E-ISSN: 2707-6644
P-ISSN: 2707-6636
Impact Factor (RJIF): 5.43
www.computersciencejournals.com/ijcpdm
IJCPDM 2025; 6(2): 121-127
Received: 21-05-2025
Accepted: 24-06-2025

Deen Mohd
Department of Computer Science and Engineering, R D Engineering College, Ghaziabad, Uttar Pradesh, India

Mohd Vakil
Department of Computer Science and Engineering, R D Engineering College, Ghaziabad, Uttar Pradesh, India

Corresponding Author:
Deen Mohd
Department of Computer Science and Engineering, R D Engineering College, Ghaziabad, Uttar Pradesh, India

An overview of machine learning's uses in recognizing common network attacks

Deen Mohd and Mohd Vakil

DOI: https://www.doi.org/10.33545/27076636.2025.v6.i2a.120

Abstract
The number of intelligent devices has increased at an unprecedented rate over the last ten years, and the spread of intelligent machines has increased dramatically in recent years. In order to guarantee constant communication amongst networked IoT devices, computer networks are essential. Unfortunately, the significant rise in the usage of smart devices has opened the door for significant unethical behavior within networks. The primary network danger under investigation in this study is the "Low Rate/Slow Denial of Service (LDoS) attack," which seriously jeopardizes the integrity of the internet. Due to the fact that these assaults do not produce large amounts of bandwidth or abrupt increases in network activity, identifying their source is quite difficult. This study investigates the use of machine learning to improve the detection.

Keywords: LDoS attack, DDoS attack, anomaly detection, ML, RL, IDS, hyper parameter optimization

1. Introduction
A growing number of technologies are emerging in this era of digitalization, but they must successfully affect "privacy" and "security" safeguards. The "Internet of Things" (IoT) increases its susceptibility to abuse. There are several security flaws in the Internet of Things space that might compromise end-user data and services. In the world of cutting-edge technology, "Denial of Service (DoS)" or "Distributed Denial of Service (DDoS)" attacks are among the most common and significant security risks.
"Denial-of-service" (DoS) attacks are a type of malicious cyberattack tactic where the attacker attempts to permanently or temporarily disrupt the service of an internet-connected host in order to prevent the targeted users from accessing the resources. The target machine is flooded in order to do this.
There is an increasing number of smart gadgets connecting to the internet, but many of them lack basic security features, leaving the internet vulnerable to many types of assaults. These smart devices are susceptible to distributed denial-of-service assaults, which are coordinated by botnets like Mirai. As a result, A significant threat to essential internet infrastructure. For example, picture a living area that has over 10 smart gadgets in it. It is possible to use these devices to perform denial-of-service attacks against the internet.
This paper thoroughly examines "low-rate denial-of-service" attacks, which are the most common type of network assault (LDoS). A stealthy network attack known as a "slow or low DoS" attack aims to degrade network service quality while staying undetectable or concealed.

1.1 Importance of the study
Even if there are many security measures in place, we still live in an insecure period despite the fact that several techniques for identifying such a subtle assault have been proposed across a variety of domains and circumstances. When it comes to thwarting "LDoS" assaults, security procedures frequently fall short against security risks. It is crucial to have a system that supports robust security measures that can manage unpredictable network traffic and increasingly dynamic types of assaults.
The following is the outline for the remainder of the paper. The forms of low-rate DoS attacks are covered in Section 2. Section 3 discusses machine learning in relation to cyber security.

Section 4 clarifies related work. Methodology: ML-based detection techniques is covered in Section 5. The study's results and comments are presented in Section 6. Section 7 discusses challenges. Research work is concluded with future directions in Section 8.

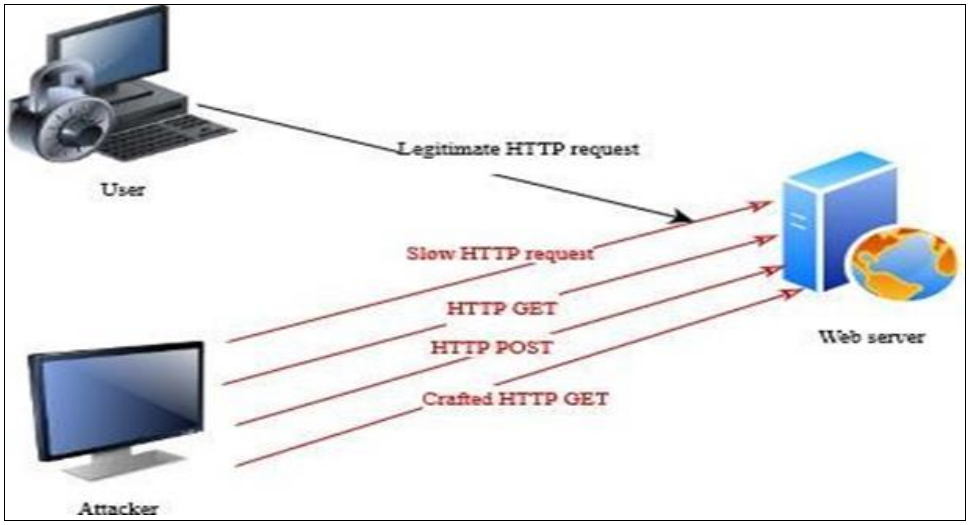

Fig 1: Low-rate DoS attack Scenario

2. Low rate DoS attacks: The term "low-rate denial of service (LDoS)" refers to an attack technique designed to interfere with or take down a target system by using techniques that gradually deplete its resources over a lengthy period of time, making it difficult to detect and counteract. Unlike classic DDoS assaults, which often include large volume and obvious patterns, LDoS attacks stream traffic slowly and persistently. A possible LDoS assault scenario is shown in Figure 1. These attacks frequently take advantage of holes in the target's protocols or resources, which enables the attacker to gradually deplete system resources.

There are large numbers of data packets in traditional ‘denial- The branch of artificial intelligence called "machine learning" tries to create models and algorithms, or "classifiers," that allow computers to learn and make decisions on their own without the need for human input. It is not necessary to use explicit programming. These days, machine learning has many applications. It is important for a number of computer network elements. A variety of machine learning applications in the field of cyber security are shown in Figure 2.

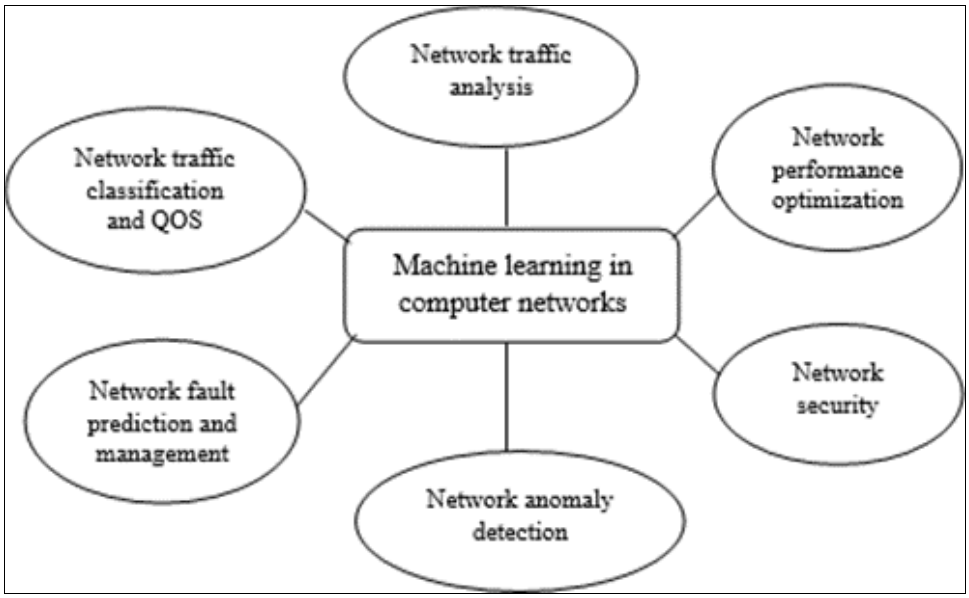

Fig 2: Applications of machine learning within the realm of cyber security

Malicious traffic in intrusion detection systems (IDS) can be identified using machine learning techniques. An algorithm known as the machine learning classifier identifies patterns in the given data and categories the data according to these patterns. An ML classifier or model is trained with a dataset (a wide range of assaults) in Intrusion Detection Systems (IDS), and the model is tested with of-service’ attacks, resulting in anomalies within the network traffic to detect DoS-related traffic. Conversely, LDoS attacks sustain consistently low average rates. and are intricately mixed within the network data stream. This leads to a reduction in the average network traffic, and attackers no longer require

a sustained high attack rate. Instead, they frequently employ short bursts of traffic when targeting their victims [1]. The average packet rate during these bursts closely resembles 10-20% of the usual data traffic, which is relatively low, making it difficult to distinguish from regular network activity. This complicates the differentiation between LDoS flows and regular data flows [2]. Its extended incubation period substantially reduces the throughput of its victims. Therefore, it is imperative to urgently devise novel methods and effective strategies for detecting and safeguarding against LDoS attacks [3].

3. Machine Learning in Cyber security

Table 1 shows different types of 'LDoS' attacks and attack target. Method of exploiting an attack is specified for each type of attack.

Table 1: Types of LDoS attacks

S.No	Attack type	Target	Method
1	Slow read attack	Servers	Sending requests that are intentionally slow to read
2	RUDY	HTTP/H TTPs protocol s	Send HTTP requests with very slow payload, keeping connections open for extended periods and consuming server resources over time.
3	Slowloris	HTTP server	Send data slowly and consume server resources.
4	HULK	Web applications	Send many HTTP GET/POST requests and keep the server busy.
5	Apache killer	Apache web servers	Crafted HTTP GET request with long-range headers and a server consumes more memory.
6	Hash collision attack	SSL/ TLS or DNS	Exploits hash collision vulnerabilities in various protocols and sends crafted inputs that generate many hash collisions.
7	Applicatio n layer protocol attacks	TCP,UDP or DNS	Exploits vulnerabilities in the protocols.

Table 2: Literature review on LDoS attack

Ref	Approach/Algorithm	Dataset	Area for Improvement
[3]	Feature-based, XGBoost (Supervised)	Abilene	May result in high false negative rate. Alternative classifiers (SVM, J48, RF, Random Tree) may improve performance.
[6]	Anomaly-based, REP Tree, Multi-layer Perceptron (SVM-derived features)	CIC DoS 2017	May result in high false positive rate. Incorporating additional features may reduce false alarms.
[10]	Feature-based, OFA (Unsupervised), SVM for model training & extraction	Simulated in NS2; Testbed	Model produces more accurate results with up-to-date datasets.
[12]	Feature-based, SVM	Simulated in NS2	Demonstration with other algorithms and multi-level classification can provide more accurate results.
[14]	Feature-based, Adaboost (Classification)	-	Demonstration with recent real-time datasets is essential for enhancing detection accuracy.
[7]	Deep Learning, FFCNN	CIC DoS 2017 & CIC IDS 2017; Testbed	Requires evaluation with recent real-time datasets to deal with dynamic & evolving attacks.
[8]	Deep Learning, Time-frequency analysis	NS-3	Advisable to explore alternative evaluation metrics and test model effectiveness using real-time datasets.
[5]	Deep Learning + HPO	Sailfish	Other optimization algorithms may further reduce false positive rate. Multiclass classification could enhance accuracy.
[11]	Hybrid, ML (Traffic analysis) + Data Mining	Public datasets	IDS should not rely solely on AI; trade-off exists between detection accuracy and speed. Needs more efficient proactive mechanism for dynamic LDoS attacks.
[13]	Hybrid, AI + Traditional (SVM)	KDD99	Detection accuracy vs. detection speed trade-off persists. Requires efficient mechanisms for dynamic attacks.
[15]	Traditional, Mathematical model	-	Infeasible to implement in IoT due to resource constraints.

4. Methodology: ML based detection approaches

Among many defense methods proposed for detecting LDoS attacks, machine learning-based methods address challenges posed by such a predominant network attack. It has significant usage in cyber security. AI-driven attack detection methods can be categorized as "signature-based" or "anomaly-based" [6]. In the "signature-based" technique, the known attacks' signature is compared with incoming network flow to identify malicious network flow. Harun *et al*. [7] "In the anomaly- based approach, the incoming network flow is contrasted with a benign flow of the model. If the flow's attributes deviate from those of the benign flow, it is categorized as malicious." The detection of 'LDoS' attacks can be categorized into two main approaches: feature-based detection and time-frequency domain detection [8]. Feature-based 'low denial of service attack detection' identifies and analyzes specific features or patterns in the traffic data to detect and mitigate slow DoS attacks. Time-frequency domain detection of LDoS attacks involves the examination of traffic data in both the time and frequency domains to detect the existence of 'low-rate DoS attacks.' This method offers a more in-depth insight into the attack attributes by capturing the time-dependent frequency aspects of network traffic [9]. These are low DoS attack

detection categories used by researchers, and these techniques may have the following drawbacks.

a) The present research has a conflict between detection rate and detection accuracy. Therefore, detection accuracy might compromise the detection rate.
b) Intensive requirement of resources
c) High false positive rate(FPR) and High false negative rate (FNR)
d) Lack of proactive and adaptive characteristics
e) Lack of detection methods for more dynamic and diverse LDoS attacks
f) Time complexity
g) Research gap between dataset and new vulnerabilities
h) Overfitting and underfitting of data

5. Results and Discussion

Machine learning classifiers are widely used in research for "anomaly detection." The selection of an appropriate dataset is an essential step in this intrusion detection research. In this survey, two different datasets are considered, and its importance and insights are observed.

5.1 Detection of 'DDoS attacks' using NSL-KDD dataset (Machine learning classifiers)

The dataset contains 42 different features. The features are extracted according to 3 different attack types. First, "TCP Syn attack" the features extracted are, "service, src_bytes, wrong_fragment, count, num_ compromised, srv_count, srv_serror_rate, serror_rate" Second, "ICMP attack" the features extracted are, "duration, src_bytes, wrong_fragment, count, urgent, num_compromised, srv_count" Third, "UDP attack" the features extracted are, "service, src_bytes, dst_bytes, wrong_fragment, count, num_compromised, srv_count, dst_host_srv_count, dst_host_diff_srv_rate" The following observations are made from Figure 3. Observation 1: The detection accuracy of UDP flood attacks is low, whereas TCP and ICMP attack detection accuracy is almost 100%.

- **Observation 2:** False alarm (FPR) is generally very high in network anomaly detection systems.
- **Observation 3:** The false positive rate (FPR) is relatively higher for UDP attacks than the other two.

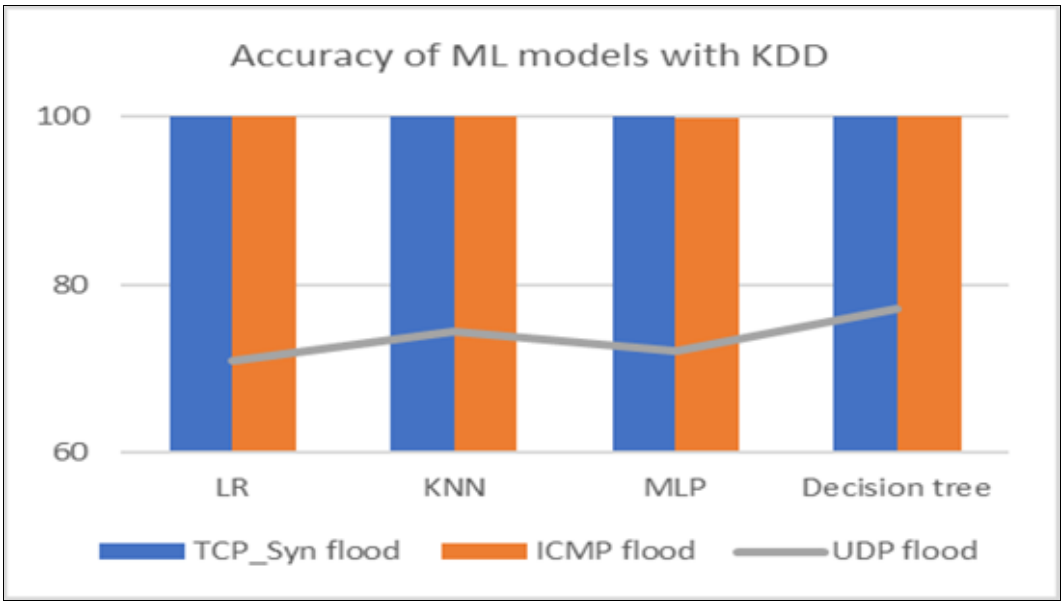

Fig 3: Accuracy of models for different attack flows

Table 3 illustrates the confusion matrix representation for the UDP flood attack. The false positive rate is high for LR, MLP, and DT. Three out of four classifiers produce high FPR.

Table 3: Confusion matrix for UDP attack

Confusion Matrix for LR: [[2852 2005] [3192835]]	Confusion Matrix for KNN: [[4046811] [12371917]]
Confusion Matrix for MLP: [[2674 2183] [513103	Confusion Matrix for DT: [[3834 1023] [8012353]]

5.2 Detection of 'DDoS attacks' using NSL-KDD dataset (Reinforcement Learning)

The dataset contains 42 features, all used by the RL system as an environment. Figure 4 shows the performance in terms of reward and loss in the RL model. Each episode in the RL model records the agent's states and actions from the start to the end state. Reward is something that an RL agent receives from its environment for its action (prediction). Loss is the difference (error) between predicted and actual values. Increasing the number of episodes leads to greater rewards and diminished losses.

Observation: When the number of episodes is less (say, episode=2 or 5), the RL system clearly shows a spike in the loss signal and a drop in the reward signal.

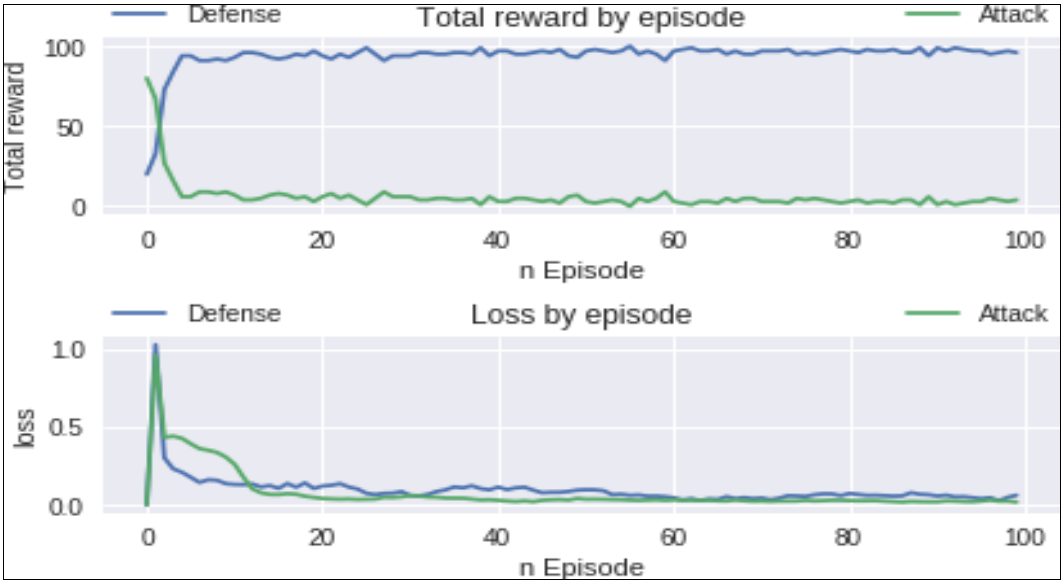

Fig 4: Performance of RL model in terms of reward & loss

5.3 Multiclass classification of network traffic (SDN dataset)

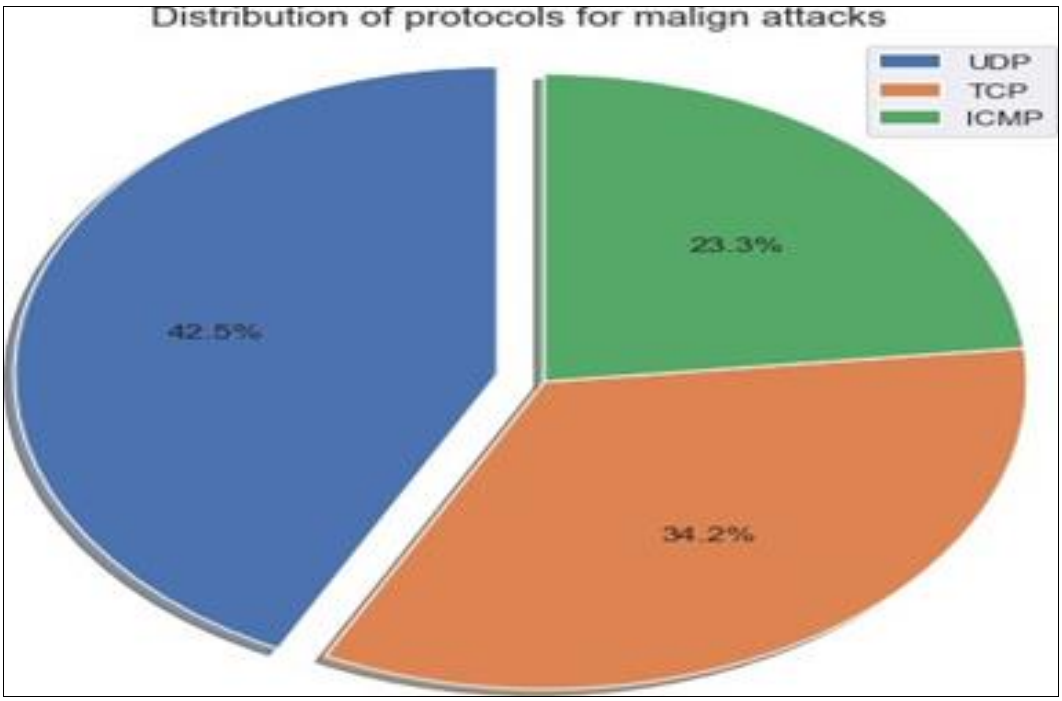

Fig 5: Distribution statistics of protocols for malicious activity

SDN-specific (generated) datasets have been used for multi-class classification of network traffic data. There are 23 features in the dataset. All the features were considered and grouped into numerical, categorical, discrete-numerical, and continuous.

Figure 5 shows the protocol distribution statistics for malicious activity in the network. In the statistics, UDP attack flows are relatively high. When the statistics in Figure 5 and the performance in Figure 3 are compared, identification of "DDoS attacks" exploited through UDP flood is challenging.

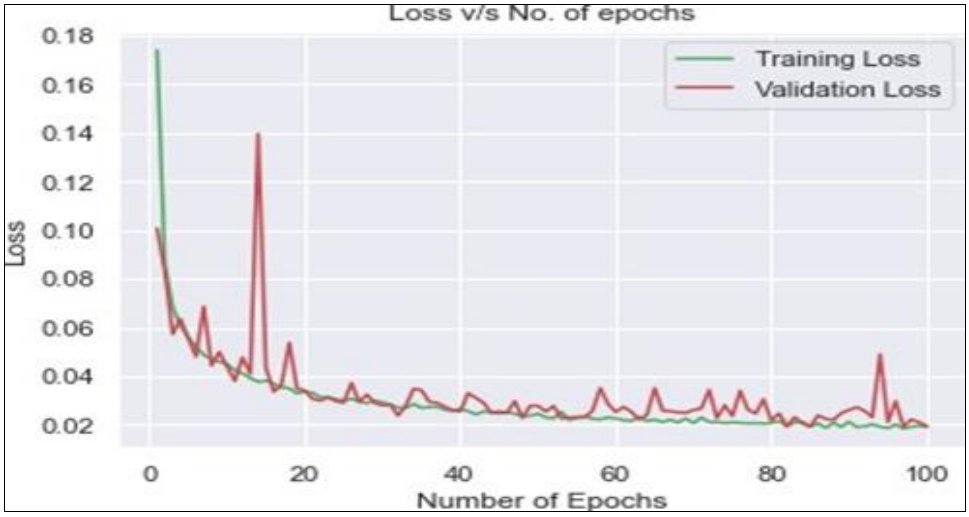

Fig 6: Performance of ML model based on epoch count & Loss

Figure 6 and Figure 7 show the performance of the ML model in terms of accuracy and loss. Epoch refers to the passing of training data through an algorithm. Each pass represents an epoch. Loss is high if there are few epochs, and accuracy increases with a hike in epochs.

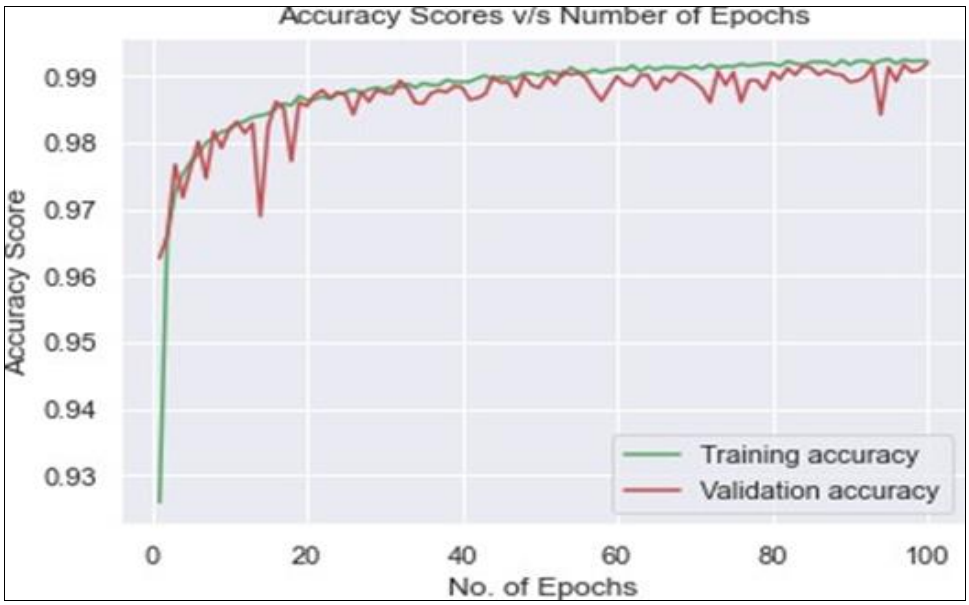

Fig 7: Performance of ML model based on epoch count & Accuracy

Observation 1: Increasing the number of passes or epochs typically leads to better outcomes and enhanced performance. Observation 2: There is an observed stability in training loss and training accuracy, whereas validation loss and accuracy experienced a sudden minor fluctuation.

6. Conclusion

The study examined the identification of slow Denial of Service (DoS) attacks using both conventional and machine learning methods. Various attack detection methods were explored, including those rooted in machine learning, deep learning, anomaly detection, and traditional techniques. Limitations in these approaches were documented. Specifically, the current binary classification methods lead to a significant number of false alarms. Furthermore, integrating reinforcement learning into hybrid approaches can greatly improve the model's effectiveness, resulting in a robust Intrusion Detection and Prevention System (IDPS) capable of effectively mitigating a broader spectrum of complex and diverse attacks.

6.1 Future scope

Reinforcement Learning (RL): Identifying 'low-rate denial-of-service (LDoS)' attacks usually entails dealing with subtle and gradual attack patterns that can readily circumvent conventional detection techniques. However, the attack can be effectively identified using Reinforcement Learning (RL) algorithms that still need to be focused in the research. In reinforcement learning (RL), the agent learns from feedback in terms of reward or punishment and adapts their behavior to maximize rewards in complex and dynamic environments. Since these RL models can be applied to complex and dynamic problems, it is most appropriate to use them to mitigate "LDoS attacks."

Research towards a vital model variable is ongoing. These variables are external to a machine learning model and are not learning from the data during the model is trained. It has

a significant role in determining its ability to learn and generalize from the data. With these characteristics, the detection rate of such dynamic attacks can be improvised. Either of methods may develop a hybrid model,

1. Through investigating such external parameters using reinforcement learning.
2. Combining reinforcement learning and a feature-based method. Some feature-based methods are traffic analysis, protocol-specific analysis, and resource utilization monitoring.

References

1. Tang D, Gao C, Li X, Liang W, Xiao S, Yang Q. A detection and mitigation scheme of LDoS attacks via SDN based on the FSS-RSR algorithm. IEEE Trans Netw Sci Eng. 2023;10(4):1952-1963. doi:10.1109/TNSE.2023.3236970.
2. Zhan S, Tang D, Man J, Dai R, Wang X. Low-rate DoS attacks detection based on MAF-ADM. Sensors. 2020;20(1):189. doi:10.3390/s20010189.
3. Liu L, Yin Y, Wu Z, Pan Q, Yue M. LDoS attack detection method based on traffic classification prediction. IET Inf Secur. 2022;16(2):86-96. doi:10.1049/ise2.12046.
4. Wu Z, Li W, Liu L, Yue M. Low-rate DoS attacks, detection, defense and challenges: a survey. IEEE Access. 2020;8:43920-43943. doi:10.1109/ACCESS.2020.2976609.
5. Sun W, Guan S, Wang P, Wu Q. A hybrid deep learning model based low-rate DoS attack detection method for software defined network. Emerg Telecommun Technol. 2022;33(5):e4443. doi:10.1002/ett.4443.
6. Ilango HS, Ma M, Su R. A feedforward-convolutional neural network to detect low-rate DoS in IoT. Eng Appl Artif Intell. 2022;114:105059. doi:10.1016/j.engappai.2022.105059.
7. Ilango HS, Ma M, Su R. Low rate DoS attack detection in IoT-SDN using deep learning. In: IEEE Int Conf iThings-GreenCom-CPSCom-SmartData-Cybermatics; 2022; Australia. doi:10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00031.
8. Liu Y, Sun D, Zhang R, Li W. A method for detecting LDoS attacks in SDWSN based on compressed Hilbert-Huang transform and convolutional neural networks. Sensors. 2023;23(10):4745. doi:10.3390/s23104745.
9. Tang D, Wang S, Liu B, Jin W, Zhang J. GASF-IPP: detection and mitigation of LDoS attack in SDN. IEEE Trans Serv Comput. 2023;1-12. doi:10.1109/TSC.2023.3266757.
10. Li X, Zheng K, Tang D, Qin Z, Zheng Z, Zhang S. LDoS attack detection based on ASNNC-OFA algorithm. In: IEEE Wireless Commun Netw Conf (WCNC); 2021; China. doi:10.1109/WCNC49053.2021.9417400.
11. Tang D, Chen J, Wang X, Zhang S, Yan Y. A new detection method for LDoS attacks based on data mining. Future Gener Comput Syst. 2022;128:73-87. doi:10.1016/j.future.2021.09.039.
12. Shi W, Tang D, Zhan S, Qin Z, Wang X. An approach for detecting LDoS attack based on cloud model. Front Comput Sci. 2022;16:166821. doi:10.1007/s11704-022-0486-1.
13. Zhang N, Jaafar F, Malik Y. Low-rate DoS attack detection using PSD based entropy and machine learning. In: 6th IEEE Int Conf Cyber Secur Cloud Comput (CSCloud/EdgeCom); 2019; Paris, France. p.59-62. doi:10.1109/CSCloud/EdgeCom.2019.00020.
14. Tang D, Tang L, Dai R, Chen J, Li X, Rodrigues JJPC. MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost. Future Gener Comput Syst. 2020;106:347-359. doi:10.1016/j.future.2019.12.034.
15. Luo J, Yang X, Wang J, Xu J, Sun J, Long K. On a mathematical model for low-rate shrew. IEEE Trans Inf Forensics Secur. 2014;9(7):1069-1083. doi:10.1109/TIFS.2014.2320635.
16. Chauhan S, Singh D, Singh AK. Artificial intelligence in the military: an overview of the capabilities, applications, and challenges. J Surv Fish Sci. 2022;9(2):984-91. doi:10.53555/sfs.v9i2.2911.
17. Kiran, Singh D, Goyal N. Analysis of how digital marketing affect by voice search. J Surv Fish Sci. 2023;30(2):407-12. doi:10.53555/sfs.v10i3.2890.
18. Tyagi Y, Singh D, Singh R, Dawra S. Analysis of the most recent Trojans on the Android operating system. Educ Adm Theory Pract. 2024;30(2):1320-1327. doi:10.53555/kuey.v30i2.6846.
19. Singh S, Singh D, Chauhan R. Manufacturing industry: a sustainability perspective on cloud and edge computing. J Surv Fish Sci. 2023;10(2):1592-1598. doi:10.53555/sfs.v10i2.2889.