AI in the Detection and Prevention of Distributed Denial of Service (DDoS) Attacks

Sina Ahmadi
National Coalition of Independent Scholars, NCIS, Seattle, USA

***Abstract*—Distributed Denial of Service (DDoS) attacks are malicious attacks that aim to disrupt the normal flow of traffic to the targeted server or network by manipulating the server's infrastructure with overflowing internet traffic. This study aims to investigate several artificial intelligence (AI) models and utilise them in the DDoS detection system. The paper examines how AI is being used to detect DDoS attacks in real-time to find the most accurate methods to improve network security. The machine learning models identified and discussed in this research include random forest, decision tree (DT), convolutional neural network (CNN), NGBoosT classifier, and stochastic gradient descent (SGD). The research findings demonstrate the effectiveness of these models in detecting DDoS attacks. The study highlights the potential for future enhancement of these technologies to enhance the security and privacy of data servers and networks in real-time. Using the qualitative research method and comparing several AI models, research results reveal that the random forest model offers the best detection accuracy (99.9974%). This finding holds significant implications for the enhancement of future DDoS detection systems.**

Keywords*—*Artificial intelligence; Distributed Denial of Service (Ddos); machine learning; detection; accuracy

I. Introduction

In today's fast-paced digital landscape, web-based services and software have seen a significant rise, with approximately 57% of the global population now using the Internet [1]. While artificial intelligence (AI) and machine learning have become powerful tools across various industries, they have also introduced a host of security challenges, particularly in maintaining the performance and security of networks. Traditional networks often struggle to keep up with the demands for efficiency and robust security, leaving businesses vulnerable to cyber threats like Distributed Denial of Service (DDoS) attacks [2]. The escalating scale and frequency of these attacks highlight a critical problem: existing network infrastructures, including those managed by software-defined networking (SDN), are increasingly incapable of providing the security required to ensure smooth business operations. SDN, which manages network traffic through software platforms rather than hardware, provides a centralised control system that enhances network flexibility and manageability [3]. However, this centralised architecture also introduces vulnerabilities, particularly at the control layer, where attackers can disrupt or manipulate network traffic through DDoS assaults. These attacks are difficult to detect, and as their intensity and frequency continue to rise, they pose significant challenges for administrators and service providers in terms of identification and mitigation [4]. Although various machine learning methods have been proposed for detecting DDoS attacks, there remains a gap in understanding which of these methods is most effective in real-time scenarios, especially within SDN environments.

This study aims to fill this gap by evaluating and comparing different AI-based detection methods to determine the most accurate technique for real-time DDoS attack mitigation in SDN. By addressing the limitations of existing detection approaches, this research seeks to provide a more effective solution for identifying and preventing DDoS attacks. The findings will offer valuable insights into how AI can enhance the security of SDN infrastructures, contributing to the broader goal of protecting businesses from network disruptions and security breaches.

Ultimately, this study's significance lies in its potential to advance current cybersecurity measures by integrating AI into SDN environments. As the intensity and sophistication of cyberattacks continue to rise, finding more accurate detection methods becomes crucial. The results of this research will be essential for administrators and service providers seeking to safeguard their networks against DDoS attacks, thus ensuring greater operational stability and data security.

II. Literature Review

This section of the paper provides a detailed understanding of existing research and guides how this research presents a different perspective in the field. Numerous researchers have investigated AI-based detection methods to understand which method is most accurate for managing detective services.

A. Performance of AI / Machine Learning in DDoS Attack Detention

Meti et al., in their experiment, observe TCP traffic from actual networks along with the number of connected devices per second as an indicator [5]. In terms of precision, accuracy, and recall levels, the results of the comparison highlight that K-Nearest Neighbour (KNN) shows the best precision and accuracy. Zekri et al. suggested that a DT is also effective in the cloud network to detect DDoS attacks [6]. Sahoo et al. present an enhanced support vector machine (SVM) model that implements genetic algorithms (GA) and kernel principal component analysis (KPCA) [7]. Bakker et al. discuss the additional costs of using AI for DDoS attack detection in SDN [8]. Another study by Polat and co-authors confirms that KNN is the most accurate method for DDoS detection and security improvements [9].

B. Use of Machine Learning for DDoS Attack Detection

Huyu et al. present techniques for optimising and creating detection models by sending real-time traffic data to an offline learning network [10]. Data is collected through routers and transmitted to the offline pipeline for data transformation and feature engineering. Optimised models combined with existing models can be used to protect networks from DDoS attacks. Chayomchai et al.'s study focuses on the impact of cybercrime and DDoS attacks on banking institutions and how these institutions are responding to these negative effects [11]. The study claims that massive malware assaults target Indian banks, resulting in the theft of private customer information and huge financial losses. It also states that poorly designed detection models that do not need annotated data to supervise DDoS attacks can be improved using latent Dirichlet allocation (LDA). Another alternative is to use an extra classification layer to remove non-attack tweets from the dataset [12]. Ashraf and Latif propose a SOM-based solution to significantly improve accuracy [13]. However, SOM principles violate SDM principles as they are built on intelligence in the data plane [14]. Peng et al. provide a detection method for anomalous SDN streams in an SDN architecture [15]. They applied the same technique to detect DDoS attacks using DPTCM-KNN as the core algorithm. The results of this study demonstrate that the deployed technique is effective; however, the detection accuracy obtained needs improvement.

C. Machine Learning Models

1) Random forest: The random forest model of machine learning refers to a method of ensemble learning that combines forecasts from different DTs. This model is used for both regression and classification. Predictions from different decision trees are combined to formulate a final forecast, and every entry in a random forest contains a different subset of the data. By deploying ensemble techniques, the individual accuracy of DTs can be improved, making them more dependable for attack detection and prevention.

2) Decision tree: A DT refers to the graphical representation of a decision-making process that separates data based on the input values into different subgroups. Each subgroup produces further branching nodes that lead to other subgroups or outcomes. In regression and classification tasks, a DT is used to generate and present predictions based on data feature values. Decision trees are simple and convenient to understand, which is why they are helpful in detecting DDoS attacks. However, the accuracy of DTs needs improvements in terms of consistency in detection.

3) *Convolutional neural network:* A CNN is used for image classification and identification. Convolutional neural networks have innumerable applications, such as face recognition, image processing, object detection, and computer vision. They are AI-powered systems that use images as input to perform. Convolutional neural networks work automatically to learn certain features that might be used for categorisation. Algorithms are adjustable to different networks in SDN, making them suitable for environments where potential attacks might occur. In terms of detecting DDoS attacks, CNNs require large amounts of labelled data that might not be available in every scenario.

4) *NGBoosT classifier*: This machine learning model is used for tasks involving data classification. NGBoosT collects different predictions from trees and evaluates those predictions to propose a final prediction. It is helpful in detecting DDoS attacks because it provides predictions about their uncertainty, which is helpful in managing unclear and uncertain situations.

5) Stochastic gradient descent: It is a straightforward and efficient method to detect DDoS attacks on networks. Stochastic Gradient Descent is used to manage complex machine learning issues commonly occurring during text categorisation and language processing tasks. This method can also be applied to different linear models and is convenient for managing different DDoS detection scenarios.

D. DDoS

Xu et al. present a technique to detect DDoS attacks in SDN. The technique mainly depends on K-FKNN and K-means++. The proposed detection system would be implemented into the controller. The experimental results of this study reveal that the implemented technique is stable and efficient [16]. However, some drawbacks that make the technique less accurate include the longer time required to detect the attack and the high load it puts on the SDN resources.

Polat et al. present an alternative method for DDoS attack detection in SDN [9]. There are two aspects to the proposed detection system. The first aspect analyses the DDoS attack traffic and normal traffic on the SDN environment dataset. Filtration wrapping and feature selection methods were deployed in the second aspect to get the most effective features for machine learning model classification. However, there is a limitation to the introduced technique: the need for further enhancement in its performance and detection accuracy.

Novaes et al. have implemented a DDoS attack and a mitigation method in SDN [17]. The whole system is called LSTM-FUZZY. The detection system comprises three stages: characterisation, detection, and mitigation. The proposed system is ineffective due to its restricted scope for addressing the vulnerabilities of other networks. In addition, the model lacks the characteristics required to test different network topologies [17].

Sarwan et al. present a space- and time-efficient DDoS attack detection technique that possesses the characteristics of identifying hosts along with the attack's origin [18]. The technique uses different traffic characteristics to identify abnormal traffic behaviour. It also uses a threshold to identify normal and compromised hosts. This DDoS detection technique is efficient as it saves time and space. However, it does have the limitation of violating SDN standards by implementing logic into switches. Thus, there is a need to improve its performance and algorithmic accuracy.

Studies reveal that DDoS attacks are often released from a single host to seize or disable access by overloading the target network or system. The degree of damage or loss depends on the strength of the attacker's resources. There are different intentions and purposes for launching a Denial-of-Service

attack, which could be personal or institutional. Attackers use botnets or zombie computers to launch a DDoS attack. These attacks are pre-planned to disrupt or destroy a target network by using land moves and targeting a specific system [19].

Existing literature covers different dimensions of the proposed research topic; however, literature about the use of AI to detect and prevent denial-of-service attacks is minimal. Artificial intelligence is evolving in every industry to automate systems and enhance network performance. Researchers must disseminate knowledge on the use of machine learning applications in different fields to protect systems from malware and security assaults. The following section of the paper defines the research problem and the significance of understanding and addressing this problem.

III. Problem Definition

Denial-of-Service (DoS) attacks happen when authorised users fail to access network data due to malicious cyber threat activities launched by third parties. These attacks, driven by various motives, are launched against emails, passwords, databases, and websites to hack the private information of individuals or organisations. Business organisations using advanced software and computing networks to perform everyday operations are prone to such attacks. For example, banks store important organisational and customer information on online databases and transform sensitive information through networks that hackers can conveniently hack and misuse. DoS attacks create enormous challenges for administrators and managers in keeping operations streamlined. Organisations with poor detection infrastructure cannot detect abnormal traffic timely, resulting in attacks and network complications. Given the technological advancements and emerging threats, the major problem lies in the timely detection of DoS attacks and the application of accurate methods to network infrastructures.

Artificial intelligence has become an essential tool for transforming business experiences. It is revolutionising every industry by redefining traditional business practices and transforming customer experiences. By using AI applications and enhancing AI-based models, defence against DoS attacks is possible. For example, AI helps reduce the surface area vulnerable to attack, thereby minimising the options available to attackers. Load balancers mitigate this issue by restricting direct Internet traffic to specific parts of the network to avoid direct attacks. Similarly, Access Control Lists (ACLs) are useful in controlling which traffic would reach applications in a given time [20].

A. DDoS Detection and Prevention

Common mechanisms for detecting and preventing DDoS include attack detection, prevention, and reaction. However, it is difficult to detect DDoS attacks in a network as it is hard to differentiate between abnormal and normal network traffic during ongoing operations. The detection of abnormal traffic in a network is the first step to detecting DDoS attacks. In addition, AI classification methods can help in identifying good and bad packets. Bed packets labelled as abnormal traffic would be dropped. The number of packets, time interval variance, average size of packets, number of bytes, size variance, and packet rate are common characteristics that help differentiate between good and bad packets.

B. Artificial Intelligence Techniques

Most relevant AI techniques include machine learning, natural language processing, and speech recognition. Machine learning algorithms are utilised in most of the settings. These techniques, including Naive Bayes, support vector machines, and neural networks, are implemented based on the nature and frequency of attacks [21].

C. Trends of DDoS Attack

In the fast-paced business world, DDoS attacks are commonplace. For instance, public networks experience frequent instances of high-intensity floods, which significantly affect the normal flow of network traffic and disrupt normal functioning. Although the security protocols of a network protect it against DDoS attacks, trends of attack vary based on the strength of the security protocols of a network. The number of organisations experiencing DDoS attacks is increasing annually, along with the growing dependence on software and databases for managing organisational processes. The integration of technology is simultaneously easing and complicating institutional processes.

D. Integration of AI Models into Networks to Prevent DDoS Attacks

Distributed Denial of Service attacks have been demonstrated to be major threats to the Internet, causing major losses to organisations and governments. With the advancement of technology, it has become convenient for attackers to launch DDoS attacks at low costs. Attackers use unknown hosts or computers to launch DDoS attacks, and it is hard to detect them without having advanced security infrastructures embedded in AI models. However, different AI models, like machine learning algorithms, are available to help detect DDoS attacks. These models vary in accuracy and performance and can be used based on network settings and requirements to prevent DDoS attacks. Fig. 1 shows a machine learning-enabled DDoS detection architecture.

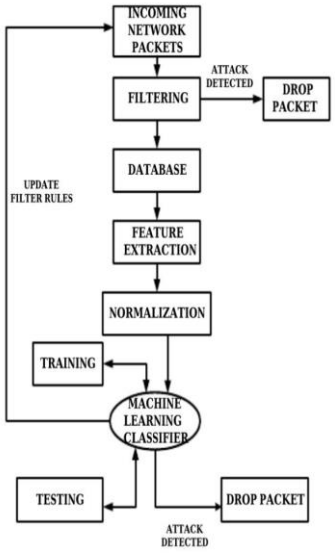

Fig. 1. DDoS attack detection architecture based on machine learning.

E. Accuracy and Adaptability

It is essential for AI-based detection models to provide accurate detection results to protect networks against unauthorised access and use. Models with the greatest accuracy rates are adaptable under certain standards. Detection models should be able to predict possible abnormalities in the network and must inform administrators to timely mitigate those abnormalities. AI-powered detection models can prevent DDoS attacks and protect networks by focusing on security and privacy [22]. The accuracy of machine learning detection models can be determined using Eq. (1).

$$Accuracy = Number\ of\ Correct\ Predictions / Total\ Number\ of\ Predictions \quad (1)$$

IV. Methodology / Approach

A. Research Design

This study uses qualitative research methodology to investigate several AI models and employ them in the DDoS detection system. Using qualitative research methodology, this study aims to explore the application of AI to detect DDoS attacks in real time in banks to find the most accurate methods to improve network security. Qualitative research methodologies encompass the use of theory and literature to explore the diverse perspectives, experiences, and behaviours of people. This approach is carefully chosen to explore and compare machine learning detection models to detect and prevent DDoS attacks. Conducting a qualitative analysis of existing literature helps in understanding the different available methods and their accuracy. This analysis may assist in determining which method is most accurate to avoid network disturbances and breaches. The objective of this study is to compare detection models based on their performance and accuracy scores and propose further improvements to enhance the security of organisational and institutional networks.

B. Research Setting and Participants

The research setting consists of private banking institutions. The participants are banks that have experienced DDoS attacks in the previous two years and used different detection and prevention techniques to prevent further attacks. They also include all researchers who presented relevant experiences regarding AI-detection methods and accuracy measures. Banks are chosen in order to study the use of AI in the detection of DDoS in real-time. Moreover, AI-powered methods are effective at detecting these attacks and maintaining security standards.

C. Data Collection

The data collection method started with the use of Google Scholar, wherein different resources were collected using several research terms such as 'Denial of Service Attacks,' 'Applications of AI in detecting network attacks,' 'network security,' and 'ML models of detection.' These search terms were chosen to retrieve relevant results from the search engine. Different articles were reviewed to collect relevant information and then compared with the observations gained from the AI detection models implemented in banks to avoid DDoS attacks. The comparison aims to understand how different models work in theory and practice as well as how they could be improved further to detect and prevent DDoS attacks in various institutional settings. Through this comparative analysis strategy, the research aimed to collect and evaluate diverse perspectives and experiences to inform its findings and conclusions. Research results would contribute to the existing literature by presenting a novel dimension of DDoS and network attacks.

D. Data Analysis

The thematic analysis approach was utilised to analyse data collected from the literature review. Resources were carefully selected and analysed to guide research problems. DDoS attacks are a wide research topic that researchers have extensively explored from different dimensions. It was ensured that the proposed research problem addressed a novel concern, and relevant literature was used to guide the research. The analysis process was detailed and comprehensive to enhance the study's credibility and guide research conclusions. Data collected from the literature review and banks using AI models to detect and prevent DDoS attacks was analysed collectively to guide discussions and the research conclusion. Three banks were randomly selected to provide e-banking services. Real-time e-banking transactions were checked to track fraudulent activities. An in-depth analysis of e-banking transaction logs was conducted. Banks employed a multi-layered security approach to prevent DDoS attacks, including the use of one-time passwords to ensure that authorised users have access to their accounts. Data from banks using AI-powered solutions to ensure their data is protected and the minimal probability of attacks was analysed. Two banks use blockchain-powered DDoS mitigation strategies and solutions to prevent DDoS attacks. Analysis of real-time e-banking transactions of banks revealed that AI and machine learning models/applications provide real-time protection to online transactions and ensure that institutional and customer data is protected from unauthorised access or breaches. The analysis of the collected data aimed to provide an in-depth understanding of Internet networks prone to DDoS attacks, the nature of attacks, causes and effects, methods to detect and prevent them, and ways in which these methods could be further improved. Furthermore, the correlation between research objectives and themes is also discussed. It highlights how information gained from these themes guides understanding of the research problem and convinces the need for improved security protocols to prevent future DDoS attacks. Thematic analysis not only summarises research findings but also contextualises these findings for readers and future researchers.

E. Ethical Considerations

Research ethics were followed throughout the research process. All resources utilised during the literature review were properly acknowledged through appropriate citations and references, giving credit to the authors. The literature analysis was presented without any personal amendments or changes. All three banks approached to investigate how AI is helpful in detecting DDoS attacks in real-time requested not to reveal their identities in the research paper. In order to respect their privacy, their identities have been concealed, and all discussions pertaining to them have been conducted anonymously. The study addresses biases and conflicts observed in research studies. It ensures that personal conflicts

and biases are avoided throughout the paper to ensure the generalisability of the results and maintain integrity throughout the research process.

V. RESULTS

A. Machine Learning Models

This research paper examined and compared five machine learning models: random forest, DT, CNN, NGBoosT classifier, and SGD. Different performance parameters were used to compare the precision and accuracy of each machine learning model. The accuracy score of each model is illustrated in Fig. 2.

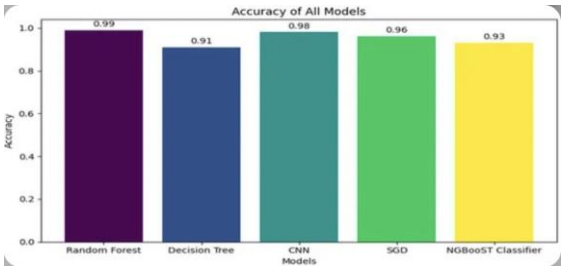

Fig. 2. Accuracy of all models.

Accuracy is a quantitative measure that quantifies the ratio of false negatives and positives to the terms present in the numerator. The numerator further specifies the sum of true negatives and true positives. Eq. (2) defines accuracy as follows:

$$Accuracy = ((TP + NP) / (FP + FN)) * 100 \quad (2)$$

The accuracy scores were used to measure the effectiveness of the five machine learning models in detecting DDoS attacks. Fig. 2 presents the ideal accuracy score of 0.99 for the random forest machine learning model. The purple bar of the random forest model shows how accurate the prediction would be compared to the rest of the four machine learning models. Similarly, CNN, SGD, NGBoosT classifier, and DT show accuracy scores of 0.98, 0.96, 0.93, and 0.91, respectively. Hence, based on the accuracy scores, the random forest machine learning model is the most effective for implementation in institutional settings, whether banks or other organisations, to detect and prevent DDoS attacks [23].

B. Comparative Analysis of Machine Learning Models

A comparative analysis of five machine learning models reveals that each model has its strengths and weaknesses. The random forest model is effective in making predictions for complex settings and is conveniently adjustable in different SDN settings compared to DT and NGBoosT classifiers. The random forest model offers flexibility in different domains compared to NGBoosT, which cancels overfitting into multiple settings. All five machine learning models differ in their approach to handling DDoS attacks in different settings. The accuracy and precision rate of each model differ, highlighting the usefulness and performance of each model in institutional settings. Each model can be individually deployed in different institutional settings based on the security requirements and infrastructure of that institution [24].

VI. DISCUSSION

A. DDoS Attack Detection and Prevention in Banking Industry

An in-depth analysis of the e-banking transaction logs of three banks reveals that AI applications are helpful in detecting and preventing DDoS attacks in real time. In banking institutions, blockchain-powered DDoS mitigation strategies are utilised to enhance security standards and protocols. Banking institutions are implementing strong security protocols and exploring new defences against DDoS attacks. They are using AI models to build strategies for identifying the origins and underlying causes of attacks. Eliminating traditional DDoS prevention approaches, banks are deploying advanced security measures to avoid financial and non-financial losses. Machine learning and AI have made it possible to automatically detect and prevent DDoS attacks [25].

Based on the analysis of existing detection and prevention models implemented by banks, some changes are proposed. With the following structure, the random forest model would provide the most accurate predictions about DDoS attacks.

The proposed changes in the DDoS detection and prevention models would yield outstanding outcomes and protect real-time customer interactions and transactions. This is depicted in Fig. 3.

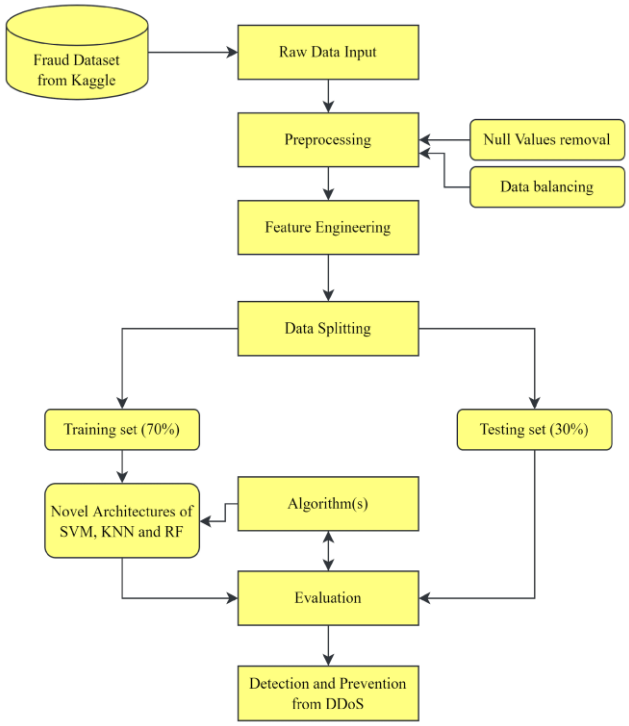

Fig. 3. Proposed machine learning model using e-banking datasets.

B. Adopting Advanced AI Solutions to Detect and Prevent DDoS Attack

In the context of cyberattacks and threats, organisations should understand the importance of advanced and updated AI models to detect and prevent DDoS attacks. Along with advancements in machine learning and AI, cyber threats are

evolving. Therefore, it is essential to timely understand the need for improved machine learning models and integrate them as needed to avoid network breaches and data thefts. Organisations and administrators can focus on evolving AI trends and models being deployed to prevent DDoS attacks. Based on the accuracy code and analysis of the machine learning models used in this study, the random forest model is most suitable for predicting DDoS attacks.

C. Privacy and Confidentiality

Banks are dealing with highly sensitive customer information that could cause major complications if breached. Banks have a paramount responsibility to protect their customers' privacy and confidentiality. This can only be achieved by using upgraded security protocols. Literature analysis reveals that corporations and organisations use different detection and prevention mechanisms to avoid financial and non-financial losses due to DDoS attacks. In dealing with customers' private information, organisations such as banks are expected to adopt ever-changing AI applications that protect network traffic and ensure no abnormalities exist. Collaborative DDoS attack detection and prevention methods can be used to detect attacks at different locations before they occur.

D. Implementation Challenges

The implementation of a machine learning model to protect organisational networks against DDoS is a challenging task. Organisations can protect their networks against these attacks by deploying advanced machine learning and AI-powered solutions and technologies. One of the biggest challenges is that machine learning and AI require a large amount of labelled data to make accurate predictions. Obtaining detailed data in any SDN setting is challenging, which limits the adaptability of these models to effectively detect and prevent DDoS attacks in every situation. Another challenge is resource allocation. The deployment of machine learning models requires heavy investments, imposing financial burdens on organisations. Moreover, not all organisations can afford the cost. In addition to purchasing and implementing machine learning models, regular updates and space requirements are also a concern. Organisations spend to mitigate cyberattacks; however, it is expensive to deploy machine learning models as they require planning from resources to training for successful deployment. To cut cyberattack costs permanently, organisations should consider and prioritise the implementation of machine learning models according to their needs and security infrastructure. This will ensure they have strong security protocols and that their assets are protected from unauthorised access and theft.

Financial institutions, such as banks, are at great risk because of the monetary value of their data. Based on our analysis, the random forest machine learning model is one of the most effective models for making accurate predictions. By enhancing its adjustability, this model can be implemented in financial organisations to timely detect and prevent DDoS attacks. The random forest model can detect abnormal traffic in a network to make predictions regarding the occurrence of a DDoS attack at a certain point. Financial institutions can effectively implement this model to avoid additional expenses associated with addressing cyberattacks and data theft [26].

VII. Conclusion

The Internet has transformed the world over the years. It has become an essential need for every institution and organisation. In this fast-paced world, the Internet is transforming lives and complicating things as well. Cyberattacks have become commonplace in the technically advanced world, wherein an unknown person can assess the private information of institutions or organisations. A DDoS attack is a form of cyberattack in which hackers take control of the central controller to disrupt or completely damage a network. Hackers can launch this attack from any server. The detection and prevention of DDoS attacks is a complicated and sometimes impossible task.

This paper aims to investigate the role of AI in the detection and prevention of DDoS attacks in real-time. To achieve this objective, data was collected and analysed from existing literature and three anonymous banks. Data analysis reveals that institutions are using attack mitigation techniques; however, these techniques are not as effective as machine learning models in defending against DDoS attacks. From the reviewed machine learning models, the random forest model is the most effective model to implement in organisational settings to detect and prevent DDoS attacks promptly. Considering the frequency of cyberattacks, researchers strongly advocate for the integration of machine learning models into the strategic planning of large organisations and institutions. This will help mitigate long-term challenges by ensuring they implement advanced security protocols. It is recommended that, with evolving technologies, organisations understand the dynamic need for security upgrades to compete efficiently in the industry.

VIII. Future Work

This research discussed five machine learning models and found that the random forest model makes more accurate predictions than the other models. Future researchers can conduct further work on the accuracy and effectiveness of the random forest model and why it is most accurate compared to other models. Future research can highlight how machine learning models are making a difference compared to traditional models in detecting and preventing DDoS attacks. Researchers can also explore how the random forest model effectively detects DDoS attacks in different network settings. The adjustability, accuracy, and precision of the random forest model can be studied in detail to justify its effectiveness in comparison to other models.

Moreover, advancements in prevention and detection techniques and mechanisms can transform organisational outcomes. Hence, by integrating and adopting advanced machine learning models to detect DDoS attacks, organisations can safeguard customers' privacy and confidentiality and streamline their everyday operations.

References

[1] Internet growth usage statistics [Internet]. 2019 [cited 2024 Jan 10]; Available from: https://www.clickz.com/internetgrowthusage-stats-2019-time-online-devices-users/235102/

[2] Singh J, Behal S. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Comput. Sci Rev 2020;37:100279.

[3] Sheikh MNA, Hwang IS, Ganesan E, et al. Performance assessment for different SDN-based controllers. In: Proceedings of the 2021 30th Wireless and Optical Communications Conference (WOCC), Taipei, Taiwan; 2021: p. 24-5.

[4] Wang Y, Wang X, Ariffin MM, et al. Attack detection analysis in software-defined networks using various machine learning methods. Comput Electr Eng 2023;108:108655.

[5] Meti N, Narayan DG, Baligar VP. Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In: Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Manipal, India; 2017: p. 1366-71.

[6] Zekri M, El Kafhali S, Aboutabit N, et al. DDoS attack detection using machine learning techniques in cloud computing environments. In: Proceedings of the 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, Morocco; 2017: p. 1-7.

[7] Sahoo KS, Tripathy BK, Naik K, et al. An evolutionary SVM model for DDOS attack detection in software defined networks. IEEE Access 2020;8:132502-13.

[8] Bakker JN, Ng B, Seah WK. Can machine learning techniques be effectively used in real networks against DDoS attacks? In: Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China; 2018: p. 1-6.

[9] Polat H, Polat O, Cetin A. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning. Sustain 2020;12:1035.

[10] Huyn J. A scalable real-time framework for DDoS traffic monitoring and characterization. In: Proceedings of the Fourth IEEE/ACM International Conference on Big Data Computing, Applications and Technologies, Austin, TX, USA: 2017: p. 265-6.

[11] Mhamane SS, Lobo LMRJ. Internet banking fraud detection using HMM. In: Proceedings of the 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, India; 2012.

[12] Chayomchai A, Phonsiri W, Junjit A, et al. Factors affecting acceptance and use of online technology in Thai people during COVID-19 quarantine time. Manag Sci Lett 2020;10:3009-16.

[13] Ashraf J, Latif S. Handling intrusion and DDoS attacks in software-defined networks using machine learning techniques [Internet]. IEEE Xplore. 2014. p. 55-60. Available from: https://ieeexplore.ieee.org/abstract/document/6998241

[14] 2014 IEEE National Software Engineering Conference [Internet]. Interdisciplinary Centre for Mathematical and Computational Modelling. 2014 [cited 2024 Aug 6]. p. 55-60. Available from: https://www.infona.pl/resource/bwmeta1.element.ieee-conf-000006979384/

[15] Peng H, Sun Z, Zhao X, et al. A detection method for anomaly flow in software defined network. IEEE Access 2018;6:27809-17.

[16] Xu Y, Sun H, Xiang F, et al. Efficient DDoS detection based on K-FKNN in software defined networks. IEEE Access 2019;7:160536-45.

[17] Novaes MP, Carvalho LF, Lloret Jaime, et al. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. IEEE Access 2020;8:83765-81.

[18] Ali S, Alvi MK, Faizullah S, et al. Detecting ddos attack on SDN due to vulnerabilities in openflow. IEEE 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), Al Madinah Al Munawwarah, Saudi Arabia; 2020: p. 1-6.

[19] Raza MS, Sheikh MNA, Hwang I, et al. Feature-selection-based DDOS attack detection using AI algorithms. Telecom 2024;5:333-46.

[20] AWS. What is a DDOS attack & how to protect your site against one [Internet]. Amazon Web Services, Inc. 2024 [cited 2024 Aug 6]; Available from https://aws.amazon.com/shield/ddos-attack-protection/

[21] D G. DDoS detection and prevention based on artificial intelligence techniques. Sci Bull Nav Acad 2019;22:134-43.

[22] Bortey L. How do you measure machine learning model accuracy after data preprocessing? [Internet]. Linkedin. 2023 [cited 2024 Aug 6]; Available from: https://www.linkedin.com/posts/loretta-bortey-b2517481_how-do-you-measure-machine-learning-model-activity-7095092695324311552-KtJM

[23] Islam U, Muhammad A, Mansoor R, et al. Detection of distributed denial of service (DDOS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustain 2022;14:8374.

[24] Noi PT, Kappas M. Comparison of random Forest, K-Nearest Neighbor, and Support vector machine classifiers for land cover classification using Sentinel-2 imagery. Sensors 2017;18:18.

[25] D G. DDoS detection and prevention based on artificial intelligence techniques. Sci Bull Nav Acad 2019;22:134-43.

[26] Zhang C, Liu C, Zhang X, et al. An up-to-date comparison of state-of-the-art classification algorithms. Expert Syst Appl 2017;82:128-50.