Computer Science Communications and Applications

DDoS Anomaly Detection in Software Defined Networks Using ML models

Malini, P* and Srinivas Murthy, H**

Department of Computer Science and Engineering, S.J.C. Institute of Technology, Chickballapur, INDIA-562101

Malini, P: M. Tech Student: *ammumalini123@gmail.com.
Srinivas Murthy, H: Associate Professor: **hsrinivasmurthy@sjcit.ac.in; hsrinivasmurthy@gmail.com

ARTICLE INFO Received 7th April 2026, Revised 12th April 2026, Accepted 19th April 2026.
www.esrapublications.com

A B S T R A C T

Software-Defined Networking (SDN) has emerged as a foundational paradigm for next-generation network management, offering programmability, centralized orchestration, and dynamic control over network resources. While these attributes enhance operational agility, they simultaneously create a concentrated attack surface, particularly at the level of the SDN controller, which is a prime target for Distributed Denial of Service (DDoS) attacks. This paper proposes a comprehensive anomaly detection framework that integrates Machine Learning (ML), Deep Learning (DL), and ensemble-based classifiers to identify DDoS threats in SDN environments. The framework evaluates multiple architectures - including RNN, LSTM, GRU, BiLSTM, CNN, and hybrid CNN–BiLSTM - alongside conventional classifiers such as Random Forest, XGBoost, and SVM, using large-scale datasets with up to 20 lakh instances. Experimental outcomes consistently demonstrate the superiority of deep learning architectures in encoding complex traffic behavior, while the proposed Voting Classifier achieves the best overall performance across all five evaluation metrics: accuracy, precision, recall, F1-score, and ROC–AUC. These findings affirm the viability of AI-integrated frameworks for scalable, real-time DDoS detection in production SDN environments.

Keywords: Software-Defined Networking; DDoS Attack Detection; Machine Learning; Deep Learning; Ensemble Learning.

1. INTRODUCTION

Modern network infrastructure is undergoing rapid transformation with the widespread adoption of Software-Defined Networking (SDN). Unlike conventional architectures where control and data functions are tightly bound to physical devices, SDN separates the forwarding plane from the decision-making layer, placing centralized intelligence within a dedicated controller [1]. This architectural shift grants administrators unprecedented flexibility, enabling dynamic policy enforcement, automated traffic management, and scalable deployment. However, concentrating control within a single logical entity creates a structural vulnerability: any successful attack on the SDN controller can disrupt the entire network. Among the attack vectors that exploit this weakness,

Address for correspondence: Department of Computer Science and Engineering, S.J.C. Institute of Technology, Chickballapur, INDIA-562101.

Distributed Denial of Service (DDoS) assaults are particularly damaging, capable of saturating controller resources and degrading service availability across the entire infrastructure.

Conventional security strategies - those relying on static rulesets or signature-matching - are increasingly inadequate for defending against modern DDoS campaigns. Sophisticated attackers continuously mutate their traffic patterns to evade known signatures, rendering rule-based defenses ineffective in dynamic environments. Intelligent, data-driven approaches offer a compelling alternative. By learning directly from historical and real-time traffic data, ML and DL algorithms can construct behavioral models of normal network activity and flag deviations that may indicate an attack. Leveraging the global traffic visibility afforded by the SDN controller, these AI-driven detection mechanisms can act rapidly, minimizing response latency while maintaining high classification accuracy [2].

The urgency of this challenge is reinforced by recent threat intelligence. Industry forecasts project that the global volume of DDoS incidents will grow from approximately 7.9 million in 2018 to exceed 15 million by 2023, reflecting a sustained escalation in both attack frequency and scale [3]. These statistics underscore the need for adaptive, intelligent security solutions that can be embedded directly within SDN control infrastructure.

Existing research on DDoS detection in SDN has explored a broad range of learning-based strategies, spanning supervised classifiers, unsupervised anomaly detectors, and hybrid architectures. Despite notable progress, most approaches individually address either detection accuracy or scalability, and rarely combine both objectives within a unified framework. Single-model approaches often fail to generalize across varied attack types, while the absence of ensemble strategies limits their robustness to concept drift and adversarial variability [4].

This work addresses these limitations by proposing an integrated detection pipeline that combines deep learning architectures with ensemble classification to provide comprehensive DDoS anomaly detection within SDN environments. The framework is evaluated at scale - across datasets ranging from 5 lakh to 20 lakh instances - to validate its practical applicability under realistic network conditions.

1.1 Motivation

The growing deployment of SDN in enterprise, cloud, and telecommunications environments has intensified exposure to controller-targeted DDoS attacks. Static defenses based on fixed rules or predefined signatures are inadequate in the face of polymorphic attack strategies that adapt to evade detection. Furthermore, the exponential growth in network traffic volumes demands detection systems that are both computationally efficient and robust enough to handle real-time classification. These constraints collectively motivate the adoption of ML and DL-based anomaly detection frameworks that can autonomously learn from traffic behavior, identify novel deviations, and support timely intervention without requiring manual signature updates.

1.2 Contribution

This paper introduces a unified anomaly detection framework for SDN environments that rigorously benchmarks multiple DL architectures, hybrid models, and ensemble classifiers on large-scale datasets containing up to 20 lakh instances. The key contributions are as follows:

- A systematic evaluation of seven deep learning models - including RNN, LSTM, GRU, BiLSTM, CNN, and CNN+BiLSTM - alongside seven conventional ML classifiers.

- Empirical demonstration that ensemble learning, specifically the Voting Classifier, achieves the highest detection accuracy, robustness, and generalization across all evaluation conditions.
- Validation of the proposed framework's scalability and suitability for real-time DDoS detection across datasets of varying magnitude.

1.3 Organization

The remainder of this paper is structured as follows: Section 2 surveys related work on ML and DL-based DDoS detection in SDN environments. Section 3 presents the proposed methodology, encompassing problem formulation, system architecture, and model design. Section 4 reports experimental results and comparative performance analysis. Section 5 discusses key findings and their implications, and Section 6 concludes the paper with directions for future research.

2. LITERATURE SURVEY

This section reviews notable contributions to ML and DL-based intrusion detection and DDoS mitigation within SDN environments. The surveyed works collectively demonstrate the maturity of AI-driven security frameworks in achieving high detection fidelity, while simultaneously revealing open challenges in real-world scalability, dataset diversity, and explainability.

Shaji et al. [5] presented Deep-Discovery, an anomaly detection system for SDN that employs a Multi-Layer Perceptron (MLP)-based feedforward neural network. The framework classifies both volume-based and protocol-based DDoS attacks, operating effectively under multi-class (six categories) and binary classification settings. In multi-class mode, the system achieved an accuracy of 98.81% with a False Alarm Rate (FAR) of just 0.002, while binary classification yielded 99.79% accuracy with an FAR of 0.0001. A central finding of this work is that competitive detection performance is achievable using architecturally simple neural networks, without imposing excessive computational overhead - an important consideration for resource-constrained SDN deployments.

Wang et al. [6] conducted a comparative evaluation of six DL architectures - DNN, CNN, RNN, LSTM, CNN+RNN, and CNN+LSTM - for intrusion detection using the modern CSE-CIC-IDS2018 dataset. The study addressed a recognized gap in prior work, namely the widespread use of outdated benchmarks, by adopting a contemporary dataset containing six attack categories alongside benign traffic. All architectures achieved multi-class accuracy exceeding 98%, though hybrid models such as CNN+LSTM introduced higher inference latency, making simpler architectures like DNN and RNN more suitable for real-time operational scenarios.

Liu et al. [7] investigated the use of feature engineering combined with ML classifiers for DDoS detection in SDNs, employing the CSE-CIC-IDS2018 dataset. The study applied meta-heuristic optimization for feature selection prior to model training and evaluated both conventional classifiers (RF, SVM, KNN, DT, XGBoost) and neural models (DNN, CNN, RNN, LSTM). Random Forest emerged as the optimal trade-off between performance and computational efficiency, with detection accuracy consistently above 98%. These results reinforce the value of intelligent feature reduction as a preprocessing strategy.

Hammad et al. [8] introduced a machine learning-based Network Intrusion Recovery (MLBNIR) mechanism for SDN, targeting the often-neglected problem of post-attack restoration. By training a flow-based ML model to select optimal backup paths based on learned traffic dynamics, the proposed approach reduced intrusion recovery time by up to 90% and improved bandwidth utilization by up to 57% over conventional recovery schemes, demonstrating that ML can contribute meaningfully beyond detection to post-incident resilience.

Ribeiro et al. [9] combined ML-based flow classification with a Moving Target Defense (MTD) strategy to both detect and mitigate DDoS attacks in SDN. Upon identifying malicious traffic from bot-coordinated sources, the system dynamically redirected attack flows to designated low-capacity servers, preserving critical service availability. The architecture achieved detection and mitigation within approximately three seconds across multiple ML classifiers, offering a practical and deployable defense model.

Table 1: Comparison of ML/DL-based DDoS Anomaly Detection Approaches in SDN

Author	Concept	Advantages	Limitations
Musa et al., 2024 [10]	Systematic survey of ML/DL methods for DDoS anomaly detection and mitigation in SDN.	Broad taxonomy, high-accuracy insights, identifies research trends.	Limited real-world validation; reliance on pre-existing datasets; scalability and deployment challenges unresolved.
Abdinasir Hirsi et al., 2025 [11]	Comprehensive taxonomy of DDoS anomaly detection across SDN layers using ML, DL, and hybrid methods (2020–2024).	Detailed layer-wise analysis; identifies effective techniques and open research gaps.	Primarily focused on detection rather than deployment; limited experimental benchmarking across unified datasets.
Moloja et al., 2025 [12]	AI-driven anomaly detection in SDN using ML/DL techniques.	High accuracy; real-time threat mitigation; adaptability to novel attack types.	Elevated computational overhead; limited explainability; real-time deployment validation lacking.
Chuang et al., 2022 [13]	ML-based early anomaly and DDoS attack detection in SDN using hierarchical multiclass classification.	High detection accuracy; improved minority class recognition; early real-time mitigation in SDN environments.	Performance dependent on dataset quality and balance; increased complexity and overhead at scale.
Mansoor et al., 2023 [14]	RNN-based IDS with cross-feature selection (IGR + Chi-square) to detect DDoS on SDN controllers.	High accuracy with reduced dimensionality and lower false positive rate.	Performance bound by selected features; scope exists for improvement using advanced DL or optimization strategies.
Taheri et al., 2023 [15]	Comprehensive review of ML/DL techniques for intrusion detection and attack mitigation in SDNs.	Extensive taxonomy; comparative analysis; insights on datasets, models, and performance metrics.	Lacks real-time validation; highlights scarcity of realistic, SDN-specific benchmark datasets.

Jafarian et al. [16] proposed an ensemble-based anomaly detection framework for SDN security, combining NetFlow-based traffic collection with Information Gain Ratio (IGR) for feature selection and stacked ensemble classifiers for improved prediction. The approach attained high accuracy (99.92%) and detection rate (99.83%), with classification error and false alarm rates of 0.08% and 0.03% respectively, while also reducing computational load on SDN controllers and OpenFlow switches.

Ahmed et al. [17] presented a comprehensive survey of ML and DL-based Intrusion Detection Systems for SDN, examining work published between 2015 and 2021. The review taxonomizes IDS approaches by learning paradigm and highlights practical limitations including scalability constraints, class imbalance, and controller overload. The survey concludes by delineating open research directions for building adaptive and efficient IDS solutions.

Satheesh et al. [18] proposed a flow-based, priority-driven intrusion detection framework that integrates ML with SDN's centralized programmability to monitor traffic and distinguish normal from anomalous flows. The framework enforces priority-based bandwidth allocation through virtual circuits, achieving improved routing speed, fault tolerance, and overall security performance compared to traditional networking schemes.

Khairi et al. [19] examined the security vulnerabilities introduced by SDN's centralized controller architecture and analyzed the characteristics of DDoS attacks that target it. The study identified anomaly detection as the most effective and scalable technique for identifying such attacks in intelligent networking systems, drawing attention to the need for lightweight and responsive detection mechanisms.

Dogan et al. [20] carried out a large-scale systematic literature review covering 433 publications on ML/DL-based cyber-attack detection and mitigation in SDN (2020–2024), of which 163 were selected for in-depth taxonomy construction. The review emphasizes the importance of high-quality, SDN-specific datasets and highlights persistent challenges in real-time detection, multi-controller scalability, and dataset adequacy, providing a structured reference for future AI-driven SDN security research.

3. METHODOLOGY

3.1 Problem Statement

DDoS attacks represent one of the most severe and persistent security threats to SDN infrastructure. By directing massive volumes of malicious traffic toward the centralized controller, attackers can exhaust computational resources, disrupt service delivery, and compromise the stability of the entire network. Addressing this threat requires anomaly detection mechanisms that can reliably distinguish attack traffic from legitimate activity at scale, with minimal false positives and low latency. This work formulates DDoS detection as a supervised classification problem and employs a range of ML and DL techniques to construct a robust, scalable detection framework tailored to SDN environments.

Objectives:

- To develop a high-accuracy DDoS anomaly detection framework for SDN environments using the CICIDS dataset.
- To construct a modular architecture capable of identifying and classifying DDoS attack traffic within SDN control flows.
- To embed detection and response functionality directly within the SDN controller layer for centralized, real-time protection.
- To benchmark the framework using standard performance metrics - accuracy, precision, recall, F1-score, and ROC-AUC - ensuring transparent and reproducible comparisons across all evaluated models.

3.2 System Architecture

Figure 1 illustrates the end-to-end workflow of the proposed ML/DL-based classification pipeline, encompassing all stages from raw data ingestion to final model deployment. The pipeline is designed to be modular, reproducible, and scalable.

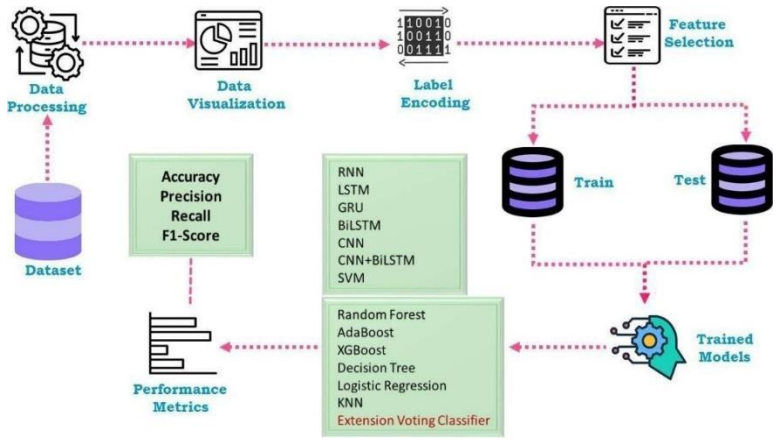

Figure 1. Workflow of the ML/DL-based intrusion detection framework.

The workflow originates at the dataset acquisition stage, where network traffic data - encompassing both normal and malicious flows - is collected as the primary input. This is followed by a data processing phase that involves denoising, handling of missing values, normalization of numerical features, and encoding of categorical attributes into formats suitable for algorithmic processing. These preprocessing steps are critical for ensuring data consistency and improving downstream model quality.

Subsequently, data visualization techniques are applied to analyze traffic patterns, feature distributions, and class imbalance characteristics. Visualization provides empirical insights that guide feature engineering decisions. Label encoding is then performed to convert categorical class labels into numerical representations compatible with the learning algorithms.

Feature selection constitutes a critical intermediate step in which statistically significant and informative attributes are identified while redundant or noise-introducing features are eliminated. This dimensionality reduction step reduces overfitting risk and improves computational efficiency. The refined feature set is subsequently partitioned into training and testing subsets through a stratified split to preserve class distribution.

During model training, a diverse portfolio of architectures is employed. Deep learning models - RNN, LSTM, GRU, BiLSTM, CNN, and the hybrid CNN+BiLSTM - are trained to capture temporal and spatial dependencies inherent in sequential network traffic. In parallel, traditional ML classifiers - including Random Forest, AdaBoost, XGBoost, Decision Tree, Logistic Regression, KNN, SVM, and the Voting Classifier - are trained to provide complementary predictions from different algorithmic perspectives.

Model evaluation is conducted on the held-out test set using accuracy, precision, recall, and F1-score. The Voting Classifier aggregates predictions from the strongest individual models to produce a consensus classification that benefits from reduced variance and improved generalization. The iterative feedback mechanism embedded in the architecture enables continuous refinement based on observed performance gaps. Overall, this pipeline provides a systematic, scalable, and reproducible framework for developing production-quality classifiers for intelligent SDN security.

4. RESULTS

4.1 Performance Evaluation

Table 2: Performance Evaluation on 5-Lakh Dataset

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RNN	0.89	0.88	0.87	0.87	0.91
LSTM	0.92	0.92	0.91	0.91	0.95
GRU	0.91	0.91	0.90	0.90	0.94
BiLSTM	0.92	0.92	0.91	0.91	0.95
CNN	0.93	0.93	0.92	0.92	0.95
CNN+BiLSTM	0.91	0.91	0.90	0.90	0.94
SVM	0.79	0.81	0.77	0.78	0.85
Random Forest	0.91	0.90	0.89	0.89	0.93
AdaBoost	0.83	0.82	0.81	0.81	0.89
XGBoost	0.90	0.89	0.88	0.88	0.92
Decision Tree	0.86	0.85	0.84	0.84	0.88
Logistic Regression	0.72	0.74	0.70	0.71	0.80
KNN	0.88	0.87	0.86	0.86	0.90
Voting Classifier	**0.95**	**0.94**	**0.93**	**0.93**	**0.96**

Table 2 presents performance results for all evaluated classifiers on the 5-lakh dataset. Deep learning architectures - particularly CNN, LSTM, BiLSTM, and GRU - consistently outperform conventional ML methods, demonstrating their capacity to encode complex, high-dimensional traffic patterns that simpler models cannot adequately represent. CNN achieves the highest accuracy among individual architectures (0.93) owing to its robust spatial feature extraction capability, while recurrent models (LSTM, BiLSTM) exhibit competitive results by effectively capturing sequential dependencies in traffic flows. Tree-based ensemble methods such as Random Forest (0.91) and XGBoost (0.90) deliver strong competitive performance over single classifiers. The Voting Classifier attains the best results across all metrics - accuracy 0.95 and ROC-AUC 0.96 - validating the benefit of combining heterogeneous models to leverage complementary classification strengths. Linear models such as Logistic Regression (0.72) and SVM (0.79) show the weakest performance, consistent with their limited capacity to model nonlinear decision boundaries in large-scale datasets.

Table 3: Performance Evaluation on 10-Lakh Dataset

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RNN	0.88	0.87	0.86	0.86	0.89
LSTM	0.91	0.91	0.90	0.90	0.93
GRU	0.90	0.89	0.89	0.89	0.92
BiLSTM	0.91	0.90	0.90	0.90	0.93
CNN	0.92	0.91	0.91	0.91	0.94
CNN+BiLSTM	0.90	0.89	0.88	0.88	0.92
SVM	0.78	0.79	0.77	0.77	0.82
Random Forest	0.89	0.88	0.87	0.87	0.91
AdaBoost	0.80	0.79	0.78	0.78	0.84
XGBoost	0.88	0.87	0.86	0.86	0.90
Decision Tree	0.83	0.82	0.81	0.81	0.85
Logistic Regression	0.70	0.71	0.69	0.69	0.76
KNN	0.85	0.84	0.83	0.83	0.87
Voting Classifier	**0.93**	**0.93**	**0.92**	**0.92**	**0.95**

Table 3 reports results at 10-lakh scale. The relative ordering among architectures remains stable, confirming that the performance hierarchy observed at 5 lakh instances is not an artifact of dataset size. CNN continues to lead individual models with an accuracy of 0.92, while recurrent architectures maintain their reliability in modeling sequential traffic patterns. The Voting Classifier again achieves the highest performance across all metrics (accuracy 0.93, ROC-AUC 0.95), reaffirming its role as the most robust classifier in the evaluated suite. Marginal reductions in absolute metric values across all models relative to Table 2 reflect the increased classification challenge introduced by a larger, more diverse data volume.

Table 4: Performance Evaluation on 20-Lakh Dataset

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RNN	0.86	0.85	0.84	0.84	0.88
LSTM	0.89	0.89	0.88	0.88	0.91
GRU	0.88	0.88	0.87	0.87	0.90
BiLSTM	0.89	0.89	0.88	0.88	0.91
CNN	0.90	0.90	0.89	0.89	0.92
CNN+BiLSTM	0.88	0.87	0.86	0.86	0.90
SVM	0.75	0.76	0.74	0.74	0.80
Random Forest	0.87	0.86	0.85	0.85	0.89
AdaBoost	0.78	0.77	0.76	0.76	0.82
XGBoost	0.86	0.85	0.84	0.84	0.88
Decision Tree	0.81	0.80	0.79	0.79	0.84
Logistic Regression	0.67	0.68	0.66	0.66	0.73
KNN	0.83	0.82	0.81	0.81	0.86
Voting Classifier	**0.91**	**0.91**	**0.90**	**0.90**	**0.93**

Table 4 presents results at maximum scale (20-lakh instances), the most demanding experimental condition. DL models - CNN, LSTM, and BiLSTM - continue to deliver the highest individual accuracy scores (0.90, 0.89, and 0.89 respectively), confirming their scalability. The Voting Classifier achieves accuracy 0.91 and ROC-AUC 0.93 at this scale, sustaining its top-ranked position despite the increased data volume. The Voting Classifier's performance advantage is most visible in the F1-score and ROC-AUC dimensions, indicating superior discriminative capability even under large-scale, heterogeneous input conditions. Logistic Regression (0.67) and SVM (0.75) show the greatest degradation at this scale, reinforcing their unsuitability for production-scale DDoS detection in complex SDN environments.

4.2 Comparative Performance Analysis

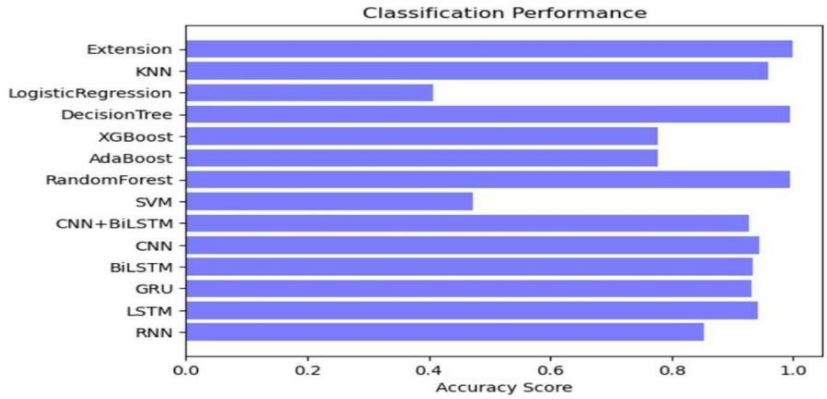

Figure 2. Accuracy Score Comparison

Figure 2 presents accuracy scores across all three dataset scales. DL architectures demonstrate consistently high accuracy, with CNN, LSTM, and BiLSTM all performing comparably and reliably across 5-lakh, 10-lakh, and 20-lakh conditions. The hybrid CNN+BiLSTM model leverages both spatial feature extraction and temporal modeling to sustain strong performance. Ensemble methods - particularly the Voting Classifier - surpass all individual models at every scale, illustrating the value of aggregating diverse predictive signals. Traditional models such as Logistic Regression and SVM exhibit consistently inferior accuracy, confirming their limited suitability for high-dimensional, complex classification tasks.

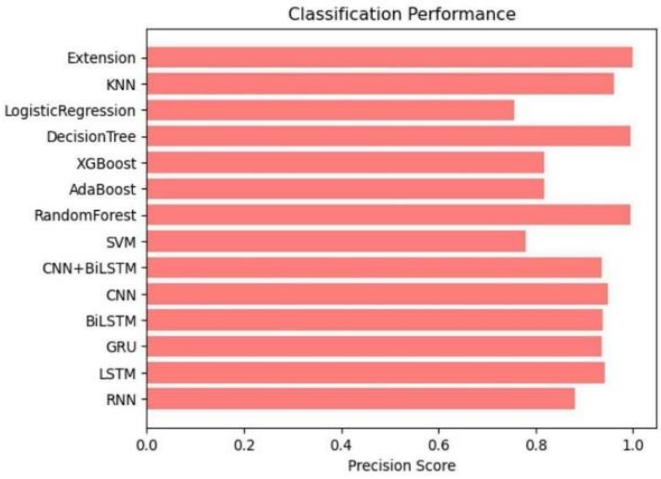

Figure 3. Precision Score Comparison

Figure 3 compares classifier precision. DL and ensemble models achieve the highest precision values, indicating minimal false positive generation - a critical requirement in network security applications where false alarms impose operational costs. The Voting Classifier and CNN deliver the most reliable precision across all scales.

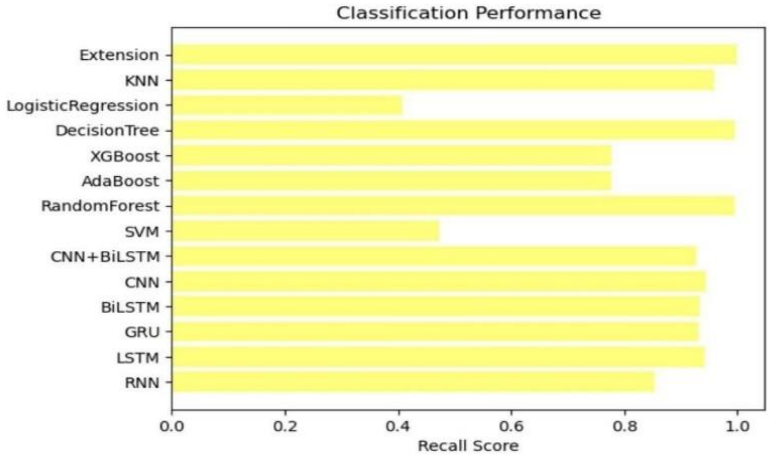

Figure 4. Recall Score Comparison

Figure 4 illustrates recall performance, which measures the fraction of actual DDoS attack instances correctly identified. High recall is essential in security contexts to minimize missed detections. DL models and ensemble methods consistently achieve higher recall than traditional classifiers, with the Voting Classifier attaining the best recall scores at all three scales.

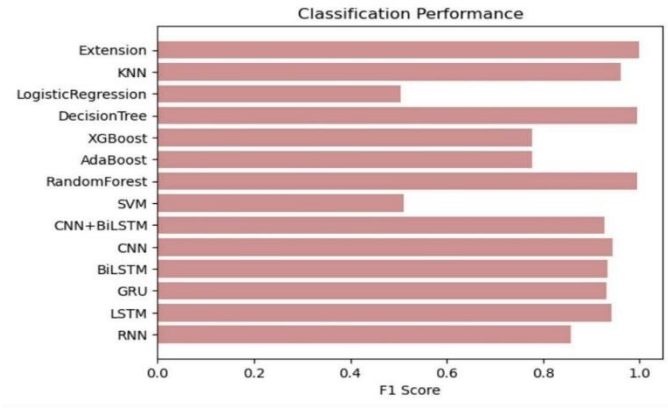

Figure 5. F1 Score Comparison

Figure 5 presents F1-scores, which balance precision and recall into a single harmonized metric. The Voting Classifier achieves the highest F1-scores, reflecting its ability to simultaneously minimize false positives and false negatives. CNN and BiLSTM demonstrate the strongest individual F1 performance among single architectures.

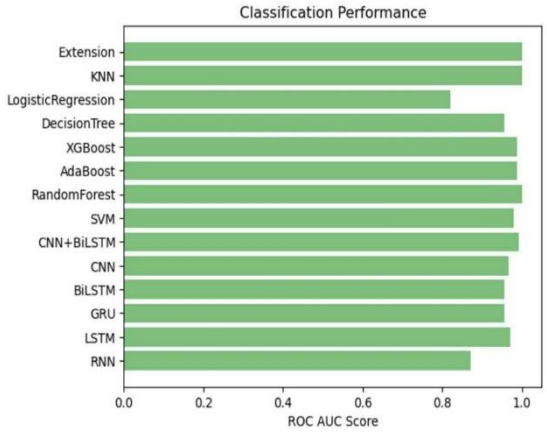

Figure 6. ROC-AUC Score Comparison

Figure 6 shows ROC-AUC scores, which measure classifier discriminative power across varying classification thresholds. The Voting Classifier achieves the highest ROC-AUC values (0.96, 0.95, and 0.93 at 5, 10, and 20 lakh respectively), confirming superior class separability. Logistic Regression and SVM again show the lowest ROC-AUC scores, particularly at larger scales, underscoring their inadequacy for the classification complexity inherent in production-scale SDN traffic data.

5. CONCLUSIONS

This paper presented an AI-driven DDoS anomaly detection framework for Software-Defined Networks, rigorously benchmarking ML, DL, and ensemble-based classifiers across large-scale datasets of up to 20 lakh instances. The experimental results demonstrate that deep learning architectures - particularly CNN, LSTM, and BiLSTM - offer materially superior detection capability compared to traditional classifiers, owing to their ability to encode non-linear and temporal dependencies in high-dimensional traffic data. Ensemble learning, embodied in the proposed Voting Classifier, achieves the best overall performance across all five evaluation metrics at every tested scale, validating the effectiveness of combining heterogeneous learners to improve generalization and reduce classification error.

The proposed framework offers a practical, scalable, and accurate solution for embedding real-time DDoS detection within SDN controller infrastructure. Future research directions include deployment and validation in live SDN testbeds, integration of adaptive online learning mechanisms to track evolving attack strategies, and incorporation of explainable AI techniques to enhance operational transparency and facilitate trust in automated security decisions.

REFERENCES

1. Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S. and Uhlig, S., **2014**. Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103 (1), pp.14-76.
2. Butt, H.A., Al Harthy, K.S., Shah, M.A., Hussain, M., Amin, R. and Rehman, M.U., **2024**. Enhanced DDoS Detection Using Advanced Machine Learning and Ensemble Techniques in Software Defined Networking. Computers, Materials and Continua, 81 (2), pp.3003-3031.
3. Cisco Annual Internet Report (2018–2023) White Paper. (**2022**, January 23). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
4. Thapliyal, S., Wazid, M. and Singh, D.P., 2025. Design of distributed denial-of-service attack prevention mechanism for IoT-driven data fusion system. Cyber Security and Applications, 3, 100092.
5. Shaji, N.S., Jain, T., Muthalagu, R. and Pawar, P.M., **2023**. Deep-discovery: Anomaly discovery in software-defined networks using artificial neural networks. Computers & Security, 132, p.103320.

6. Wang, Y.C., Houng, Y.C., Chen, H.X. and Tseng, S.M., **2023**. Network anomaly intrusion detection based on deep learning approach. Sensors, 23 (4), p.2171.
7. Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z. and Shan, Y., **2023**. A DDoS detection method based on feature engineering and machine learning in software-defined networks. Sensors, 23 (13), p.6176.
8. Hammad, M., Hewahi, N. and Elmedany, W., **2023**. Enhancing Network Intrusion Recovery in SDN with machine learning: an innovative approach. Arab Journal of Basic and Applied Sciences, 30 (1), pp.561-572.
9. Ribeiro, M.A., Fonseca, M.S.P. and de Santi, J., **2023**. Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks. Computers & Security, 134, p.103462.
10. Musa, N.S., Mirza, N.M., Rafique, S.H., Abdallah, A.M. and Murugan, T., **2024**. Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions. IEEE Access, 12, pp.17982-18011.
11. Hirsi, A., Alhartomi, M.A., Audah, L., Salh, A., bin Mad Sahar, N., Ahmed, S., Ansa, G.O. and Farah, A., **2025**. Comprehensive analysis of DDoS anomaly detection in software-defined networks. IEEE Access.
12. Moloja, D. and Malele Prof, V., **2025**. Software-Defined Networking powered by AI-driven Anomaly Detection. Journal of Cybersecurity Education, Research and Practice, 2025 (1), p.24.
13. Chuang, H.M., Liu, F. and Tsai, C.H., **2022**. Early Detection of Abnormal Attacks in Software-Defined Networking Using Machine Learning Approaches. Symmetry, 14 (6), p.1178.
14. Mansoor, A., Anbar, M., Bahashwan, A.A., Alabsi, B.A. and Rihan, S.D.A., **2023**. Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller. Systems, 11 (6), p.296.
15. Taheri, R., Ahmed, H. and Arslan, E., **2023**. Deep learning for the security of software-defined networks: a review. Cluster Computing, 26(5), pp.3089-3112.
16. Jafarian, T., Masdari, M., Ghaffari, A. and Majidzadeh, K., **2020**. Security anomaly detection in software-defined networking based on a prediction technique. International Journal of Communication Systems, 33 (14), p. e4524.
17. Ahmed, M.R., Shatabda, S., Islam, A.M. and Robin, M.T.I., **2021**. Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques—A Comprehensive Survey. Authorea Preprints.
18. Satheesh, N., Rathnamma, M.V., Rajeshkumar, G., Sagar, P.V., Dadheech, P., Dogiwal, S.R., Velayutham, P. and Sengan, S., **2020**. Flow-based anomaly intrusion detection using machine learning model with software defined networking for OpenFlow network. Microprocessors and Microsystems, 79, p.103285.
19. Khairi, M.H., Ariffin, S.H., Latiff, N.M., Abdullah, A.S. and Hassan, M.K., **2018**. A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN). Engineering, Technology & Applied Science Research, 8 (2).
20. Dogan, S.M., Alkan, M., Kocak, A., Kocak, A. and Alkan, M., **2025**. Detection and mitigation of cyber-attacks in software defined networks using machine learning/deep learning: a systematic literature review, research challenges and future directions. International Journal of Information Security, 24 (5), p.209.