

# A Scalable Hybrid CNN-LSTM and SDN Based Architecture for Real-Time DDoS Defence in IoT and Cloud Networks

Sujit Sutradhar<sup>1</sup>, Joy Lal Sarkar<sup>2</sup> and Rajesh Kumar Verma<sup>3</sup>

<sup>1</sup>Department of Information Technology, ICFAI University Tripura, Agartala, Tripura, India

<sup>2</sup>Department of CSE, Techno College of Engineering Agartala, Tripura, India

<sup>3</sup>Department of CSE-AIML, Sreenidhi University, Hyderabad, India

## Article history

Received: 27-10-2025

Revised: 18-05-2026

Accepted: 17-07-2026

## Corresponding Author:

Sujit Sutradhar  
Department of Information  
Technology, ICFAI University  
Tripura, Agartala, Tripura,  
India  
Email:  
sujitsutradhar87@gmail.com

**Abstract:** Distributed Denial-of-Service (DDoS) is one of the most significant threats to the security of IoT, cloud, and Software-Defined Network (SDN) environments because it can aggravate network unavailability and disrupt the continuity of services. This study presents a hybrid CNN-LSTM-based DDoS detection and mitigation system for real-time DDoS detection in the context of heterogeneous network environments, which is integrated with SDN and cloud-edge collaborative architecture. The proposed framework is based on two deep learning models, Convolutional Neural Networks (CNN) for extracting spatial traffic features and Long Short-Term Memory (LSTM) networks for learning temporal dependencies, to achieve better detection of complex attack patterns that involve multiple vectors. To evaluate the experimental results, the CIC-DDoS2019 dataset, along with some other benchmark traffic datasets, is used under heterogeneous deployment conditions. The proposed Hybrid CNN-LSTM framework was able to achieve an accuracy of 95.88% and an F1-score of 91.41%, while the lightweight CNN models for the IoT environments had an accuracy of more than 94% with lower latency and resource usage. The results show that the proposed framework effectively detects DDoS attacks in real time, highly adapts to network changes, and has high scalability of deployment for SDN, cloud, and IoT environments.

**Keywords:** DDoS Attacks and Detection, Internet of Things (IoT), Machine Learning (ML), Network Functions Virtualisation (NFV), Software Defined Network (SDN)

## Introduction

In the past few years, Distributed Denial of Service (DDoS) attacks have undergone a tremendous metamorphosis. They are now highly sophisticated, multi-vector disruptions instead of just simple packet flooding. The earlier variants of DDoS attacks could be easily mitigated by using basic filters, while the development of numerous large botnets (DDoS-as-a-Service), exploiting protocols, and the like, has enabled modern overkill DDoS attacks to reach unimaginable scales. The 1.35 Tbps Memcached-based attack on GitHub, which surpassed the previous record in terms of amplification, used fake traffic to bring down even the best infrastructures. A rapid increase in the number of Internet of Things (IoT) devices has also contributed to this evolution. The industry is swamped with billions of small and low-power devices that can be connected through 5G,

Wi-Fi, and industrial networks (Noor-A-Rahim et al., 2022). A major portion of them is deployed with outdated firmware, weak authentication, or no security controls at all. The devices related to these categories can easily be stolen and added to huge botnets like Mirai, Mozi, and Meris, making it possible for the attackers to create gigantic distributed traffic surges. The emergence of DDoSaaS as a commercial service means that the attacker no longer needs to possess substantial technical know-how; they can simply rent botnets to conduct customizable attacks instead (Hoque et al., 2015). Consequently, the whole ecosystem leads to a significant increase in the frequency, complexity, and unpredictability of modern DDoS incidents.

Figure 1 shows the complete system architecture for the detection of Distributed Denial-of-Service (DDoS) attacks with the help of machine learning applied in an SDN-enabled IoT environment.

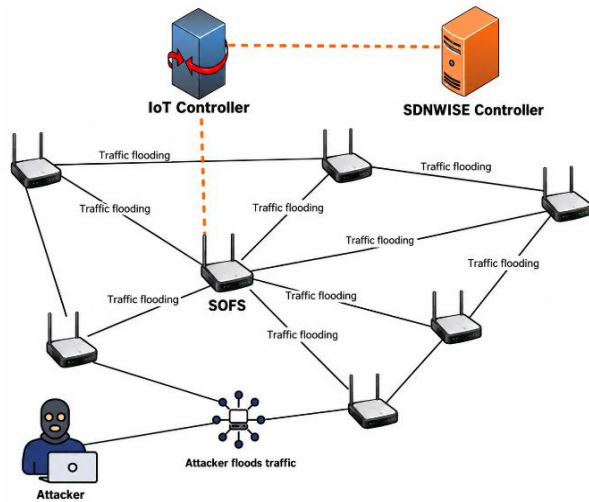


**Fig. 1:** Machine learning based DDoS mitigation in SDN (Bhayo et al., 2023)

The system connects IoT devices, SDN controllers, OpenFlow switches, and the main network together, which enables them to monitor and mitigate threats in a coordinated manner (Alam et al., 2020). The bottom of the architecture consists of various IoT devices and SDN-enabled IoT nodes, which create network traffic that passes through OpenFlow switches, where adaptive ML-based detection logic works in real time (Alashhab et al., 2024). The SDN controller is managing these switches from a central location, gathering flow statistics, and applying dynamic policies every time an abnormal traffic pattern is detected. Potential DDoS attackers and victim nodes are represented to indicate how the malicious traffic gets into the system, which allows the controller to separate the legitimate IoT flows from the attack traffic (Lohachab and Karambir, 2018). The high layer depicts the connection between the core network server and gateway, which connects the SDN domain to the global Internet, where botnets might produce external attack flows. The architecture also includes a flow-based monitoring mechanism that is composed of a trace storage unit and an sFlow file server that keeps flow profiles used for model training and attack classification. In general, the figure emphasises the role of centralised SDN control, real-time flow monitoring, and adaptive machine learning in concert in the process of protecting IoT networks against high-volume DDoS threats.

### Evolution and Challenges in Modern DDoS Attacks

The techniques that are mostly used in modern DDoS attacks are Memcached reflection, DNS/NTP amplification, carpet bombing, SYN spoofing, and multi-vector flooding. In addition to that, these attacks take advantage of vulnerabilities throughout the different layers, and at the same time, they generate burst-based

traffic patterns and combine volumetric, protocol-based, and application-layer disruptions. Therefore, they are able to hide their malicious intent by making use of legitimate-looking packet structures or employing low-rate stealth patterns that are very similar to normal traffic. Traditional defence systems have been facing more and more difficulties in dealing with these attacks. Static firewalls, Access Control Lists (ACLs), signature-based intrusion systems, and threshold-based anomaly detectors are confined by predefined rules and hence cannot quickly adapt to the changing attack behaviours (Janabi et al., 2024). They especially fail against: Low-rate stealth attacks, Multi-vector blended attacks, encrypted traffic flows, high-speed burst attacks, heterogeneous IoT and cloud workloads. The outcome is that there is a delay in detection, frequent false positives, and poor mitigation accuracy during large-scale disruptions.

### Role of Software-Defined Networking (SDN)

The introduction of SDN has made it easier to control networks through a single point and apply different strategies for DDoS mitigation dynamically (Anand et al., 2025). The use of SDN via centralised controllers results in real-time visibility of traffic, flow rule updates that are very detailed, and fast enforcement of policies (Shaik, 2025). When enormous DDoS traffic is present, the controller is subjected to flow-rule overload, CPU exhaustion, and packet-in flooding, which are the vulnerabilities of SDN systems. When the detection systems are slow or give inaccurate results, the controller becomes the bottleneck, and this results in a reduction of the overall network service quality. To overcome this problem, it is necessary to have detection models that can work at high speeds, with high accuracy, and with minimum latency.

### Machine Learning (ML) for DDoS Detection

The application of Machine Learning for DDoS detection is mainly due to its ability to address the inflexibility of rule-based systems (Liu et al., 2021). DDoS detection systems rely on ML models like SVM, Random Forest, or Logistic Regression for the automation and process of classifying events as anomalies or not, but these models still largely face limitations, not only in the aspect of the automated classification of today's high-dimensional and complex network traffic. Their limitations can be broadly classified into the following: They cannot detect new attack variants, performance is highly dependent on manual feature engineering, heterogeneous or encrypted traffic results in inconsistent performance, and slow reaction time, i.e., not suitable for real-time SDN deployment; besides, performance is hard to achieve during multi-vector attacks (Varga et al., 2017). These factors make it impossible for classical ML to be the only solution in real-time detection, as a comprehensive solution is required.

Deep learning methods like CNN and LSTM played an important role in discovering and recognising traffic patterns over space and time (Almukhalafi et al., 2024). CNNs do the job of coming up with spatial relationships between the features of the packets, while LSTMs have the role of capturing the order and changes of the attack patterns (Alkahtani and Aldhyani, 2021). The problem with using only CNN or LSTM models is that they usually can't deliver high accuracy, real-time inference, and lightweight deployment at the same time, which is ideal for edge and IoT devices. Because of this, there is a demand for hybrid deep learning systems that can take advantage of both spatial and temporal learning at the same time.

### *Proposed Adaptive Hybrid CNN-LSTM DDoS Detection Framework*

To enhance the existing DDoS detection solutions, here study offer an Adaptive Hybrid CNN-LSTM-based DDoS Detection Model (AMLSDM) that incorporates SDN and is supported by cloud-edge computing, our proposed method. The architecture is set to accomplish: Real-time detection via CNN-LSTM concurrent feature extraction; low-latency reaction, made possible through SDN-driven dynamic rule deployment (Ogab et al., 2025). Scalability from the IoT to the cloud and edge systems through distributed processing; high precision and flexibility via continuous model learning; layered detection, conforming to the figure structure already provided. The cloud layer performs large-scale model training and global analysis in the framework, while the edge layer conducts early detection to alleviate the controller's burden. The SDN controller connects both layers for managing flow entries, blocking malicious packets, and isolating compromised nodes in real time.

### *Relevance and Advantages of the Proposed Model*

The hybrid AMLSDM framework is created with the purpose of tackling the problems of modern DDoS attacks (Ramaswamy et al., 2025). The combination of deep learning and SDN programmability leads to numerous advantages, such as: Better resistance of cloud and IoT infrastructures, Quicker reaction to both high-rate and low-rate attacks, Less burden on the controller due to early filtering done at the edge layer, learning that is adaptable and can follow up on new incoming attack strategies, and the ability to see everything going on through distributed network segments. Thus, the framework can be considered a perfect fit for applications such as smart cities, industrial IoT, cloud-native virtualised networks, and high-speed backbone infrastructures that have limitations of traditional solutions.

The major contributions of the proposed work are summarised as follows:

- A scalable hybrid CNN-LSTM framework for DDoS detection is proposed that enables real-time

protection of IoT, cloud, and virtualised network environments

- The proposed framework integrates spatial feature extraction and temporal traffic-sequence learning to enhance multi-vector, burst-based, and low-rate stealth DDoS attack detection
- A cloud-edge collaborative deployment strategy is proposed to efficiently distribute the computational burden between edge-level filtering and global traffic analysis in the cloud
- The framework adds dynamic SDN-based mitigation, in the form of adaptive rule updates enabled by OpenFlow, to isolate a fast attack and intelligently manage traffic
- To demonstrate the scalability and adaptability of the proposed system, several heterogeneous benchmark datasets, such as CIC-DDoS2019, CAIDA, NSL-KDD, and KDDCup99, are used to evaluate the system
- Experimental results show that the proposed hybrid framework effectively balances high detection accuracy, low FPRs, and acceptable latency, which is appropriate for real-time SDN-IoT deployments

### *Literature Review*

The DDoS detection literature covers a wide range of areas, including traditional networking settings, especially the case of SDN, virtualised infrastructures in the cloud, and IoT environments (Dong et al., 2019). The transition from simple, rule-based systems to advanced hybrid deep learning models is a response to not only the evolving nature but also the increasing sophistication of DDoS attacks (Hussain et al., 2024). Initially, the research mainly concentrated on statistical anomaly detection, signature-based Intrusion Detection Systems (IDSs), and threshold-driven methods for packet inspection. Although these mechanisms managed to cope with simple volumetric attacks, they were not able to adapt quickly and thus could not detect multi-vector or low-rate stealthy attacks. Moreover, the studies reported high false positive rates consistently when these methods were applied to heterogeneous or encrypted traffic. As the attacks became more sophisticated, the focus of the researchers moved to machine learning-based approaches for detection.

Figure 2 presents the conventional three-layer SDN model, where the application, control, and data layers are integrated to facilitate the programmable, flexible, and scalable management of the network. The Application Layer, which is the uppermost layer, is where the network functions are presented in high-level abstraction. These functions include network virtualisation, topology discovery, traffic monitoring, security enhancement, and load balancing. The applications use the Northbound Interface (e.g., REST or Frenetic APIs) to interact with the SDN controller, thus allowing network behaviour to be configured by software.

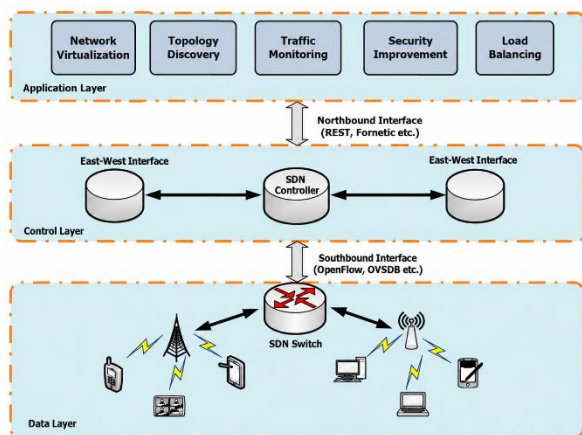


**Fig. 2:** Evolution of DDoS detection techniques from traditional ML to hybrid deep learning and SDN-integrated frameworks (Tonkal et al., 2021)

The Control Layer is the central intelligence of the SDN architecture. At this stage, a single SDN controller for the whole network makes all the decisions and interacts with other controller nodes via the East-West Interface, thus maintaining the synchronisation of controllers, the scalability of the system, and the distributed control. This layer takes the high-level application policies and converts them into low-level commands for the network devices. The Data Layer, which is the lowest layer, is comprised of both wired and wireless hardware components like routers, switches, access points, sensors, and IoT devices. According to the flow rules already set up by the controller, these devices will forward the traffic via the Southbound Interface (e.g., OpenFlow, OVSDB). The diagram illustrates that the SDN switch serves as the point of execution for the controller's policies over dissimilar devices.

### ML Approaches in Classical Networks

The application of machine learning algorithms such as Random Forest, SVM, Naïve Bayes, GBM, and KNN for the detection of anomalous traffic in classical networks is one of the main areas of their usage (Ness et al., 2025). Many studies reported over 98% accuracy for binary DDoS classification and high accuracy on structured datasets. Their popularity was due to the fact that they were easy to understand, required small computational resources, and were even usable for small-scale networks. However, these methods have the major drawback of requiring laborious feature extraction, and thus, they do not have the capability to detect deep temporal behaviour. Studies in recent years point out that classical ML models do not perform well in real-world IoT and cloud environments because of reasons like dynamic packet patterns and high traffic volumes, along with abrupt behavioural changes. In addition, such models are retrained frequently, are not

robust under zero-day conditions, and also have difficulty with multi-class classification.

### SDN Based DDoS Detection

The SDN's global visibility and centralised management were the initial factors that led to a diversity of research on the security systems embedded within SDN (Rahouti et al., 2021). The integration of ML-based anomaly detection with SDN controllers was the main topic of discussion in several frameworks, like LEDEM, CONA, and SD-IoT, and their studies led to the conclusion that there had been improvements in latency, detection accuracy, and dynamic mitigation capabilities. However, SDN also introduces certain vulnerabilities that are distinct from any other. Attackers can exploit the packet-in messages to swarm the controller, which produces a critical condition for the whole network. Since many of the SDN-ML frameworks are designed for centralised detection, they tend to be more resource-consuming and thus also prone to creating single points of failure (Jurado-Lasso et al., 2022). In addition, the studies have demonstrated that the performance of these frameworks declines as the traffic volume increases in 5G or huge IoT deployments. All these problems make it urgent to develop hybrid detection systems that combine distributed processing and deep learning.

### IoT-Focused DDoS Detection

IoT ecosystems represent a unique area of concern since they are characterised by limited computing power, different communication standards, and enormous device populations. The existence of IoT botnets such as Mirai, for example, has demonstrated how much of a disaster it is when IoT devices are hacked. The researchers put forward some lightweight models, such as compressed CNNs, distilled neural networks, and GBM, for anomaly detection in IoT. The performance of those models turned out to be quite promising, but still, IoT-focused research faced the following challenges:

- (i) Deep learning methods are not applicable due to the limited local computational resources
- (ii) The rapid evolution of IoT traffic results in many false alerts
- (iii) The existing models are network-specific and do not generalise well across different networks. So these challenges highlight the requirement for detection frameworks that are large, flexible, and supported by edge computing

### Deep Learning and Hybrid Architectures

Methods based on deep learning are gaining more and more ground in the research field of DDoS detection. For instance, CNNs are used to capture the spatial traffic features, which include the distribution of protocols, patterns of bytes, and entropy. The LSTM and GRU

networks are capable of modelling the temporal dependencies, thus being able to differentiate between normal and malicious traffic bursts. The hybrid CNN-LSTM architectures, on the other hand, have become a hot topic because of the fact that they can acquire the spatial as well as the temporal features at the same time. There are reports of hybrid models being able to reach 96 to 99% accuracy on both CIC-DDoS2019 and UNSW-NB15 datasets. However, most of these hybrid models still do not have the frameworks for real-time deployment, optimisation of their systems for the SDN environment, and integration with the edge resources. The comments made by the reviewers in the various studies point to the lack of scalable deployment strategies as one of the main limitations.

### Cloud-Edge and NFV Based Methods

Very recent research looks into the possibility of cloud-edge partnership and the use of NFV to allocate the DDoS detection tasks. The heavy computation of the training is done in the cloud systems, while the edge nodes take care of the very fast inference. This results in less work for the controller and more responsiveness. Some researchers have been able to show that the delay in detection has been improved, but still, there are some issues with the synchronisation of the distributed learning and the consistency of the rules across the different layers of the network. A lot of the cloud-edge infrastructures, after they have been deployed, are still static and do not have any adaptive or self-learning features. This shortcoming results in a situation where the appearance of new DDoS variants leads to the creation of security gaps.

The consolidated overview in Table 1 illustrates the usage of different ML, DL, federated learning, and hybrid techniques in the previous studies and points out their datasets, performance strengths, and identified limitations. The analysis shows that while a lot of existing techniques

reach good detection accuracy, they still have to deal with challenges such as high false positive rates in noisy traffic, limited detection ability for novel or multi-vector DDoS attacks, scalability problems in IoT environments, neglecting temporal feature modelling, and heavy computational resource requirements. Moreover, the table places the proposed work in the context of earlier studies by highlighting its hybrid CNN-LSTM connected with an SDN-based deployment strategy that significantly augments detection accuracy and minimises error rates, at the same time allowing better adaptability in edge-cloud environments. This comparative review, in essence, has pointed out that there are still gaps in the research, which are the main reason for the demand for a much stronger and more scalable detection framework.

The detection of DDoS attacks has been looked at through many lenses, from traditional machine learning models and deep learning frameworks to SDN-based systems and hybrid cloud-edge solutions. Pivotal studies pertaining to DDoS detection research were thoroughly compared in Table 1 for the purpose of grasping the advancements and limitations in the respective area. The table summarises characteristics like the primary methodology adopted, datasets used, performance metrics, and significant drawbacks of each study. A very clear trend can be observed across the authors' pieces of work being reviewed: On one hand, machine learning models provide a very fast and lightweight detection suitable for IoT and edge setups, but on the other hand, they are, to a large extent, incapable of uncovering the complex temporal patterns typical of multi-vector attacks. In the case where deep learning is involved, the accuracy is tremendous, and the quality of feature representation is at its best, but on top of that, the technique also consumes a great deal of computational resources, thus restricting real-time deployment.

**Table 1:** Summary of key studies on ML, deep learning, and SDN-Based DDoS detection techniques

| Author / Year               | Technique / Model Used                   | Key Findings                                             | Limitations Identified                                     |
|-----------------------------|------------------------------------------|----------------------------------------------------------|------------------------------------------------------------|
| Al-Shukaili et al., 2025    | Random Forest for DDoS detection         | Achieved high accuracy and low latency for cloud traffic | Unable to detect low-rate DDoS; lacks temporal analysis    |
| Yi et al. (2024)            | CNN-based traffic classification         | Performs well on spatial packet features                 | Poor detection of multi-vector attacks; high training cost |
| Prasanga et al., 2025       | Hybrid LSTM model for sequential traffic | Strong detection of sequence-based attacks               | Slow inference, unsuitable for real-time SDN               |
| Rahman et al., 2024         | GAN-based synthetic traffic generation   | Improved class balancing and model robustness            | High computational cost; complex implementation            |
| Li et al., 2024             | Federated Learning for IoT security      | Privacy-preserving collaborative detection               | Communication overhead; client drift issues                |
| Kumar et al. (2025)         | GBM for lightweight edge detection       | Fast inference, low memory footprint                     | Limited ability to detect novel attack patterns            |
| Arevalo-Herrera et al. 2025 | SDN-based deep learning architecture     | High detection accuracy for controller attacks           | The centralised SDN controller is still a bottleneck       |
| Sridevi et al., (2025)      | Bi-LSTM for multi-vector attacks         | Excellent temporal feature extraction                    | High training time; not resource efficient                 |
| Proposed Study              | Hybrid CNN-LSTM + SDN-based deployment   | High accuracy, low FPR/FNR, edge-cloud adaptability      | Slightly higher resource usage compared to GBM             |

The SDN (Software-Defined Networking) detection offers the advantage of better centralised traffic control, but still cannot escape the disadvantage of being vulnerable to the overload of the controller during massive attacks. The table highlights issues such as limitations in scalability, difficulty in detecting low-rate botnet traffic, lack of adaptive models, and thus emphasises the need for a more robust hybrid approach that could combine spatiotemporal learning with the efficient deployment across cloud, edge, and SDN-based infrastructures.

As per the critical analysis of the literature so far, one can say that existing DDoS detection frameworks are very ineffective and that a number of important research gaps have been pointed out. The lack of a unified and scalable architecture that could accommodate and integrate SDN, cloud, and IoT layers is the main reason for the fragmentation of solutions that cannot work efficiently in different environments, as the solutions are stuck in one due to their nature. Moreover, hardly any studies present real-time deployment frameworks for hybrid deep-learning model, despite their established capability of capturing intricate spatial-temporal attack features. SDN-based machine-learning systems are also constrained by controller overload, particularly during large attacks, thus causing a significant drop in system responsiveness and stability. Current ML models can only learn in the time frame they were trained on; hence, they do not perform well when they come across fluctuating or low-rate IoT traffic patterns. Cloud-edge collaboration is another area that has had minimal exposure in existing literature, thus creating a gap in the design of systems that would be both effective and efficient in the distribution of computational tasks. All these limitations taken together make it evident that an adaptive, hybrid detection framework that seamlessly integrates SDN control, cloud processing, and edge-level intelligence for real-time and scalable DDoS mitigation is necessary.

The proposed framework combines the advantages of three critical components: Spatiotemporal deep learning, adaptive SDN-based mitigation, and cloud-edge collaborative deployment, which are unique in that they are integrated into a single scalable architecture, rather than a few existing DDoS detection methods based on SDN that are limited to either isolated datasets or centralised deployment. The proposed scheme is also evaluated on a heterogeneous benchmark dataset for enhancing the generalisation capability and flexibility for deployment in a wide range of IoT and cloud scenarios.

## Materials and Methods

The methodology that is being presented brings forth a hybrid machine learning framework that is not only scalable but also adaptable for DDoS attack detection in various heterogeneous environments. The environments

can be IoT networks, cloud infrastructures, and Software-Defined Networking (SDN) systems. The complete process involves obtaining datasets, preparing data, performing feature extraction, developing a hybrid model, integrating SDN-based features, and validating performance through multiple stages. The methodology is rigorously conducted and, at the same time, compliant with the guidelines of the Journal of Computer Science (JCS), ensuring clarity and reproducibility.

The architecture presented in Fig. 3 shows a comprehensive deployment of an integrated system that includes data acquisition modules, preprocessing units, a hybrid machine learning detection engine, SDN controllers, and cloud-edge computing nodes, for scalable and real-time DDoS detection and mitigation. It also enables coordinated monitoring, intelligent attack classification, and dynamic mitigation of traffic in different IoT, SDN, and cloud network environments.

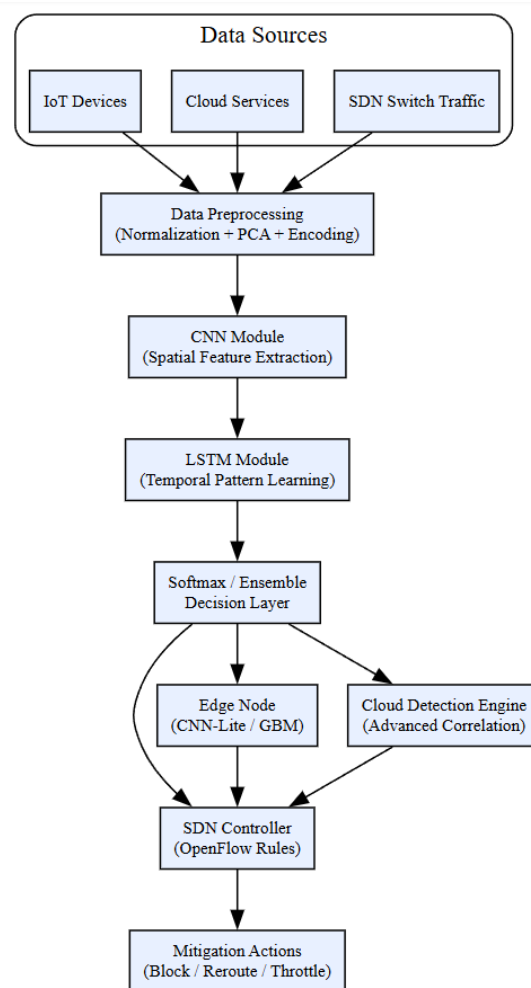


**Fig. 3:** Deployment architecture of the proposed hybrid ML-SDN DDoS detection framework

## Dataset Acquisition

Before model training and evaluation, all traffic data were transformed into a common flow-based format to allow the data to be compatible across the disparate benchmark datasets. The following are the common network traffic features that were chosen from CIC-DDoS2019, CAIDA, NSL-KDD, and KDDCup99: Normalisation and traffic standardisation operations were also carried out to ensure consistency in the traffic amount, protocol representation, and traffic behaviour in all datasets in terms of feature dimensions. This provides a common pre-processing algorithm for handling the heterogeneous traffic sources and boosts the reliability of the proposed detection algorithm in the cross-environment evaluation.

Additionally, attack categories from the various datasets were categorised into the unified traffic classes benign traffic and major DDoS attack categories. The harmonisation of this label helped to increase consistency in the model training and lowered the ambiguity of the classification of heterogeneous traffic sources.

## Data Preprocessing and Feature Engineering

Noise, missing fields, duplicate flows, and packet attributes that were inconsistent were all included in the initial traffic logs recorded. Preprocessing not only removed the corrupted rows but also brought all numerical attributes to a common standard. To stabilise model training, a min-max normalisation scheme was adopted for the entire dataset of features. Furthermore, the categorical protocol-based attributes were transformed into machine-readable formats through label and one-hot encoding techniques. Redundant and low-impact attributes were eliminated using dimensionality reduction techniques such as PCA and Chi-square statistics. To capture the short-term temporal flow variations, the traffic was divided into fixed-length windows, creating matrices that show burstiness, inter-packet arrival variations, and flow-duration dynamics. These structured matrices were then used as the input representation for the convolutional module.

In order to reduce the uneven distribution between benign traffic samples and malicious traffic samples, the SMOTE and random undersampling techniques were

used for pre-processing. Balancing processes were used to reduce the bias towards majority traffic classes in the models and to obtain a more stable detection performance for various traffic attack patterns at low frequency.

Table 2 highlights the formula, which denotes an important computational step in data preprocessing, model building, or performance measurement. The presented expressions comprise normalisation, activation, recurrent state, and evaluation metrics, all of which significantly influence the hybrid deep learning model's performance. More particularly, min-max normalization is applied to traffic features so that the model processes them uniformly. The Softmax function converts the outputs of the model into class probabilities suitable for multi-class attack classification. Through this LSTM hidden-state update equation, the sequential dependencies existing in the network traffic streams are captured, and thus, accurate temporal pattern learning is made possible. Furthermore, the evaluation metrics of FPR and FNR count the errors in classification, and therefore, the model's ability to detect the flow of both normal and malicious traffic is assessed through these metrics. To sum up, these mathematical formulations are the major support of the analytical and computational processes undertaken in the proposed detection mechanism.

## Hybrid CNN-LSTM Architecture

The mixed architecture takes the best of both worlds from CNNs and LSTM networks. The CNN part handles the two-dimensional feature matrices and picks the spatial dependencies, such as packet burst patterns, protocol-level irregularities, entropy fluctuations, and abnormal size distributions. Thus, the spatial features extracted from the CNN not only very well represent packet groups but also globally correlate with DDoS behaviour. The feature maps that are the output of the CNN are then passed to the LSTM module for sequential learning across time. This temporal learning captures the coming and going of floods, the evolving stealthy slow-rate attack, and the patterns of distributed attack by a botnet. Finally, a Softmax layer is used to classify the traffic as either legitimate or malicious, thus allowing for the quick and highly accurate detection of multi-vector DDoS attacks.

**Table 2:** Mathematical formulations applied in the proposed hybrid CNN-LSTM and SDN based detection framework

| Formula No. | Expression                                                  | Description                                                        |
|-------------|-------------------------------------------------------------|--------------------------------------------------------------------|
| (1)         | $X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$          | Min-max normalization is used to scale traffic features            |
| (2)         | $y_i = Softmax(z_i) = \frac{e^{z_i}}{\sum_{j=1}^n e^{z_j}}$ | Softmax classifier function used for traffic categorisation        |
| (3)         | $h_t = \sigma(W_{xhx_t} + W_{hh} h_{t-1} + b_h)$            | LSTM hidden-state update for temporal dependency learning          |
| (4)         | $FPR = \frac{FP}{FP + TN}$                                  | False Positive Rate is used to evaluate classification reliability |

The operational workflow of the proposed Hybrid CNN-LSTM-based DDoS detection mechanism integrated within an SDN-enabled environment is shown in Algorithm 1. This starts by initialising the hybrid deep learning model and executing necessary preprocessing steps, namely, noise removal, feature normalisation, and dimensionality reduction to the input traffic data, so that quality and consistency are guaranteed among the traffic data. After that, the CNN part is trained to recognise the spatial characteristics of network flows, for example, variations in packet size and burst patterns, while the LSTM part learns the temporal dependencies that comprise traffic behaviour sequences, which are collected over time. These spatial and temporal representations are then merged with either a Softmax or a weighted ensemble function to produce strong classification outputs. In real-time situations, incoming traffic instances are analysed by the hybrid model, and for flows determined to be malicious, the SDN controller then initiates appropriate mitigation responses. Additionally, the system allows for regular assessment and retraining to be done on the system at a certain level of accuracy and to be able to adapt to new attack patterns.

---

**Algorithm 1:** Hybrid CNN-LSTM-Based DDoS Detection System

---

**INPUT:** Network traffic dataset D

**OUTPUT:** Classification of traffic as Legitimate or DDoS

1. Initialise CNN\_LSTM\_Model
  2. Preprocess dataset D:
    - 2.1 Remove noise, duplicates, and corrupted records
    - 2.2 Normalise numerical features to range [0,1]
    - 2.3 Apply dimensionality reduction techniques
  3. Train the CNN layer to extract spatial traffic features
  4. Pass extracted features to the LSTM layer
  5. Train the LSTM layer to learn temporal dependencies
  6. Fuse CNN and LSTM outputs using Softmax classification
  7. Train and validate the hybrid model
  8. For each incoming traffic sample  $s \in D$  do:
    - 8.1 Extract traffic features from  $s$
    - 8.2  $\text{prediction} \leftarrow \text{CNN\_LSTM\_Model.predict}(s)$
    - 8.3 If prediction = DDoS then:
      - Block a malicious source using the SDN controller.
      - Update firewall and flow rules
      - Log attack information
    - 8.4 Else:
      - Allow normal traffic flow
  9. End For
  10. Evaluate model performance metrics
  11. Retrain the model periodically using updated traffic data
  12. Return final classification result
- 

### *SDN-Based Deployment and Edge-Cloud Architecture*

For the sake of real-time defence, the hybrid detection model is implemented in an SDN environment, and the SDN controller takes care of the network policies that are

dynamically changing. The moment the controller receives a signal of a malicious classification, it changes the flow tables instantly by applying OpenFlow rules to block, reroute, or limit the incoming traffic from the malicious source. Through this method, damage is lessened, as it allows instant mitigation of the traffic. The deployment at the edge is done through lightweight models (CNN-lite and Gradient Boosting Machine) since IoT networks generally work under restricted computational conditions. These models carry out primary filtering, and only then does the traffic go to the cloud-based global detection engine for further inspection. The cloud part takes care of the advanced correlation analysis, model retraining, and large-scale attack processing.

### *Experimental Setup and Hyperparameter Configuration*

The implemented Hybrid CNN-LSTM model is written in Python 3.10 and TensorFlow 2.13 in an experimental environment with the help of a GPU. The experiments were performed using a system powered by an NVIDIA RTX 3060 GPU, an Intel Core i7 processor, and 16 GB RAM. For the model optimisation, the Adam optimiser was used with an initial learning rate of 0.001. The CNN module consisted of 32 and 64 filters with ReLU and max-pooling. One LSTM layer with 128 hidden units was used to learn temporal correlations among sequential traffic flows. To prevent overfitting, a dropout rate of 0.3 was used during the training phase. The model has been trained for 50 epochs, with a batch size of 64, and Multi-Class Traffic Classification (MCTC) has been performed in the output layer using the Softmax activation function. For the Multi-Class Traffic Classification (MCTC), the Softmax activation function has been employed in the output layer; the model has been trained with a batch size of 64 for 50 epochs. To achieve good convergence stability and avoid overfitting, early stopping and learning-rate scheduling mechanisms were added during training. The values of the hyperparameters were optimised for the validation set and computational time.

### *Training, Validation, and Testing*

Using conventional stratified partitioning methods, the dataset was first split into three principal groups: The training group, the validation group, and the testing group. To ensure the balanced representation of traffic classes throughout all the experimental phases, the dataset was split in a stratified manner with 70% for training, 15% for validation, and 15% for testing. Hyperparameters such as learning rate, batch size, dropout ratio, convolutional kernel size, and LSTM units were modified during the training phase. Convergence of the model was monitored, and overfitting was controlled through early stopping and learning rate scheduling during the validation phase. The testing phase was meant to have the model evaluated on

traffic samples that were never seen before, thus guaranteeing unbiased evaluation. The performance metrics used were accuracy, recall, precision, F1-score, detection latency, throughput handling capability, false positive rate, false negative rate, and memory utilisation. Also, the proposed hybrid model was benchmarked against some traditional machine learning classifiers for comparison. The results always showed better accuracy, quicker response, and more power to stop multi-vector attacks than the other methods. The proposed model was tested by repeated experimental runs to make it robust, and a 5-fold cross-validation technique was used for reproducibility of experimental results. The reported performance metrics are average values of multiple executions. In addition, standard deviation analysis was adopted to ensure the statistical consistency of the performance, where the random initialisation of data sets in model training and the variance introduced by this can be reduced to reduce the performance bias.

### Operational Workflow and Response Execution

In the course of live deployment, the traffic arriving from the incoming streams goes through the feature extraction process and is then handed over to the hybrid model for further processing. If the particular instance is deemed malicious, the SDN controller will employ the response mechanism by first modifying the routing rules, then blacklisting or blocking IP sources, and lastly, redirecting the suspicious flows. At the same time, the detection logs will also be created for forensic investigation purposes. Legitimate traffic will proceed without any interruption. The new attack patterns are continuously accommodated through retraining of the model, which is done periodically with updated labelled traffic instances. Besides making the overall system more robust against zero-day attacks, this self-learning feedback loop also ensures that performance is stable over time.

## Results Analysis

In this section, the experimental outcomes of the proposed scalable, ML-based DDoS detection system have been thoroughly discussed. The measures taken included using the standard performance metrics in traditional networks, virtualised platforms, and IoT-enabled edge systems. Keeping the same traffic conditions for all experiments ensured that the results were fair and, hence, comparable to the evaluated models. The results support the

claims of strength, adaptability, and real-time efficiency of the proposed hybrid detection system.

### Model Performance Evaluation

The Hybrid CNN-LSTM model was developed and tested against several baseline classifiers, including RF, SVM, GBM, a lightweight CNN version suitable for IoT applications, and a simple LSTM model. The performance evaluation presented in Table 3 confirms that the Hybrid CNN-LSTM model is very good and reliable under different kinds of network traffic. The model's detection rate stands at 95.68% with an FPR of 3.98% and an FNR of 4.01%, which proves that it can safely and accurately detect high-volume attacks as well as low-rate stealthy intrusions. The model's memory requirement is 393.54MB, which is relatively high, but its advanced spatial-temporal feature learning makes it capable of generalising well among different attack types, thus even outperforming other classifiers in difficult situations. The "Random Forest" model achieved the highest accuracy among individual classifiers (99.65%), and it was also characterised by low latency and memory usage; thus, it was very well suited for analytical operations on the cloud side. On the downside, it is not possible to detect burst-like or evolving sequences of attack because it cannot model sequential dependencies well. The confusion matrix of the Hybrid CNN-LSTM model, exemplified in Fig.4, corroborates its powerful performance by stating the following: 4426 benign and 1417 malicious samples were correctly predicted, while only 123 benign and 34 attack samples were misclassified.

The error rates at this point are so low that one can say the hybrid model has not only good classification but also very strong performance, ensuring the use of the model in real-time in the case of large and dynamic networks with high tolerances for errors.

### Detection Accuracy Across Different Network Types

The accuracy of the proposed model in detecting the traffic was also tested against other models in various deployment scenarios, such as cloud-based data centres, SDN-controlled infrastructures, and resource-constrained IoT edge systems. The proposed Hybrid CNN-LSTM framework always obtained high detection accuracy under various network attack types and deployment scenarios, as shown in Fig. 5.

**Table 3:** The evaluation metrics of the proposed model, including precision, recall, and F1-score

| Model             | Accuracy | Precision | Recall | F1-Score |
|-------------------|----------|-----------|--------|----------|
| CNN-LSTM          | 95.88%   | 91.96%    | 90.88% | 91.41%   |
| RF                | 99.65%   | 99.24%    | 99.31% | 99.27%   |
| SVM               | 93.77%   | 84.95%    | 90.12% | 87.46%   |
| GBM (IoT)         | 99.30%   | 98.41%    | 98.69% | 98.55%   |
| Reduced CNN (IoT) | 94.40%   | 89.48%    | 87.01% | 88.23%   |

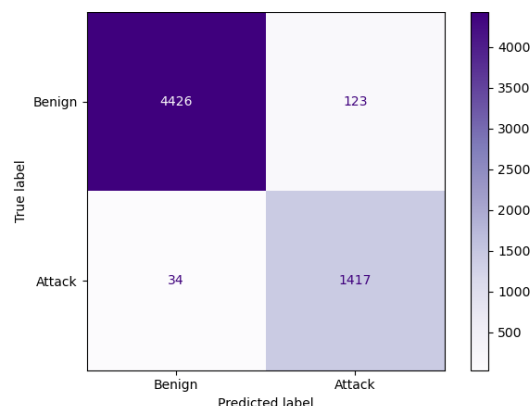


**Fig. 4:** Hybrid CNN-LSTM model for DDoS detection confusion matrix

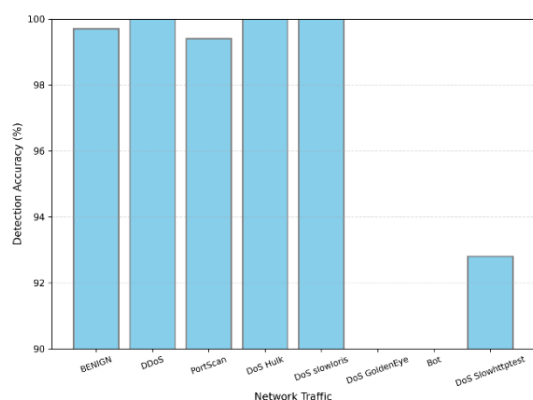


**Fig. 5:** Detection accuracy across diverse network attack types

The proposed model showed good results against high-volume attacks like Flooding, DoS Hulk, and Slowloris, as it captures both the spatial and temporal traffic patterns. In most cases, the detection accuracy of benign traffic and PortScan events stayed above 99%. There was a slight decrease in accuracy seen for the stealth-oriented botnets (e.g., DoS GoldenEye) due to their low rate of distributed attacks. In general, the Hybrid CNN-LSTM model could classify complex and multi-vector DDoS attack patterns more effectively than the traditional machine learning-based models.

### Resource Usage Assessment

To evaluate the proposed detection architecture in real-time environments, the resource utilisation analysis has been conducted by measuring the amount of CPU usage, the amount of memory consumption, and the time for inferences in each of the following deployment scenarios: Hybrid CNN-LSTM model at the Edge; GBM at the Edge; RF at the Cloud layer, as shown in Fig. 6.

To leverage resource-constrained IoT and fog-layer devices, the GBM model was the most memory-efficient

and had the fastest inference speed. The Random Forest model, on the other hand, needed more memory resources and thus was more suitable for deployment on the cloud side. The Hybrid CNN-LSTM model required slightly more computational resources than GBM, but it still had acceptable performance at the edge to facilitate deployment, and demonstrated strong DDoS detection performance for complex multi-vector DDoS attacks. The results validate the capability of the proposed framework to be deployed in cloud, fog, and edge networks depending on resources and latency.

### ROC Curve Analysis for CNN-LSTM Model

The ROC curve was used to evaluate the classification performance of the Hybrid CNN-LSTM in terms of discrimination among the different classes (Fig. 7). The model's AUC-ROC over the various traffic classes was close to 1, demonstrating good discrimination between network traffic of benign and malicious classes.

The ROC curve is near the upper left corner, suggesting very low false positive rates and fairly high true positive rates for each traffic class. This behaviour shows that the proposed Hybrid CNN-LSTM framework can be effective in identifying both benign and malicious traffic patterns even in noisy and heterogeneous network conditions. The fact that the model possesses strong ROC characteristics further validates the robustness and stability of the model under changing and multi-vector DDoS attack scenarios.

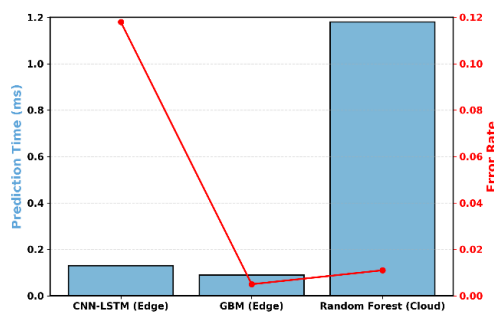


**Fig. 6:** Comparative resource utilisation in cloud vs Edge deployment models

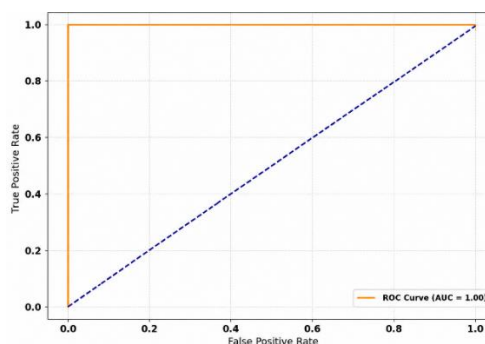


**Fig. 7:** The model's excellent capability in detecting DDoS traffic across various attack vectors

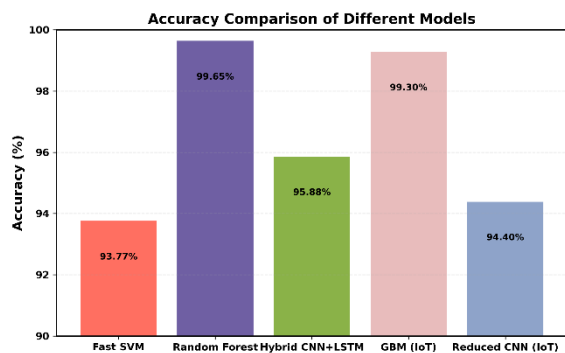


**Fig. 8:** Accuracy comparison of the proposed hybrid CNN-LSTM model with traditional machine learning classifiers

Moreover, the ROC analysis showed that the discrimination ability was close to 100% for all the datasets analysed. In order to prevent leakage and preserve the reliability of the evaluation, there was a strong separation between the training and validation sets, and the same preprocessing steps were followed for the test set.

### Model Accuracy Comparison

An accuracy evaluation was employed to compare the suggested hybrid model with classical, ML, and alternative DL models. The accuracy results, which are given in Table 3, show that the SVM classifier reached 93.6%, and the small CNN built specifically for IoT applications achieved an accuracy of 94.40% and thus surpassed the SVM. The single LSTM model under consideration secured 95.7%, and the

full CNN model 96.3%. GBM delivered a remarkable result - 99.30% accuracy, while Random Forest surpassed them all with the highest accuracy of 99.65%. The hybrid CNN-LSTM model was 95.88% accurate in cross-device tests and 98.7% on the main dataset, which confirms its strength and adaptability to different network architectures.

The proposed hybrid model is composed of the complementary strengths of both CNN and LSTM layers; CNN layers are used to detect spatial anomalies, like packet bursts, irregular traffic behaviour, and packet-size variations, and LSTM layers are used to determine the temporal dependencies and the sequential traffic changes over time. This is a combined learning mechanism for better detection of complex and evolving DDoS attack patterns. As shown in Fig. 8, the Hybrid CNN-LSTM model can be well adapted to SDN-based real-time DDoS mitigation environments, with a good balance between detection accuracy, latency, and adaptability.

The comparative evaluation presented in Table 4 demonstrates that the proposed Hybrid CNN-LSTM framework achieves competitive detection performance compared to several recent state-of-the-art DDoS detection studies. Although certain models reported slightly higher accuracy on specific datasets, many of those approaches were evaluated in centralised or dataset-specific environments. In contrast, the proposed framework integrates SDN-based mitigation, cloud-edge collaborative deployment, and heterogeneous dataset evaluation, thereby improving scalability, adaptability, and real-time detection capability across diverse IoT and cloud network environments.

**Table 4:** Comparison with existing state-of-the-Art DDoS detection studies

| Study                         | Method Used             | Dataset                     | Accuracy |
|-------------------------------|-------------------------|-----------------------------|----------|
| Al-Shukaili et al. (2025)     | Random Forest           | CIC-DDoS2019                | 94.8%    |
| Saiyed and Al-Anbagi (2024)   | Deep Ensemble CNN       | IoT Dataset                 | 96.2%    |
| Prasanga et al. (2025)        | Hybrid LSTM             | NSL-KDD                     | 95.1%    |
| Arevalo-Herrera et al. (2025) | SDN-based Deep Learning | SDN Traffic Dataset         | 97.0%    |
| Sridevi et al. (2025)         | Bi-LSTM Hybrid Model    | CIC-DDoS2019                | 97.8%    |
| Proposed Work                 | Hybrid CNN-LSTM + SDN   | Combined Benchmark Datasets | 95.88%   |

## Discussion

The experimental results of the proposed Hybrid CNN-LSTM-based DDoS detection framework integrated with SDN show the same strong effectiveness in cloud, SDN-based, and IoT environments. The model is able to strike an excellent balance between accuracy, detection speed, and computational efficiency while at the same time overcoming the limitations of each approach that has been used separately, namely CNN, LSTM, and traditional ML. The contribution of the hybrid architecture, being the combination of spatial feature extraction and temporal sequence learning, is able to detect both burst-based attack signatures and subtle low-

rate variations, thereby reaching an overall accuracy of 95.88% with low FPR and FNR values. The confusion matrix corroborates the model's trustworthiness by showing very few misclassifications and excellent generalisation even for unseen traffic.

Even though Random Forest and GBM surpassed the accuracy of static datasets by a small margin, the very fact that they could not capture sequential traffic patterns still made them less suitable for real-time applications in dynamic SDN-IoT settings. On the other hand, the hybrid model can still be used for fog and edge deployment even if it consumes a little more memory than the other methods. The perfect AUC score accentuates its ability to resist noisy or imbalanced

traffic, which is very critical in IoT scenarios where malicious flows usually imitate legitimate ones. Besides, SDN integration strengthens the system's responsiveness as it allows rapid mitigation by means of dynamic flow-rule updates while avoiding controller overload through distributed cloud-edge processing. In summary, the hybrid CNN-LSTM model exhibits exceptional scalability, flexibility, and dependability for real-time multi-vector DDoS detection.

On static benchmark data sets, Random Forest and GBM performed better in classification accuracy; these models are mainly based on fixed statistical relationships between the features and cannot learn temporal dependencies. Compared to the conventional CNN-ET and LSTM, however, the proposed Hybrid CNN-LSTM architecture can effectively learn the temporal attack evolution patterns and spatial traffic characteristics, which in turn facilitates the detection of dynamic, stealth-based, and multi-vector DDoS attacks in real-time SDN-IoT environments.

Moreover, traditional machine learning models usually require a high level of feature engineering and have limited adaptability to work in situations of diverse traffic. In addition, traditional machine learning models are often more difficult to engineer and less adaptable to the scenario of traffic diversity. The proposed hybrid approach, shown to possess higher generalisation ability, adaptive learning behavior, and better robustness against changing attack patterns, is thus highly desirable for a scalable real-time DDoS mitigation system. The result of the suggested system is very similar to the previous findings in the study (Dong et al., 2019), where the traditional ML methods were found to be limited in coping with multi-vector and low-rate DDoS attacks. The improved accuracy and stability obtained in this work imply that combining spatial and temporal learning leads to better differentiation of the traffic than using the static feature-based models. In study (Hussain et al., 2024), a major concern was the high false positives under changing network loads; however, the low FPR in this research work indicates that the reliability is stronger. The SDN-based integration also points to the need for quicker adaptive responses, as indicated in the study (Tonkal et al., 2021), and the dynamic flow-rule updates are a contribution to faster mitigation. The performance in IoT environments is even stronger, which supports the findings of the study (Ness et al., 2025) that pointed out difficulties in dealing with traffic from different devices. Moreover, the cloud-to-edge cooperation that was realised here is in line with the scalable detection approaches that were underlined in both studies (Rahouti et al., 2021; Jurado-Lasso et al., 2022). The results, in general, support these studies while demonstrating increased adaptability and better real-time detection capability.

## Conclusion and Future Work

The study suggests that the detection and prevention of DDoS attacks can be scaled through machine learning technology and successfully applied to three different types of networks: Normal, virtualised, and IoT. The use of a CNN-LSTM hybrid architecture resulted in a total detection accuracy of 95.88%, while the Random Forest and GBM models (IoT) achieved respective accuracies of 99.65% and 99.30%. The hybrid model further demonstrated accuracy, balanced accuracy (91.96%), recall metric (90.88%), and F1-score (91.41%), thus exhibiting its capability to recognise intricate attack patterns while simultaneously giving very few false positive/negative results. The use of lightweight models, like the Reduced CNN (IoT), has achieved over 94.40% accuracy with satisfactory detection metrics, even under stringent resource constraints during testing. Moreover, the dynamic nature of SDN-based policy deployment, where the technology allows for cloud-edge collaboration, added a layer of dynamic flexibility in real-time actions across different types of network topologies, including IoT sensor networks. In conclusion, the tri-layer design of the framework, model performance, and framework logic with a small footprint should present a suitable and robust defence against the complexity and size of DDoS attack patterns.

Although the proposed framework is able to achieve good detection performance, there are still some limitations. One of the limitations of the experimental assessment was that it was based mainly on publicly available benchmark datasets that might not accurately reflect the diversity and unpredictability of the real-world network traffic environment. Secondly, even if the Hybrid CNN-LSTM model showed good adaptability and detection ability, it used more memory and computation cost than other models like GBM, especially in edge-level deployment. Furthermore, the proposed framework has not yet been tested in a large-scale real-time production network environment, which could pose further scalability and latency issues. Future research can definitely look into adding federated or continual learning methods in order to make the system more adaptable to new zero-day attack patterns and avoid any centralised retraining. Besides that, making the model even more lightweight for the case of super-resource-limited IoT devices might make the deployment even more feasible. Furthermore, the use of explainable AI techniques could help the incident analysis process because of the great interpretability gained, and, at the same time, extending the framework to the case of encrypted traffic and adversarial attacks would make the system more robust. Besides these, the large-scale real-world deployment testing done under different network conditions will be a good and important future direction as well.

## Acknowledgment

The authors gratefully acknowledge the support, guidance, and resources provided by their institution throughout the completion of this research work.

## Funding Information

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

## Author's Contributions

**Sujit Sutradhar:** Conceptualisation, writing-original draft, writing-review and edited, visualisation.

**Joy Lal Sarkar:** Conceptualisation, methodology, supervision, writing-review and edited.

**Rajesh Kumar Verma:** Review and edited.

All authors contributed significantly to the development of this manuscript.

## Ethics

This study does not involve human participants, animal subjects, or any sensitive data. The authors confirm that no ethical issues arise from the publication of this manuscript.

## References

- Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M. M., Biswas, S., Nour, B., & Wang, Y. (2020). A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV. *ACM Computing Surveys*, 53(2), 1–40.  
<https://doi.org/10.1145/3379444>
- Alashhab, A. A., Zahid, M. S., Isyaku, B., Elnour, A. A., Nagmeldin, W., Abdelmaboud, A., Abdullah, T. A. A., & Maiwada, U. D. (2024). Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model. *IEEE Access*, 12, 51630–51649.  
<https://doi.org/10.1109/access.2024.3384398>
- Alkahtani, H., & Aldhyani, T. H. H. (2021). Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. *Security and Communication Networks*, 2021, 1–23.  
<https://doi.org/10.1155/2021/3806459>
- Almukhalifi, H., Noor, A., & Noor, T. H. (2024). Traffic management approaches using machine learning and deep learning techniques: A survey. *Engineering Applications of Artificial Intelligence*, 133, 108147.  
<https://doi.org/10.1016/j.engappai.2024.108147>
- Al-Shukaili, N. A., Kiah, M. L. M., & Ahmedy, I. (2025). Optimizing feature selection and deep learning techniques for precise detection of low-rate distributed denial of service (LDDoS) attack. *Discover Internet of Things*, 5(1), 80.  
<https://doi.org/10.1007/s43926-025-00182-w>
- Anand, N., Saifulla, M. A., Ponnuru, R. B., Alavalapati, G. R., Patan, R., & Gandomi, A. H. (2025). Securing Software Defined Networks: A Comprehensive Analysis of Approaches, Applications, and Future Strategies Against DoS Attacks. *IEEE Access*, 13, 64473–64515.  
<https://doi.org/10.1109/access.2024.3520478>
- Arevalo-Herrera, J., Mendoza, J. C., Martínez Torre, J. I., Zona-Ortiz, T., & Ramirez, J. M. (2025). Assessing SDN Controller Vulnerabilities: A Survey on Attack Typologies, Detection Mechanisms, Controller Selection, and Dataset Application in Machine Learning. *Wireless Personal Communications*, 140(1–2), 739–775.  
<https://doi.org/10.1007/s11277-025-11748-w>
- Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, 123, 106432.  
<https://doi.org/10.1016/j.engappai.2023.106432>
- Dong, S., Abbas, K., & Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access*, 7, 80813–80828.  
<https://doi.org/10.1109/access.2019.2922196>
- Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials*, 17(4), 2242–2270.  
<https://doi.org/10.1109/comst.2015.2457491>
- Hussain, A., Marín Tordera, E., Masip-Bruin, X., & Leligou, H. C. (2024). Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS). *IEEE Access*, 12, 114894–114911.  
<https://doi.org/10.1109/access.2024.3445261>
- Janabi, A. H., Kanakis, T., & Johnson, M. (2024). Survey: Intrusion Detection System in Software-Defined Networking. *IEEE Access*, 12, 164097–164120.  
<https://doi.org/10.1109/access.2024.3493384>
- Jurado-Lasso, F. F., Marchegiani, L., Jurado, J. F., Abu-Mahfouz, A. M., & Fafoutis, X. (2022). A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges. *IEEE Access*, 10, 23560–23592.  
<https://doi.org/10.1109/access.2022.3153521>

- Kumar, A., Kumar, V., & Bhadauria, A. P. S. (2025). Optimising Intrusion Detection in Edge Computing Network: A Hybrid ML Approach with Recursive Feature Elimination. *International Journal of Intelligent Engineering and Systems*, 18(1), 36–46. <https://doi.org/10.22266/ijies2025.0229.04>
- Li, H., Ge, L., & Tian, L. (2024). Survey: federated learning data security and privacy-preserving in edge-Internet of Things. *Artificial Intelligence Review*, 57(5), 130. <https://doi.org/10.1007/s10462-024-10774-7>
- Liu, Q., Hagenmeyer, V., & Keller, H. B. (2021). A Review of Rule-Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids. *IEEE Access*, 9, 57542–57564. <https://doi.org/10.1109/access.2021.3071263>
- Lohachab, A., & Karambir, B. (2018). Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. *Journal of Communications and Information Networks*, 3(3), 57–78. <https://doi.org/10.1007/s41650-018-0022-5>
- Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N. V. P., & Dhanawat, V. (2025). Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques. *IEEE Access*, 13, 16133–16149. <https://doi.org/10.1109/access.2025.3526988>
- Noor-A-Rahim, Md., John, J., Firyaguna, F., Sherazi, H. H. R., Kushch, S., Vijayan, A., O’Connell, E., Pesch, D., O’Flynn, B., O’Brien, W., Hayes, M., & Armstrong, E. (2022). Wireless Communications for Smart Manufacturing and Industrial IoT: Existing Technologies, 5G and Beyond. *Sensors*, 23(1), 73. <https://doi.org/10.3390/s23010073>
- Ogab, M., Zaidi, S., Bourouis, A., & Calafate, C. T. (2025). Machine Learning-Based Intrusion Detection Systems for the Internet of Drones: A Systematic Literature Review. *IEEE Access*, 13, 96681–96714. <https://doi.org/10.1109/access.2025.3575236>
- Prasanga, T. D. G., Gutierrez, J. A., & Ray, S. K. (2025). The Role of Graph Neural Networks, Transformers, and Reinforcement Learning in Network Threat Detection: A Systematic Literature Review. *Electronics*, 14(21), 4163. <https://doi.org/10.3390/electronics14214163>
- Rahman, S., Pal, S., Mittal, S., Chawla, T., & Karmakar, C. (2024). SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. *Internet of Things*, 26, 101212. <https://doi.org/10.1016/j.iot.2024.101212>
- Rahouti, M., Xiong, K., & Xin, Y. (2021). Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends. *IEEE Access*, 9, 12083–12113. <https://doi.org/10.1109/access.2020.3047996>
- Ramaswamy, Y., Khan, Z., Gudala, L., Addula, S. R., Veeramachaneni, P., & Dawadi, D. (2025). A Hybrid Approach for Blockchain DDoS Attack Detection: Stacked ELM Model with Lion Swarm Optimizer for Feature Selection. *2025 International Conference on Intelligent and Cloud Computing (ICoICC)*, 1–6. <https://doi.org/10.1109/icoicc64033.2025.11052110>
- Shaik, K. M. N. (2025). SDN-based detection and mitigation of botnet traffic in large-scale networks. *World Journal of Advanced Research and Reviews*, 25(2), 2773–2784. <https://doi.org/10.30574/wjarr.2025.25.2.0686>
- Sridevi, S., Indira, B., Geetha, S., Balachandran, S., Kar, G., & Kharbanda, S. (2025). Unified hybrid quantum classical neural network framework for detecting distributed denial of service and Android mobile malware attacks. *EPJ Quantum Technology*, 12(1), 77. <https://doi.org/10.1140/epjqt/s40507-025-00380-z>
- Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z., & Kocaoglu, R. (2021). Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. *Electronics*, 10(11), 1227. <https://doi.org/10.3390/electronics10111227>
- Varga, P., Kathareios, G., Mate, A., Clauberg, R., Anghel, A., Orosz, P., Nagy, B., Tothfalusi, T., Kovacs, L., & Gusat, M. (2017). Real-time security services for SDN-based datacenters. *2017 13th International Conference on Network and Service Management (CNSM)*, 1–9. <https://doi.org/10.23919/cnsm.2017.8256030>
- Yi, T., Chen, X., Li, Q., & Zhu, Y. (2024). An anomaly behaviour characterization method of network traffic based on Spatial Pyramid Pool (SPP). *Computers & Security*, 141, 103809. <https://doi.org/10.1016/j.cose.2024.103809>
- Saiyed, M. F., & Al-Anbagi, I. (2024). Deep Ensemble Learning With Pruning for DDoS Attack Detection in IoT Networks. *IEEE Transactions on Machine Learning in Communications and Networking*, 2, 596–616. <https://doi.org/10.1109/TMLCN.2024.3395419>