IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI-Enable DDoS Anomaly Detection in Software Defined Networks Using Machine Learning Models.

[1] Malini P [2] Dr. Murthy S V N

M Tech Scholar Associate Professor

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

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 CICIDS dataset is employed to assess the performance of different machine learning and deep learning techniques in identifying DDoS-related anomalies.The techniques explored include The research incorporates time-dependent neural architectures, notably Recurrent Neural Networks, Long Short-Term Memory models, and Gated Recurrent Units.Bidirectional LSTM (BiLSTM), Convolutional Neural Networks (CNN), CNN+BiLSTM, Support **Vector** Machines (SVM), Random Forest, AdaBoost, XGBoost, Decision Trees, Logistic Regression, KNearest Neighbors (KNN), and a Voting Classifier. Among Among the evaluated models, the Voting Classifier achieved the best results, delivering higher accuracy and surpassing other techniques in precision, recall, and F1-score. The findings emphasize the strength of ensemble learning in improving DDoS anomaly detection., thereby providing a robust solution for network security in SDNs. The findings suggest that the Voting Classifier represents a strong candidate for future investigations in SDN-based anomaly detection.

Index terms: distributed denial of service, Anomaly detection, software defined networks, deep leaning, machine learning, CICIDS dataset, voting classifier.

I. INTRODUCTION

The emergence of Software Defined Networking (SDN) has reshaped the way networks are designed and managed. Unlike conventional architectures that bind control and data planes together, SDN separates them, enabling a programmable and centralized control plane. This flexibility improves network scalability and management but simultaneously creates new security vulnerabilities, particularly against large-scale cyber threats. One of the most significant security threats is the Distributed Denial-of-Service (DDoS) attack.where malicious traffic overwhelms network resources, rendering services unavailable. This project addresses the security gaps in SDN by proposing an automated detection and mitigation framework. The system processes live traffic data through multiple stages, including anomaly recognition and response mechanisms, To reduce the severity of active attacks, the framework integrates detection and mitigation components within the SDN controller, enabling real-time interaction and rapid decision execution.Traditional methods of safeguarding SDN, such as rule-based or signature-driven approaches, remain ineffective in addressing the constantly evolving nature associated with DDoS-based attacks. Attackers change their strategies frequently, making static detection mechanisms less effective in real environments. To overcome this limitation, The incorporation of Machine Learning (ML) and Deep Learning (DL) techniques within Software-Defined Networking (SDN) provides a more flexible and adaptive security solution.. These models can study network flows at scale, recognize unusual traffic patterns, and automatically trigger countermeasures. By taking advantage of the

centralized view of the SDN controller, learning-based systems are able to improve detection accuracy, shorten response times, and provide a scalable framework for protecting against sophisticated attacks.

Reports from industry leaders such as CISCO highlight the urgency of such solutions. Their research indicates that DDoS attacks pose a significant threat.are not only increasing in frequency but also growing in size and impact. The number of global incidents is expected to rise sharply from 7.9 million in 2018 to over 15 million by 2023This accelerated expansion, together with the financial and operational consequences associated with such attacks, highlights the necessity for AI-driven security frameworks that can be integrated into SDN architectures to provide robust, real-time defense mechanisms.Software-Defined Networking (SDN) adopts an architecture that decouples the control logic from the forwarding mechanisms, as illustrated in Figure 1. The framework is structured into three primary layers: the application plane, control plane, and data plane. Network devices such as switches and routers reside in the data plane, where packet forwarding operations are executed under the guidance of the control plane. Communication between these devices and the controller occurs through a southbound interface.

The control plane hosts the SDN controller, which functions as the central intelligence of the network, overseeing and coordinating the behavior of data-plane devices. The application plane contains various SDN applications that define user-specific networking requirements. These applications interact with the controller via a northbound interface, enabling programmable specification of desired network policies and behaviors. By maintaining a global view of the network topology, the controller simplifies traffic management by shifting complex decision-making away from individual switches and routers. This architectural separation enhances scalability, flexibility, and programmability, while also improving traffic control and resource-utilization efficiency. Despite these advantages, ensuring robust network security remains a significant challenge in SDN environments.

.

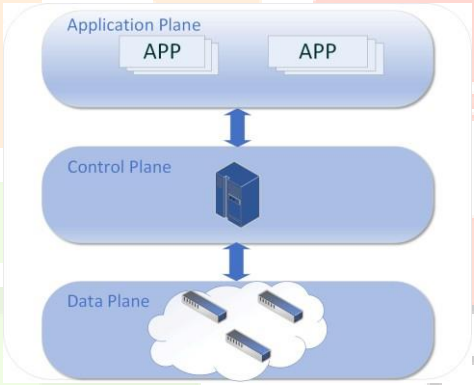


Figure 1: SDN architecture.

Moreover, adversaries are adopting increasingly advanced attack strategies, which significantly complicates the detection and mitigation of DDoS attacks. When the SDN controller is targeted, it becomes unable to process incoming requests, potentially leading to network-wide service disruption. Alternatively, attacks directed at the data plane generate excessive volumes of illegitimate traffic, exhausting available bandwidth and computational resources.

This abnormal traffic interferes with the forwarding of legitimate packets and triggers the SDN controller to install redundant flow rules on switches, thereby consuming limited flow-table memory and further overloading the data plane. As a result, the efficient identification and suppression of DDoS attacks has become a major focus of research in SDN-based networks.

II. Related Work

Numerous research works have proposed ML-based approaches for DDoS detection in SDN. Shafiq et al. (2020) explored Random Forest and SVM classifiers for flow-based intrusion detection. Nguyen et al. (2019) Their findings confirmed that applying feature selection techniques enhances detection performance. More recent studies have increasingly adopted deep learning approaches, where models such as CNN and LSTM have reported superior accuracy on benchmark datasets like CICDDoS2019.Hybrid approaches combining ML and DL methods have also gained traction, enabling adaptive learning and reduced false positives. However, most existing systems lack real-time adaptability and struggle with feature scalability in large SDN environments.

This study employs the CSE-CIC-IDS2018 dataset to conduct comprehensive intrusion detection experiments. Given the presence of redundant and repetitive records within large-scale network traffic data, significant emphasis is placed on data preprocessing and optimization. Furthermore, a range of deep learning architectures, including DNN, CNN, RNN, LSTM, hybrid CNN–RNN, and CNN–LSTM models, are implemented to identify malicious network activities. Both binary and multi-class classification frameworks are utilized to distinguish between benign traffic and various types of cyberattacks. The key contributions of this work are outlined as follows.

This study introduces a proposed framework that improves the detection of Distributed Denial-of-Service (DDoS) attacks within Software-Defined Networks (SDNs), by combining Machine Learning (ML) as well as Deep Learning (DL) approaches are employed in this study. For performance evaluation, experiments are conducted using the InSDN dataset across a diverse set of models such as Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Bidirectional LSTM (BiLSTM), Convolutional Neural Networks (CNN), as well as hybrid CNN–BiLSTM architectures. In addition, several traditional machine learning classifiers—namely Support Vector Machine (SVM), Random Forest, AdaBoost, such as XGBoost, Decision Trees, and Logistic Regression models, K-Nearest Neighbor (KNN), and a Voting-based ensemble classifier—are implemented for comparative analysis.Each of these models is assessed for their effectiveness in identifying abnormal traffic associated with DDoS activities in SDN environments. By combining different algorithms, the system provides a more comprehensive and reliable detection mechanism. This integrated approach aims to deliver high accuracy, real-time adaptability, and stronger resilience, ensuring that SDN infrastructures are better protected from evolving DDoS threats.

This work integrates both Machine Learning (ML) and Deep Learning (DL) methods aimed at improving detection accuracy and system adaptability. Such integration allows the framework to identify diverse attack patterns and reinforces the overall security posture of Software-Defined Networks (SDNs). By leveraging multiple models, including RNN, LSTM, GRU, BiLSTM, and CNN, the system effectively learns temporal relationships and spatial characteristics present in network traffic data, enabling accurate detection of complex and sophisticated DDoS attack behaviors.

The utilization of the InSDN dataset facilitates evaluation under realistic network conditions, offering detailed insight into the effectiveness of each algorithm within SDN environments and ensuring resilience against emerging and evolving threats. Furthermore, the adoption of ensemble methods encompassing Voting Classifiers enhances classification reliability by aggregatingthe capabilities of each model resulting in improved generalization, robustness, and real-time detection performance, even in the presence of dynamic traffic patterns and varying attack profiles.

This paper aims to enhance the security of Software Defined Networks (SDNs) by developing an intelligent framework capable of accurately detect and respond to Detection of Distributed Denial-of-Service (DDoS) attacks using Machine Learning as well as Deep Learning techniques.The framework is designed for real-time operation, with both detection and mitigation modules embedded in the SDN controller to ensure centralized monitoring and quick response against malicious traffic. The system is built for real-time operation, embedding both detection and mitigation components within the SDN controller to enable centralized oversight and quick reaction times. The approach employs a veriety of models, such as RNN, LSTM, GRU, and CNN.and ensemble techniques like the Voting Classifier, to enhance detection performance and adapt to constantly evolving cyber threats. The scope extends to handling and preprocessing network traffic from the InSDN dataset, training multiple learning models, assessing their outcomes, and deploying a user-friendly web interface for user interaction. This system is applicable across several domains such as enterprise networks, cloud computing platforms, and telecom infrastructures utilizing SDN technology. It can aid Internet Service Providers (ISPs), cloud providers, and data centers in identifying and preventing DDoS attacks before they degrade system performance. Furthermore, the proposed framework acts as a foundation for future research in AI-powered network security, offering value to both academic research and industrial deployment.

With the widespread adoption of the internet and the escalating frequency of cyberattacks, Deep learning methods have seen growing adoption in network security for improving the identification of advanced and emerging attacks. These architectures utilize multiple layers of nonlinear transformations to automatically extract and interpret features from raw input data. By operating on large-scale datasets, multilayer networks are able to capture intricate patterns, thereby enhancing the accuracy and reliability of detection results.A review of the current deep learning methods in this domain is presented below, with a summary provided in Table 1..

Table 1. Summary of recent approaches.

Table 1. Summary of recent approaches.

Paper	Year	Dataset	Methods	Classification	Accuracy
[9]	2019	CSE-CIC-IDS2018	LSTM + AM	Multi-class	96.19%
[10]	2019	NSLKDD	Improved CNN	Multi-class	95.36%
[11]	2019	CSE-CIC-IDS2018	LSTM	Multi-class	96%
[12]	2020	CSE-CIC-IDS2018	Adaboost	Multi-class	99.69%
[5]	2020	CSE-CIC-IDS2018	DNN, RNN, CNN	Multi-class	97.28%, 97.31%, 97.38%
[13]	2020	NSLKDD	ADASYN + CNN	Multi-class	80.08%
[14]	2020	NSL-KDD UNSW-NB15	CNN + BiLSTM	Multi-class	83.58% 77.16%
[15]	2020	KDD99	LSTM	Binary	98.94%
[16]	2020	CSE-CIC-IDS2017	LSTM + CNN	Multi-class	98.60%
[17]	2021	KDD99 CSE-CIC-IDS2018	TCN + LSTM	Multi-class	92.05% 97.77%
[6]	2021	KDD99 CSE-CIC-IDS2018	TCN + LSTM	Multi-class	92% 97%
[18]	2021	NSLKDD	BiLSTM	Binary Multi-class	94.26% 91.36%
[19]	2021	KDD99	LSTM	Binary	98.88%
[20]	2022	Collected data	CNN + LSTM	Multi-class	97.30%
[21]	2022	NSLKDD	DSN	Multi-class	86.80%

In Ref. [9], Xiao et al. employed CNNs are utilized in IDS to learn and extract relevant features from input data from dimensionally reduced data. Ref. [10] introduced an improved CNN-based method for detecting intrusions in wireless networks. In Ref. [11], Lin et al. proposed a hybrid LSTM with attention mechanism (AM) model to enhance network recognition capabilities. The LSTM model, with its inherent memory features, captures historical network traffic, and within a hierarchical neural network, it effectively integrates current input with previously learned features to improve classification performance. The core principle of deep learning emulates the functioning of the human neural system, where the LSTM structure mirrors memory retention, and the attention mechanism resembles cognitive attention processes.

In Ref. [12], Karatas et al. utilized the CSE-CIC-IDS2018 dataset and evaluated six machine learning algorithms: AdaBoost, Decision Tree (DT), Random Forest (RF), K-Nearest Neighbor (KNN), Gradient Boosting (GB), and Linear Discriminant Analysis (LDA). To address imbalanced attack classes, the Synthetic Minority Oversampling Technique (SMOTE) was applied to generate additional samples, enhancing detection efficiency for underrepresented attacks.

Ref. [5] by Ferrag et al. analyzed seven deep learning approaches—DNN, RNN, CNN, Restricted Boltzmann Machine (RBM), Deep Belief Network (DBN), Deep Boltzmann Machine (DBM), and Deep Autoencoder (DAE)—using the Bot-IoT and CSE-CIC-IDS2018 datasets. In Ref. [13], Hu et al. combined CNN integrated with the ADASYN oversampling technique(ADASYN) to strengthen IDS performance. Ref. [14] by Jiang et al. integrated hybrid sampling with CNN and BiLSTM for network intrusion detection, while in Ref. [15], Jiang et al. applied LSTM-RNN in a multichannel attack detection system, proposing an end-to-end framework covering data preparation, feature engineering, model training, and detection. Finally, Ref. [16] presents a security protection platform designed for the control plane of Software-Defined Networks (SDNs).

They utilize LSTM and CNN models *to develop a high-performance and adaptive intrusion detection system (IDS)*. In Ref. [17], Kim et al. employed the KDD99 and CSE-CIC-IDS2018 datasets, which include multiple attack types; however, hey concentrated particularly on Denial-of-Service (DoS) attacks. These attack samples were comparable in number to other attack categories, providing sufficient data to train and evaluate the proposed CNN architecture. The convolutional layer is particularly effective in extracting critical features from large datasets. To leverage the image recognition capabilities of CNNs, the authors transformed feature vectors into image representations.

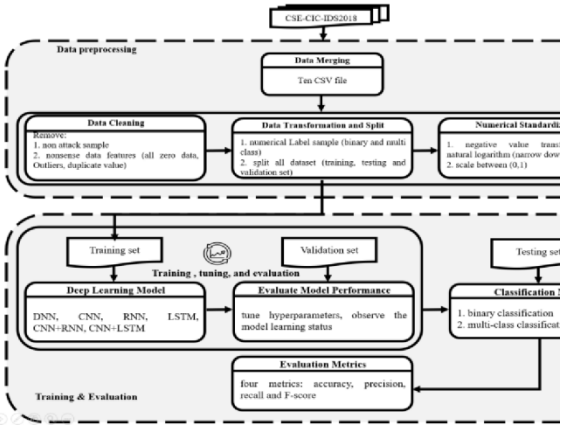
In Ref. [6], Mezina et al. used the KDD99 and CSE-CIC-IDS2018 datasets and applied U-Net and Temporal Convolutional Networks (TCN) for network attack detection. They combined TCN with LSTM, achieving higher accuracy; the TCN handles time-series data by using dilated convolutions, which extend the receptive field of the network.

Ref. [18] by Imrana et al. proposed a Bidirectional Deep LSTM (BiDLSTM) for IDS, targeting User-to-Root (U2R) and Remote-to-Local (R2L) attacks, and demonstrated improved accuracy compared to standard LSTM. In Ref. [19], the researchers employed Principal Component Analysis (PCA) along with Mutual Information to reduce dimensionality and feature selection, followed by LSTM for attack detection.

In Ref. [20], CNN and CNN-LSTM models were applied to secure autonomous vehicle networks against spoofing, flooding, replay attacks, and benign traffic, using a real-world dataset for training and evaluation. Ref. [21] by Tang et al. also contributed to this body of research.

III. Methodology

The methodology of the architecture of the proposed network intrusion detection model is presented in Figure



The quality of these predictions is strongly influenced by the volume and diversity of the training dataset. Since ML operates on large -scale data, it is able to extract patterns and insights with minimal manual involvement. Adaptive ML models further enha nce this process by improving their accuracy as mor e data becomes DDoS Anomaly Detection in Software Defined Networks Using ML and DL available. The diagram below depicts the overall flow of data handling in Machine Learning before generating predictions.

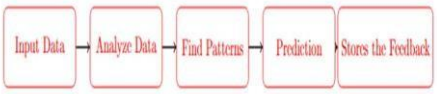


Figure 4 : Machine Learning Works.

2, which is divided into two primary sections: data preprocessing and training & evaluation.
Figure 2: Methodology diagram.

i. MACHINE LEARNING:

Artificial Intelligence (AI) includes the domain of Machine Learning (ML), which focuses on enabling systems to learn patterns from data and build predictive models. The main objective of ML is to process structured information and transform it into models that can be interpreted and applied by humans. It is considered one of the most fascinating technologies in computer science, with wide-ranging applications across industries..

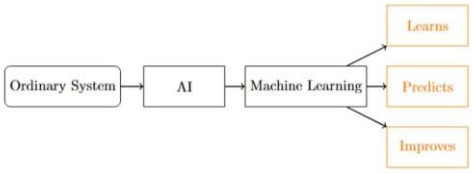


Figure 3: Overview of Machine Learning.

Machine Learning is a branch of study that enables computers to improve their performance By inferring behavior from data instead of following manually programmed directives.As the term suggests, it allows systems to gain knowledge and adapt automatically. Today, ML is already applied in numerous domains, and its usage is anticipated to expand further in the future. Falling under Artificial Intelligence, Machine Learning differs from classical computing methods by emphasizing data-driven learning.since it focuses on adaptability and pattern recognition instead of rigid rule-based programming.

• HOW MACHINE LEARNING WORKS:

Machine Learning models function by analyzing previous data and building predictive frameworks. Each time new input is supplied, the system generates an output based on the trends it has already captured.

- MACHINE LEARNING TECHNIQUES:

1. Classification – A method where a computer program learns from the input data supplied to it. It can categorize unseen observations, forecast discrete outcomes, and estimate qualitative target values.
2. Categorization – A technique to organize information into categories for the most productive and successful use.
3. Clustering – A technique for assembling a collection of items based on similarity and dissimilarity between them.
4. Anomaly Detection – A technique to identify instances that are unique within the data. It solves intrusions by indicating a presence of intended or unintended induced attacks, defects, or faults.
5. Visualization – A process to display information in pictorial format. It allows decision-makers to see analytics presented visually whenDisplayed as a representative case of apicture, making it easier to

understand. 6. Decision Making – A technique or skill that provides the ability to influence managerial decisionmaking using data as evidence.

Two major classification schemes exist for machine learning algorithms:
1. By learning style – How the model learns.
2. By structural similarity – The resemblance in structure or function.

• TYPES OF MACHINE LEARNING:

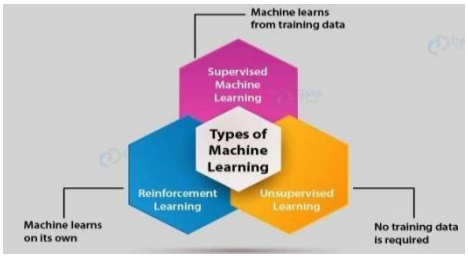


Figure 5: Types of Machine Learning.

Machine learning can be categorized into three types:

1. Supervised Learning – The model learns from labelled training data.
2. Unsupervised Learning – The model identifies patterns in unlabelled data.
3. Reinforcement Learning – The model learns by interacting with an environment.

• Implementation Areas of Machine Learning models

The proposed machine learning techniques consist of used in various applications such as: ✓ Vision processing
 Language processing
 Forecasting things like stock market trends,
weather ✓ Pattern recognition
 Games
 Data mining
 Expert systems

ii. DEEP LEARNING:

Deep Learning is an advanced technique within Artificial Intelligence (AI) that mimics The method by which the human neural system assimilates information from experience. In this approach, representations are developed through a structured training process. To enable a system to identify objects, it is first trained on large sets of labeled images that belong to different categories. elative to classical Machine Learning, deep learning architectures typically involve higher data requirements and extended computation durations.Identifying distinct features for object or character recognition is a challenging and time-intensive task. Whereas classical methods depend on engineered features, deep learning models autonomously identify important data patterns from the original dataset.Neural networks that incorporate multiple hidden layers are classified as deep neural networks.. Such architectures gradually build complex representations from simpler ones. For example, when an image is processed, the network initially detects basic attributes such as lines, edges, and corners. As the information progresses through deeper layers, the system learns to combine these simple attributes into more complex shapes, eventually recognizing objects such as faces, letters, or other detailed structures. In essence, each successive layer captures higher-level features. Deep learning techniques have excelled in computer vision tasks, with facial recognition and image classification among the most influential applications.

• DEEP LEARNING FOR DDOS DETECTION IN SDN

Several intrinsic benefits of Deep Learning contribute to its superior performance over traditional ML methods for identifying anomalies in Software-Defined Networks:

1. Ability to Learn Complex Patterns

 Traditional ML algorithms rely heavily on handcrafted features chosen by experts.

 Unlike traditional methods, Deep Learning models derive features directly from raw traffic data, which minimizes human intervention and uncovers hidden relationships among attributes such as packet size, flow duration, and transmission frequency.

2. Handling High-Dimensional Data

 Modern network traffic datasets (e.g., CICIDS2017, NSL-KDD) contain dozens to hundreds of features.

 DL architectures such as CNNs and LSTMs handle high-dimensional inputs efficiently, uncovering patterns that may remain invisible to shallow ML models.

3. Temporal Awareness

 Many DDoS attacks are time-dependent, where abnormal traffic builds up gradually.

 RNN, LSTM, GRU, and BiLSTM can model sequential dependencies, capturing both short-term spikes (e.g., UDP floods) and long-term patterns (e.g., slow DoS attacks).

4. Better Generalization to New Attacks

 Attackers often modify packet headers or vary attack strategies to evade detection.

 Since DL learns non-linear relationships, it can detect novel attack variants better than rule-based or linear ML classifiers.

5. Integration with SDN Controllers ✓ In SDN, the controller has a global view of the network.

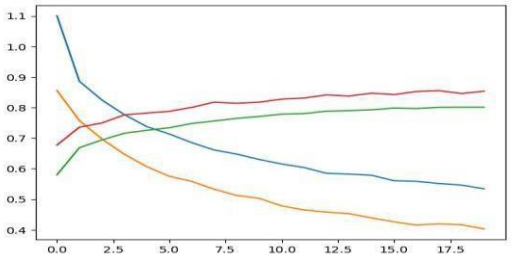
✓ DL models can be integrated into controllers to process real-time traffic statistics, allowing instant anomaly detection and mitigation (e.g., blocking malicious flows by updating flow tables).

iii. CYBER SECURITY:

Cyber security involves safeguarding networks, applications, sensitive data, and users from unauthorized access or malicious cyber threats. These threats often come in the form of cyber attacks deliberate actions by individuals or groups aiming to infiltrate systems,Leveraging Machine Learning and Deep Learning for DDoS Anomaly Detection in Software-Defined Networksdisrupt services, steal information, or cause broader damage. Some of the most prevalent forms of cyber attacks include phishing, malware (such as ransomware), social engineering techniques, and denial-of-service (DoS) as well as distributed denial-of-service (DDoS) attacks.

iv. DATA SET:

The dataset leveraged in the current study is the NSL-KDD intrusion detection dataset, which serves as an enhanced variant of the well-known KDD'99 dataset. It includes records of both legitimate and malicious network traffic, each labeled for use in supervised learning models. In total, the dataset provides 41 attributes, which are grouped as: basic features (e.g., connection duration, protocol type, service), content-related features (e.g., number of unsuccessful login attempts), and traffic-based features (e.g., total connections directed to the same host). The malicious activities are classified into four broad categories: The categories considered include Denial-of-Service (DoS), Probe, User-to-Root (U2R), and Remote-to-Local (R2L) attacks. For evaluating the model, the dataset is divided into training and testing subsets. As part of preprocessing, irrelevant fields such as num_outbound_cmds were discarded, categorical attributes (e.g., protocol and service) were converted into numerical form, and continuous values were normalized.



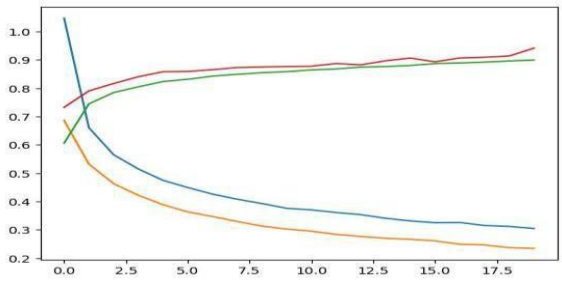
v. RNN (Recurrent Neural Network):

Recurrent Neural Networks (RNNs) are designed for analyzing sequential information. Unlike conventional feed-forward networks, they incorporate loops that allow past information to be retained across multiple time steps. For DDoS detection in SDN environments, traffic streams can be interpreted as sequences of packets received over time. RNNs handle each packet's attributes (such as duration, number of bytes, and flags) step by step, while the hidden state preserves contextual knowledge of earlier traffic. This ability makes RNNs suitable for spotting timedependent irregularities, such as abrupt surges in traffic or recurring attack behaviors. Nevertheless, basic RNNs encounter challenges in capturing longterm dependencies due to the vanishing gradient issue, which is why enhanced architectures like LSTM and GRU are generally employed.

vi. LSTM (Long Short-Term Memory):

LSTMs are an advanced form of RNNs that solve the vanishing gradient problem by introducing a memory cell and gating mechanisms (input, output, and forget gates). These gates regulate how much past information is stored, forgotten, or passed to the next time step. In SDN anomaly detection, this means that LSTM can remember important patterns across long sequences of traffic, such as sustained high packet rates that indicate slowbuilding DDoS attacks. By selectively "forgetting" irrelevant details, LSTMs improve accuracy in distinguishing between normal traffic bursts (like legitimate heavy usage) and malicious flooding attempts.

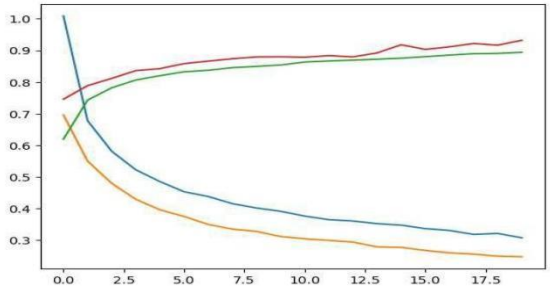
Accuracy Curve:



vii. GRU (Gated Recurrent Unit):

Gated Recurrent Units (GRUs) provide a streamlined alternative to LSTMs by combining the input and forget gates into a single update gate, while employing a reset gate to manage the influence of past information. This design lowers the number of parameters yet preserves the capacity to learn longterm dependencies. In the context of SDN traffic monitoring, GRUs prove effective as they capture essential temporal patterns without the computational overhead associated with LSTMs. Their efficiency makes them well-suited for realtime DDoS detection in high-speed networks, where quick response is vital. Moreover, GRUs perform well with noisy datasets, effectively identifying subtle attack indicators that may be hidden within traffic sequences.

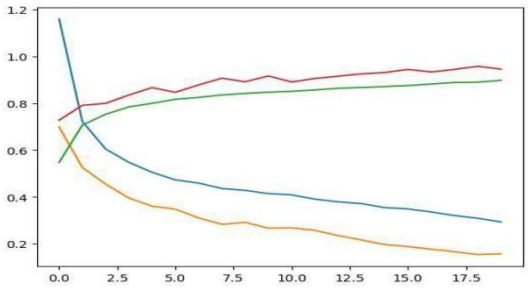
Accuracy Curve



viii. CNN (Convolutional Neural Network).

CNNs are primarily designed for image and spatial data, but they are also effective for analyzing structured traffic flows by treating them as matrices or one-dimensional sequences. CNNs use convolution filters automatically extract local features, such as abrupt changes in packet rate, byte counts, or unusual header patterns. In SDN anomaly detection, these local features are critical because DDoS attacks often generate sudden, sharp traffic variations that normal flows don't exhibit. By stacking convolution and pooling layers, CNNs reduce complexity while retaining important patterns. Compared to RNNs, CNNs are faster because they do not rely on sequential processing, making them suitable for large-scale traffic analysis.

Accuracy Curve



IV. CONCLUSION

In summary, the evaluation of diverse machine learning and deep learning techniques for detecting Distributed Denial-of-Service (DDoS) anomalies in Software-Defined Networks (SDNs) underscores the strength of ensemble methods in enhancing network security. The study considered models including RNN, LSTM, GRU, BiLSTM, CNN, SVM, Random Forest, AdaBoost, XGBoost, Decision Tree, Logistic Regression, and KNN. Among these, the Voting Classifier consistently outperformed the others, achieving high accuracy (90–93%) and leading across metrics such as precision, recall, F1-score, and ROC-AUC, demonstrating its robustness and reliability in identifying DDoS anomalies.

These paper highlight the effectiveness of ensemble learning for constructing accurate and efficient anomaly detection systems, contributing substantially to the security and resilience of SDN architectures. Looking ahead, the future of DDoS detection in SDNs may involve advanced ensemble techniques, hybrid models, and transfer learning to further improve detection accuracy and minimize false positives. Additionally, integrating real-time data and adaptive learning can enhance system robustness, while emerging technologies such as deep reinforcement learning and blockchain-based decentralized detection could provide more scalable and secure solutions for protecting SDN infrastructures.

V. REFERENCES

[1] N. S. Shaji, T. Jain, R. Muthalagu, and P. M. Pawar, ‘‘Deep discovery: Anomaly discovery in software-defined networks using artificial neural networks,’’ Comput. Secur., vol. 132, Sep. 2023, Art. no. 103320.
[2] Y.-C. Wang, Y.-C. Houng, H.-X. Chen, and S.M. Tseng, ‘‘Network anomaly intrusion detection based on deep learning approach,’’ Sensors, vol. 23, no. 4, p. 2171, Feb. 2023.
[3] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, ‘‘A DDoS detection method based on feature engineering and machine learning in softwaredefined networks,’’ Sensors, vol. 23, no. 13, p. 6176, Jul. 2023.
[4] M. Hammad, N. Hewahi, and W. Elmedany, ‘‘Enhancing network intrusion recovery in SDN with machine learning: An innovative approach,’’ Arab J. Basic Appl. Sci., vol. 30, no. 1, pp. 561–572, Dec. 2023.
[5] M. A. Ribeiro, M. S. P. Fonseca, and J. de Santi, ‘‘Detecting and mitigating DDoS attacks with moving target defense approach based on automated flow classification in SDN networks,’’ Comput. Secur., vol. 134, Nov. 2023, Art. no. 103462.
[6] 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. [7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.

[12] 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.
[13] 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.
[14] 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. [15] Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, 118, 102748.
[16]. Malik, J.; Akhunzada, A.; Bibi, I.; Imran, M.; Musaddiq, A.; Kim, S.W. Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN. IEEE Access 2020, 8, 134695–134706. [CrossRef] [17]Kim, J.; Kim, H.; Shim, M.; Choi, E. CNNbased Network Intrusion Detection Against Denialof-Service Attacks. Electronics 2020, 9, 916. [CrossRef]
[18]. Imrana, Y.; Xiang, Y.; Ali, L.; Abdul-Rauf, Z. A Bidirectional LSTM Deep Learning Approach for Intrusion Detection. Expert Syst. Appl. 2021, 185, 115524. [CrossRef]
[19]. Laghrissi, F.; Douzi, S.; Douzi, K.; Hssina, B. Intrusion Detection Systems using Long Short-Term Memory (LSTM). J. Big Data 2021, 8, 65. [CrossRef]
[20]. Aldhyani, T.H.H.; Alkahtani, H. Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. Sensors 2022, 22, 360. [CrossRef] [21]. Tang, Y.; Gu, L.;Wang, L. Deep Stacking Network for Intrusion Detection. Sensors 2022, 22, 25. [CrossRef] [PubMed]