

Federated Zero Trust Multi-Agent System for DDoS Defense with Blockchain

¹Mr. Janga Rajendar, ²Mr. A. Swamy Goud, ³Mr. Thirupathi Nanuvala, ⁴Dr. Bodla Kishor, ⁵Mr. R. Dileep Kumar, ⁶Mr. Ravindra Pappula

¹Assistant Professor, Dept. of CSE-DS, CMR Engineering College, Hyderabad, Email: janga.rajendar@cmrec.ac.n

²Assistant Professor, Dept. of Information Technology, BVRIT, Narsapur.

Email: swamygoud.a@bvr.it.ac.in

³Assistant Professor, Dept. of CSE, VNR Vignana Jyothi Institute of Engineering and Technology, Vignana Jyothi Nagar, Pragathi Nagar, Nizampet, Hyderabad

E-mail: thirupathi_n@vnr.vjiet.in

⁴Associate Professor, Dept. of CSE, CMR Engineering College, Hyderabad Email: trml.kishore@gmail.com

⁵Assistant Professor, , Dept. of CSE, CMR Engineering College, Hyderabad E-mail: dileep6@gmail.com

⁶ Assistant Professor, , Dept. of CSE, Matrusri Engineering College, Hyderabad E-mail: ravindragec539@gmail.com

HOW TO CITE:

Janga Rajendar, A.Swamy Goud, Thirupathi Nanuvala, Bodla Kishor, R.Dileep Kumar, Ravindra Pappula (2026). Federated Zero Trust Multi-Agent System for DDoS Defense with Blockchain. International Journal of Special Education, 41(16s), 1228-1239

ABSTRACT:

The spread of distributed network environments has led to a rise in the risk of Distributed Denial-of-Service (DDoS) attacks, which interrupt services by flood-ing network resources. Centralized traditional intrusion detection systems have various shortcomings such as issues with scalability, communication overhead, and privacy concerns of data. In order to tackle these problems, the present work puts forward a Federated Learning-based DDoS detection method that ensures privacy and security. The proposed system uses a combined CNN-BiLSTM model to accurately identify spatial and temporal features in network traffic. An RL-DQN, which stands for reinforce men learning-based feature selection, method is implemented to select the most relevant features there by reducing the time complexity and at the same time ensuring high detection accuracy. Besides, security has been improved by the incorporation of Zero Trust Architecture for continuous node verification, Byzantine-resilient aggregation methods to prevent adversarial updates, and homomorphic encryption for secure communication of model parameters. Furthermore, a Multi-Agent System permits adaptive decision- making, while blockchain technology provides transparency and the immutability of system logs. Based on the CIC-DDoS2019 dataset, the results show that the proposed framework can attain high precision, be scalable, and resilient in ever- changing and hostile environments which makes it a viable solution for the next generation of distributed cyber security systems.

Keywords: Denial-of-Service (DDoS) Dete1ction Federated Learning, Zero Trust Security, Privacy-Preserving Systems, and Network Security.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.

Open access publication under the terms and conditions

of the Creative Commons Attribution (CC BY)

license (<http://creativecommons.org/licenses/by/4.0/>).

Introduction

In today's networked environments, Distributed Denial-of-Service (DDoS) attacks have become

one of the most damaging and common threats. These attacks target resources of the systems by sending malicious traffic and consuming

and crippling their band-width, memory, and processing resources. Digital transformation in every industry, including cloud computing, e-commerce, healthcare, financial services, has increased reliance on uninterrupted network connectivity. It has also increased the impact of DDoS attacks, creating more service outages, causing financial losses and damaged data, and increasing the erosion of trust. Additionally, multi-vector attacks, reflection, amplification, and application-layer attacks have become more sophisticated, making detection and overcoming traditional defenses more difficult [1], [2]. Traditional DDoS detection systems rely heavily on centralized architectures, where network traffic information from various sources is gathered and analyzed in one central location. These systems usually use signature-based detection methods, statistical thresholding, or classical machine learning models to spot abnormal traffic patterns. Such approaches can detect moderate known attack types; however, they have several drawbacks. A major one is that being centralized, these systems have a single point of failure, making them extremely vulnerable to large-scale attacks. Besides that, the regular transmission of large amounts of network data increases communication overhead, latency, and bandwidth use. Most importantly, sharing sensitive network data among different entities poses serious privacy and security issues, especially in multi-organizational or cloud-based environments. Traditional systems also have difficulties in detecting zero-day attacks and changing attack patterns because they depend on predefined rules and static models, thus restricting their flexibility in dynamic network environments [3], [4]. Decentralized, collaborative approaches for intrusion detection have become increasingly popular as a response to these problems. Federated Learning (FL) is a distributed machine learning model that is being adopted by many since it is privacy-preserving by nature. It allows multiple nodes to work together in training a global model while keeping their data private. Thus, in this

model, a node trains its local model on its own dataset and only shares the model parameters or gradients with the aggregation server. Besides hiding the data, this method also lessens the amount of data exchanged between nodes and makes the system scalable. In DDoS detection, federated learning can provide a way to expose the system to different types of traffic from a variety of network domains. This, in turn, could improve the accuracy and robustness of the detection model [5], [6].

Along with its advantages, the decentralized aspects of federated learning also lead to new problems in terms of trust, security, and reliability. As a global model is determined by updates from multiple distributed nodes, the system becomes susceptible to adversarial attacks such as model poisoning where the malicious participants make changes to model update deliberately to degrade performance. Besides that, the different data distributions and the presence of unreliable nodes affect negatively the convergence and accuracy of the model. To deal with these problems, it is necessary to incorporate strong security mechanisms that can guarantee the genuineness and reliability of the learning process. Zero Trust Architecture (ZTA) has been recognized

as an excellent approach in this respect, as it requires every entity involved in the system to be continuously verified based on the main idea: "never trust, always verify." By constantly monitoring node activity and limiting the power of possibly compromised participants, zero trust strategies increase the ability of federated systems to withstand adversarial attacks [7], [8].

Besides security, another reason for using smart and adaptive detection methods is that cyber-attacks keep getting more complicated. One way to do this is through Multi-Agent Systems (MAS), which are essentially a set of independent agents each with their own intelligence, that work together to monitor the behavior of a system, analyze the network

conditions, and help in decision making. These agents can work on their own but by sharing the information they can collectively improve the performance of the system. This capacity to adapt in real-time to the changing attack patterns is one of the features of MAS. Besides, using MAS provides ways to increase fault tolerance, makes the system scalable and responsive, which is why it fits very well to the dynamic and distributed environments. Moreover, the blockchain technology is also considered the possibility of creating trust and transparency in decentralized systems. With the help of an unchangeable and tamper-proof ledger of system activities, blockchain can provide a layer of security that would make it hard for any unauthorized changes to be made to the system, hence giving an overall strengthening of the security framework [9], [10].

Deep learning has been a game changer for intrusion detection, in fact it completely changed the way the systems extract features from network traffic data, by learning complicated and high dimensional patterns. Machine learning techniques only allowed the expert to feed the features manually however deep learning techniques can identify the features automatically by learning hierarchies. Therefore, they are more adept at identifying old as well as new attack patterns. Especially, hybrid CNN-BiLSTM models have efficiently captured spatial and temporal features of network traffic giving great results. CNN layers find local spatial features while BiLSTM networks discover sequential dependencies and temporal dynamics thus offering an overall understanding of traffic behavior. Such hybrid models can detect both abrupt traffic changes and slow attack patterns leading to greater detection accuracy in challenging scenarios [11], [12]. Besides changing the model structure, choosing the right features is also very important for making detection systems work better and be more efficient. Network traffic data with many dimensions usually has redundant and irrelevant features that may reduce the model

performance and also increase the computational complexity. To deal with this problem, advanced feature selection methods focusing on reinforcement learning have been introduced to choose the most informative features dynamically. These methods analyze the balance between the accuracy and the computational efficiency so that the deployment of detection systems in real-time with limited resources becomes possible. Operating in real-time environments is another feature of modern intrusion detection systems that is really important. As network traffic keeps increasing in both volume and speed, it becomes not only desirable but also necessary for detection systems to be capable of handling data efficiently and at the same time issuing quick responses to potential threats. Using real-time data processing techniques along with adaptive learning mechanisms allows systems to update

their models based on recent data continuously and. This way, they can always be effective in fighting against changing attack methods. As a result of these technological advancements, there is an increasing demand for all-encompassing frameworks that not only combine distributed learning and sophisticated analytics but also include strong security measures to tackle the problems of DDoS detection in contemporary network scenarios. These frameworks are designed to offer solutions that are scalable, keep user data private, and are resilient to changes, all the while ensuring high levels of detection accuracy. Merging decentralized learning methods with smart decision-making and layered security techniques can lead to the creation of state-of-the-art intrusion detection systems that are more capable of dealing with the complexities of current cyber threats. Under these circumstances, federated learning combined with deep learning, zero trust security, multi-agent intelligence, and blockchain technology integration constitutes an excellent avenue for future work. These technologies jointly overcome the drawbacks of the old methods by making the system

more scalable, protecting the privacy of the data, enhancing the accuracy of detection, and making the system robust. In the face of evolving cyber threats, the formulation of such integrated and adaptable frameworks will become indispensable in protecting modern digital infrastructures and facilitating secure and reliable network operations.

1 Proposed Methodology

Fig. 2.1 illustrates the multi-layered architecture of the proposed system in which each layer combines different technologies that will enable the DDoS detection to be efficient, secure, and scalable. Each layer has a different job but working together they make the system strong and flexible.

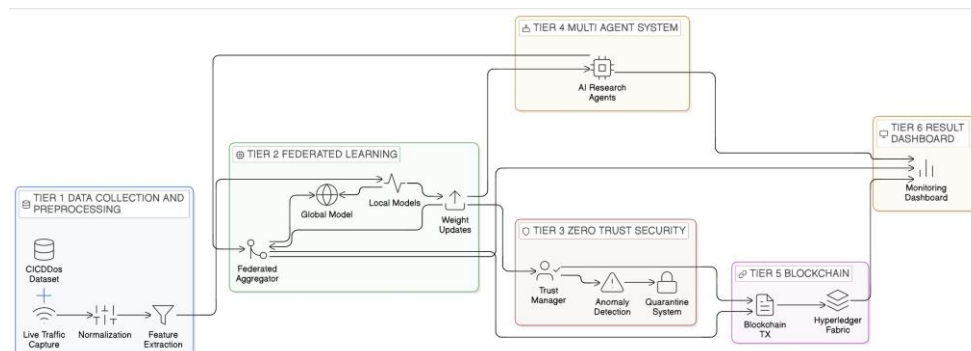


Fig. 2.1: System Design of Proposed System

Tier 1: Data Collection and Preprocessing

This tier collects network traffic data directly and changes it to structured data ready for machine learning. For packet collection, the live capture is done via Scapy, while for offline training the datasets like CIC-DDoS2019 are used. The raw packets

are first processed to extract flow-based features like packet count, byte count, flow duration, inter-arrival times, and TCP flags. Then, normalization, standardization, and class balancing are performed to keep the data consistent. Feature engineering and preprocessing must be used because raw network traffic is unstructured and not suitable for machine learning models. By representing packets with relevant numerical features, the system makes learning more efficient and also results in better detection. The role of this layer cannot be overstated since the performance of the model is highly dependent on the quality of input data. Good preprocessing can help get rid of irrelevant information, make important features more prominent, and also allow the system to work well in

different network environments.

Tier 2: Federated Learning

Federated Learning (FL) is a decentralized machine learning paradigm that allows multiple distributed nodes to jointly train a global model without exchanging their raw data. This way, it safeguards data privacy and minimizes communication costs. In our DDoS detection system, federated learning acts as the main platform, where each participating node first collects and processes its local network traffic data independently and then trains a local deep learning model- CNN-BiLSTM. Instead of sending sensitive traffic data to a central server, only the trained model parameters or gradients are shared in a secure manner. These updates are then combined at the central server using, for example, Federated Averaging (FedAvg), while more sophisticated methods like Krum and Trimmed Mean are used to resist adversarial or malicious updates in untrusted environments. The global model derived after aggregation is sent back to all nodes, thus facilitating collaborative learning across multiple rounds. Usually, there are 5 federated

nodes in the system, each of them manages about 10, 000 samples, and training goes on for many rounds (e.g., 10 rounds), with local training carried out for a few epochs per round. The model gradually enhances its detection performance by learning different traffic patterns from distributed sources through this repeated process. Moreover, the system also uses homomorphic encryption to secure model updates during transmission and has Zero Trust principles embedded to continually assess the trustworthiness of the nodes, thereby improving security and privacy. The federated learning approach leads to large-scale, scalable, and real-time distributed intrusion detection that is not only efficient but also capable of supporting massive network environments of the present and future. Test outcomes show that the federated model, while training, can reach a high accuracy of up to 94.10 percentage and at the same time keeps a strong level of generalization on validation and test datasets, which is a proof of its capability of detecting Distributed Denial of Service (DDoS) attacks in a privacy-preserving and distributed manner.

Tier 3: Zero Trust Security

The Zero Trust layer guarantees that all participating nodes are not only verified but also monitored on an ongoing basis. Rather than giving trust on the basis of assumption, the system assesses each node according to various aspects such as gradient consistency, contribution accuracy, historical behavior, and similarity with global updates. A Node is allotted a changing trust score, and the ones with the lowest trust

scores are marked or even disconnected. Zero Trust Architecture is the choice because federated environments are susceptible to the attacks of malicious participants who may try to poison the model. Continuous verification acts as a safeguard in making certain only trusted nodes affect the global model. This layer has led to enhanced security and robustness as a result of which adversarial

attacks are kept at bay, the risk of compromised nodes is minimized, and the integrity of the federated learning process is maintained.

Layer 4: Multi Agent System

This layer brings intelligence and adaptability to the whole system by implementing a multi-agent system (MAS). That is a system composed of several agents, for example, the Byzantine Detection Agent, Convergence Analysis Agent, Adaptive Aggregation Agent, and DDoS Intelligence Agent. These agents scrutinize system behavior, identify anomalies, keep a tab on training progress, and dynamically choose the best aggregation strategies. Implementing MAS is a significant step, as static systems are not able to adjust themselves to evolving network conditions or new forms of attacks. Allowing different agents to collaborate and make decisions at the same time will definitely make the system more flexible and capable of reacting promptly. With this layer, the system benefits from better decisions and enhanced optimization. It not only boosts the system's tolerance to faults but also helps in taking adaptive measure against threats, and most importantly, it guarantees steady performance even when the system is under adversarial conditions.

Tier 5: Blockchain

Blockchain technology helps to offer transparency, trust, and immutability in the system. Distributed ledger technologies like Hyperledger Fabric are used to track the ledger changes. The critical events such as model updates, trust scores, aggregation decisions, and performance metrics are thus being recorded. Smart contracts facilitate the automation of the process ensuring validations are in place and their logging is securely done. Among various uses of blockchain, a helpful one is to solve the trust problems in distributed systems. With multiple nodes involved in the training process, it becomes necessary to keep a tamper-proof record of all activities. The net effect of this layer is to

provide a greater level of visibility and hold more people accountable. It disallows data tampering, guarantees the traceability of actions, and establishes trust between the participating entities. This merits the system a place in highly secure environments.

1.1 Dataset description

Our proposed system utilizes the CIC-DDoS2019 dataset, a benchmark dataset created by the Canadian Institute of Cybersecurity, which has been specifically designed for the purpose of assessing DDoS detection systems. This dataset is a collection of real network traffic with a mix of normal flows and several types of distributed denial-of-service (DDoS) attacks. The dataset contains a total of 18 different attack methods, among them are reflection- and amplification-based attacks such as DNS, NTP, SSDP, LDAP, and SYN flood. It is a large-scale one, approximately 30 GB in size, and a

small portion of over 50, 000 samples is taken for the training and testing of the model in this research.

It covers 18 different types of attacks, among them are reflection- and amplification-based attacks like DNS, NTP, SSDP, LDAP, and SYN flood. Besides being 30 GB in size, the dataset used for model training and evaluation is a subset of over 50, 000 samples.

Each traffic sample is described by 82 numerical features which provide a thorough representation of network behavior. These features are flow statistics (e.g., duration, packets), packet-level attributes (e.g., size), temporal characteristics (e.g., inter-arrival times), and protocol-specific indicators (e.g., TCP flags, port information). The dataset format is binary classification, where the label of the traffic can be either benign or attack.

Picking this dataset guarantees the incorporation of varied and genuine attack scenarios that lead to the enhancement of the effectiveness and adaptability of the proposed detection system. Besides the static CIC-

DDoS2019 benchmark used as a baseline training dataset for the models, the presented system also runs a dynamic real-time network ingestion pipeline for online testing. This running component using the scapy library remains live packet sniffing directly from the host's Network Interface Card (NIC), dividing the traffic into buffered 5-second overlapping sliding windows. On-the-fly, these raw packet sequences are mathematically analyzed to reconstruct the exact statistical flow features (e.g., inter-arrival times and flag counts) required by the hybrid architecture. This two-source strategy guarantees that the system is able to move easily from the historical offline validation to the ongoing, real-world, zero-day threat detection."

1.2 Feature selection

A key feature of our DDoS detection framework is feature selection which not only reduces the dimensionality of network traffic data but also ensures that only the most informative features are used for accurate classification. In this research, we have chosen the CICDDoS2019 dataset which contains 82 flow-based features representing statistical, temporal, and protocol-level attributes. The use of all features may result in redundancy, causing an increase in computational load and possibly affecting adversely the capability of the system to detect in real time. So, a robust feature selection approach is very important to improve both efficiency and model generalization. In order to find the features that contribute most effectively, various feature selection techniques were examined. These include statistical methods like Mutual Information, and ANOVA F-Test, machine learning methods that use feature importance scores from Random Forest and XGBoost, and wrapper-based methods like Boruta. We also investigated more sophisticated methods such as Ensemble feature selection and Reinforcement Learning-based Deep Q-Network (RL-DQN). A brief comparison of these methods can be found in Table 1 which shows different outcomes in terms of detection accuracy and feature reduction for

the various methods.

Figure 2.2 shows that, on average, traditional statistical methods have moder-

ate performance, while tree-based methods like Random Forest and XGBoost are able to improve detection accuracy by modelling complex, non-linear interactions

Table 1: Feature Selection Validation

Selection Method	Selected Features	Model Accuracy	Precision	Recall
Chi-Square (ANOVA)	40	95.20%	0.94	0.95
Mutual Information	40	96.15%	0.95	0.96
Random Forest RFE	40	97.40%	0.97	0.97
Autoencoder DB	40	96.80%	0.96	0.96
XGBoost Importance	40	97.85%	0.98	0.97
Boruta Wrapper	63 (Adaptive)	98.45%	0.98	0.98
Ensemble Intersection	40	98.67%	0.98	0.98
RL-DQN (Optimal)	11	98.80%	0.99	0.98

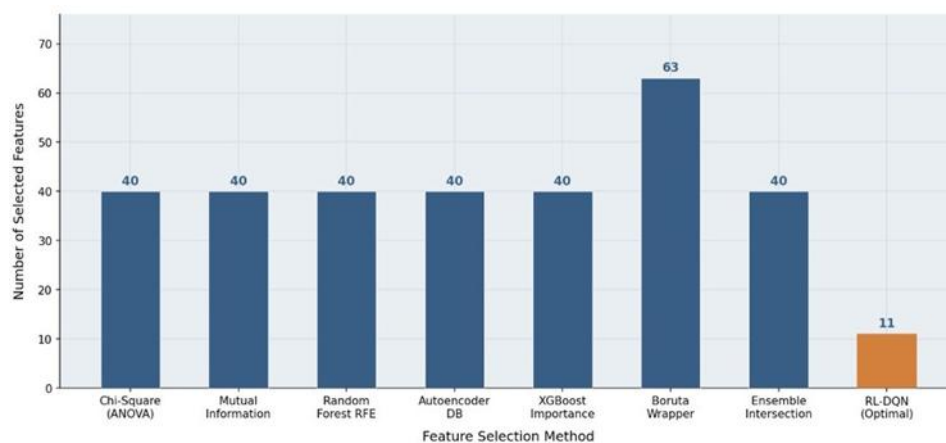


Fig. 2.2: Feature Selection Methods and Number of Selected Features

among features. The Boruta technique yields a bigger selection of relevant features, which exposes a certain amount of feature redundancy in the dataset. Going one step further, Ensemble feature selection helps to

strengthen stability by picking features that remain on top through different selection techniques, thus achieving a good compromise between accuracy and robustness.

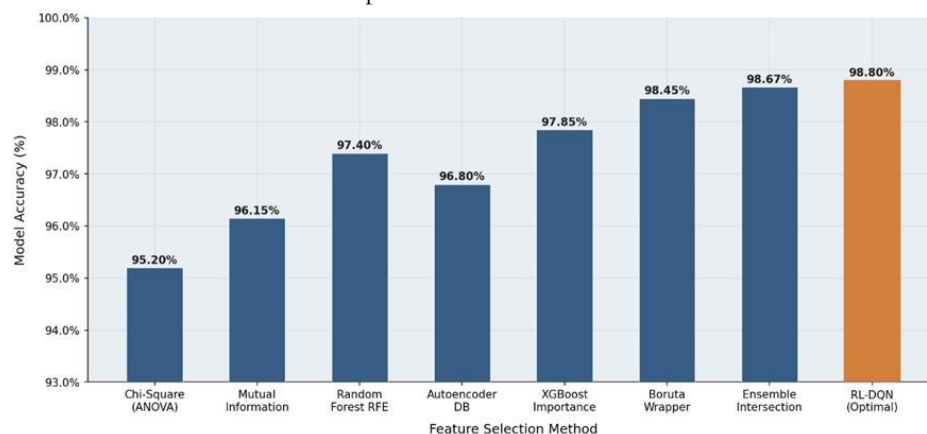


Fig. 2.3: Feature Selection Methods and Model Accuracy

By viewing feature selection as a sequential decision-making problem, the RL-DQN-based method for feature selection achieves remarkably better results. It aims to pick a very small number of highly informative features with the least sacrifice of classification accuracy. Among other things, in Fig. 2.3, it is illustrated that by greatly reducing the feature set, RL-DQN not only attains the highest detection accuracy but also enhances computational efficiency and results in quicker real-time detection. Nonetheless, if the number of features is reduced too much, the system may become less robust against attacks in adversarial environments, where attackers might exploit the dependencies of the limited features. Hence, after weighing the pros and cons of accuracy, stability, and resilience, the proposed system uses the Ensemble-based feature subset for deployment. This way, the system will still have a strong performance, be able to generalize well, and be resistant to feature-level attacks, all the while keeping computational efficiency. The experimental study shows that although RL-DQN can attain peak accuracy using very few features, Ensemble based feature selection turns out to be a dependable and strong choice for real-time DDoS detection in distributed and adversarial network scenarios.

2 Simulation Methodology

To assess the effectiveness of the suggested federated learning based DDoS detection system, we have carried out detailed experiments both on standard and actual network traffic. The evaluation criteria of the study focused on the detection and classification capabilities of the model, efficiency of the feature selection algorithm, capacity to withstand adversarial attacks, and the adaptability of the system to the changing environment.

2.1 Evaluation metrics

System performance has been measured using widely accepted classification metrics such as accuracy, precision, recall, and F1-score. These metrics help in thoroughly characterizing the

detection capability of the system as well as ensuring a balanced evaluation of the presence of imbalanced attack distributions.

2.2 Performance of distributed learning architectures

The effectiveness of the federated learning-based DDoS detection system that utilizes deep learning models at distributed nodes was measured by comparing various architectures. The research involved three models, CNN-BiLSTM, Transformer, and a Hybrid CNN-BiLSTM + Transformer architecture, federated learning framework. The assessment was primarily based on classification accuracy, loss convergence, as well as the capability to work with distributed and heterogeneous network traffic. Table 2 presents a summary where the Hybrid CNN-BiLSTM + Transformer model has the top performance, reaching an accuracy of 97.45 percent and a loss of 0.1843. Such excellent results are a consequence of the merging strengths of different architectures as the CNN layers take spatial features from the traffic data, BiLSTM provides tempo-ral dependencies, and the Transformer part models the long-range relationships. The integration allows the model to understand both short-term and long-term traffic patterns related to DDoS attacks. Compared to that, the CNN-BiLSTM model reaches 89.29 percent accuracy with a loss of 0.2431, showing that it can effectively capture spatial and temporal features but it still lacks modeling global dependencies. In the same vein, the Transformer model yields 88.30 percent accuracy with a loss of 0.2512, revealing a high potential for modeling long-range dependencies but also a limited ability to extract localized spatial features. Indeed, hybrid architectures significantly surpass single models by utilizing the best features of each. Besides, federated learning is a great step forward in model generalization as it allows the collaborative learning of models across distributed nodes without sharing raw data. Each node has different traffic patterns, which gives the global model a chance to be used in various network environments.

Table 2: Performance comparison of deep learning architectures

Architecture	Final Accuracy (%)	Final Loss
Hybrid (CNN-BiLSTM + Transformer)	97.45	0.1843
CNN-BiLSTM (Base)	89.29	0.2431
Transformer	88.30	0.2512

Besides comparing the models, the effect of aggregation strategies is also examined. On one hand, the original FedAvg algorithm is very efficient from the computational point of view. But on the other hand, it is quite dependent on the number of loyal nodes (only a small fraction of disloyal nodes is usually tolerated). This means that only a very limited amount of disloyal nodes is tolerated and, if this number is exceeded, FedAvg-based systems can be made faulty by an attack. Thus, the FedAvg is less resistant to poisoning attacks, which present one major way of damaging a system, and it is the easiest point of attack. Implementing a poisoning, an attacker may cause a system to malfunction or to degrade the quality of its outputs. Subsequently, resilient to byzantine aggregation algorithms like Krum and Trimmed Mean raise the level of security by making it difficult for an attacker to influence the system. At the same time, they maintain performance that does not fluctuate even when there are adversaries. By rejecting most unexpected, outlying, or erroneous updates, Krum and other robust aggregation methods do not allow the attacker to steer the updates in his desired direction. So, the final performance of the system remains stable regardless of the presence of adversaries. Altogether, these findings indicate that combining hybrid deep learning models with federated learning and robust aggregation methods results in a DDoS detection system that is accurate, scalable, and secure.

2.3 Multi-agent system decision analysis

To make the system more flexible and resilient, it uses a Multi-Agent System (MAS)

that works during each federated learning round. The MAS gets to know the system, including how the model is doing, the behavior of a node, trust scores, and changes in gradients, making decisions that are both intelligent and based on context. The system comprises four distinct agents. The Byzantine Detection Agent locates malicious or compromised nodes by investigating abnormal changes in gradient updates through similarity and divergence measures. It downgrades the trust scores of nodes behaving abnormally and marks them as potential threats. The Convergence Analysis Agent evaluates training development by analyzing the changes in accuracy and loss, making sure the model converges effectively without instability or overfitting. The Adaptive Aggregation Agent updates the aggregate strategy in real-time based on the system situation. It normally uses the switching mechanism to alternate between conventional methods like FedAvg and robust ones such as Krum or Trimmed Mean according to the anomalies and trust assessments. By dissecting the traffic pattern and the model prediction, the DDoS Pattern Intelligence Agent is able to define which actions are normally associated with this type of attack and thereby evaluate the level of threat. The final decision is reached through a weighted consensus mechanism that takes into account the output from these agents, each contributing according to its role and level of confidence. Higher priority is given to security-critical agents, especially the Byzantine Detection Agent, in order to maintain the system's integrity. For example, if the presence of the abnormal gradients is detected, the standard aggregation decisions are overridden and the system switches to the robust method

to avoid model poisoning. This team-based multi-agent strategy will allow continuous adjustment of the federated learning process in real time, thereby enhancing fault tolerance and guaranteeing consistent model performance even when the environment is hostile. By combining hybrid deep learning systems within a multi-agent decision-making setup, we can adapt, safeguard, and smartly optimize federated learning, thus providing dependable DDoS detection even in changing and hostile network scenarios.

2.4 Real-time system evaluation

The real-time performance of the proposed DDoS detection system has been successfully measured to see if it can still effectively handle continuous network traffic under a variety of changing conditions. The core of this testing was to verify the system's capability of processing streaming data, generating predictions swiftly, and still keeping a steady detection performance level during a live operation. The system that has been implemented captures and processes the incoming network traffic continuously and in a streaming fashion. In order to effectively manage sequential traffic flows, a sliding window mechanism is used for data organization. While on-the-fly feature extraction is done, the output feature vectors are immediately sent to the trained model for inference. This workflow guarantees that predictions are made with the least possible delay, which in turn allows for quick identification of malicious traffic. Another aspect of the testing was to check how well the system adapts to the changes in traffic patterns. The model during its real-time operation showed that it can keep the performance level rather stable even when it is dynamically exposed to normal as well as attack traffic conditions. When an optimized feature subset is used, the features extraction step is much faster, hence, without any loss in detection capability, the system can perform rather efficiently. Another key area that the evaluation focused on was how stable the system is when it is continuously running. The

model shows very similar prediction patterns from one observation interval to the next, which means that it can be trusted to work well even when the traffic is heavy for a long time. Processing the data with a sliding window technique makes sure that the system keeps up with the changes in traffic and therefore gets better at detecting new types of attacks. The monitoring interface allows for live monitoring by showing the prediction results and the status of the system, thus it makes it possible to closely follow the detection behavior during the run. This makes it easier to check how well the system is doing and ascertains that any irregularities can be flagged without delay. The realtime analysis illustrates how the mechanism keeps a steady and effective performance of detecting the system under a continuous flow of traffic, thereby backing its applicability to the actual DDoS detection situations.

3 Conclusion

The FL-DDoS, a federated learning-based DDoS detection system, has been proposed as a solid, scalable and privacy-preserving solution to the security of current distributed network environments. The system, which combines hybrid deep learning methods (CNN-BiLSTM with Transformer), federated learning, blockchain-based logging, and a Zero Trust security model, has proven capable of overcoming the challenges of conventional centralized intrusion detection systems. A detailed review of the CIC-DDoS2019 dataset and scenario testing with real-time network traffic revealed that the system has the ability to accurately detect attacks and at the same time is able to tolerate faults and withstand hostile attempts such as Byzantine attacks. Furthermore, efficient feature selection leads to a drastic drop in the computational load while the ability to maintain high precision is not compromised, which makes the model a good candidate for real-time use on the edge and in IoT scenarios. The addition of the multi-agent adaptive framework strengthens the system's ability for smarter decision-making as it can select aggregation strategies in

a way that depends on the condition of the network, while blockchains are used for the record of decisions which are transparent and immune to tampering. These features aid in the development of an effective, decentralized, and smart security tool for combating extensive DDoS attacks in networks of today. The suggested system is very effective but there are several ways that it can be further enhanced and expanded to allow a wider range of applications and different use cases. One direction of the future research could be to explore the use of Graph Neural Networks (GNNs) to capture the structure of the network which may help in the detection of distributed attack dissemination patterns. Also, the expansion of the model from two-class classification to multi-class classification will facilitate the accurate recognition of various types of DDoS attacks. The usage of continual learning methods like Elastic Weight Consolidation (EWC) will lead to the model being capable of learning new threats without forgetting the old ones completely. Lastly, testing the model on diverse datasets as well as in actual settings will help in proving its adaptability and readiness for practical deployment.

4 Further Work

While the proposed FL-DDoS framework demonstrates strong performance in terms of accuracy, scalability, and security, several enhancements can further improve its effectiveness and real-world applicability. One important direction is the integration of

Graph Neural Networks (GNNs) to model network traffic as a graph structure, enabling the system to capture spatial dependencies and better identify distributed attack propagation across multiple nodes.

Another key extension involves transitioning from binary classification to multi-class classification, allowing the model to distinguish between different types of DDoS attacks (such as SYN flood, UDP flood, and reflection attacks). This would enable more targeted and automated mitigation strategies, improving response efficiency in dynamic network environments.

To address the challenge of evolving cyber threats, future work can incorporate continual learning techniques, such as Elastic Weight Consolidation (EWC), to allow the model to learn new attack patterns without forgetting previously learned behaviors. Additionally, enhancing the federated learning framework with adaptive aggregation strategies and improved handling of non-IID data can further strengthen model robustness across heterogeneous edge devices.

Finally, the system can be validated on multiple real-world and large-scale datasets and deployed in live network environments to evaluate its generalization capabilities. Integrating lightweight optimization techniques for edge devices and improving blockchain efficiency to reduce latency and transaction costs will also be critical for large-scale practical deployment.

References

- Qamar, R., Zardari, B.A., Hussain, Z., Ghoto, A.A., Arain, A.A.: Detection of Distributed Denial of Service (DDoS) Cyber Attacks through Deep Learning Neural Network. *Pakistan Journal of Engineering Technology & Science* 12(2), 28–36 (2024)
- Ahmed, F., Khan, I.: Distributed Denial of Service Attack Detection in IoT Networks Using Deep Learning and Feature Fusion. *Malaysian Journal of Computer Science* 37(1), 12–25 (2024)
- Verma, S., Mishra, A.: Prevention and Detection of DDoS Attacks in Virtual Cloud Computing Environment Using Naïve Bayes. In: *Advances in Computing and Data Sciences*. Springer (2019)
- Khan, U., Ahmed, S.: Intrusion Detection in Internet of Things Systems: A Comprehensive Survey of Machine Learning Approaches. *IEEE Access* 10, 41608–41628 (2022)
- Rehman, T., Tariq, N., Khan, F.A.: Federated Learning-Based Solution for DDoS Detection in SDN. *Sensors* 25(1), 10 (2024)

-
- Rahman, T., Chowdhury, H.: Leveraging Federated Learning for DoS Attack Detection in Distributed IoT Environments. *Internet of Things* 27, 101344 (2025)
- Zhang, W., Chen, L.: A Federated Learning-Based Zero Trust Intrusion Detection System for IoT. *Computers & Security* 134, 103597 (2023)
- Basu, A., Kumar, N.: Zero Trust Architecture and AI: A Synergistic Approach to Modern Cybersecurity. *International Journal of Scientific Research in Automation* 2(1), 30–36 (2024)
- Banu, R., Prakash, L.: Blockchain-Driven Federated Learning-Based Intrusion Detection System for IoMT Networks. *Journal of Personalized Medicine* 14(8), 794 (2024)
- Alzahrani, A., Lee, Y.: Blockchain-Based Zero Trust Networks with Federated Transfer Learning for Secure IoT Communications. *PLOS ONE* 19(4), e0323241 (2024)
- Kim, D.-H., Wang, Y.: An Optimal Federated Learning Based Intrusion Detection for IoT Environments Using Feature Selection. *Scientific Reports* 15, 93501-8 (2025)
- Patel, M., Reddy, H.: Blockchain Enhanced Distributed Denial of Service (DDoS) Attack Detection Using a Deep Learning Model. *Scientific Reports* 15(2), 06568-8 (2025)