University of Mumbai

PRACTICAL JOURNAL – PAPER I

PSIT301a

Technical Writing and Entrepreneurship Development

SUBMITTED BY

Akshay Santosh Rane

SEAT NO 1323011

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR QUALIFYING M.Sc. (I.T.) PART-II (SEMESTER – III) EXAMINATION 2024-2025

DEPARTMENT OF INFORMATION TECHNOLOGY

3RD FLOOR, DR. SHANKAR DAYAL SHARMA BHAVAN, VIDYANAGRI, SANTACRUZ (E), MUMBAI – 400098.

University of Mumbai

Department of Information Technology

Certificate

This is to certify that Mr. **Akshay Santosh Rane Seat No. 1323011** studying in **Master of Science** in **Information Technology Part II Semester III** has satisfactorily completed the Practical of **PSIT301a Technical Writing and Entrepreneurship Development** as prescribed by University of Mumbai, during the academic year **2024-25**.

---------- ----------

Signature **Signature**

Subject-In-Charge **Head of the Department**

Signature

External Examiner

College Seal: **Date:**

INDEX

CHAPTER I:
INTRODUCTION

BACKGROUND:

The Internet is now becoming a critical resource of our lives and it is impacting our lives. The Internet is evolving through different aspects. As the network infrastructure is expanding, the frequency of cyberattacks are also increasing, so finding different approaches to deal with these threats has become essential in this cyber world. These attacks range from application-layer exploits (e.g., phishing, SQL injection) to network-layer threats (e.g., Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), and botnet attacks). Among these, network-based attacks are particularly concerning as they disrupt services, compromise sensitive data, and exploit vulnerabilities in communication protocols.

There are so many types of cyberattacks to deal with and these threats are evolving significantly, with attackers constantly developing new techniques to exploit vulnerabilities across different layers of the network. Traditional security mechanisms such as firewalls, intrusion detection systems (IDS), and signature-based methods are no longer sufficient due to the evolving complexity of cyber threats. Attackers can target various aspects of network infrastructure. Because of the diverse nature of the attacks, we need different detection techniques and mitigation strategies.

Introduction

The rapid growth of internet-connected devices and cloud-based services has made networks more vulnerable to cyber threats. Among these threats, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks pose a significant risk. These attacks overwhelm network resources by sending a massive volume of malicious traffic, leading to service disruptions, financial losses, and security breaches.

This research focuses on the comparative analysis of machine learning (ML) models for detecting and mitigating these threats. Specifically, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks in network monitoring.

We are comparing machine learning and AI techniques because the traditional techniques like rule-based and signature-based intrusion detection systems (IDS) are not performing better against the evolving attack patterns. They require constant updates and manual interventions. Zero-day attacks and adversarial tactics make it difficult to rely solely on predefined rules. Moreover, Attackers are leveraging automated tools, AI-driven malware, and botnets to bypass conventional defenses. This has led to the need of study of machine

learning (ML) and deep learning (DL) models for network traffic analysis and anomaly detection.

That's why this research aims to compare and evaluate ML models for network anomaly detection, focusing on DoS and DDoS attacks. By analyzing various datasets, preprocessing techniques, feature selection methods, and performance metrics, we seek to determine the most effective and computationally efficient approach for detecting malicious network behavior.

DoS (Denial of service attack) and DDoS (Distributed Denial of service attack)

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are particularly impacting the network infrastructure. Threats which aim to overcrowd networked computer systems or resources and consequently make unavailable legitimate services are typically referred to as Denial-of-Service (DoS) attacks [1]. When such a threat is activated through a large group of compromised machines, called zombies or bots, which send coordinated traffic to the victim, in an attempt to exhaust the network resources such as CPU, memory or link bandwidth of the victim, we refer to it as

Distributed Denial-of-Service (DDoS) flooding attack. [1]

A denial-of-service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. [2]. DDoS attacks make computer systems inaccessible by flooding servers, networks, or even end-user systems with useless traffic so that legitimate users can no longer gain access to those resources. In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets. [2].

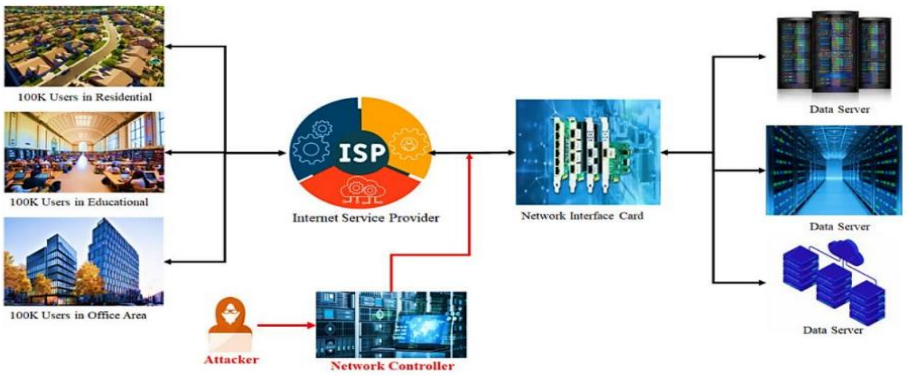


Figure 1. DDoS attack scenario

Figure is referred from [3]

When a device or network is overloaded, it becomes unusable due to a DDoS attack. Attackers

achieve this by flooding the target with more traffic beyond what is capable of handling, which leads to a failure and prevents it from being able to service its normal users. Attacks can be launched against any service that depends on a specific computer or network, including websites, online banking, email, and other services [4], [5].

There are 3 types of DDoS attack [3]:

Volume based

Protocol based

Application based

CHAPTER II:
LITERATURE SURVEY

The increasing sophistication of Distributed Denial-of-Service (DDoS) attacks necessitates the study of effective detection and mitigation strategies as traditional techniques are struggling to detect evolving attack patterns. This literature review aims to compare different detection and mitigation techniques explored previously in resources. We tried to collect research papers, books etc. to study the techniques to deal with evolving attack type.

Below are some of the observations collected from the research papers from 2021 to 2025. The research was done in different network environments. After reviewing the papers, we found that most researched environments were IoT and SDN (Software defined network).

Most of the papers are the surveys done to compare different machine learning and deep learning techniques by analyzing various datasets, pre-processing techniques, feature selection methods, and performance metrics. We tried to find the most effective and computationally efficient approach.

The first paper reviewed was based on the IoT -network environment. It reviewed multiple machine learning algorithms and deep learning algorithms with different optimization and feature selection techniques. Below is the comparison of some previous methods for detecting DDoS.

Among the different models, SVM, KNN, FR had high accuracy in classification. However, linear SVM have weak performance, KNN is time consuming whereas random forest has real time suitability issue [6]. Utilizing ML techniques leads to increased accuracy in network attack detection. However, computational complexity limits the detection of new attacks. [7].

Among different machine learning algorithms, some of the best algorithms are compared which are SVM, K-means, PCA, KNN, random forest, decision-tree. [7]. These algorithms are implemented with different optimization and feature selection techniques.

The first approach was implementation of SVM algorithm with different techniques. ONE-SVM with PSO optimization method helped to reduce the number of features which ultimately showed improved performance and reduction in detection time. However, algorithm complexity is very high, and it requires high storage. [8]. The next method is SVM-logistic regression coefficient which has less complexity because of which it has improved performance however the linear SVM requires longer training time. [9]. Support vector machine (SVM), Fuzzy Tsukamoto are more flexible however it requires more training data and longer training time. Gray Wolf Optimization and One Class Support Vector Machine requires less detection time and reduced feature count but algorithm requires more training samples and it is highly dependent on labeled data.[7]

In the next approach, K nearest neighbor is used with different techniques. The KNN algorithm shows enhanced performance when the parameter optimization is used, however, it relies on training data. Now the KNN with dimensionality reduction algorithm shows improved performance by reducing computational complexity and it has real time analysis capabilities also. [7], [10]. K- means clustering algorithm and K-means semi supervised algorithm using

computationally complex. [7].

Then the decision tree with different techniques is also tested. So, the decision tree method with Pearson correlation-based recursive feature removal mode has improved system performance and enhanced data quality. The lightweight decision tree algorithm has lowered resource usage due to the employment of a limited set of chosen features. [11],[12].

Different boosting techniques are also implemented to test the detection accuracy. Among different boosting techniques AdaBoost and XGBoost outperform achieve the highest accuracy in DDoS detection. [13]. Among both the boosting techniques, XGBoost shows accurate prediction however, it needs precise configuration, and it is computationally complex. [14]. GB and XGBoost achieved high accuracies of 99.99% and 99.98%. [13]. SVM and XGBoost combined using soft voting perform well. [15]. This paper suggested that the performance of anomaly detection was improved using feature extraction by PCA. [15].

Hyperparameter tuning also improves performance.

Naïve Bayes: Smoothing parameter (α).

XGBoost: Learning rate (η), maximum depth, and num-ber of estimators.

LightGBM: Number of leaves, learning rate, and feature fraction.

SVM: Kernel type (RBF), regularization parameter (C), and gamma.

Isolation Forest: Number of estimators and contamination. These parameters are suggested in the paper [15].

Below are some general observations from different research papers about machine learning and deep learning algorithms with the objectives.

This paper aims to enhance DDoS attack detection by leveraging Deep Residual Neural Networks (ResNets) and synthetic oversampling techniques (SMOTE) to balance dataset representation and improve detection accuracy. This model tried to deal with dataset imbalance and minimize false positive. This paper concluded that the combination of Deep Residual Neural Networks (ResNets) and Synthetic Minority Oversampling Technique (SMOTE) achieved 99.98%. [17]

The objective of this paper is to develop a proactive DDoS detection strategy by integrating innovative packet marking techniques, traffic analysis, and machine learning

models. It implemented different algorithms like Logistic Regression, Random Forest, Support Vector Machine (SVM), Naive Bayes, K-Nearest Neighbors (KNN), Decision Tree, and XGBoost. Among these approaches, KNN achieved 98.4%. [18]

The objective of the paper is to conduct a comprehensive analysis of ML and DL-based solutions for DDoS attack detection in SDN environments. SVM, Naive Bayes, KNN, ANN, Decision Tree, Random Forest, Logistic Regression, XGBoost, LSTM, CNN, GRU, SAE algorithms are implemented out of which KNN showed higher accuracy of 99.98%. It suggested that combining ML and DL techniques enhances DDoS attack detection accuracy and reduces false positives. [19]

The objective of the study is to study and compare various approaches to detecting DDoS attacks and recommend solutions for high-speed networks (HSN). It showed the detail description about DDoS attack. DDoS attacks might be volume-based, protocol-based, or application-layer attacks.[20]

The objective of the study is to investigate the application of machine learning algorithms for detecting Low-Rate Denial-of-Service (LDoS) attacks within Software-Defined Networks (SDNs). The paper concluded that Logistic Regression and BIRCH achieved high detection accuracy of 99.96% in detecting LDoS within SDN.[21]

The objective of the study is to improve network attack traffic detection by comparing Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) models. It concluded that AUC metric of SVM (0.73) is significantly greater than that of KNN (0.66), indicating superior classification performance by SVM. SVM performs better with high-dimensional and complex datasets, while KNN is more effective with simpler data structures.[22]

This paper tried to enhance the classification of multi-class DDoS attacks using machine learning techniques. This paper used Multilayer Perceptron, Reduced Error Pruning (REP) Tree, Partial Decision Tree (PART), RandomForest, J48. Among these algorithms, J48 achieved an overall accuracy of 99.97%.[23]

This paper aims to develop an anomaly detection system using machine learning to mitigate DDoS attacks in IoT networks. In this paper. Different machine learning algorithms are compared such as Multiple machine learning algorithms, including Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbors (KNN). It concluded that SVM achieved 99.85%, RF 96.80%, and KNN 98.90%.[24]

This paper systematically reviews deep learning approaches for detecting DDoS attacks. It reviewed Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Autoencoders (AE), Hybrid

models (e.g., CNN-LSTM, RNN-AE), Transfer Learning models. It concluded that the hybrid models have accuracy ranging from 95% to 99.99%. CNN shows the highest performance.[25]

This paper aims to perform an experimental analysis of various machine learning methods for detecting Botnet DDoS attacks. This study compares Support Vector Machine (SVM), Artificial Neural Network (ANN), Naïve Bayes (NB), Decision Tree (DT), and Unsupervised Learning (USML) (K-means, X-means, etc.). It concluded that unsupervised machine learning achieved the highest accuracy at 94.78% for UNBS-NB 15 dataset and 98.08% for KDD99 dataset.[26]

This paper provided an overview of how ML, DL, and RL are applied in cybersecurity, including their usage in malware detection, intrusion detection, vulnerability assessment, and other areas, while discussing their challenges and limitations. This paper studied different approaches such as Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL). This paper also suggested that hybrid models have accuracy ranging from 95% to 99.99%. CNN shows the highest performance.[27]

This paper tried to analyze the detection performance of various machine learning algorithms for DDoS attacks using the CICDDoS2019 dataset for that they have selected K-Nearest Neighbors (K-NN), Support Vector Machine (SVM), Naïve Bayes (NB), Decision Tree (DT), Random Forest (RF), Logistic Regression (LR). This paper concluded that Decision Tree and Random Forest achieved the highest accuracy of 99%.[28]

This paper uses Fuzzy Logic, Multi-Layer Perceptron (MLP) neural network, K-Nearest Neighbors (K-NN), Support Vector Machine (SVM), and Multinomial Naive Bayes (MNB) to detect the DDoS attack. It concluded that MLP achieved an F1-score of 98.04% for attack traffic and 99.30% for legitimate traffic with emulated data. Using the FL, MLP, and ED combined approach, F1-scores reached 98.80% for attack traffic and 99.60% for legitimate traffic with emulated data, and 100% for both traffic types with real data.[29]

This paper also includes different algorithms like Decision Tree (DT), K-Nearest Neighbors (KNN), Random Forest (RF), Logistic Regression (LR), Naïve Bayes (NB), Bayesian Network (BN), Support Vector Machine (SVM), One Rule (OneR), K-Means, Expectation-Maximization (EM), and Univariate Gaussian algorithm. It concluded that the Decision Tree model achieved an accuracy of 0.999 with a False Positive Rate of 0.001. It suggested that Supervised algorithms outperform unsupervised and semi-supervised ones in terms of detection performance. Decision Tree, KNN, and Random Forest showing the best results. [30]

Both papers suggested that Random Forest gives great performance and accuracy. [31],

[32]

The best accuracies achieved were Logistic Regression (99.98%), AdaBoost (99.98%), KNN (99.98%), Naive Bayes (99.98%).[33]

Random Forest are effective in detecting and classifying DDoS attacks in IoT environments. [34]. This paper aims to classify DDoS attacks using a semi-supervised machine learning approach with clustering and voting methods. It includes Agglomerative Clustering (AC), K-means clustering with Principal Component Analysis (PCA), k-Nearest Neighbors (kNN), Support Vector Machine (SVM), Random Forest (RF). This paper concludes that the proposed semi-supervised approach effectively reduces false positives by using multiple clustering algorithms and a voting method.[35]

Objective of this paper is to detect DDoS attacks by using feature selection techniques combined with machine learning algorithms. Decision Table achieved 88.43% accuracy, Naïve Bayes 87.74%, and ANN 84.66%. Decision Table and Naïve Bayes classifiers performed the best. [36]

This paper aims to investigate the detection performance of DDoS attacks using various machine learning algorithms with the NSL KDD dataset. It concluded that K-Nearest Neighbors (KNN) achieved 98% accuracy.[37]

This paper explores the application of machine learning algorithms for predicting and mitigating Distributed Denial of Service (DDoS) attacks. It uses different algorithms such as Support Vector Machines (SVM), Random Forests, Neural Networks, k-means clustering, and Isolation Forests.[38]

This paper aims to develop an effective and efficient detection system for DDoS attacks using the Multi-Layer Perceptron (MLP) deep learning algorithm. It uses different deep learning techniques such as Multi-Layer Perceptron (MLP), Naïve Bayes, Decision Stump, Logistic Model Tree, Naïve Bayes Updateable, Naïve Bayes Multinomial Text, AdaBoostM1, Attribute Selected Classifier, Iterative Classifier, and OneR. It concluded that the proposed MLP algorithm achieved an efficiency of 98.99% with a false positive rate of 2.11%.[39]

This paper aims to identify and prevent DDoS and DoS attacks (i.e., SYN, Slowloris) in a D2D communication environment using machine learning models. It concluded that Random Forest achieved the highest accuracy of 99.8%. [40]

The objective of this paper is to analyze recent studies concerning DDoS detection methods that have adapted single and hybrid ML approaches in modern networking environments. It uses different machine learning techniques such as Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbor (KNN), Long Short-Term Memory

(LSTM), Convolutional Neural Network (CNN), Deep Reinforcement Learning, and others. It concluded that Machine learning techniques, particularly hybrid models, provide high accuracy in detecting DDoS attacks. [41]

This paper concluded that RF achieved the highest accuracy of 99.997% with 19 features selected using the RFFI method [42] whereas CNN-based model achieved 99.99% accuracy for binary classification and 99.30% accuracy for multi-class classification. [43]

CHAPTER III:

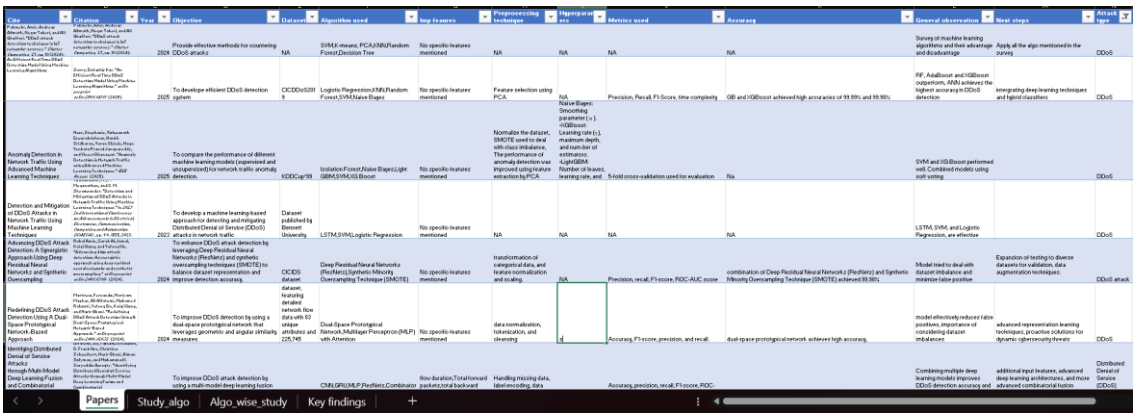
METHODOLOGY/ APPROACH

This research focuses on analysing machine learning models used for detecting DDoS attacks in network monitoring. The study involves reviewing past research, extracting insights, and designing a framework for further experimentation and validation.

2. Literature Review Methodology

2.1 Data Collection

The selection of research papers was based on relevance and recent advancements in DDoS detection. A total of 40 research papers published in the between 2021 to 2025 were chosen for review. The primary criteria for selection included a focus on DDoS attack detection using machine learning techniques. The extracted information was structured in an Excel sheet containing fields such as Cite, Citation, Year, Objective, Dataset, Algorithm used, Important features, Preprocessing techniques, Hyperparameters, Metrics used, Accuracy, General observation, Next steps, Attack typees. This structured dataset helped in the identification of key trends and gaps in existing research.



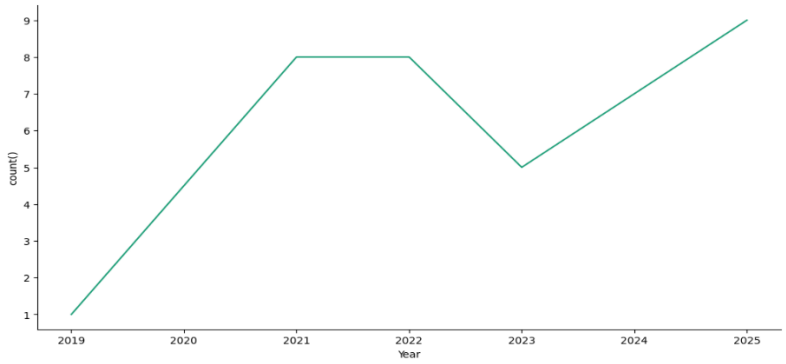
2.2 Analysis Conducted

The analysis of the collected research papers revealed several important insights. The performance of machine learning models is highly dependent on the dataset and the environment in which they are tested. Both machine learning and deep learning techniques demonstrate superior performance in detecting DDoS attacks, with hybrid models often outperforming standalone approaches. One key challenge identified is the issue of data imbalance, which significantly affects model performance. Addressing this imbalance is crucial in enhancing the reliability of detection mechanisms.

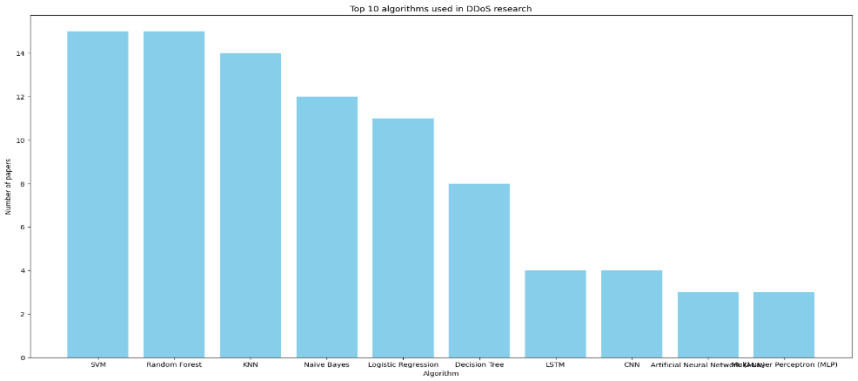
False positive reduction remains an essential focus area, as minimizing false alarms is critical for real-world deployment. Studies indicate that combining multiple deep learning models improves accuracy and robustness. Furthermore, DDoS attacks can be classified into three primary categories: volume-based attacks, protocol-based attacks, and application-layer attacks. This classification helps in designing specialized detection mechanisms for each type.

Hyperparameter tuning has been found to significantly enhance the performance of machine learning models, emphasizing the importance of systematic optimization techniques. Unsupervised machine learning (USML) methods, particularly in detecting botnets, have shown high accuracy with minimal false alarm rates, making them a promising approach for anomaly-based detection. Additionally, real-time detection and threat response are critical components for practical network security applications. Future research should focus on testing models on diverse datasets to ensure their generalizability and robustness across different network environments.

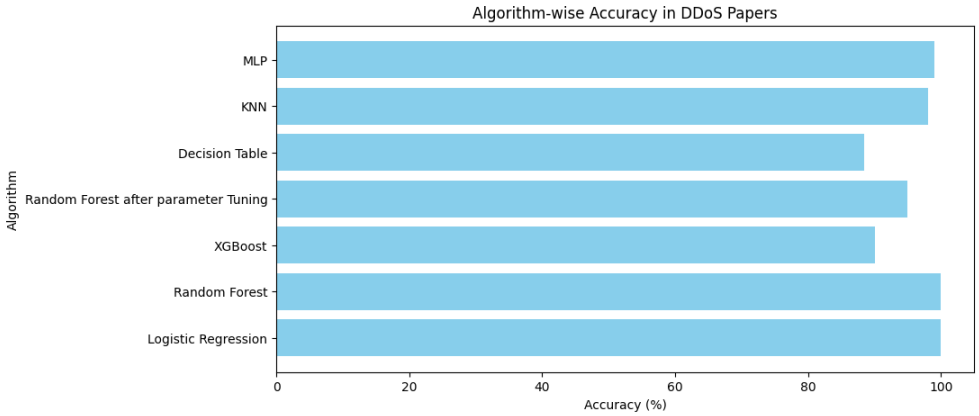
By analysing the 40 papers, I found that the research in this field shows an increasing trend over the past 5 years.



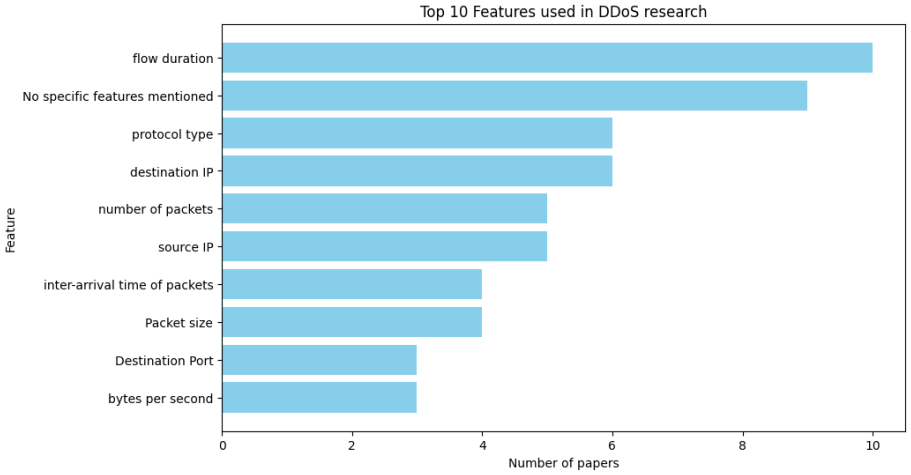
The top 10 algorithms used in DDoS research as per the papers reviewed is depicted in below bar chart.



And below chart shows the algorithm wised accuracy as per the papers reviewed.



As per the papers reviewed, some important features are extracted which is illustrated in below chart.



The above analysis was done in google colab with the help of python libraries. For the study, we have used the custom excel sheet made by reviewing the papers.

3. Proposed Research Methodology

3.1 Research Objectives

The primary objectives of this research include the development of an optimized model for DDoS attack detection, comparison of traditional and advanced ML/DL models, identification of effective feature selection and preprocessing techniques, and implementation of a real-time detection framework.

3.2 Proposed Approach

The first phase of the research involves an extended literature review to explore additional research papers and surveys on anomaly detection in networks. This phase aims to refine the research scope and identify potential areas for improvement. In the second phase, appropriate datasets such as CICDDoS2019, NSL-KDD, or CSE-CIC-IDS2018 will be selected. Preprocessing techniques will be applied to clean and transform the data, including feature

scaling, handling missing values, and encoding categorical data.

The third phase focuses on model selection and implementation. Various baseline models, including Random Forest, XGBoost, LSTM, CNN, and Transformer-based models, will be tested. Feature selection methods such as Recursive Feature Elimination and Mutual Information will be applied to identify the most relevant features. Hyperparameter tuning using Grid Search or Bayesian Optimization will be conducted to improve performance. The trained models will be evaluated based on accuracy, precision, recall, F1-score, false positive rate, and detection time.

The fourth phase involves experimental validation and comparative analysis. The models will be tested on multiple datasets to assess their effectiveness across different network conditions. Emphasis will be placed on real-time traffic detection and threat response capabilities.

In the final phase, a proposed model and UI design will be developed. The detection framework will integrate the optimized model into a real-time network monitoring system. A dashboard will be designed to visualize detected anomalies, attack trends, and model performance metrics. The research aims to contribute towards improving the accuracy and efficiency of DDoS detection systems by leveraging advanced machine learning techniques and robust evaluation methodologies.

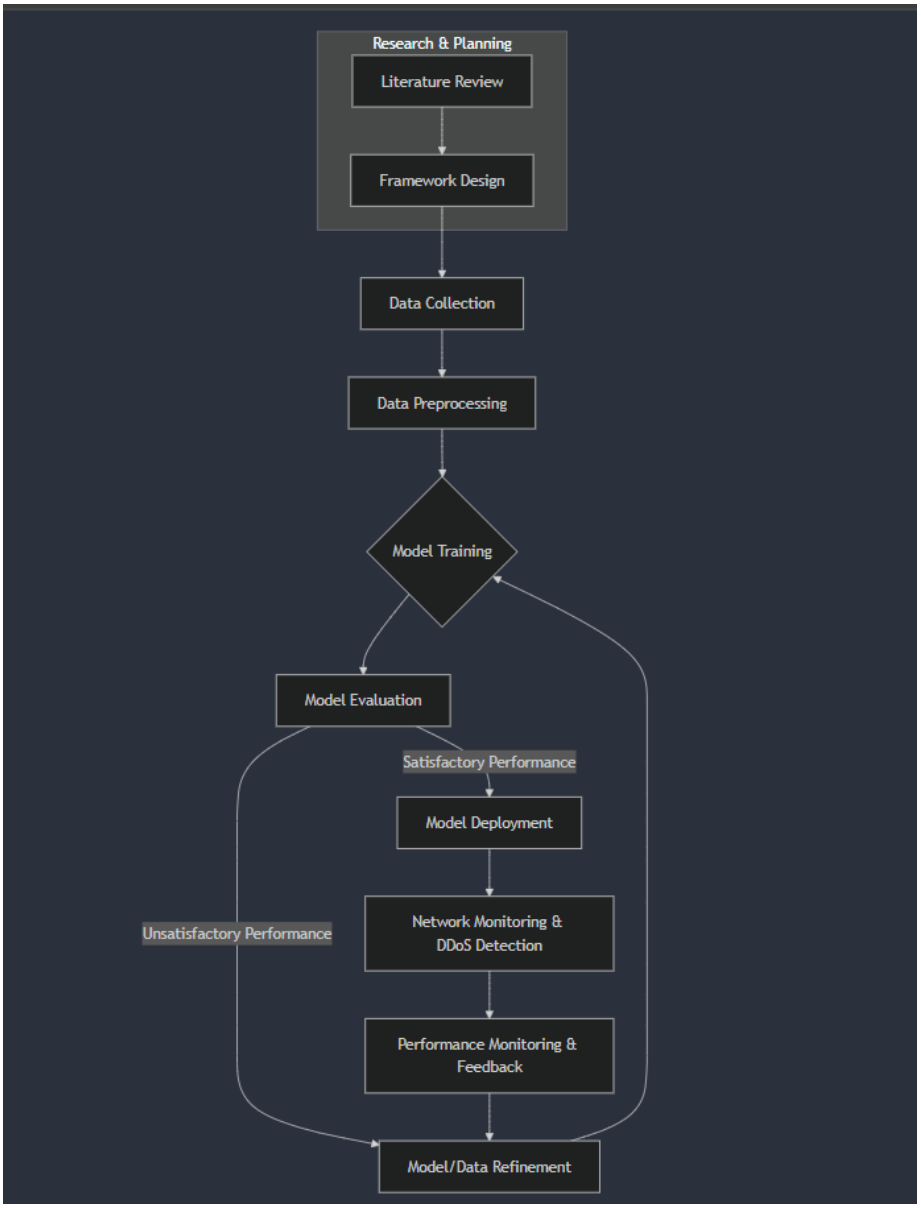
5. Conclusion

This methodology ensures a systematic approach to identifying the most effective machine learning models for DDoS detection. The next steps involve dataset selection, model experimentation, and performance validation. Future research will emphasize developing a scalable detection framework that can operate effectively in real-time environments and adapt to evolving cyber threats.

CHAPTER IV:
PROPOSED DESIGN

4. Proposed Research Design

4.1 Research Workflow Diagram



4.2 Proposed UI Design

The proposed UI will provide an interactive dashboard that presents real-time analytics of detected anomalies. It will display critical insights such as attack classification, detection confidence levels, and statistical comparisons of different models. The visualization will support decision-making by network administrators, enabling faster responses to potential threats.

REFERENCES:

[1] Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. CRC Press, 2016.

[2] Stallings, William. *Network security essentials: applications and standards*. Pearson, 2016.

[3] Habib, AKM Ahasan, Ahmed Imtiaz, Dhonita Tripura, Md Omar Faruk, Md Anwar Hossain, Iffat Ara, Sohag Sarker, and AFM Zainul Abadin. "Distributed denial-of-service attack detection short review: issues, challenges, and recommendations." Bulletin of Electrical Engineering and Informatics 14, no. 1 (2025): 438-446.

[4] M. K. Hasan, A. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," Energy Reports, vol. 9, pp. 1318-1326, 2023, doi: 10.1016/j.egyr.2023.05.184.

[5] H. Liao et al., "A survey of deep learning technologies for intrusion detection in internet of things," IEEE Access, vol. 12, pp. 4745-4761, 2024, doi: 10.1109/ACCESS.2023.3349287.

[6] Yu, S., Zhou, W., Doss, R., Jia, W.: Traceback of DDoS attacks using entropy variations. IEEE Trans. Parall. Distrib. Syst. 22(3), 412–425 (2010)

[7] Pakmehr, Amir, Andreas Aßmuth, Negar Taheri, and Ali Ghaffari. "DDoS attack detection techniques in IoT networks: a survey." Cluster Computing 27, no. 10 (2024): 14637-14668.

[8] Salam, M.A.: Intelligent system for IoT botnet detection using SVMand PSO optimization. J. Intell. Syst. Internet Things 3(2), 68–84 (2021)

[9] M. M. Azmi and F. D. S. Sumadi, ''Low-rate attack detection on SD-IoT using SVM combined with feature importance logistic regression coefficient. In: Kinetik: Game

Technology, Information System, Computer Network, Computing, Electronics, and Control, 2022.

[10] S. Salaria, S. Arora, N. Goyal, P. Goyal, and S. Sharma, Implementation and Analysis of an Improved PCA technique for DDoS Detection.‘‘ In: 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), 2020, pp. 280–285: IEEE.

[11] G. Lucky, F. Jjunju, and A. Marshall, A lightweight decisiontree algorithm for detecting DDoS flooding attacks. In: 2020 IEEE 20th international conference on software quality, reliability and security companion (QRS-C), 2020, pp. 382–389: IEEE.

[12] Yu, J., Kang, H., Park, D., Bang, H.-C., Kang, D.W.: An indepth analysis on traffic flooding attacks detection and system using data mining techniques. J. Syst. Architect. 59(10), 1005–1012 (2013)

[13] Suvra, Debashis Kar. "An Efficient Real Time DDoS Detection Model Using Machine Learning Algorithms." arXiv preprint arXiv:2501.14311 (2025).

[14] . Dhaliwal, S.S., Nahid, A.-A., Abbas, R.: Effective intrusion detection system using XGBoost. Information 9(7), 149 (2018)

[15] Ness, Stephanie, Vishwanath Eswarakrishnan, Harish Sridharan, Varun Shinde, Naga Venkata Prasad Janapareddy, and Vineet Dhanawat. "Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques." IEEE Access (2025).

[16] Vishnukumar, M., P. Meganathan, and C. M. Shyamsunder. "Detection and Mitigation of DDoS Attacks in Network Traffic Using Machine Learning Techniques." In 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), pp. 1-6. IEEE, 2023.

[17] Alfatemi, Ali, Mohamed Rahouti, Ruhul Amin, Sarah ALJamal, Kaiqi Xiong, and Yufeng Xin. "Advancing ddos attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling." arXiv preprint arXiv:2401.03116 (2024).

[18] Pasupathi, Subbulakshmi, Raushan Kumar, and L. K. Pavithra. "Proactive DDoS detection: integrating packet marking, traffic analysis, and machine learning for enhanced network security." Cluster Computing 28, no. 3 (2025): 210.

[19] Aslam, Naziya, Shashank Srivastava, and M. M. Gore. "A comprehensive analysis of machine learning-and deep learning-based solutions for DDoS attack detection in SDN." Arabian Journal for Science and Engineering 49, no. 3 (2024): 3533-3573.

[20] Habib, AKM Ahasan, Ahmed Imtiaz, Dhonita Tripura, Md Omar Faruk, Md Anwar Hossain, Iffat Ara, Sohag Sarker, and AFM Zainul Abadin. "Distributed denial-of-service attack detection short review: issues, challenges, and recommendations." Bulletin of Electrical Engineering and Informatics 14, no. 1 (2025): 438-446.

[21] Salih, Ali Osman Mohammed. "Exploring LDoS Attack Detection in SDNs using Machine Learning Techniques." Engineering, Technology & Applied Science Research 15, no. 1 (2025): 19568-19574.

[22] Han, Zhuoxi. "A Comparative Analysis of Support Vector Machine and K-Nearest Neighbors Models for Network Attack Traffic Detection." In ITM Web of Conferences, vol. 70, p. 01018. EDP Sciences, 2025.

[23] Abood, Mohammad Jawad Kadhim, and Ghassan Hameed Abdul-Majeed. "Enhancing Multi-Class DDoS Attack Classification using Machine Learning Techniques." Journal of Advanced Research in Applied Sciences and Engineering Technology 43, no. 2 (2025): 75-92.

[24] Mohammed, Baydaa Hashim, Hasimi Sallehudin, Nurhizam Safie Mohd Satar, Hamed Dhary Murhg, Shaymaa Abdelghany Mohamed, Fadele Ayotunde Alaba, Alvaro Rocha, and Isaias Bianchi. "Anomaly detection of distributed denial of service (DDoS) in IoT network using machine learning." In Digital Technologies and Transformation in Business, Industry and Organizations: Volume 3, pp. 41-64. Cham: Springer Nature Switzerland, 2025.

[25] Mittal, Meenakshi, Krishan Kumar, and Sunny Behal. "Deep learning approaches for

detecting DDoS attacks: A systematic review." Soft computing 27, no. 18 (2023): 13039-13075.

[26] Tuan, Tong Anh, Hoang Viet Long, Le Hoang Son, Raghvendra Kumar, Ishaani Priyadarshini, and Nguyen Thi Kim Son. "Performance evaluation of Botnet DDoS attack detection using machine learning." Evolutionary Intelligence 13, no. 2 (2020): 283-294.

[27] Tuan, Tong Anh, Hoang Viet Long, Le Hoang Son, Raghvendra Kumar, Ishaani Priyadarshini, and Nguyen Thi Kim Son. "Performance evaluation of Botnet DDoS attack detection using machine learning." Evolutionary Intelligence 13, no. 2 (2020): 283-294.

[28] Alzahrani, Rami J., and Ahmed Alzahrani. "Security analysis of ddos attacks using machine learning algorithms in networks traffic." Electronics 10, no. 23 (2021): 2919.

[29] de Miranda Rios, Vinícius, Pedro RM Inácio, Damien Magoni, and Mário M. Freire. "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms." Computer Networks 186 (2021): 107792.

[30] Saghezchi, Firooz B., Georgios Mantas, Manuel A. Violas, A. Manuel de Oliveira Duarte, and Jonathan Rodriguez. "Machine learning for DDoS attack detection in industry 4.0 CPPSs." Electronics 11, no. 4 (2022): 602.

[31] M NALAYINI, C., and Jeevaa Katiravan. "Detection of DDoS Attack Using Machine Learning Algorithms." Available at SSRN 4173187 9, no. 7 (2022).

[32] Peneti, Subhashini, and E. Hemalatha. "DDOS attack identification using machine learning techniques." In 2021 International conference on computer communication and informatics (ICCCI), pp. 1-5. IEEE, 2021.

[33] Dasari, Kishore Babu, and Nagaraju Devarakonda. "Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms." Ingénierie des Systèmes d Inf. 26, no. 5 (2021): 461-468.

[34]Chopra, Amardeep, Sunny Behal, and Vishal Sharma. "Evaluating machine learning

algorithms to detect and classify DDoS attacks in IoT." In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 517-521. IEEE, 2021.

[35] Aamir, Muhammad, and Syed Mustafa Ali Zaidi. "Clustering based semi-supervised machine learning for DDoS attack classification." Journal of King Saud University-Computer and Information Sciences 33, no. 4 (2021): 436-446.

[36] Azmi, Muhammad Aqil Haqeemi, Cik Feresa Mohd Foozy, Khairul Amin Mohamad Sukri, Nurul Azma Abdullah, Isredza Rahmi A. Hamid, and Hidra Amnur. "Feature Selection Approach to Detect DDoS Attack Using Machine Learning Algorithms." JOIV: International Journal on Informatics Visualization 5, no. 4 (2021): 395-401.

[37] Mondal, Biswajit, Chandan Koner, Monalisa Chakraborty, and Subir Gupta. "Detection and investigation of DDoS attacks in network traffic using machine learning algorithms." Int. J. Innov. Technol. Explor. Eng 11, no. 6 (2022): 1-6.

[38] Naseer, Iqra. "Machine Learning Algorithms for Predicting and Mitigating DDoS Attacks." (2024).

[39] Ahmed, Sheeraz, Zahoor Ali Khan, Syed Muhammad Mohsin, Shahid Latif, Sheraz Aslam, Hana Mujlid, Muhammad Adil, and Zeeshan Najam. "Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron." Future Internet 15, no. 2 (2023): 76.

[40] Rani, SV Jansi, Iacovos Ioannou, Prabagarane Nagaradjane, Christophoros Christophorou, Vasos Vassiliou, Sai Charan, Sai Prakash, Niel Parekh, and Andreas Pitsillides. "Detection of DDoS attacks in D2D communications using machine learning approach." Computer Communications 198 (2023): 32-51.

[41]Aljuhani, Ahamed. "Machine learning approaches for combating distributed denial of service attacks in modern networking environments." IEEE Access 9 (2021): 42236-42264.

[42] Alduailij, Mona, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailij, and Fazila Malik. "Machine-learning-based DDoS attack detection using mutual

information and random forest feature importance method." Symmetry 14, no. 6 (2022): 1095.

[43] Akgun, Devrim, Selman Hizal, and Unal Cavusoglu. "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity." Computers & Security 118 (2022): 102748.