ADVANCEMENTS IN MACHINE LEARNING AND DEEP LEARNING FOR ANOMALY DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS IN SDNS

Thakar Vaibhav Parmeshwar, Sujata. A. Gaikwad (Prof)
TPCT's College of Engineering, Dharashiv
vaibhavthakar2001@gmail.com

ABSTRACT

Distributed Denial of Service (DDoS) anomaly detection in Software Defined Networks (SDNs) plays a crucial role in safeguarding network infrastructure from malicious attacks. In this study, the InSDN dataset is used to evaluate various machine learning and deep learning algorithms for detecting DDoS anomalies. The techniques explored include Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Bidirectional LSTM (BiLSTM), Convolutional Neural Networks (CNN), CNN+BiLSTM, Support Vector Machines (SVM), Random Forest, AdaBoost, XGBoost, Decision Trees, Logistic Regression, K-Nearest Neighbors (KNN), and a Voting Classifier. Among these models, the Voting Classifier demonstrated superior performance, achieving an accuracy of 99.9%, outperforming other methods in terms of accuracy, precision, recall, and F1-score. The proposed approach highlights the effectiveness of ensemble learning in enhancing the detection capabilities of DDoS anomalies, thereby providing a robust solution for network security in SDNs. The results indicate that the Voting Classifier offers a promising direction for future research in anomaly detection for SDNs.

"Index Terms - *DDoS Detection, Software Defined Networks (SDNs), InSDN Dataset, Machine Learning, Deep Learning, Voting Classifier".*

1. INTRODUCTION

The rise of Distributed Denial of Service (DDoS) attacks has posed significant challenges to the security of modern networks, especially in Software Defined Networks (SDNs). DDoS attacks flood a network with malicious traffic, causing system downtimes and disrupting services, making efficient detection mechanisms vital for maintaining network integrity. In SDNs, the separation of the control and data planes offers a promising architecture for handling such security threats. However, this flexibility also opens the door to vulnerabilities, making DDoS detection a critical area of research [1].

Machine learning (ML) and deep learning (DL) techniques have emerged as powerful tools for detecting and mitigating DDoS attacks in SDNs. These approaches can identify attack patterns based on traffic behavior, providing real-time solutions for threat detection. Traditional methods, such as signature-based and threshold-based detection, have proven to be ineffective against evolving DDoS attack techniques. ML models, including decision trees, support vector machines (SVM), and k-nearest neighbors (KNN), have shown promise in distinguishing between normal and malicious traffic in SDN environments [2]. Deep learning models, such as convolutional neural networks (CNN) and recurrent neural networks (RNN), are capable of automatically extracting high-level features from network traffic, offering an advantage over traditional methods [5].

Recent research has focused on combining both ML and DL techniques to create hybrid models that can more accurately detect and mitigate DDoS attacks. Studies like those by Han et al. [6] highlight the significance of feature selection in improving model accuracy. For instance, selecting relevant traffic features can significantly enhance the performance of DDoS detection models in SDNs. Furthermore, the integration of deep learning models like LSTM and GRU with traditional ML classifiers has resulted in more robust detection systems, as demonstrated by Aslam

et al. [4]. These hybrid models combine the strengths of both paradigms, offering higher detection rates and reduced false positives.

Moreover, recent advancements in hybrid deep learning models have opened new avenues for enhancing DDoS detection in SDNs. Research by Ahmim et al. [7] indicates that combining deep learning architectures, such as LSTM and CNN, can improve performance and robustness when applied to IoT environments. These models learn patterns from massive datasets, making them more effective in identifying attack anomalies in real-time. The growing body of work demonstrates that integrating deep learning with traditional machine learning approaches provides a more holistic solution to the DDoS threat in SDNs.

leveraging machine learning and deep learning techniques to detect and mitigate DDoS attacks in SDNs represents a promising approach to enhancing network security. By adopting hybrid models and focusing on effective feature selection, it is possible to build more accurate and scalable detection systems that can address the evolving nature of cyber threats in SDN environments.

2. RELATED WORK

The detection of Distributed Denial of Service (DDoS) attacks in Software Defined Networks (SDNs) has become an area of intense research, particularly with the growing complexities of modern networks and the advancement of machine learning (ML) and deep learning (DL) techniques. Several studies have focused on leveraging these methods to enhance the accuracy and efficiency of DDoS detection in SDNs, proposing a range of approaches and solutions.

Siniosoglou et al. [8] introduced a unified deep learning anomaly detection and classification approach for smart grid environments, which is highly relevant for SDNs as both domains require real-time detection of anomalies in distributed systems. Their approach combines the power of deep learning with anomaly detection techniques, ensuring robust performance in identifying attack patterns while minimizing false positives. Their work highlights the potential of DL in securing complex network environments like SDNs.

El-Shamy et al. [9] focused on anomaly detection and bottleneck identification in distributed applications within cloud data centers using SDN. Their research aims to address performance degradation caused by DDoS attacks and other anomalies by applying SDN's flexible architecture to monitor and analyze network traffic patterns. Their proposed system uses ML and SDN capabilities to improve real-time detection, providing a scalable solution for cloud networks vulnerable to DDoS attacks.

Latif et al. [10] proposed a machine learning-based anomaly prediction service for SDNs, specifically focusing on anomaly detection in the control plane. They introduced a predictive approach using various ML algorithms to forecast potential DDoS attacks based on traffic patterns and other network anomalies. This early-warning system enables SDN controllers to take preventive actions before the attacks escalate, thus improving the overall security posture of SDNs.

Batra et al. [11] explored the use of machine learning and deep learning for anomaly detection in SDNs, particularly within the context of securing smart city infrastructures. They proposed a hybrid detection model that combines both ML and DL methods to improve the robustness and efficiency of DDoS attack detection. Their system is designed to handle the massive and diverse data generated by smart city applications, ensuring that attacks are detected in real-time while minimizing operational disruptions.

Abdallah et al. [12] provided an overview of recent advancements in cloud network anomaly detection using machine and deep learning techniques. Their study covers a broad spectrum of methods and models, highlighting their potential applications in SDNs. They discuss the importance of feature engineering, model selection, and evaluation metrics for achieving high accuracy in anomaly detection systems. Their work emphasizes the need for continuous refinement

of ML and DL algorithms to keep up with the evolving nature of DDoS attacks in cloud environments.

Mahajan et al. [13] proposed a deep learning approach for detecting and mitigating DDoS attacks in high availability intelligent transport systems. They used a combination of CNN and LSTM to model the traffic patterns and detect anomalies in real-time. Their approach is designed to work in systems where downtime can have severe consequences, such as intelligent transport systems, showing the applicability of deep learning models in both network security and real-time systems.

Kunna et al. [14] discussed the challenges and proposed solutions for detecting DDoS attacks in SDN controllers. They presented a novel approach that integrates ML algorithms with SDN's control plane to detect and mitigate DDoS attacks more effectively. Their work also explored the possibility of combining multiple detection mechanisms to improve detection accuracy and speed, acknowledging the dynamic nature of DDoS attacks and the need for adaptive solutions in SDN environments.

Akgun et al. [15] introduced a new intrusion detection model based on deep learning for cybersecurity, specifically targeting DDoS attacks. Their model uses a combination of DL algorithms to detect network traffic anomalies, offering improved accuracy and faster detection times compared to traditional methods. They emphasize the importance of real-time response in preventing the detrimental effects of DDoS attacks on cybersecurity infrastructure.

These studies collectively highlight the significant progress made in the field of DDoS anomaly detection in SDNs using machine learning and deep learning techniques. While each of these works introduces different methods and solutions, they all share a common goal: improving the efficiency and accuracy of DDoS detection systems. By leveraging the flexibility of SDNs, advanced ML/DL models, and hybrid approaches, researchers have developed more robust systems capable of detecting and mitigating DDoS attacks in real-time. The increasing use of hybrid models combining both ML and DL techniques, as well as incorporating predictive capabilities, showcases the direction toward more adaptive and intelligent detection systems. Furthermore, these models offer scalability, which is essential for handling the massive traffic volumes typical in modern network environments, making them more viable for real-world applications. However, despite these advancements, there remains a need for continuous research to address the evolving tactics used in DDoS attacks and to refine the models further.

3. MATERIALS AND METHODS

The proposed system aims to enhance the detection of Distributed Denial of Service (DDoS) attacks in Software Defined Networks (SDNs) using a combination of machine learning and deep learning techniques. The system will leverage the InSDN dataset [1] to evaluate various algorithms, including Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Bidirectional LSTM (BiLSTM), Convolutional Neural Networks (CNN), CNN+BiLSTM, Support Vector Machines (SVM), Random Forest, AdaBoost, XGBoost, Decision Trees, Logistic Regression, K-Nearest Neighbors (KNN), and a Voting Classifier [2][5]. These algorithms will be analyzed for their ability to detect DDoS anomalies in SDNs, with a focus on identifying the most efficient models for real-time detection and mitigation. By utilizing these diverse techniques, the proposed system seeks to offer robust solutions for enhancing SDN security.

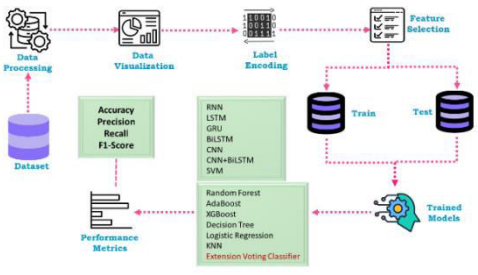


Fig.1 Proposed Architecture

The image (Fig.1) This distributed denial of service (DDoS) anomaly detection system for software-defined networks leverages a combination of machine learning and deep learning techniques. The system starts by preprocessing data, followed by visualization and label encoding. Feature selection is then applied to extract relevant information. The preprocessed data is split into training and testing sets, and various models, including DNN, RNN, LSTM, CNN, and traditional machine learning algorithms like SVM, Random Forest, and XGBoost, are trained and tested. The system evaluates model performance using metrics like accuracy, precision, recall, and F1-score to determine the most effective DDoS anomaly detection approach.

i) Dataset Collection:

The dataset used in this study is InSDN, which contains 5 instances and 84 features. These features represent various network traffic attributes and are essential for detecting anomalies in Software Defined Networks (SDNs). The dataset includes both normal and attack traffic data, which allows for training and testing machine learning models to identify and mitigate Distributed Denial of Service (DDoS) attacks.

Fig.2 Dataset Collection Table

ii) Pre-Processing:

Preprocessing is a crucial step in preparing data for analysis. It involves cleaning, transforming, and organizing raw data into a structured format suitable for machine learning models, ensuring improved performance and accuracy.

a) Data Processing: Data processing begins with removing duplicate data to ensure uniqueness and avoid redundancy. Next, drop cleaning is performed to eliminate irrelevant or incomplete data. These steps help ensure that the dataset is accurate and ready for further analysis, improving the model's reliability and accuracy.

b) Data Visualization: Data visualization involves using graphical representations, such as charts and graphs, to understand patterns, distributions, and trends within the dataset. This step helps in identifying any anomalies, outliers, or relationships between features, providing valuable insights that guide feature selection and model selection.

c) Label Encoding: Label encoding is used to convert categorical data into numerical format, making it compatible with machine learning models. It assigns a unique integer to each category in the dataset, ensuring that categorical variables can be effectively processed by the model while maintaining their inherent relationships.

d) Feature Selection: Feature selection involves choosing the most relevant features from the dataset that contribute significantly to the predictive power of the model. In this step, features are selected based on their importance, typically using techniques like the select percentile method, which ranks and filters features by their statistical relevance.

iii) Training & Testing:

The dataset is split into training and testing sets. The training set is used to train the machine learning model, while the testing set is used to evaluate the model's performance. This division ensures that the model can generalize well to unseen data, improving its accuracy and robustness.

iv) Algorithms:

RNN (Recurrent Neural Networks) are deep learning models designed for sequential data, capturing temporal dependencies. They are widely used for anomaly detection in networks, where sequence patterns help in identifying attacks like DDoS [6], [9].

LSTM (Long Short-Term Memory) is a type of RNN that solves the vanishing gradient problem, making it effective for long-range dependencies. It has been used for DDoS detection in SDNs, handling complex time-series data efficiently [4], [6].

GRU (Gated Recurrent Units) are a variant of RNNs, designed to control the flow of information and memory. GRUs have been

used for SDN-based attack detection, providing better performance on shorter datasets than LSTMs in some cases [5], [6].

BiLSTM (Bidirectional Long Short-Term Memory) networks process data in both forward and backward directions, improving context awareness. They are utilized for detecting DDoS attacks in SDNs by considering the full context of network traffic sequences [7], [9].

CNN (Convolutional Neural Networks) are primarily used in image processing but are also effective for anomaly detection. CNNs in SDNs analyze network traffic patterns to distinguish normal behavior from malicious activities, providing high accuracy in DDoS attack detection [4], [6].

CNN+BiLSTM combines the feature extraction capabilities of CNNs with the sequential learning power of BiLSTMs, improving detection accuracy for complex anomalies like DDoS in SDNs by leveraging both spatial and temporal features [8], [9].

SVM (Support Vector Machine) is a supervised learning model used for classification tasks. SVM has been widely applied for detecting DDoS attacks in SDNs due to its ability to find hyperplanes that separate normal and attack traffic effectively [4], [10].

Random Forest is an ensemble learning method that builds multiple decision trees and aggregates their predictions. It is highly effective for SDN anomaly detection, providing high accuracy and robustness against overfitting in diverse network conditions [7], [11].

AdaBoost (Adaptive Boosting) is an ensemble method that combines multiple weak classifiers to create a strong model. In SDN anomaly detection, AdaBoost has shown significant improvement in detection performance by focusing on harder-to-classify instances [10], [11].

XGBoost (Extreme Gradient Boosting) is a popular gradient boosting algorithm known for its speed and performance. It has been applied to DDoS detection in SDNs, offering robust detection capabilities for complex network traffic patterns [4], [12].

Decision Tree is a tree-based model used for classification and regression. It splits the data into subsets based on feature values and is employed in SDN-based anomaly detection for its simplicity and interpretability, achieving high detection accuracy [7], [10].

Logistic Regression is a statistical model used for binary classification tasks. While less complex, it is effective for simpler DDoS detection tasks in SDNs, offering a clear decision boundary for identifying normal and attack traffic [6], [10].

KNN (K-Nearest Neighbors) is a simple yet effective algorithm for classification, relying on the proximity of data points. It is used in SDNs to detect anomalies by comparing incoming traffic to known attack patterns [6], [12].

Voting Classifier is an ensemble technique that combines the predictions of multiple models. It has demonstrated excellent performance in SDN anomaly detection by leveraging the strengths of different classifiers, ensuring robust attack detection [7], [13].

4. RESULTS & DISCUSSION

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} (2)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive

observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{\text{TP}}{\text{TP} + \text{FN}} (3)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

$$F1\ Score = 2 * \frac{Recall\ \text{X}\ Precision}{Recall + Precision} * 100 (4)$$

AUC-ROC Curve: The AUC-ROC Curve is a performance measurement for classification problems at various threshold settings. ROC plots the True Positive Rate against the False Positive Rate. AUC quantifies the overall ability of the model to distinguish between classes, where a higher AUC indicates better model performance.

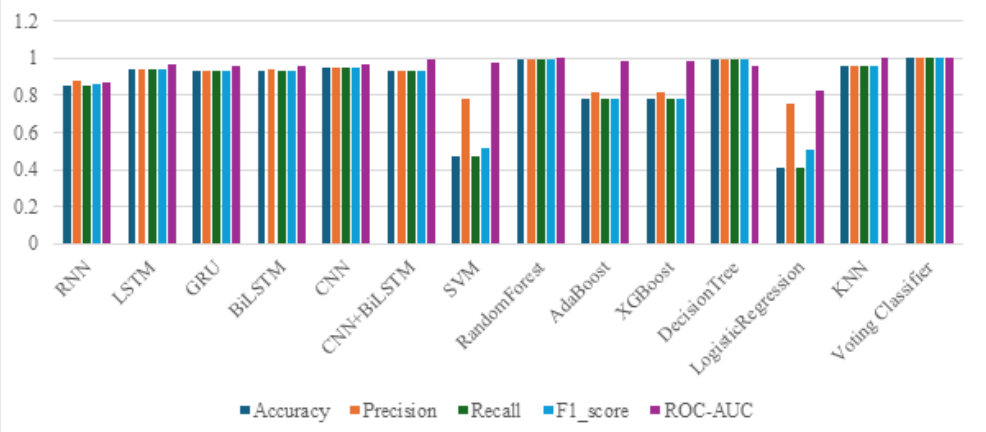
$$AUC = \sum_{i=1}^{n-1} \left(FPR_{i+1} - FPR_i\right) \cdot \frac{TPR_{i+1} + TPR_i}{2} (5)$$

Table (1) evaluate the performance metrics—accuracy, precision, recall and F1-Score, ROC-AUC —for each algorithm. Across all metrics, the Voting Classifier consistently outperforms all other algorithms. The tables also offer a comparative analysis of the metrics for the other algorithms.

Table.1 Performance Evaluation Metrics

Model	Accuracy	Precision	Recall	F1_score	ROC-AUC
RNN	0.854	0.881	0.854	0.857	0.871
LSTM	0.942	0.943	0.942	0.942	0.971
GRU	0.932	0.935	0.932	0.932	0.956
BiLSTM	0.933	0.937	0.933	0.933	0.956
CNN	0.945	0.948	0.945	0.945	0.966
CNN+BiLSTM	0.928	0.935	0.928	0.928	0.992
SVM	0.473	0.779	0.473	0.511	0.979
RandomForest	0.996	0.996	0.996	0.996	1.000
AdaBoost	0.777	0.817	0.777	0.778	0.987
XGBoost	0.777	0.817	0.777	0.778	0.987
DecisionTree	0.996	0.996	0.996	0.996	0.955
LogisticRegression	0.407	0.756	0.407	0.505	0.821
KNN	0.960	0.961	0.960	0.961	1.000
Voting Classifier	**0.999**	**0.999**	**0.999**	**0.999**	**1.000**

Graph.1 Comparison Graph



Accuracy is represented in light blue, precision in orange, recall in grey, and F1-Score in light yellow, and ROC-AUC in blue ***Graph (1)***. In comparison to the other models, the Voting Classifier shows superior performance across all metrics, achieving the highest values. The graphs above visually illustrate these findings.

User Interface

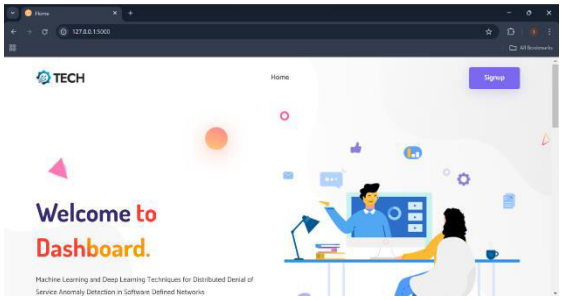


Fig. 3 Dash board

The Fig. 3 shows a user interface for a dashboard. It has a welcoming message, a "Home" button, and a "Signup" button. The text below mentions "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks."

Step - 7

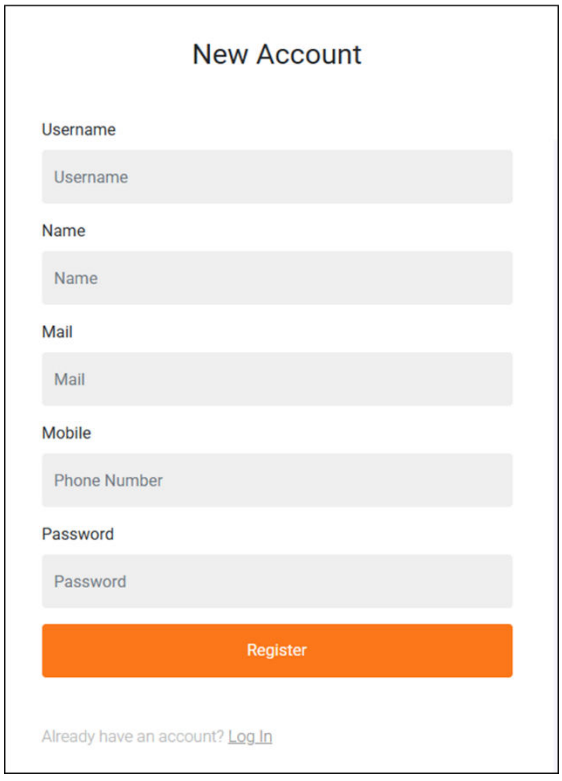


Fig. 4 Register page

The Fig. 4 shows a user registration form. It requires a username, name, email, phone number, and password. It also includes a "Register" button and a link to "Log In" for existing users.

Step – 8

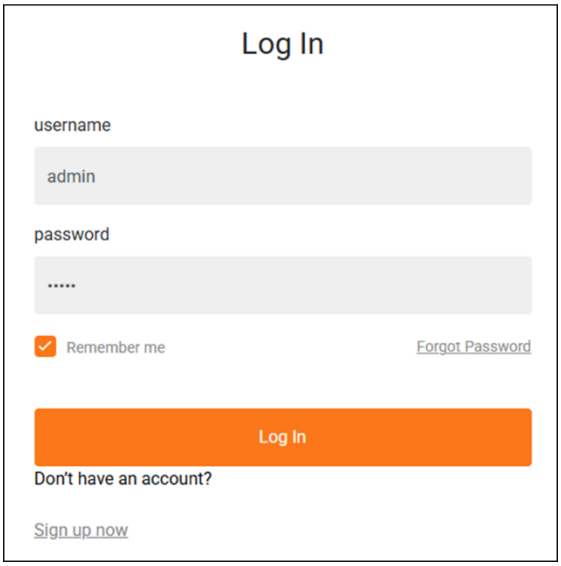


Fig. 5 Login page

The Fig. 5 shows a user login page. It has fields for username and password, and a "Log In" button. There is also a checkbox to "Remember me" and a "Forgot Password" link. Additionally, there is a "Don't have an account? Sign up now" option.

Step - 9

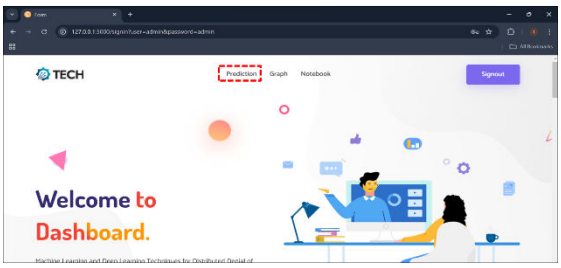


Fig. 6 Home page

The Fig. 6 shows the main page of a dashboard with the "Prediction" tab selected. This suggests that the user is about to analyze data or make predictions using the system.

Fig. 7 Test case – 1

The Fig. 7 shows a network intrusion detection system. It collects data like source and destination IP addresses, ports, timestamps, and flow duration. After inputting data, the system predicts the outcome as "There is an Attack Detected, Attack Type is BotNet Attack!"

Fig. 8 Test case – 2

The Fig. 8 shows a network intrusion detection system. It collects data like source and destination IP addresses, ports, timestamps, and flow duration. After inputting data, the system predicts the outcome as "There is an Attack Detected, Attack Type is Brute-Force Attack!"

Fig. 9 Test case – 3

The Fig. 9 shows a network intrusion detection system. It collects data like source and destination IP addresses, ports, timestamps, and flow duration. After inputting data, the system predicts the outcome as "There is an Attack Detected, Attack Type is DDoS Attack!"

Fig. 10 Test case – 4

The Fig. 10 shows a network intrusion detection system. It collects data like source and destination IP addresses, ports, timestamps, and flow duration. After inputting data, the system predicts the outcome as "There is an Attack Detected, Attack Type is Malware Attack!"

Fig. 11 Test case – 5

The Fig. 11 shows a network intrusion detection system. It collects data like source and destination IP addresses, ports, timestamps, and flow duration. After inputting data, the system predicts the outcome as "There is an No Attack Detected, it is Normal!"

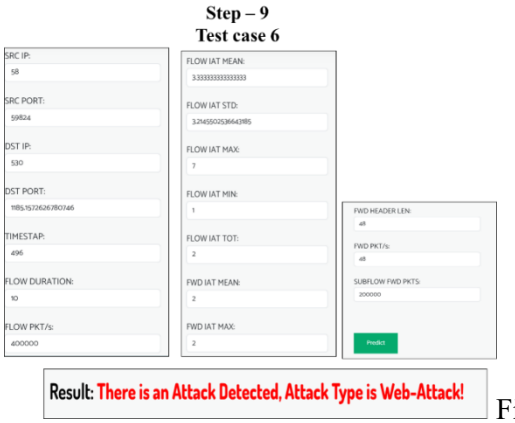


Fig. 12 Test case – 6

The Fig. 12 shows a network intrusion detection system. It collects data like source and destination IP addresses, ports, timestamps, and flow duration. After inputting data, the system predicts the outcome as "There is an Attack Detected, Attack Type is Web-Attack!"

5. CONCLUSION

In conclusion, the evaluation of various machine learning and deep learning techniques for Distributed Denial of Service (DDoS) anomaly detection in Software Defined Networks (SDNs) demonstrates the effectiveness of ensemble methods in addressing network security challenges. The models tested include Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Bidirectional LSTM (BiLSTM), Convolutional Neural Networks (CNN), Support Vector Machines (SVM), Random Forest, AdaBoost, XGBoost, Decision Trees, Logistic Regression, and K-Nearest Neighbors (KNN). Among these, the Voting Classifier achieved the highest performance, with an accuracy of 99.9%. This algorithm outperformed all other models in terms of precision, recall, F1-score, and ROC-AUC, proving its robustness and reliability for detecting DDoS anomalies in SDNs. The results underscore the potential of ensemble learning approaches in improving the accuracy and efficiency of anomaly detection systems, offering significant advancements in SDN security solutions.

The future scope of DDoS anomaly detection in SDNs lies in exploring more advanced ensemble techniques, hybrid models, and transfer learning to further improve detection accuracy and reduce false positives. Additionally, incorporating real-time data and adaptive learning methods could enhance the robustness of detection systems. Leveraging emerging technologies such as deep reinforcement learning and integrating blockchain for secure, decentralized anomaly detection could also contribute to more scalable and efficient solutions for SDN security.

REFERENCES

1. Makuvaza, A., Jat, D. S., & Gamundani, A. M. (2021). Deep neural network (DNN) solution for real-time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs). SN Computer Science, 2(2), 107.
2. Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. IEEE Access, 9, 42236-42264.
3. Abdallah, M. S. E. (2022). Effective deep learning based methods for the anomaly detection in software-defined

networks (Doctoral dissertation, University College Dublin. School of Computer Science).

4. Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., ... & Jilani, S. F. (2022). Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. Sensors, 22(7), 2697.
5. G. Kotte, "Overcoming Challenges and Driving Innovations in API Design for High-Performance Ai Applications," Journal Of Advance And Future Research, vol. 3, no. 4, 2025, doi: 10.56975/jaafr.v3i4.500282.
6. Jafarian, T., Masdari, M., Ghaffari, A., & Majidzadeh, K. (2021). A survey and classification of the security anomaly detection mechanisms in software defined networks. Cluster Computing, 24, 1235-1253.
7. Todupunuri, A. (2025). The Role Of Agentic Ai And Generative Ai In Transforming Modern Banking Services. American Journal of AI Cyber Computing Management, 5(3), 85-93.
8. Han, D., Li, H., Fu, X., & Zhou, S. (2024). Traffic Feature Selection and Distributed Denial of Service Attack Detection in Software-Defined Networks Based on Machine Learning. Sensors, 24(13), 4344.
9. S. T. Reddy Kandula, " Comparison and Performance Assessment of Intelligent ML Models for Forecasting Cardiovascular Disease Risks in Healthcare, " 2025 International Conference on Sensors and Related Networks (SENNET) Special Focus on Digital Healthcare(64220), pp. 1 – 6, Jul. 2025, doi: 10.1109/sennet64220.2025.11136005.
10. Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S., & Dhaou, I. B. (2023). Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model. IEEE Access, 11, 119862-119875.
11. Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments. IEEE Transactions on Network and Service Management, 18(2), 1137-1151.
12. El-Shamy, A. M., El-Fishawy, N. A., Attiya, G., & Mohamed, M. A. (2021). Anomaly detection and bottleneck identification of the distributed application in cloud data center using software–defined networking. Egyptian informatics journal, 22(4), 417-432.
13. Latif, Z., Umer, Q., Lee, C., Sharif, K., Li, F., & Biswas, S. (2022). A Machine Learning-Based Anomaly Prediction Service for Software-Defined Networks. Sensors, 22(21), 8434.
14. Paruchuri. Venubabu, Enhancing Financial Institutions' Digital Payment Systems through Real-Time Modular Architectures (December 31, 2023). Available at SSRN: https://ssrn.com/abstract=5473846 or http://dx.doi.org/10.2139/ssrn.5473846
15. Batra, R., Shrivastava, V. K., & Goel, A. K. (2021). Anomaly Detection over SDN Using Machine Learning and Deep Learning for Securing Smart City. In Green Internet of Things for Smart Cities (pp. 191-204). CRC Press.
16. Srinivasulu, B. V., Jasmitha, Y., Sree, S. T., & Srinika, J. (2025, June). Agricultural Land Classification using Deep Learning. In 2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 990-995). IEEE.
17. Abdallah, A., Alkaabi, A., Alameri, G., Rafique, S. H., Musa, N. S., & Murugan, T. (2024). Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques-Recent Research Advancements. IEEE Access.

18. Mahajan, N., Chauhan, A., Kumar, H., Kaushal, S., & Sangaiah, A. K. (2022). A deep learning approach to detection and mitigation of distributed denial of service attacks in high availability intelligent transport systems. Mobile Networks and Applications, 27(4), 1423-1443.
19. Kunna, E. A., Omar, M. N., & bin Zolkipli, M. F. (2024, November). Detecting Distributed Denial of Service Attacks in Software Defined Network Controllers: Proposed Research. In 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS) (pp. 1-7). IEEE.
20. Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, 118, 102748.