overfitting and enhances the overall DDoS attack detection capability in multi-tenant cloud environments

Table 4. PSO Optimized Hyper parameters

Hyper-parameter	Optimized Value	Hyper-parameter	Optimized Value
Learning Rate	0.001	Learning Rate	0.001
Batch Size	64	Batch Size	64
Dropout Rate	0.2	Dropout Rate	0.2

. Results And Discussion

5.1 Experimental Environment

The proposed PSO-Optimized Federated CNN-LSTM framework was designed and developed using Python language by means of different libraries; Tensor Flow, Keras, Scikit-learn and NumPy. The experiment design was set up on a simulated multi-tenant cloud using Amazon Web Service (AWS) EC2 instances. For the training and testing of the proposed system the DRDoS dataset developed by the Canadian Institute for Cybersecurity (CIC) was employed. Initially the dataset was pre-processed, cleaning it, normalizing, label encoding, train -test split. Then, it was divided into two separate tenants for a simulated multi-tenant federated environment. The data in each tenant was used

to train the local CNN-LSTM independently and privately without exposing raw network traffic records of each other. The CNN-LSTM was trained using hyper-parameters tuned through Particle Swarm Optimization (PSO). Performance was evaluated on a number of metrics: Accuracy, Precision, Recall and F1-Score. The comparison was between the proposed PSO-FL CNN-LSTM framework and other existing deep learning methods

5.2 Performance Metrics

The performance of the developed PSO-Optimized Federated CNN-LSTM system has been evaluated using standard classification metrics utilized in the fields of cyber security and intrusion detection. In this research, the following evaluation metrics are used: Accuracy, Precision, Recall and F1-Score.

Accuracy depicts the overall performance of the proposed model to distinguish between malicious and normal network traffic. Precision determines the fraction of detected attack traffic over the total predicted attack traffic. Recall shows the portion of attack traffic that the proposed model correctly detected. F1-Score gives a unified measure of a classifier and is computed as the weighted harmonic mean of Precision and Recall.

The mathematical expression for the classification accuracy is as:

$$Accuracy = (TP+TN)/ (TP+TN+FP+FN) \quad (2)$$

Where, TP indicates the True Positive TN indicates the True Negative FP indicates the False Positive FN indicates the False Negative

5.3 Performance of Local CNN-LSTM

The local CNN-LSTM model was trained independently on each of the tenants' datasets in order to examine how well the proposed framework can learn the behaviour of traffic in a tenant environment. This separate training was aimed to observe how well the CNN-LSTM network is capable to learn DDoS attacks before the process of federated learning and PSO optimization is initiated. The outcomes of this local training are as follows: when the model was trained on the data of Tenant 1 it attained the classification accuracy of 98.61%, while the model trained on Tenant 2 attained a classification accuracy of 97.25%. The difference of classification accuracy between two tenants is based on varied distribution of traffic and attack behavior. The training outcomes demonstrate that CNN-LSTM network can learn the spatiotemporal features from the network traffic record. Convolutional layers were effective for learning the significant traffic features, while recurrent LSTM layers captured the spatio-temporal behaviour of attacks from the network traffic. The training accuracy graph of the local CNN-LSTM network can be depicted in Figure 2

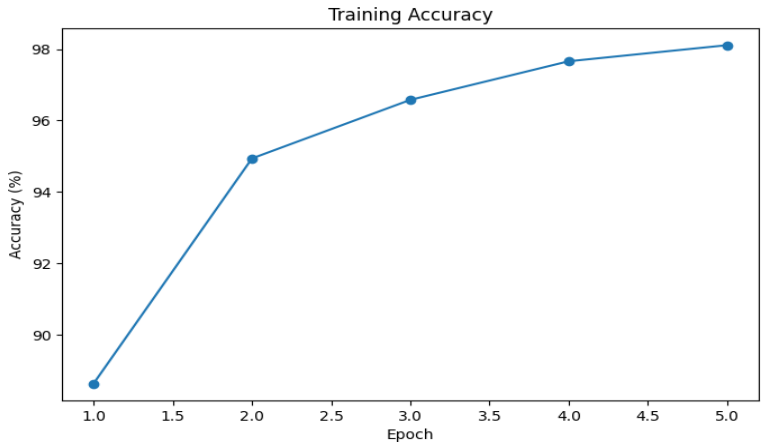

Figure. 2 Training Accuracy Graph

These results portray the successful ability of the presented CNN-LSTM network to provide an effective DDoS detection performance in a distributed multi-tenant environment even without the techniques of federated learning and optimization

5.4 Federated Learning Performance

The proposed federated learning was employed to cooperatively train the model from several tenants without sharing raw network traffic data. In federated learning, each tenant trained its local CNN-LSTM model with its own traffic data individually and only shared the obtained model parameters to a federated server. The parameters from different local models were aggregated using Federated Averaging (Fed-Avg) algorithm, thus to obtain a common global model parameters. Subsequently, aggregated global model parameters were shared to each tenant in the subsequent round to continuously improve the model performance through federated learning and the tenant data privacy is maintained. Experimental results indicated that the developed federated CNN-LSTM system achieved 98.56% for global classification accuracy. The obtained results exhibit that federated learning can effectively increase the generalization performance to various tenant environments and avoid the direct communication of private network traffic-data.

Figure 3 shows the progress in federated learning for this cooperative model training approach. It can be seen that the global model converged stable during the federated learning rounds.

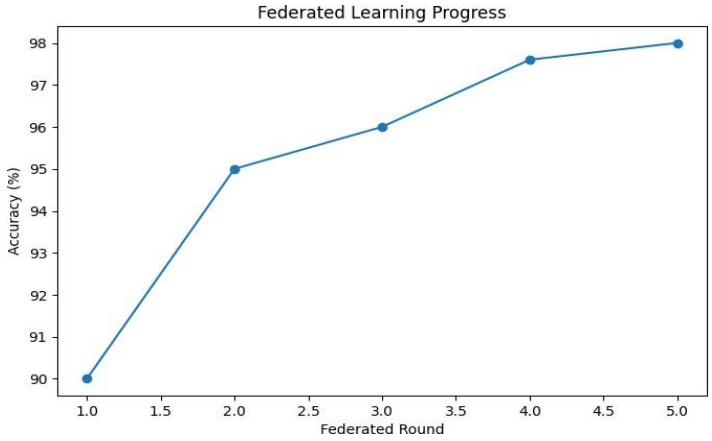

Figure. 3 Federated Learning Progress Graph

The presented results prove that the federated learning mechanism proposed here presents an effective and privacy-friendly approach to attack detection in a multi-tenant cloud scenario.

5.5 PSO Optimized Performance

To optimize key hyper-parameters including learning rate, batch size, dropout rate and hidden layer structures of the federated CNN-LSTM approach proposed herein, the Particle Swarm Optimization (PSO) technique was adopted to enhance model convergence, suppress overfitting and boost overall DDoS attack detection accuracy. During the optimization procedure, numerous particles representing varying hyper-parameter settings were randomly initiated. Following its individual optimum while considering the global optimum among particles, each particle refined its coordinates iteratively and thus, sought for superior hyper-parameter configurations that were able to obtain maximum classification accuracy and minimum loss through a global search. From the experimentation conducted, it can be seen that by utilizing PSO for hyper-parameter optimization, it was able to boost the federated CNN-LSTM performance, showing better convergence stability and high detection rate in comparison to the not optimized model. Also, the optimum hyper-parameters used led to less variation during the training process and improved model generalisation ability. The

convergence process during PSO optimization is depicted in Figure 4 below:

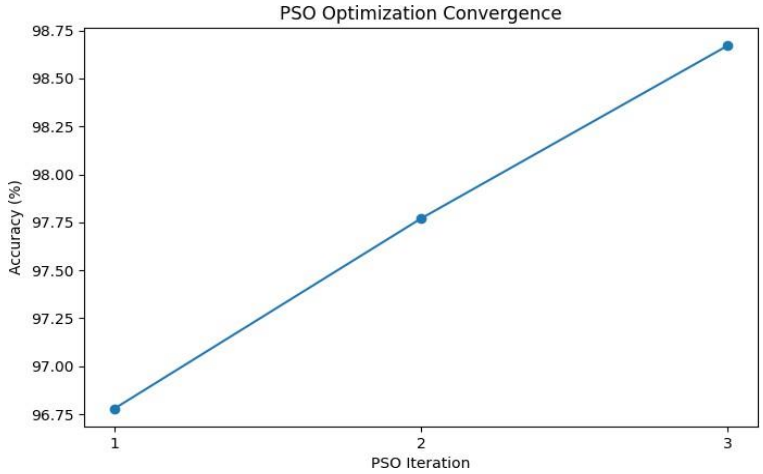

Figure. 4 PSO Optimization Convergence

The result obtained shows that, in each iteration, the optimization process steadily reached the optimum fitness value.

A comparative analysis was conducted in order to determine how well the proposed PSO-Optimized Federated CNN-LSTM approach compared against the various other learning approaches employed throughout the experimentation process. The classification accuracy attained by the local CNN-LSTM, federated CNN-LSTM, and PSO-optimized federated CNN-LSTM were the primary components of this analysis. The classification accuracy obtained by the local CNN-LSTM when it was trained using the data belonging to Tenant 1 was 98.61% and the accuracy when it was trained using the data belonging to Tenant 2 was 97.25%. For the federated CNN-LSTM the overall classification accuracy achieved by the federated model was 98.56%. It is clearly visible that a collaborating federated learning approach can effectively improve generalization without compromising tenant's privacy. Upon using Particle Swarm Optimization (PSO), the proposed PSO-FL-CNN-LSTM attained the highest classification accuracy, 98.62%. This indicates that PSO optimized the CNN-LSTM's hyper-parameters and improved convergence of training. The comparative performance of the models used in this study are provided in Table 4:

5.5 Comparison Analysis

A comparative analysis was conducted in order to determine how well the proposed PSO-Optimized Federated CNN-LSTM approach compared against the various other learning approaches employed throughout the experimentation process. The classification accuracy attained by the local CNN-LSTM, federated CNN-LSTM, and PSO-optimized federated CNN-LSTM were the primary components of this analysis. The classification accuracy obtained by the local CNN-LSTM when it was trained using the data belonging to Tenant 1 was 98.61% and the accuracy when it was trained using the data belonging to Tenant 2 was 97.25%. For the federated CNN-LSTM the overall classification accuracy achieved by the federated model was 98.56%. It is clearly visible that a collaborating federated learning approach can effectively improve generalization without compromising tenant's privacy. Upon using Particle Swarm Optimization (PSO), the proposed PSO-FL-CNN-LSTM attained the highest classification accuracy, 98.62%. This indicates that PSO optimized the CNN-LSTM's hyper-parameters and improved convergence of training. The comparative performance of the models used in this study are provided in Table 5:

Table 5. Model Results

Model	Accuracy (%)
CNN-LSTM (Tenant 1)	98.61
CNN-LSTM (Tenant 2)	97.25
CNN-LSTM (Tenant 3)	98.14
CNN-LSTM (Tenant 4)	97.89
CNN-LSTM (Tenant 5)	98.32
Federated CNN-LSTM	98.01
PSO-FL-CNN-LSTM	98.62

5.6 Analysis on Confusion Matrix

Confusion matrix analysis is implemented to judge the performance of the proposed PSO-Optimized Federated CNN-LSTM framework for various kinds of DDoS traffic classes. Confusion matrix will show the detailed analysis about what records has been classified correctly and which records are classified incorrectly while testing the model.

As it can be seen from the obtained confusion matrix, the proposed framework has classified most of the network traffic records without any misclassification. It shows a large number of correctly classified records in normal traffic and malicious traffic respectively, indicating that the CNN-LSTM architecture has learned efficiently on classifying traffic records.

Figure 6 is illustrating the confusion matrix for proposed PSO-FL-CNN-LSTM framework, where diagonal values are the records that have been classified correctly and non-diagonal values are misclassified traffic records.

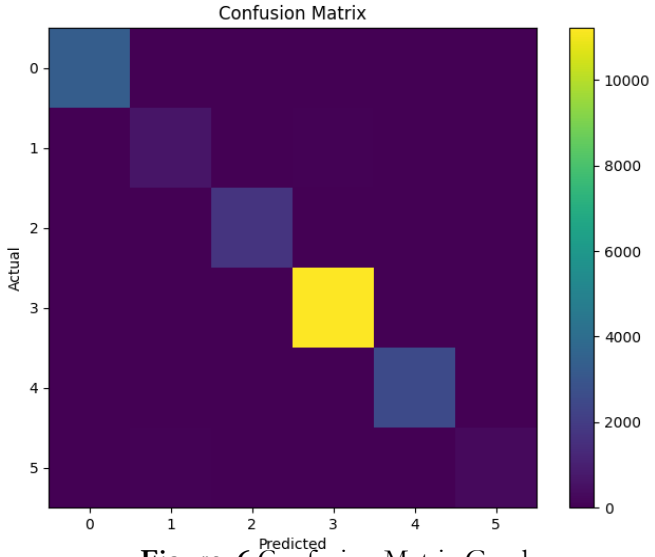

Figure. 6 Confusion Matrix Graph

Conclusion

The PSO-Optimized Federated CNN-LSTM framework for effectively detecting DDoS attacks in a multi-tenant cloud system has been presented in this study. The framework utilizes CNN for feature extraction, LSTM for learning sequences and time series data for network traffic, federated learning for privacy preserving learning over distributed tenants and particle swarm optimization (PSO) to find optimal hyper parameters. This framework helps to identify the attacks while protecting the privacy of each tenant without direct sharing of sensitive traffic data. The proposed framework was evaluated on a dataset of 193,956 traffic records with 70 network traffic features and named the DRDoS dataset. The dataset was divided into various tenants for simulated a federated multi-tenant cloud environment. Experimental results show that the local CNN-LSTM models can detect accurately the attacks. Also, the federated learning framework supports the collaboration with privacy preservation. With the combination of PSO, the federated CNN-LSTM model obtains the highest accuracy of 98.62%, showing good convergence and accuracy.

Further work of the proposed framework will focus on deploying in large scale real-time AWS cloud environment with multiple tenants and real-time traffic monitor system. Also, advanced federated learning mechanisms can be further investigated to enhance the scalability, communication efficiency and detection performance.

Declaration of Competing Interests

The authors declare no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Use of Generative Artificial Intelligence

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

Author Contributions

All authors contributed to the conceptualization, implementation, experimental analysis, manuscript preparation and review of the proposed research work

References

N. Vattikonda, A. K. Gupta, A. R. Polu, B. Narra, D. V. K. R. Buddula, and H. H. S. Patchipulusu, “Machine Learning-Based Approaches for Detecting and Mitigating Distributed Denial of Service (DDoS) Attacks to Improve Cloud Security,” European Journal of Technology, vol. 8, no. 6, pp. 28–48, 2024.

S. Zehra, H. J. Syed, and U. Faseeha, “FedMon: Federated eBPF Monitoring for Distributed Anomaly Detection in Multi-Cluster Cloud Environments,” IEEE Transactions on Cloud Computing, pp. 1–10, 2025.

Y. Wang, H. Liu, N. Long, and G. Yao, “Federated Anomaly Detection for Multi-Tenant Cloud Platforms with Personalized Modelling,” Proceedings of the IEEE International Conference on Cloud Computing, pp. 1–8, 2024.

R. Kumar and V. Vijayakumar, “Hybrid CNN-LSTM Deep Learning Framework for DDoS Detection in Cloud Environments,” IEEE Access, vol. 13, pp. 1–15, 2025.

H. Nguyen, K. Kim, and J. Kim, “A CNN-LSTM Based Framework for DDoS Attack Detection in Cloud Computing,” Proceedings of the IEEE International Conference on Big Data, pp. 2432–2439, 2021.

M. Alazab, S. P. RM, P. M., P. K. R.Maddikunta, T. R. Gadekallu, and Q.-V. Pham, “Federated Learning for Cybersecurity: Concepts, Challenges and Future Directions,” IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 1–15, 2022.

J.Zhang, X. Chen, and Y. Xiang, “Federated Learning Based Intrusion Detection for Cloud Networks,” IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 1545–1557, 2022.

R.Diro and N.Chilamkurti, “Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things,” IEEE Internet of Things Journal, vol. 7, no. 1, pp. 1–11, 2020.

S.Chatterjee, A. Roy, and P. Bhattacharya, “PSO-CNN-LSTM-ANFIS Framework for Intelligent DDoS Attack Detection in Cloud Networks,” Journal of Network and Computer Applications, vol. 225, pp. 103–118, 2024.

A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A Deep Learning Approach for Network Intrusion Detection System,” Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine, pp. 21–26, 2020.

L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT Security Techniques Based on Machine Learning,” IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1606–1618, 2020.

X. Li, W. Zhou, and Z. Tian, “Deep Learning-Based DDoS Detection in Software Defined Networking,” IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1–13, 2021.

M. Kim, J. Lee, and H. Kim, “PSO-Based Optimization of Deep Neural Networks for Network Intrusion Detection,” IEEE Access, vol. 9, pp. 1–14, 2021.

A. R. Abou El Kalam, A. K. Bashir, and M. Atiquzzaman, “Federated Learning for Privacy-Preserving DDoS Detection in Cloud Computing,” IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 1–12, 2023.

S.Khan, S. Parkinson, and Y. Qin, “Fog Computing Security: A Review of Current Applications and Security Solutions,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1144–1172, 2020

M. Rahmati and A. Pagano, “Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities,” IEEE Access, vol. 13, pp. 1–21, 2025.

H. Alkahtani and M. Aldossary, “Federated Deep Learning Framework for DDoS Attack Detection in Cloud Computing Environments,” IEEE Access, vol. 10, pp. 112345–112358, 2022.