Detection and Mitigation of DDOS Attack Using Deep Learning

Imran Mir

ABSTRACT: Attacks known as distributed denial of service (DDoS) are becoming more and more dangerous for organisations and governments. They hurt company branding, restrict access to information and services, and hurt online companies. Because they mimic real users, attackers deploy application layer DDoS attacks, which are difficult to identify. We analyse incoming packet characteristics such as the size of HTTP frame packets, the number of conveyed Internet Protocol (IP) addresses, the number of constant port mappings, and the number of IP addresses employing proxy IP in order to combat unique application layer DDoS attacks in this work. Using standard datasets, the CTU-13 dataset, real weblogs (dataset) from our organisation, and experimentally constructed datasets from DDoS attack tools, we examined client behaviour in public attacks. Metrics-based attack detection is assessed using a deep learning method called a multilayer perceptron (MLP). The suggested MLP classification system has a 98.99% detection efficiency for DDoS attacks, according to simulation findings. When compared to traditional classifiers, our suggested technique's performance yielded the lowest proportion of false positives—2.11%.

Keywords — *DDoS attack; attack; attack detection; botnet; MLP classifier*

1. INTRODUCTION

Information security is becoming absolutely necessary in today's fast-paced environment, where the number of internet-connected devices is growing and online applications are growing at a rapid pace. 1.2 billion websites have been created since the World Wide Web's inception [1], and a vast array of online applications, including those for e-commerce, online banking, online shopping, online education, e-healthcare, and industrial control systems (ICS) for critical infrastructure, have been integrated with various web services. Cybercriminals of days are extremely knowledgeable and prepared to launch successful attacks on organisations and governmental institutions [2]. Today, cybercrime is a lucrative industry with massive amounts of stolen data. Malware can be divided into a wide variety of categories [3]. Global governments, corporations, and consumers are all at grave risk from this. We don't have to go far back in history to recall the major bank attack in Bangladesh that resulted in the reported theft of USD 81 million. The fact that the bank's own systems were utilised to move substantial amounts of money serves as a constant reminder of how successful these attacks can be. No matter how big, no firm is secure. According to statistics, 20% of impacted companies are classified as small firms, 33% as SMEs, and 41% as major businesses. The need to recognise the problems and safeguard sensitive data increases with the extent of the threat. At least one or more attacks including the theft of data and its use to impair the victim's services have affected 82% of organisations. 26 percent of the impacted organisations reported a decline in service performance as a result of DDoS assaults, and 41 percent reported a service outage [3]. A scene with DDoS assaults is depicted in Fig 1.

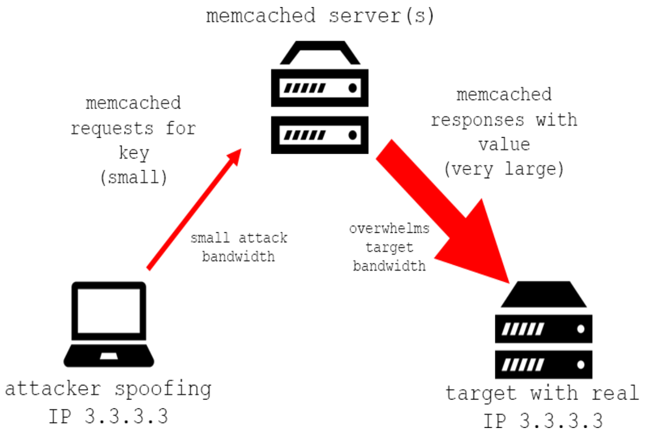

memcached server(s)
memcached requests for key (small)
memcached responses with value (very large)
small attack bandwidth
overwhelms target bandwidth
attacker spoofing IP 3.3.3.3
target with real IP 3.3.3.3

Fig.1 environment of DDoS attack

Information servers, internet servers, and cloud computing servers are all severely impacted by denial-of-service attacks [10,11]. Among the most common threats are botnets, DDoS, hacking, malware, pharming, phishing, ransomware, spam, spoofing, and spyware [12]. A cyberattack poses the greatest risk to any and all firms globally, according to IBM CEO Ginni Rometty. Cybercriminals are on the rise as a result [9]. Cybercriminals employ a variety of hacking techniques to compromise client servers. DDoS attacks are quite widespread and can happen in between other cyberattacks; it might be challenging to identify them. The three primary categories of DDoS assaults are explained here.

1.1. Volume Based DDoS Attack:

DDoS assaults based on volume involve the use of fictitious packet floods, including UDP and ICMP floods, among others. This attack aims to utilise the whole bandwidth, which is expressed in bits per second (bps), on the target site. Figure 2 displays a number of well-known DDoS attack methods.

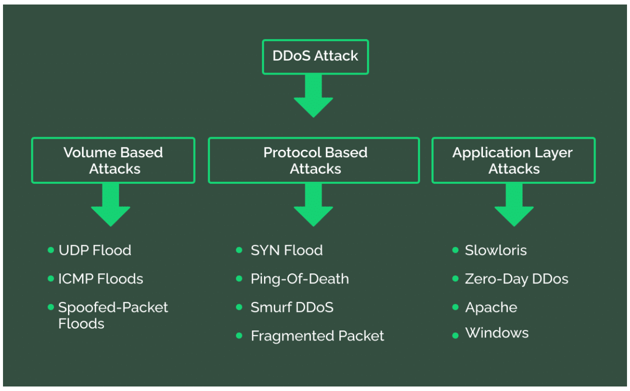


Fig.2 Typical DDoS attack types

1.2 Protocol Based DDoS Attack:

SYN floods, fragmented pack attacks, ping of death, smurf DDoS, and other attacks are examples of protocol-based DDoS attacks. The unit of measurement for attacks is packets per second (pps). These assaults make use of the resources of actual servers as well as firewalls and load balancers, which are central communications devices.

1.3. TCP/IP Layer Based DDoS Attack:

GET/POST floods, low- and slow-speed attacks, possible Windows or Open BSD attacks, Apache-driven attacks, and more are examples of TCP/IP layer-based DDoS attacks. These attacks, which look to be harmless and genuine programmes, are directed towards the web server.

Requests per second are used to quantify the scope. Both the volume of related traffic and the number of attacks are steadily rising. Attack traffic needs to be filtered as close to the attack sources as feasible since at this level of traffic intensity, the network infrastructure upstream of the targeted victim is also negatively impacted. Nevertheless, as attacks originate from widely dispersed nodes and propagate across numerous sites, it is challenging to anticipate and detect such nodes. The mitigation solution must identify malicious traffic and react with the least amount of disturbance to genuine traffic in order to successfully respond by disrupting traffic. A fresh attack known as an escalating DDoS attack and a proxy DDoS attack is launched by the attacker. In order to address this issue, we create a detecting method. Deep learning techniques are employed by the detection algorithm to identify malicious traffic and distinguish it from normal traffic. Three types are identified by the algorithm: (1) regular traffic; (2) suspicious traffic; and (3) malicious traffic.

Below is a summary of this study's primary contributions.

1. To combat the unique application layer DDoS attack, we examined the features of incoming data packets, such as the size of HTTP frame packets, the quantity of IP addresses transmitted, the consistent port mappings, and the quantity of IP addresses utilising proxy IP.

2. Using both experimentally generated datasets from DDoS attack tools and normal datasets, we examined the client's actions during public attacks.

3. To assess the efficacy of attack detection based on metrics, the multilayer perceptron (MLP) deep learning classification technique is presented.

4. When we compared our suggested MLP classification model to other models and traditional classifiers like Naïve Bayes, it produced the fewest false positives.

This is how the rest of the article is structured. The literature review is briefly described in Section 2, and the problem rationale is covered in Section 3. Section 4 presents the research technique and chart flow. Section 5 provides a brief description of the suggested attack categorization model, while Section 6 elaborates on the simulation results. Section 7 brings this study to a close and outlines future research.

2. LITERATURE REVIEW

The scientific community uses machine learning algorithms extensively in all facets of life. Machine learning algorithms find widespread applications in fields such as image processing, robotics, forecasting, recommendation systems, healthcare, banking, defence, and education [1]. A subset of machine learning is called deep learning. In this work, we have employed the multilayer perceptron (MLP), a deep learning technique, to detect DDoS attacks in an effective and efficient manner. The most recent research on DDoS attack detection is compiled here.

The authors of [2] suggested looking into how attackers' tactics, like message-delayed and message-dropped attacks, affect MANET execution of MITM attacks. This work's output demonstrates how these attacks severely affect legal entities in MANETs by increasing the quantity of compromised messages, E2ED, and PLD in the network. And last, this plan will prevent MITM attacks that eavesdrop on legitimate nodes' communications by employing symmetry or asymmetry cryptographies.

In order to detect attacks and irregularities in the Internet of Things system, the authors of [5] emphasised how crucial it is to create an intrusion detection system. They have examined the most recent DDOS assault detection techniques in this work and have likewise determined that they are inadequate. They have suggested an ideal approach based on deep learning technology to get beyond that restriction and will be able to identify both zero-day and active distributed denial of service threats.

With the innovative use of the Morphological Fractal Dimension (MFD) to this problem, the authors of [8] suggest an online method built on a sliding window. Compared to entropy-based methods, the study's findings demonstrate that using MFD to the most recent CICIDS2017 public data set can significantly enhance DDoS attack detection. This research also suggests a new approach for automatically defining the sliding window size. This work presents the effects of several hyper-parameters, such as those found in the MFD definition, and evaluates the distance measures, with the Chebyschev distance offering the best detection accuracy. The outcomes provide a 99.30% detection accuracy, outperforming comparable methods on the same dataset.

In order to properly handle cybersecurity management in SDN architectures, the authors of [11] investigated the potential of AI and ML algorithms to carry out automated DDoS Attacks Detection (DAD), with a focus on Transmission Control Protocol SYN flood attacks. The two DAD architectures that are compared in this study are Standalone and Correlated DAD. In Standalone DAD, traffic features are collected locally at network switches, whereas in Correlated DAD, attack detection is done within a single entity (such as an SDN controller). and finally integrate P4-enabled data planes with ML capabilities to provide real-time DAD. In the majority of scenarios, all examined machine learning algorithms exhibit accuracy, precision, recall, and F1-scores above 98%, while the worst-case classification time is only a few hundred milliseconds. These are demonstrated by illustrative numerical data. When features are extracted at the data plane using the P4 language, a significant reduction in latency is achieved when considering real-time DAD implementation.

Although the authors of [12] suggested a method for detecting DDoS attacks, it is still very difficult to quickly diagnose these attacks using feature selection algorithms. By using feature selection techniques on machine learning classifiers, the suggested approach employs a hybrid methodology for feature selection. For the purpose of early DDoS attack detection on Internet of Things devices, four classifiers—Random Forest, Decision Tree, k-Nearest Neighbours, and XGBoost—have been subjected to feature selection techniques, specifically chi-square, Extra Tree, and ANOVA. We train and evaluate the suggested methodology in a cloud-based environment (Google Colab) using the CICDDoS2019 dataset, which contains comprehensive DDoS attacks. Based on the experimental findings, the suggested hybrid technique assists in the early detection of DDoS assaults on IoT devices and offers superior performance with a feature reduction ratio of 82.5% by reaching 98.34% accuracy with ANOVA for XGBoost.

writers of [15] It is crucial to identify the type of DDoS attack that has been launched against the targeted network or system before focusing on appropriately defending it. This study presents several ensemble classification methods that integrate several algorithms' performances. Then, using accuracy, F1 scores, and ROC curves, they are compared against the state-of-the-art Machine Learning Algorithms to see how well they recognise various DDoS assault types. The outcomes demonstrate good performance and high precision.

The authors of [17] used a cutting-edge SDN model and a novel technique called State Sec. for DDoS detection and mitigation. As seen in Fig. 3, they illustrated the advantages of this kind of approach.

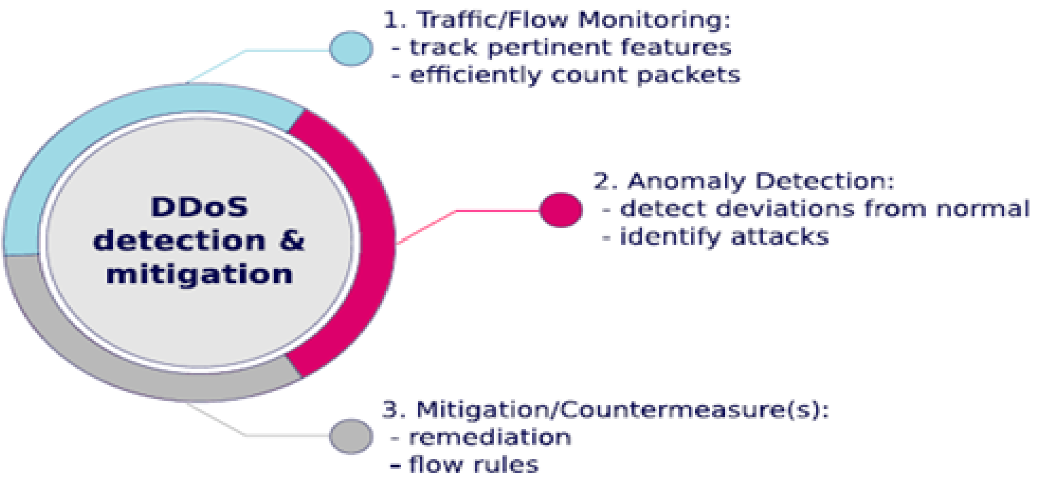

1. Traffic/Flow Monitoring:
- track pertinent features
- efficiently count packets
DDoS detection & mitigation
2. Anomaly Detection:
- detect deviations from normal
- identify attacks
3. Mitigation/Countermeasure(s):
- remediation
- flow rules

Fig 3. Crucial procedures for software-defined networking's DDoS mitigation and detection.

3. MOTIVATION

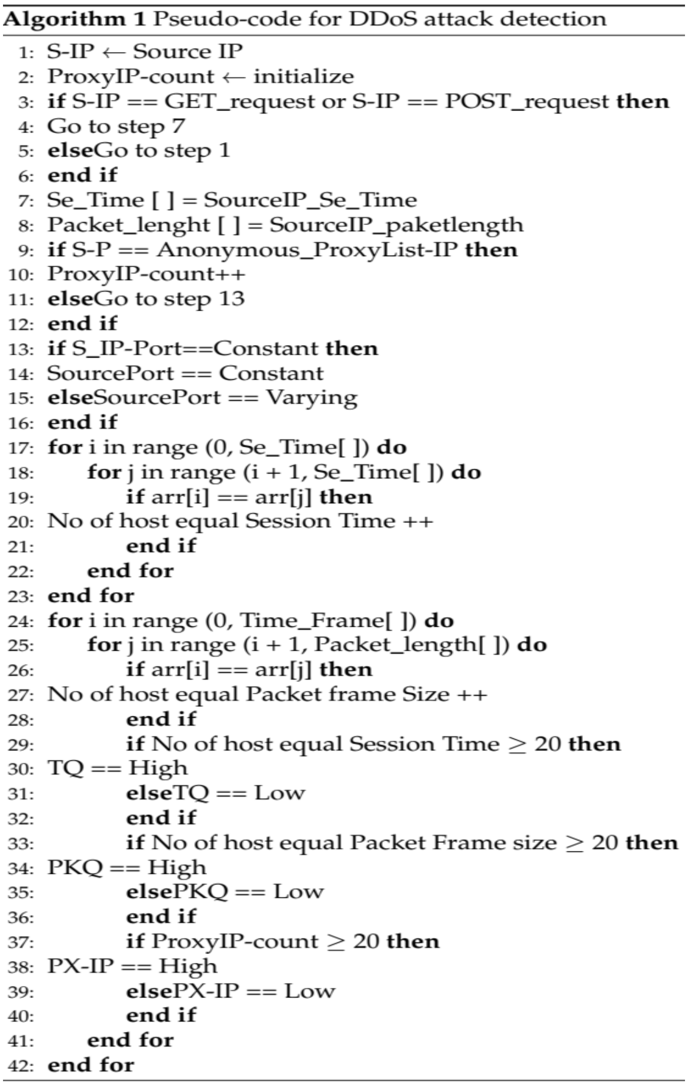
DDoS mitigation is essential as a protective layer for edge-running organisations that cannot afford to experience any interruption in their mission-critical operations. DDoS mitigation helps to ensure the continuous availability of these kinds of operations and services. SDN makes it possible to plan, build, and run networks. Distributed denial-of-service (DDoS) attacks pose a significant risk to data centres. SDN networks are regularly the target of new security threats and attacks, particularly Distributed Denial of Service (DDoS) attacks.

We have found a gap in the current study while examining the aforementioned studies. The demand for both present-day and emerging technologies is rising. According to the literature study, a number of academics have studied DDoS attacks; however, they have mostly only studied one or two kinds of attacks, ignoring the others. Increasing DDoS attack strategy and Proxies DDoS attack strategy are the two main DDoS attacks that must be tackled concurrently. All of this will assist us in creating algorithms that are safe enough to thwart attackers' attempts to compromise them and prevent services from becoming unavailable.

4. METHODOLOGY

Algorithm 1 displays our suggested DDoS attack categorization methodology (MLP classifier) algorithm. Figure 6 displays the proposed system's flowchart. The primary HTTP functions, such as GET and POST, are examined in relation to other methods, such as TRACE, HEAD, DELETE, CONNECT, OPTIONS, and PUT. There should be no more than 15–20 HTTP GET and POST requests per IP address from regular, reputable clients. When bots grow smarter, they start to behave like people. The same bots typically make the same HTTP request, spend the same amount of time, send the same packet frame size, and employ escalating DDoS attack techniques in order to accomplish their objectives. Within 160 seconds, the number of HTTP GET and POST request durations and packet sizes are recorded using Algorithm 1. The following feature says that the IP address count is counted and compared to the anonymous proxy server's IP address list. The fraudulent user has used proxy servers to execute several DDoS attacks in an attempt to obscure or reverse the progress of his bots, whereas genuine users often use their real IP address to access the URL. The malicious user has used many bots to access the web server. When a cooperative bot reaches a particular destination port number, it opens a different port and sends a lot of requests to the victim's web server. There are extended stretches of time when no port connections are closed. Generally, a valid client opens ports, sends information, and then closes the connections. It was noted that genuine clients' port numbers hardly ever changed. On the other hand, malicious machines often have distinct port numbers that increase in sequence. The initial value of the source port number was generated randomly. It has also been observed that a lot of DDoS attack software start their source port numbers with an arbitrary number. The following port number is just one digit higher than the previous one. A reliable mapping to the port numbers of the destination server is established. A bot's or its master's head character naturally allows for the usage of multiple bots to form a bot network. To shut down a web server, a lot of vendor bots use different kinds of modifying codes. It is well knowledge that a client-side bot executes its code for a predetermined amount of time and log size.

5. PROPOSED CLASSIFICATION MODEL



Algorithm 1 Pseudo-code for DDoS attack detection

```
 1: S-IP ← Source IP
 2: ProxyIP-count ← initialize
 3: if S-IP == GET_request or S-IP == POST_request then
 4: Go to step 7
 5: elseGo to step 1
 6: end if
 7: Se_Time [ ] = SourceIP_Se_Time
 8: Packet_lenght [ ] = SourceIP_paketlength
 9: if S-P == Anonymous_ProxyList-IP then
10: ProxyIP-count++
11: elseGo to step 13
12: end if
13: if S_IP-Port==Constant then
14: SourcePort == Constant
15: elseSourcePort == Varying
16: end if
17: for i in range (0, Se_Time[ ]) do
18:     for j in range (i + 1, Se_Time[ ]) do
19:         if arr[i] == arr[j] then
20: No of host equal Session Time ++
21:         end if
22:     end for
23: end for
24: for i in range (0, Time_Frame[ ]) do
25:     for j in range (i + 1, Packet_length[ ]) do
26:         if arr[i] == arr[j] then
27: No of host equal Packet frame Size ++
28:         end if
29:         if No of host equal Session Time ≥ 20 then
30: TQ == High
31:         elseTQ == Low
32:         end if
33:         if No of host equal Packet Frame size ≥ 20 then
34: PKQ == High
35:         elsePKQ == Low
36:         end if
37:         if ProxyIP-count ≥ 20 then
38: PX-IP == High
39:         elsePX-IP == Low
40:         end if
41:     end for
42: end for
```

6. EXPERIMENTAL EVALUATION

We compute metrics like accuracy, false positive rate (FPR), and false negative rate (FNR) in this study. Models are assessed in relation to these criteria.

6.1 Evaluation Criteria

6.1.1. Accuracy

correctness is one of the evaluation factors that establishes the overall correctness of the model. Overall accuracy is the proportion of all samples that the classifier successfully classifies. Calculating accuracy can be done using equation (1).

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

A true positive (TP) observation is one that is both expected to be good and is positive in reality. An observation that is predicted to be negative and is actually negative is called a true negative (TN). Observations that were predicted to be positive but turned out to be negative are known as false positives (FP). Observations that are predicted to be negative but turn out to be positive are known as false negatives (FN).

6.1.2. Receiver Operating Characteristic (ROC) Curve

A graph called a ROC curve shows how well a classification model performs at each categorization level. It stands for the true-positive rate (TRP) and the false-positive rate (FPR), two measurements. Since the TPR, also known as sensitivity, is a stand-in for the recovery rate, it is given in Equation (2).

$$TPR = \frac{TP}{TP + FN}$$

(2)

Equation (3) can be used to express FPR or specificity.

$$FPR = \frac{FP}{FP + TN}$$

(3)

Plotting TPR vs FPR at various categorization criteria is done using the ROC. More items are identified as positive at a lower classification threshold, which raises the FPR and TPR.

6.2 Dataset

The entire dataset has been split up into three data sets: a training set (70%), a test set (15%), and a verification set (15%). The network efficiency is measured using the verification set, and training is stopped using standard stopping criteria. Since the test set has no effect on training, it offers a separate gauge of network performance. Our suggested model is trained using the training set. The 37th round of the training phase yields the best verification performance, and it is at this point that the network is configured. Table 5's evaluation of the test input yields the corresponding values for the given mistakes.

Table 1. Assessment of the test data.

Parameter(s)	**Train**		**Validation**		**Test**		**Best**	
	X	**Y**	**X**	**Y**	**X**	**Y**	**X**	**Y**
Min	0	2.969×10^{-7}	0	2.856×10^{-7}	0	2.78×10^{-7}	0	9×10^{-8}
Max	40	0.712	40	0.6377	40	0.6668	40	1.1
Mean	20	0.03123	20	0.02871	20	0.02995	NaN	NaN
Median	20	7.524×10^{-5}	20	7.166×10^{-5}	20	7.222×10^{-5}	NaN	NaN
Mode	0	2.969×10^{-7}	0	2.856×10^{-7}	0	2.78×10^{-7}	40	2.856×10^{-7}
Std	11.98	0.1157	11.98	0.1044	11.98	0.1092	NaN	NaN
Range	40	0.712	40	0.6377	40	0.6668	40	1.1

The performance diagram is shown in Fig. 4. The user can view the training process's current state by referring to the performance diagram. In this diagram, the Y-axis represents the cross-entropy value for each iteration, while the X-axis represents the number of iterations. The training results are represented by the blue line graph, the validation results by the green line graph, and the testing results by the red line graph. Each training cycle iteration results in the computation of this performance graph. The greatest performance is determined by looking at the graph where the three results of training, validation, and testing agree in nearly every point. With a best performance value of 2.9778 × 10−7, the network exhibits steady behaviour and a high enough degree of generalizability.

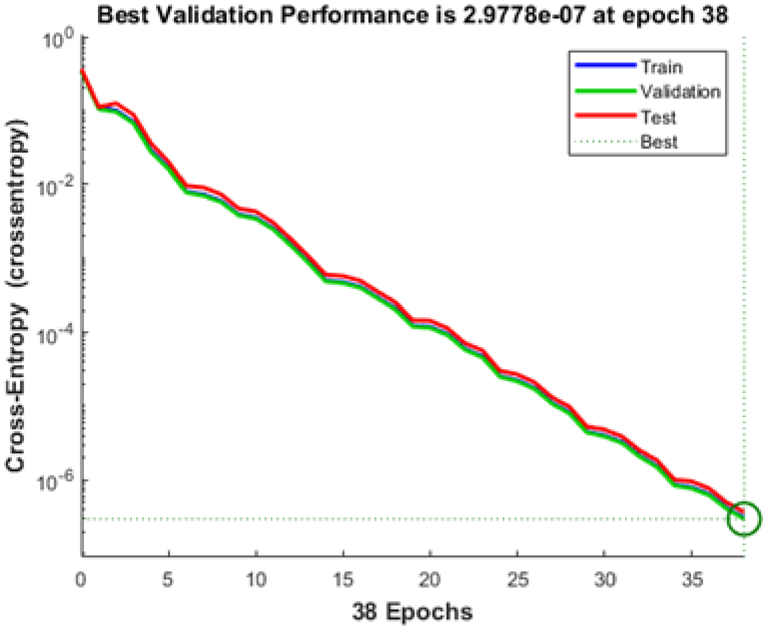


Fig 4 Plot showing the chosen network's performance.

As indicated in Fig. 5, we computed the accuracy of our suggested MLP classification model.

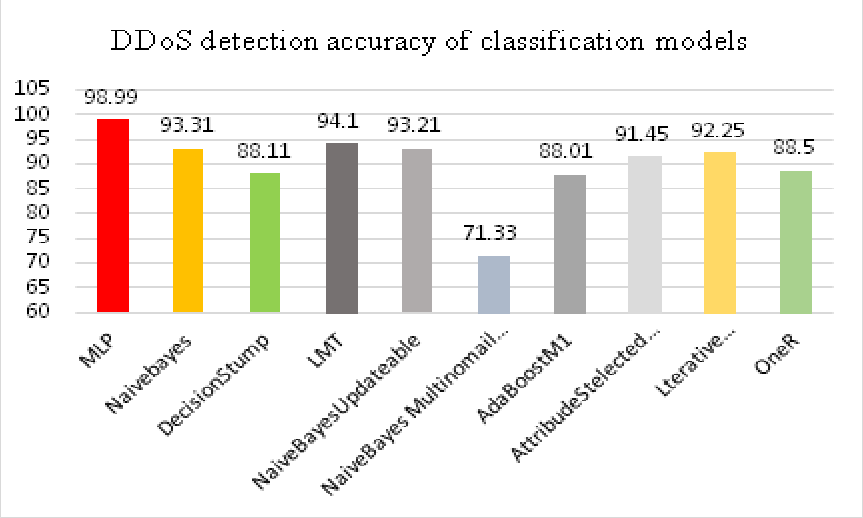


Fig 5. Comparison of the suggested MLP classifier's accuracy to different classification models.

With an effectiveness of 98.99%, the results demonstrate that the MLP classifier performs better than all other classification models. At the application level, we can promptly identify DDoS attacks with our suggested MLP classifier. Using the proposed MLP classifier, we are able to distinguish between legitimate clients and attackers. Meanwhile, several of the assumed IP addresses don't match the description of a regular client or an attacker. In this work, we evaluated the efficacy of our proposed method by applying it to detect attacks in real-world DDoS attack datasets, such as our own dataset, our company's site logs from 2019, and CTU-13 (2011). Fig. 5 displays the examination of ten classifiers' detection accuracy.

7. CONCLUSION AND FUTURE SCOPE

For internal data, this study suggests an MLP classification model to detect DDoS attacks at the application level. This study takes into account features from the incoming network data that differ greatly in terms of their attributes. All potential subsets of attack characteristics were identified in this study, and a rule was designed to differentiate between an attacker, a suspect, and a legitimate client. According to the study findings, our suggested MLP classification model can detect DDoS attacks at the application level with 98.99% accuracy and an FP of 2.11%. We intend to tackle the issue of raising the accuracy of DDoS attack detection in the future. By examining the various access behaviours, we will expand our research to differentiate application-level DDoS attacks from flash events. We will also look into the viability and potential of applying our suggested MLP DDoS attack classification technique to a cyberattack detection system that operates in real-time.

Subsequent efforts may concentrate on developing a programme or service that employs the researcher's chosen algorithms to swiftly evaluate and compare every fresh dataset. Which dataset works best with what methods would be able to be answered by the application. Researchers looking for a high-performing dataset and a consistent methodology to findings by utilising the best datasets and algorithms will find this to be of great assistance. The future expansion of the current research will include calculate and address computational complexity.

REFERENCES

[1] Haq, M.A.; Khan, M.A.R.; Alshehri, M. Insider Threat Detection Based on NLP Word Embedding and Machine Learning. Intell. Autom. Soft Comput. 2022, 33, 619–635

[2] M. A. Al-Shareeda and S. Manickam, "Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation," Symmetry, vol. 14, no. 8, p. 1543, Jul. 2022, doi: 10.3390/sym14081543.

[3] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," IEEE Sensors Journal, vol. 21, no. 2, pp. 2422–2433, Jan. 2021, doi: 10.1109/JSEN.2020.3021731.

[4] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on internet of things," Journal of Network and Computer Applications, vol. 97, pp. 48–65, Nov. 2017, doi: 10.1016/j.jnca.2017.08.017.

[5] R. R. Papalkar and A. S. Alvi, "Analysis of de fense techniques for DDos attacks in IoT–A review," ECS Transactions, vol. 107, no. 1, pp. 3061–3068, Apr. 2022, doi: 10.1149/10701.3061ecst.

[6] A. S. Albahri et al., "Role of biological data mining and machine learning techniques in detecting and diagnosing the novel coronavirus (COVID-19): A systematic review," Journal of Medical Systems, vol. 44, no. 7, pp. 1–11, Jul. 2020, doi: 10.1007/s10916-020-01582-x.

[7] M. A. Al-Shareeda et al., "CM-CPPA: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," Sensors, vol. 22, no. 13, p. 5026, Jul. 2022, doi: 10.3390/s22135026.

[8] G. Baldini and I. Amerini, "Online distributed denial of service (DDoS) intrusion detection based on

adaptive sliding window and morphological fractal dimension," Computer Networks, vol. 210, pp. 1–13, Jun. 2022, doi: 10.1016/j.comnet.2022.108923.

[9] M. A. Al-Shareeda et al., "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks," Applied Sciences, vol. 12, no. 12, p. 5939, Jun. 2022, doi: 10.3390/app12125939.

[10] A. A. Zaidan et al., "A survey on communication components for IoT-based technologies in smart homes," Telecommunication Systems, vol. 69, no. 1, pp. 1–25, Sep. 2018, doi: 10.1007/s11235-018-0430-8.

[11] F. Musumeci, A. C. Fidanci, F. Paolucci, F. Cugini, and M. Tornatore, "Machine-Learning-enabled DDoS attacks detection in P4 programmable networks," Journal of Network and Systems Management, vol. 30, no. 1, pp. 1–27, Jan. 2022, doi: 10.1007/s10922-021-09633-5.

[12] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices," Arabian Journal for Science and Engineering, vol. 47, no. 2, pp. 1353–1374, Feb. 2022, doi: 10.1007/s13369-021-05947-3.

[13] J. G. Greener, S. M. Kandathil, L. Moffat, and D. T. Jones, "A guide to machine learning for biologists," Nature Reviews Molecular Cell Biology, vol. 23, no. 1, pp. 40–55, Jan. 2022, doi: 10.1038/s41580-021-00407-0.

[14] M. Talal et al., "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," Journal of Medical Systems, vol. 43, no. 3, pp. 1–34, Mar. 2019, doi: 10.1007/s10916-019-1158-z.

[15] Z. Liu, L. Qian, and S. Tang, "The prediction of DDoS attack by machine learning," in Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021), Mar. 2022, pp. 681–686, doi: 10.1117/12.2628658.

[16] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks," Sensors, vol. 22, no. 5, p. 1696, Feb. 2022, doi: 10.3390/s22051696.

[17] Rebecchi, F.; Boite, J.; Nardin, P.; Bouet, M.; Conan, V. DDoS protection with stateful software-defined networking. Int. J. Netw. Manag. 2019, 29, e2042.

[18] H. Hindy et al., "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104650–104675, Jun. 2020, doi: 10.1109/ACCESS.2020.3000179.

[19] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," Jan. 2017.

[20] S. Axelsson, "Intrusion detection systems: A survey and taxonomy." pp. 1–27, 2000, doi: 10.1.1.1.6603.

[21] A. Qayyum, M. H. Islam, and M. Jamil, "Taxonomy of statistical based anomaly detection techniques for intrusion detection," in Proceedings of the IEEE Symposium on Emerging Technologies, 2005., 2005, pp. 270–276, doi: 10.1109/ICET.2005.1558893.

[22] U. Islam et al., "Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models," Sustainability, vol. 14, no. 14, p. 8374, Jul. 2022, doi: 10.3390/su14148374.

[23] M. H. Ali et al., "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)," Electronics, vol. 11, no. 3, p. 494, Feb. 2022, doi: 10.3390/electronics11030494.

[24] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," IEEE Access, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[25] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight," Symmetry, vol. 13, no. 2, p. 227, Jan. 2021, doi: 10.3390/sym13020227.

[26] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication

Review, vol. 34, no. 2, pp. 39–53, Apr. 2004, doi: 10.1145/997150.997156.

[27] E. Džaferović, A. Sokol, A. A. Almisreb, and S. M. Norzeli, "DoS and DDoS vulnerability of IoT: A review," Sustainable Engineering and Innovation, vol. 1, no. 1, pp. 43–48, Jun. 2019, doi: 10.37868/sei.v1i1.36.

[28] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and detection of ddos attacks on cloud computing environment using machine learning techniques," in 2019 Amity International Conference on Artificial Intelligence (AICAI), Feb. 2019, pp. 870–875, doi: 10.1109/AICAI.2019.8701238.

[29] E. Alpaydin, Introduction to machine learning, 4th ed. Cambridge: MIT Press, 2020.

[30] A. Fadlil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensic s," Bulletin of Electrical Engineering and Informatics, vol. 6, no. 2, pp. 140–148, Jun. 2017, doi: 10.11591/eei.v6i2.605