Open
Full Length Article

ORIGINAL ARTICLE

Mitigating the Knock-on-Effect of DDoS Attacks on Application Layer using Deep Learning Multi-Layer Perceptron

Mujahid Shah[1], Sheeraz Ahmed[2], Mujtaba Hussain[3], Sadeeq Jan[4]

[1,2]Iqra National University Peshawar, Pakistan
[3]Ripha International University Islamabad, Pakistan
[4]University of Engineering & Technology (UET), Peshawar Pakistan

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a significant threat to the Internet today, and application-layer DDoS attacks that use legitimate HTTP requests to overwhelm victim resources are imperceptible. As a result, neither the intrusion detection system (IDS) nor the victim's server can detect malicious packets. This research is intended to take a new approach, deep learning, to detect novel application layer DDoS attack strategies, known as increasing DDoS and proxy DDoS attack. The proposed attack detection model has been validated by performing simulation experiments with MATLAB and Python. Finally, the preliminary result compared with the various machine learning techniques for classification: Naïve Bayes, SVM, Decision trees, and Genetic Algorithm (GA) in terms of Accuracy Rate (AR), Detection Rate (DR), Sensitivity, specificity, (ROC) curve. The results show that our detection model effectively detects DDoS attacks at the application layer. The proposed deep learning multi-layer perceptron architecture can identify and use the most relevant high-layer features of packet flows with an accuracy of 98% on the generated dataset containing a novel DDoS attack.

Keywords: DDoS attack, Application Layer Attack, Attack detection, Botnet, MLP

Author`s Contribution
[1,2,3,4]Manuscript writing, Data Collection Data analysis, interpretation, Conception, synthesis, planning of research, and discussion

Address of Correspondence
Mujahid Shah
Mujahidshah51@gmail.com

Article info.
Received: Aug 16, 2019
Accepted: April 29, 2020
Published: June 30,2020

Cite this article: *Shah M, Ahmed S, Hussain M, Jan S. Mitigating the Knock-on-Effect of DDoS Attacks on Application Layer using Deep Learning Multi-Layer Perceptron. J. Inf. commun. technol. robot. appl.2020; 11(1):15-30..*

Funding Source: *Nil*
Conflict of Interest: *Nil*

INTRODUCTION

DDoS attacks have severely damaged servers, and servers will intimidate the development of further new internet services. According to Kaspersky the second quarter of 2019, the total number of DDoS attacks grew by 18% compared to the same period in 2018. Application-layer attacks, which are more difficult to recognized and detect, grew significantly by a third (32%) compared to the second quarter of 2018. New types of DDoS attacks are continuously generated by hackers or black hackers, which are multi-stage but occur primarily on the network and application layer of the OSI model. These attacks use bogus IP addresses to avoid identifying the source and carry out the attack on a large scale. Such attacks are immense since the available bandwidth in the bottleneck is completely exploited by the attack traffic and therefore causes legitimate packets to drop. Surprisingly, the victims are government agencies, financial companies, defense agencies, and military

departments. Popular websites like Facebook, Twitter, Wikileaks, PayPal, and eBay have become victims of DDoS, which has disrupted normal operations and led to financial losses, poor performance, and unavailability

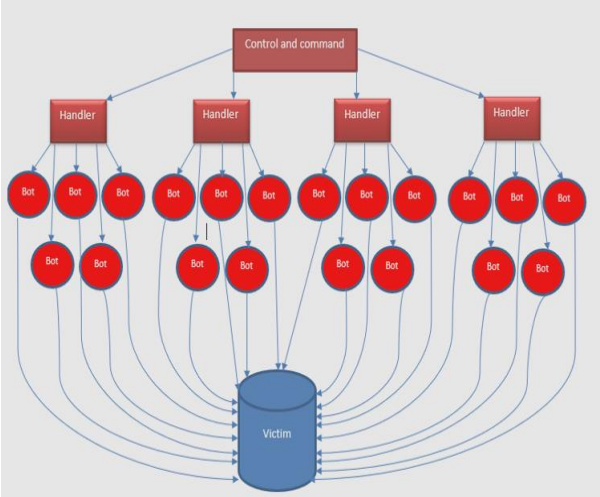

Figure 1. DDoS Attack Infrastructure

figure 1 show DDoS attack infrastructure how, the attacker controls the bots and send a command to the handler and attack the victim, there are mainly three types of DDoS attack

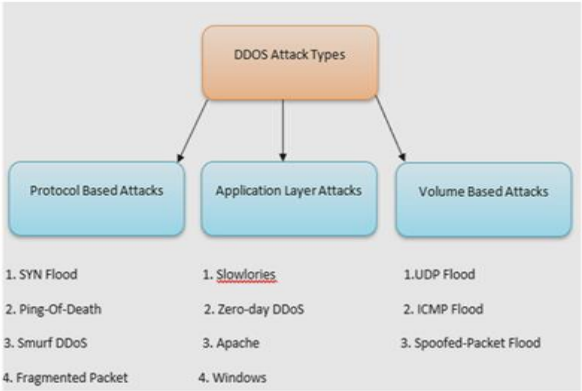

Figure 2. Main types of DDoS attack

Figure 2 shows the main three types of DDoS attack,

a) Volume Base: This includes UDP flooding, ICMP flooding, and other spoofed-packet flooding and the target of the attack is to saturate the bandwidth of the attacked space, and the scale is measured in bps.
b) Protocol Attacks. Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS, and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).
c) Application Layer Attacks: They comprise low as well as slow attacks, the GET/POST floods, Windows or OpenBSD susceptibilities, attacks that target Apache, and more. Encompassed of apparently legitimate and innocent requests and goal of these attacks is to crashing webserver and scale is measured in Requests per second.

Hypertext Transfer Protocol HTTP-GET Flood Upstream attention in the range of discovery of DDoS attacks Various important problems and challenges developed from recent research, many challenges, partially addressed or unresolved, work near-collision HTTP-GET flood DDoS Time is seen in front of attacks [1]. DDoS attacks are thrown over disciplined, scattered and distantly organized networks so that settled computers (known bots or zombies) will be used for transfer immense size of nonstop and synchronic happening requests the victim system(s), DDoS attacks are amplified in strength, regularity, and complexness. The malicious users square measure perpetually advancement their experience and adapt their procedure and square measure intense up-to-date technologies to launch varied DDoS attacks. Although, various resolutions are prompt by the students to spot, avert or diminish DDoS attacks, however still the malicious user square measure persistently increasing very different approaches and means that to bypass these countermeasures [2]. DDoS occurrences square measure still between the best crucial threats to this net. In recent times, application-layer DDoS outbreaks aboard internet server's square to measure attracting common, inflicting in torrential revenue losses to targets [3]. Application layer occurrence where it will smash the online server and it is restrained in requests per second. This sort of attack contains, Slowloris, Zero-day attack, and DDoS attack that aim Apache or Windows vulnerabilities [4].

In this paper, we make the following significant research contributions.

- We present novel DDoS attacks known as increasing and proxy DDoS attacks.
- Proposes a deep learning multi-layer perceptron architecture using eight hidden layers for classifying legitimate users and malicious users on the application layer.
- A technique for automatically tuning hidden layers of ANN to detect macro patterns in

network flows iteratively.

- A systematic approach employed to generate the benchmark dataset for novel DDoS attack labeled dataset and simulating various network normal and attack behaviors
- A thorough evaluation of the proposed model using the generated dataset for novel DDoS detection.

LITERATURE REVIEW

DDoS attack detection (Application DDOS Assault) is generally based on the biologically induced inconsistency, which generally aims to achieve a quick and early position. The offered prototype could be a bio-animated algorithmic bat program that gets used to reaching the fast and expected position of the DDOS application over an HTTP flood [5]. A classification framework for the detection and avoidance of TCP-DDoS overvoltage attacks (CS_DDoS) in the fog in broad daylight. The proposed CS_DDoS framework offers an answer to the protection of stored data records [6].

A look at the execution of exponentially weighted normal movements (EWMA) to undermine colossal learning and the discovery of DDoS attacks the foundation of the Internet of Things (IoT). The authors checked the compromise between the calculation identification rate, the warning, and the localization delay [7]. Intrusion detection device capable of locating nearby attacks in the RPL protocol and a stable root method to prevent the effects of the attack on this protocol. IDS is included with the help of Taking into account the facts regarding the position and the signal strength, the perception of harmful nodes results [8]. The concept of application-layer DDoS attacks on the Internet is real-time prevention (ARTP), which is mainly based on anomalies aimed at quick and quick detection. ARTP is a gadget study method that can be used to quickly find app DDoS using multi-edit flood requirements. The experiments were performed in benchmarking the LLDOS data sets, while the assigned results increase the importance of the proposed version to determine the cause of the article [9]. Standard methods and a proposed hybrid protocol were used, which is more suitable in terms of cloud structures to detect DDoS attacks [10]. Due to the existence of melting nodes, attacks can be activated that are classified as active and passive attacks [11].

A version of DDoS attack detection and mitigation using feature selection techniques. In the studies provided, visitors to the community, in particular, are analyzed using the Hellinger distance function. If a long way is kept, all statistical packages are analyzed and divided into two classes, since DDoS and requirement groups are classified as legitimate [12]. Problem with creating a secure mechanism for critical systems through machine learning [13]. A botnet detection technique that uses this technique can manage multiple records and identify bots in the network [14]. Demonstrate hybrid detection models by introducing an advanced and effective method to prevent DDoS attacks and protect flood attacks from overload [15]. Several new entropy-based features that help you properly detect DDoS attacks, and a multi-class system that is based on a set of mainly entropy-based features with classifiers for machine learning fashion and increases accuracy with low intensity and high detection. The intensity of the DDoS attack [16]. Plans against network-based attacks with a focus on four primary source defense systems, core end, victim end, and two inventive models, Gossip and D-Ward [17].

A mitigation framework is based on a fuzzy control system. This entry consists of two new recognition matrices [18]. A new function selection algorithm is known as a dynamic ant colony system with a selection of three-stage update functions. The technique presented uses various layers of pheromones that help ants to inhibit their properties [19]. The method is compared with another hybrid algorithm mentioned and 10-fold cross-validation. Experimental results based on the KDD CUP'99 data set suggest that the proposed methodology has a better detection accuracy and frequency as well as an inaccurate alarm frequency than the others [20]. One possible new package marking technique is to manage the way forward to penetrate the locations to the victim's location. In this way, victims can delegate security to Internet Service Providers (ISPs) [21]. A protection machine called Sky Shield. The system uses a sketch data structure to quickly identify and mitigate DDoS attacks for individual applications. First, they recommend recalculating the deviations in the sketches, which improves the results of the dynamics of the network and also increases the accuracy of the reputation. Second, he

used an unusual sketch to simplify the identification of malicious hosts from permanent attacks [22]—the idea of a confident system. The system automatically rearranges security applications for incoming traffic. To achieve this, we suggested implementing a model-dependent learning, logic, and performance cycle (LRA-M). For this purpose, it describes the architecture of the associated system and interprets its basic components [23].

In this way, MPTCP-H significantly increases the attacker's intensity for a successful attack without detecting the trace of WAMS information. Experimental consequences recommend that the MPTCP-H proposal offers significant mitigation of DoS / DDoS attacks for WAMS at affordable overhead costs, ie additional latency and messaging [24]. This article examines 5G security by combining the physical and logical layers for the automatic attack and automatic defense. He is dedicated to providing a framework for automated 5G security solutions [25]. The authors provided the latest in DDoS attacks in SDNN and cloud computing situations. Particular attention is paid to the analysis of SDN and the structure of cloud computing. The researchers also found that the studies work and pose problems in identifying and managing DDoS attacks [26]. A comprehensive assessment of numerous mitigation processes and their identification in three extraordinary lessons based solely on his malicious visitor management technique. Also, the researchers examined some capacity limitations in these mitigation methods and the proposed capacity characteristics of a standard response to DoS attacks. For the great understanding of the researchers, these images are the first attempt to classify DoS reduction strategies and to discover their limits in SDN environments [27]. This article explains a new sentence classifier that has been trained with new features that are reflected in traffic flow characteristics, so that traffic flow has a distribution diversity that is considered and linked to individual classifiers. The set classifier and AdaBoost are used to measure the flow by determining the similarity of the distribution involved in several classifiers in the set classification model [28]. Distributed Denial of Service (DDoS) attacks at the application level have advantages in increasing the complexity and variety of network protocols and services. This type of attack is very popular these days instead of DDoS attacks. AL-DDoS attacks are critical threats to the Internet and the corporate web server [29]. This study suggests a new paradigm to mitigate the impact of DDoS attacks on NFV. When DDoS detects the application level DDoS attack, it typically migrates server and IP spoofing. The effectiveness of DDoS was tested by calculating the processing time during load migration and IP spoofing [30]. A Distributed Denial of Service (DDoS) attack is an attack that threatens the bandwidth of the entire network by blocking all publicly available network resources and making access to this resource unavailable. The DDoS attack is more vulnerable than a normal Dos attack because there is more than one source for the origin of the attack, so users cannot even guess how to identify and where to take action to resolve the attack. DDoS attacks in the smart home can be more serious since, in an intelligent home network, the embedded operating system is open and can be easily compromised, and the authentication mechanism in a smart device is always associated with risk [31].

The reliability of devices that are connected to the Internet of Things (IoT) largely depends on the security model that is used to protect user data and prevent malicious device activity. Existing approaches to detecting phishing, DDoS (Distributed Denial of Service), and botnet attacks often focus on the device or the back end [32]. Zero-day denial of service (DoS) attacks are underway today are common on high-speed networks Growing several vulnerabilities. Also, the attacks are becoming more sophisticated and so are difficult to detect before damaging multiple networks and hosts. For these reasons, monitoring, processing, and real-time the detection of anomalies in the network must be one of the main features of a Modern DoS prevention system [33]. DDoS (distributed denial of service) attacks are increasing rapidly and become one of the fatal threats to the Internet. Automatically Detecting packets with DDoS attacks is one of the primary defenses Mechanisms. Conventional solutions monitor network traffic and identify the activity of attacking legitimate network traffic based on statistical divergence. Machine learning is a different Method to improve statistical identification performance Properties. Conventional machine learning techniques They are limited by models of superficial representation [34]. One of the most important Challenges in detecting an

application-level DDoS attack the unavailability of functions to detect such attacks. That's the way it is It is difficult to model normal user behaviour based on attack behaviour. The authors introduce the architecture of deep learning, DDoS attack properties at the application level. Deep learning architecture consists of a very deep neural network, typically more three layers [35].

Many methods have been developed in previous publications to protect systems from distributed IP and TCP denial levels Service attacks instead of the application layer. However, it will no longer work well when it hit the application layer Distributed denial of service. The authors introduce the grouping method to discuss the DDoS application levels in this article [36]. Counter Distributed Denial of Service (DDoS) Attacks become more difficult with the vastness Resources and techniques increasingly available for Attackers DDoS attacks are usually carried out on the Network level. However, there are indications of this Application-level DDoS attacks that may be more effective as the traditional in this article the authors consider Demanding attacks that use legitimate applications HTTP request level of the legally connected network Machines to overwhelm the webserver. From the attack, the signature of each level of the DDoS application is displayed in the abnormal behavior of the user, and the authors propose a countermeasure based on the surfing behavior of the web user for Protect servers from these attacks [37]. Distributed denial-of-service attacks are increasing Threat to organizations and how defense mechanisms are More and more advanced hackers are targeting the app Layer. For example, the application level is distributed low, and slowly Denial of service attacks is becoming a severe problem because Due to the low resource consumption, they are challenging to identify. In this research, the authors propose a reference architecture Minor and slowly distributed denial of service reduction Attacks via software-defined infrastructure capacities. Researchers also offer two concrete architectures based on the reference architecture: a performance-based model e Architecture based on off-platform components. Us Introduce the concept of Shark Tank, a detailed low group Monitoring with full application functionality, and where Suspicious requests are redirected for additional filters [38].

Denial of Service Attack (DDoS) seriously threatens the survival of web services. To attempt on a server, the resources run out (e.g., I / O bandwidth, CPU, and Storage resources) because no resources are available for legitimate user requests. Some attackers have been launched a Web DDoS attack recently from the application layer (e.g., DDoS) that can bypass most of the existing detection Approaches that mainly focus on flooding the DDoS bandwidth and TCP SYN-Flooding DDoS. The authors cover the detection of web DDoS applications and present two different models to characterize user web access behavior, d. H. Click-based model and Markov-based process Model. With these functions as a reference, we take on big one's Variance theory to estimate the likelihood that every one the login behavior of the users matches the corresponding Reference characterization and proposes two different surveys Schemes, LD-IID, or LD-MP [39]. Distributed denial of service (short DDoS) The attack is a severe problem for network services. This role discussed some solutions for the DDoS application layer (abbreviated App-DDoS) and suggested a relative entropy Detection method based on the DDoS application. Our scheme includes two Phases: the learning phase and the recognition phase. First, when learning extracts the main click properties of web objects with the Grouping methods. Then calculate the in the detection phases relative entropy for each session based on learning outcomes. The higher the session's relative entropy, the more suspicious it is the session is. Finally, the simulation results suggest that this method could Distinguish the attack session with a high and low detection rate false negative report [40].

Distributed Denial of Service (DDoS) attacks are one of the most critical security challenges for network operators. Networks defined by the software (SDN) enables a rapid response to these threats through dynamic application Forwarding/blocking rules as a countermeasure. Centralization, however, in addition to network management, the SDN controller is required for the control plan Operations also need to collect information to identify and mitigate security threats. A significant disadvantage of this approach is that it can be overloaded the controller and the control channel. On the other hand, SDN with status is a new concept developed

to improve responsiveness and download the controller Delegate local treatments to counters. In this article, we hug This paradigm for protecting end hosts from DDoS attacks. The authors suggest StateSec, a New approach based on switch processing capabilities to detect and mitigate Flood hazard. States monitor packets that correspond to the configurable data traffic works without using the controller. Feeding an entropy detection Algorithm with such monitoring functions, recognizes and mitigates various Threats like (D) DoS with high precision. The authors implement StateSec in an SDN Platform that compares it to the most modern approaches. It shows that states it is much more efficient [41]. Cloud computing services are often provided over the HTTP protocol. This facilitates access to services and reduces the cost of both suppliers and end-users. However, this increases the vulnerability of cloud services to HTTP DDoS attacks. HTTP Request methods are commonly used to address web server vulnerabilities and create multiple HTTP DDoS attack scenarios, such as Low and slow or flooded attacks. Existing HTTP DDoS detection systems are challenged by large amounts of network traffic generated by these attacks, low detection accuracy, and high false-positive rates. In this article, the authors introduce an HTTP detection system DDoS attacks in a cloud environment are based on entropy and the learning algorithm of the random forest theory. A time-based sliding window algorithm is used to estimate the entropy of the network header properties of the incoming network traffic [42]

The DDoS attack is a challenging problem that needs to be tackled in SDN. An efficient control scheduling method is offered to help the controller whether the DDoS. The proposed control planning method uses the normalized waiting time, length, and extent of the switch to select the request that the controller has to process. The results of the evaluation confirm that the proposed method can significantly reduce the link failure rate and delay compared to the polling-based controller scheduling method [43]. This research illustrates the identification methods by removing the features from the web server logs and also discusses the reduction of the features' dimensionality using a diffusion map. The anomalies are detected by clustering technique for affinity propagation and also by virtual machine status monitoring. The Dempster – Shafer hypothesis further focuses on identifying the suspect person. From the experimental results, it is concluded that the proposed approach increases the detection efficiency with very few false alarms compared to current methods[44].

Applications such as remote communication and control systems are in critically integrated configuration. Supervisory control and data acquisition (SCADA) frameworks define the monitoring of such networks. This research, using an advanced model of machine learning technologies, explores the analysis and classification mechanism of attack. The types of attacks are classified by the optimal selection of functions extracted from the sensor data. The features are labeled in this, and the cluster is extracted between the matrixes. These clusters form the initial processing of identification of the attack, which prevents the result which is not matched. Such data clustering is achieved by way of a clustering algorithm for mean changes. Using the genetically seeded flora optimization algorithm, the features irrelevant for the classification process are identified and suppressed from that clustered data[45]. The use of the congestion control mechanism to deteriorate the network quality of services in low-rate denial of service (LDoS) attacks. As a classic active queue management algorithm, random early detection (RED) algorithm is widely used to prevent network congestion. However, RED is vulnerable to attacks by LDoS. LDoS attacks with well-configured attack parameters force the RED queue to fluctuate severely, thus throttling the transmission control protocol (TCP) transmitter rate [46]. Internet of Things (IoT) has recently become more popular because it is flexible, usable, diverse, and easy to deploy. However, security issues are less investigated. The IoT devices have low computational strength, low battery life, and low memory. Becoming resource-intensive with security features, IoT devices are often found to be less protected, and recently, due to high-profile security defects, more IoT devices were routinely attacked. This study examines the safety faults of IoT devices, particularly those utilizing low power broadband (LPWAN) networks [47]. In traditional detection and prevention measures, a large number of data is generated to help network analysts evaluate the network security situation, but it is not fully and effectively used, and there is no holistic view of the network situation

on it for now. In order to deal with this issue, a framework for evaluating the safety situation of the network from the three aspects threatened, vulnerable and stable is proposed and for measuring the safety situation of the entire network to merge the results at the decision level. In the case of studies, the authors show how the framework is used in the network and how it is used in real-time for reflecting the network security situation[48]. Cyber-physical systems (CPSs), and physics-based threats, i.e., electronic object targeting threats. In this study, the emphasis is on a systematic study of both credibility and denial of service attacks on CPS sensors and actuators, and the timing implications of these attacks [49]. Threat detection has long been seen as a crucial tool to minimize the harm done by a malware attack. Recently intra-level security systems have been proposed that can monitor system software efficiently and securely without involving a more privileged entity. Unfortunately, there is no complete intra-level security system that can operate universally on ARM at any level of privilege. However, as malware and attacks increase against virtually every level of privileged software, including an operating system, a hypervisor, and even the highest privileged TrustZone-based software [50]. Location-based systems (LBS) offer useful systems and simple functionality for smartphone devices. Nevertheless, the location and other information revealed to the LBS by every question violates the privacy of the customer. This is of particular concern because LBS providers can be honest-but curious-by collecting queries and tracking the whereabouts of users and inferring sensitive user data [51]. An electronic data theft detection method from computer systems is described, capable of detecting remote exfiltration patterns that happen over days to weeks. Standard traffic flow data, in the form of host ingress and egress bytes over time, is used to train a group of one-class learners [52]. Security challenges in mobile cloud computing including privacy issues, access controls, service level agreements, interoperability, charging patterns, etc. In this article, we focus on the safety challenges in mobile cloud computing and key features in an MCC security framework. First, we describe key architectures for various applications of mobile cloud computing, and then, in terms of privacy management, security, and attacks, we discuss few security frameworks suggested for MCCs [53]. Cloud computing allows users with small resources to use their data on a pay-per-use basis in the cloud for computing, bandwidth, storage, and services. Researchers around the world are thus trying to address data protection issues with users by proposing different methods, such as encrypted outsourcing of data [54]. This article aims at proposing new quantitative models to evaluate security threats to information systems. The authors adopt methods to estimate the cost of failure due to safety failures. Indeed, the importance of quantification of security threats continues to expand with a growing reliance on analytical structures for individuals, businesses, and governments [55]. Data protection and data processing are two similarly important criteria for assessing the efficiency of data placement in the implementation of data placing approaches for cloud storage platforms. As these two factors typically clash, a combination of data protection and transfer time is important to guarantee the level of support that the network/cloud service provider guarantees. The positioning strategy should be adaptable to take into account risk features to ensure the integrity of data from the stored network nodes in case of threats or cyber-attacks [56]. Network devices not only allow users to build robust local networks but also protect from unwanted intruders for their data and their transmissions. However, security within local networks is important since internal attacks can be disastrous for users [57]. Network applications handle sensitive data that demand maximum security and privacy [58]. Social networking has been both an unavoidable catchment for adolescents and the older generation of today. The remarkable growth in social networking sites has been observed in recent years, especially in terms of adaptability as well as visibility in both the media and academia. The information on social networking sites is used in social, geographical, and economic analysis and thus provides meaningful insights [59]. Dataset plays an important role in detecting intrusions [60]. A modern mode of information service is provided by the smart health care system (SHS). It significantly enhances diagnostic performance by tracking information about symptoms of patients via different wearable devices. The security and privacy issues have drawn wide attention to ensuring the confidentiality of sensitive information. The searchable encryption

technology is suitable for addressing these problems, as it supports searching over encrypted data and protects data privacy [61]. Despite numerous advantages offered by the CSPs, however, some security issues may dissuade users. Various virtual machines (VMs) often share the same physical resources in cloud computing, which are known as co-resident VMs. The shared physical resources pose a significant threat to users since resources can belong to competing organizations as well as to unknown attackers [62].

MOTIVATION

In the review of the above papers, we have come to a gap between the ongoing research—the necessity for the present and future technology rise. Different researchers, according to the literature review, have addressed DDOS attacks, but to some extent, they have addressed one or two types of attacks but have not touched the rest of them. There are two major DDOS attacks, which are to be addressed, are at a time which is below

- Increasing DDOS attack Strategy
- Proxies DDOS attack strategy.

These collectively will help to design such an algorithm that will be stopping enough so that the attacker cannot be easily breakdown, and the unavailability of the services should be accessible. Organizations have invested considerable resources in cybersecurity. Firewalls, web application firewalls, intrusion detection and prevention, and the like all serve unique goals. However, they are insufficient to stop widely distributed attacks. This proposed model will mitigate those DDoS attacks which are not detected by this firewall and IDS.

DATASETS

In this research, a new dataset is generated because there are no existing data sets that contain an increasing DDoS and proxy DDoS attack. Furthermore, other available data sets may include a great deal of duplicate and redundant records, and that may result in an ultimate unrealistic outcome. Our generated dataset contains two types of DDoS attack without redundant and duplicate records. A systematic approach is employed to generate a benchmark dataset for application layer IDS, a dataset is labeled, normal traffic, suspicious traffic and attack traffic, dataset generation infrastructure is showing in figure 3, The details given in Table 1.

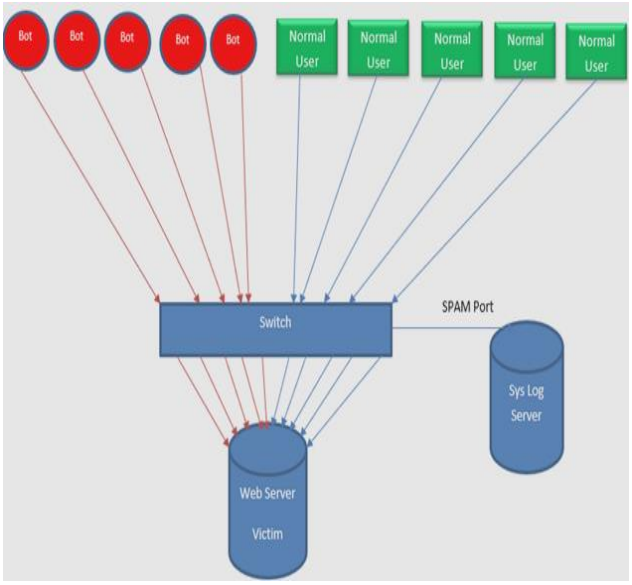

Figure 3. Dataset generation Infrastructure

- Slow HTTP Test is a highly configurable tool that simulates the Application Layer Denial of Service attacks.
- Low Orbit Ion Cannon (LOIC) is an open-source denial-of-service attack application layer.
- High Orbit Ion Cannon (HOIC) is an open-source denial of service attack application for network stress tests that can attack up to 256 URLs at the same time.
- R.U.D.Y. is a popular low and slow attack tool that can block a web server by sending long-form fields.
- Tor's Hammer is a slow testing tool written in Python. It can also be managed through the Tor network to be anonymized.
- DAVOSET is a tool for committing distributed denial of service attacks using execution on other sites.
- GoldenEye is a potent full DDoS attack tool that brings down the site almost within 30 seconds, depending on how big their memory pool is.
- With OWASP's HTTP Post Tool, it can test the web applications to ensure their stability against HTTP GET and HTTP POST attacks.
- DDOSIM simulates multiple zombie hosts (with random IP addresses) that establish full TCP connections to the target server. After the

connection has been completed, DDOSIM starts the conversation with the listener application (e.g. the HTTP server).

DEEP LEARNING MULTI-LAYER PERCEPTRON CLASSIFICATION MODEL

This research presents a Deep Leering Multi-Layer Perceptron based DDoS detection technique. The proposed model architectures consist of input, hidden, and output layers; the input layer is fed the patterns representing the characteristics of network flows, whereas the output layer classifies the flows as either benign or one of the attacks mentioned above.

Table 1. Configuration of Attacks Tools

S.#	Tools Name	Operating System	Memory (GB)	Processors	HardDisk (GB)
1	Slowhttptest	Windows 10	2	2	200
2	LOIC	Windows 10	2	2	250
3	HOIC	Windows 10	2	2	200
4	R.U.D. Y	Kali Linux	2	2	300
5	Tor's Hammer	Ubuntu	2	2	150
6	DAVOSET	CentOS	2	2	200
7	GoldenEye	Kali Linux	2	2	400
8	OWASP HTTP POST	CentOS	2	2	250
9	DDoSIM	Ubuntu	2	2	200
10	Tor's Hammer	Kali Linux	2	2	300

The hidden layers deal with the intermediate patterns contained within the flow to assist in the classification computation. In this propose an ANN architecture based on feed-forward Propagation architecture as shown in Figure 4, which includes:

4 input layers: for selected functions and bias factor 8 hidden layers initializing synaptic weights and connections3 output layer yielding probabilities of three classes (Normal, Suspicious and Attack)

In the proposed model, the information moves in only one direction, i.e., forward, from the input nodes through the hidden nodes and to the output nodes. There are no cycles or loops in the network. See Figure 4.

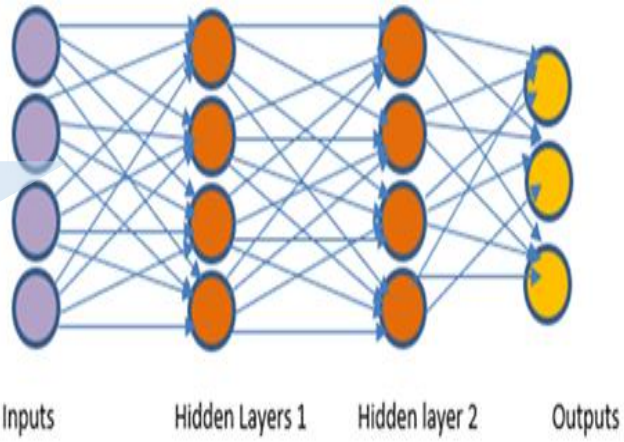

Figure 4. Structure of the chosen network

Below given equations for derivatives of the error with respect to (w.r.t) output weights Wjk:

$$\partial E/\partial Wjk=\partial k\alpha j \quad (1)$$

Output layer biases, bk

Following gradient for the output biases:

$$\partial E/\partial bk=(\alpha k-tk)gtk(zk)(1) \quad (2)$$

Gradients for Hidden Layer Weights

$$\partial E/\partial Wij = \sum k€K\ (ak\ -\ tk)\ gtk\ (zk)\ Wjk\ gtj\ (zj)\ ai$$
$$= gtj\ (zj)\ ai\ \sum k€K\ (ak\ -\ tk)\ gtk\ (zk)\ Wjk$$
$$=aigtj(zj)\sum k€\partial Wjk \quad (3)$$

Gradients for Output Layer Weights

The given below equation for derivative of error w.r.t output weights Wjk:

$$\partial E/\partial wjk=\partial k\alpha j \quad (4)$$

The Receiver Operating Characteristic Curve: This curve is a graph depicting the performance of a classification model at every classification threshold. It plots 2 metrics that are the True Positive Rate (TRP) and the False Positive Rate (FPR).

TPR is a substitute for recall, hence expressed as below:

$$TPR=TPTP+FN \quad (5)$$

$$TPR=TP/TP+FN \quad (6)$$

FPR expressed as below:

$$FPR=FP/FP+TN \quad (7)$$

$$FPR=FPFP+TN \quad (8)$$

RESEARCH METHODOLOGY

The major characteristics of HTTP such as GET, POST between other techniques, identical TRACE, HEAD, DELETE, CONNECT, OPTIONS, and PUT are examined. Common legitimate clients do not have more than 15– 20 HTTP GET and the POST demand per IP address now bots become intelligent mimic human behaviors, normally same bots have same HTTP request and spend the same time, same packet frame size using increasing DDoS attack strategy to set up their objective of DDoS.

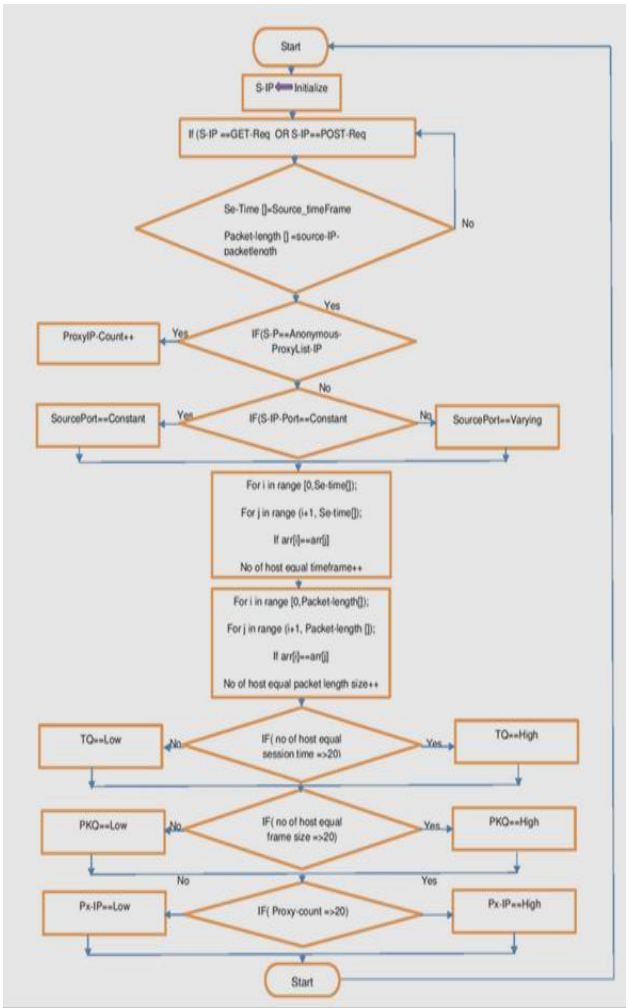

Figure 5. Flow chart of the proposed model

Algorithm 1 calculating the client session time and counting the number of clients is equal session time during 20 second

```
Step 1 S-IP ← Source IP
Step 2 ProxyIP-count ← initialize
Step 3 IF (S-IP == GET_request or S-IP ==
       else Go to step 1
Step 4  Se_Time [] = SourceIP_Se_Time
Step 5 for i in range (0, Se_Time [] ):
       for j in range (i + 1, Packet_lenght []):
            if arr[i] == arr[j]:
              No of Host equal  Session Time++
Step 6 IF (No of Host equal Session Time =>20)
       TQ == High
Else
       TQ  == Low
```

Algorithm 2 calculating the client packet window size time and counting the number of clients is equal packet window size during 20 second

```
Step 1 S-IP ← Source IP
Step 2 ProxyIP-count ← initialize
Step 3 IF (S-IP == GET_request or S-IP ==
                  else Go to step 1
Step 4 Packet_lenght [] = SourceIP_paketlength
Step 5 for i in range (0, Time_Fram [] ):
            for j in range (i + 1, Se_Time[]):
                  if arr[i] == arr[j]:
       No of host equal Packet frame Size ++
Step 6 IF (No of Host equal Packet Frame size =>20)
PKQ == High
Else
PKQ  == Low
```

Algorithm 3 calculating the source IP and comparing the source IP with anonymous proxy IP list during 20 seconds that how many proxy IP requests recorded

```
Step 1 S-IP ← Source IP
Step 2 ProxyIP-count ← initialize
Step 3 IF ( S-IP == GET_request or S-IP ==
            else Go to step 1
Step 4 Step 4 IF (S-P == Anonymous_ProxyList-IP)
                  ProxyIP-count++
Step 5 IF (ProxyIP-count =>20)
          PX-IP == High
      Else
          PX-IP  == Low
```

Algorithm 4 calculating the source port number is constant or varying during 20 second

```
Step 1 S-IP ← Source IP
Step 2 ProxyIP-count ← initialize
Step 3 IF (S-IP == GET_request or S-IP ==
            else Go to step 1
Step 4 IF (S_IP-Port==Constant)
                SourcePort ==Constant
    Else
                        SourcePort==Varying
```

Table 2 shows the detection criteria of the labelled dataset to distinguish the normal, suspicious and attack traffic

Table 2. Detection Criteria

S. No	No of Host Spent Equal Session Time (TQ)	No of Host Equal Packet Length (PKQ)	No of host use Proxy Server (PX-IP)	Host changing Ports (SourcePort)	Detection Pattern
1	Low <=20	Low <=20	Low <=20	Constant <=20	Normal
2	Low	Low	Low	Varying	Suspicious
3	Low	Low	High	Constant	Normal
4	Low	Low	High	Varying	Suspicious
5	Low	High	Low	Constant	Normal
6	Low	High	Low	Varying	Suspicious
7	Low	High	High	Constant	Suspicious
8	Low	High	High	Varying	Attack
9	High	Low	Low	Constant	Normal
10	High	Low	Low	Varying	Suspicious
11	High	Low	High	Constant	Suspicious
12	High	Low	High	Varying	Suspicious
13	High	High	Low	Constant	Attack
14	High	High	Low	Varying	Attack
15	High	High	High	Constant	Attack
16	High	High	High	Varying	Attack

SEMULATION, RESULT AND DISCUSSION

The plot in figure 6 gives us a clear picture as the predicted probability of the classes gets closer to zero. it shows that the best performance value is 2.9778e-07 depicting that network behaviour is stable and its generalizability is high enough. The best validation performance graph for training the input dataset is given in Figure 6. The X-axis represents the number of epoch and Y-axis represents the mean square error (mse). The best validation performance is 2.9778e-07 at epoch 38. In Figure 4, the validation process, training process, and test error decrease with the increase in period or volume of training.

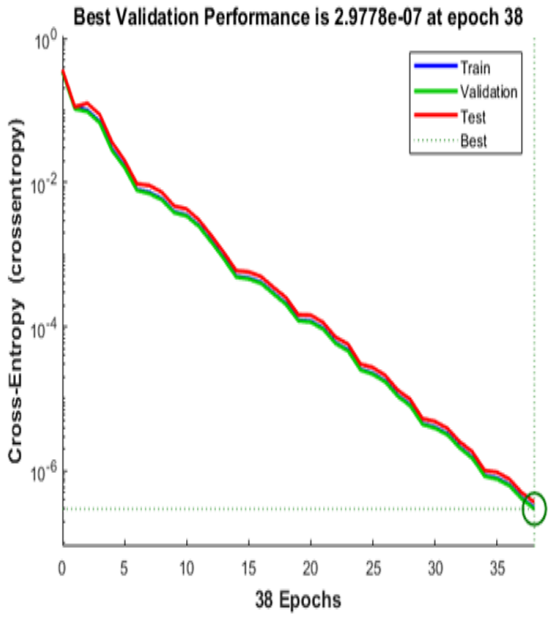

Figure 6. Performance-plot of the proposed model

Figure 7 shows that the trained model accurately fits the dataset and prediction is very close to the actual dataset.

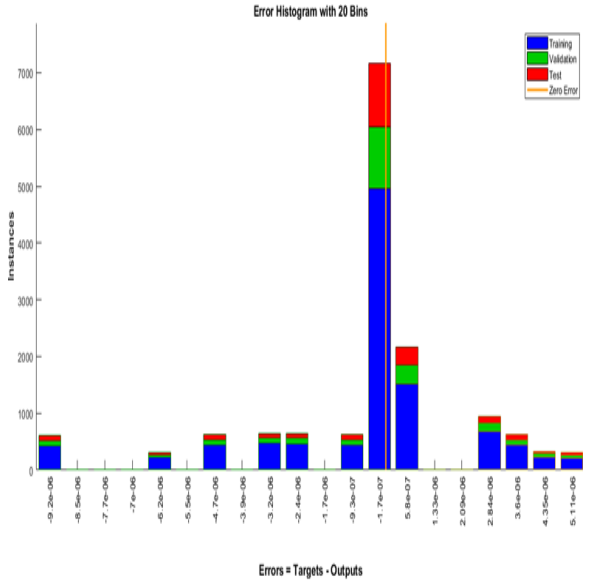

Figure 7. Error Histogram of the Proposed Model

Figure 8. 2178 samples are taken from class 1, 1267 samples are taken from class 2, and 1555 samples taken from class 3, after simulation, the result shows all classes are accurately classified.

Figure 8. Confusion Matrix of Proposed model

Figure 9. The ROC curve of the test results on the right side is a plot of the true positive rate (sensitivity) against the false positive rate (specificity). A test indicates dots in the upper-left with sensitivity as well as specificity 100%. This matrix depicts properly accurately recognizing attacks and normal traffic with FPR = 0 and TPR > 98.85%. By ROC curve, the ROC curve shows the proposed model accurately classify the normal and attack traffic.

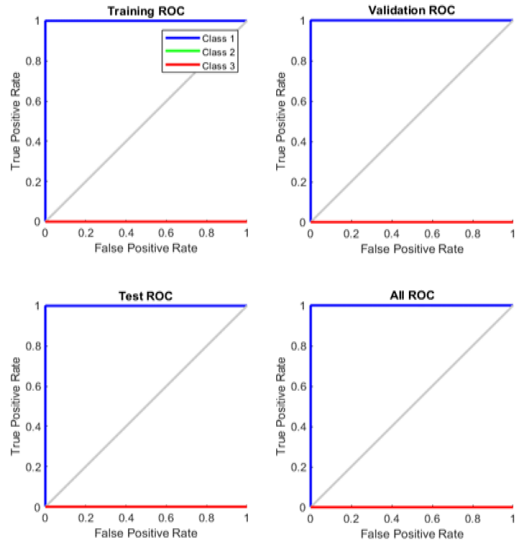

Figure 9. ROC of Proposed Model

COMPARISON OF DIFFERENT MODELS

After the successful classification into either attack or normal class, we compared the classification strength of DL-MLP with that of other state-of-the-art classification models, such as GA, naive Bayes, SVM, and decision trees. We tested the accuracy of detecting the attack class and normal class, and the sensitivity and specificity of the whole dataset. To compare the different classifiers, we compared the receiver operating characteristic (ROC) of the above-stated classifiers with DL-MLP, as shown in Figure 10, and construct a confusion matrix shown in Table 3. The plotted in figure 10 shows with X-axis representing false positive rate and Y-axis representing true positive rate using python.

To calculate the accuracy, sensitivity, and specificity from the confusion matrix for the classifiers,

we use Equations (9) – (11), respectively. The comparison between the various classifier models is given in Table 3.

$$\text{Accuracy} = a + d / a + b + c + d \quad (9)$$

$$\text{Sensitivity} = a / a + c \quad (10)$$

$$\text{Specificity} = d / b + d \quad (11)$$

From the comparison of the ROCs, it is concluded that DL-MLP has the perfect curve compared with the remaining classifiers

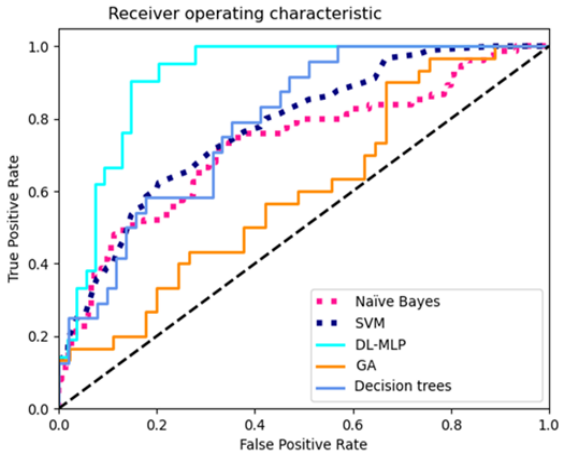

Figure 10. ROC of all models

Figure 11 shows a comparative analysis of proposed and existing techniques to analyze the detection rate. The proposed model shows a high detection rate among other classifiers.

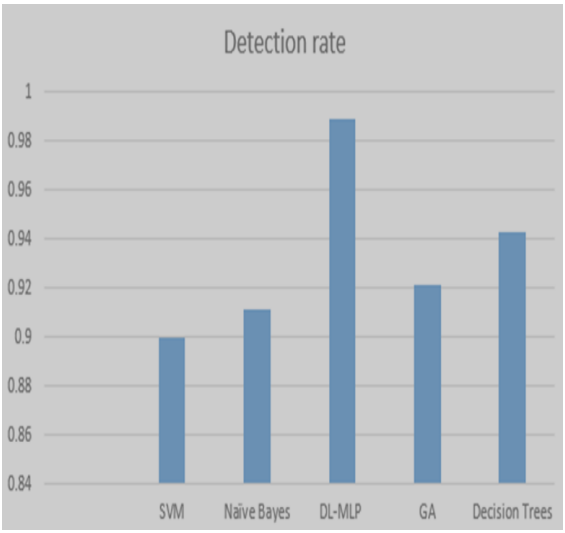

Figure 11. Detection rate of all models

Figure 12 shows the sensitivity graph comparison of the proposed model with the other model, the proposed model is a high sensitivity rate.

Criteria	DL-MLP	SVM	NaivBay	GA	Decision Trees
Confusion Matrix	267 (a) 5(b) 1(c) 84(d)	420(a) 45(b) 22(c) 10(d)	400(a) 40(b) 35(c) 200(d)	435(a) 33(b) 40(c) 5(d)	410(a) 44(b) 25(c) 34(d)
Accuracy	0.9831	0.8651	0.8888	0.7266	0.9032
Sensitivity	0.9999	0.9550	0.9195	0.9157	0.9425
Specificity	0.0561	0.8181	0.090	0.568	0.158

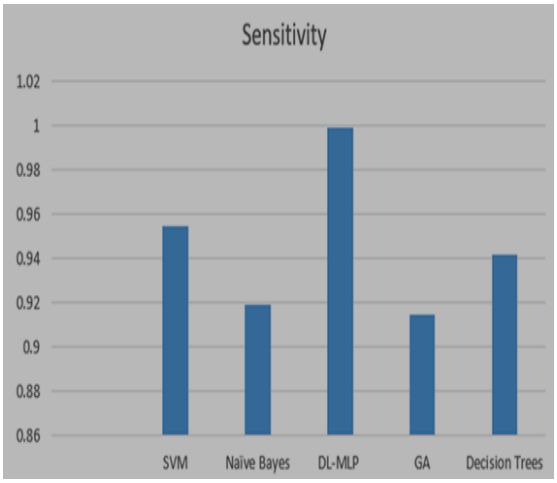

Figure 12. Sensitivity of all Models

Figure 13 shows the specificity graph comparison of the proposed model with other models, the proposed model is low specificity rate.

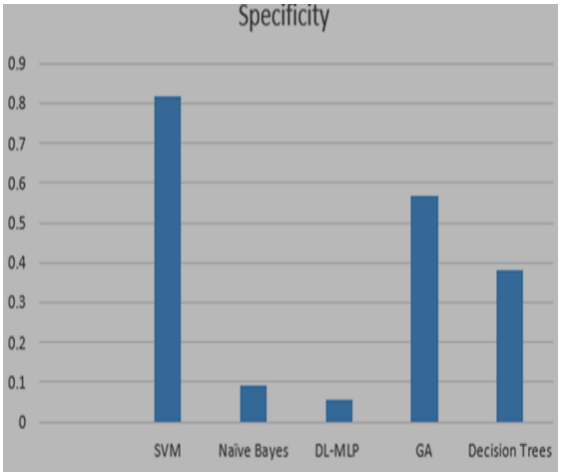

Figure 13. Specificity of all models

Figure 14 shows the accuracy comparison of the proposed model with the other model; the proposed model is a high accuracy rate.

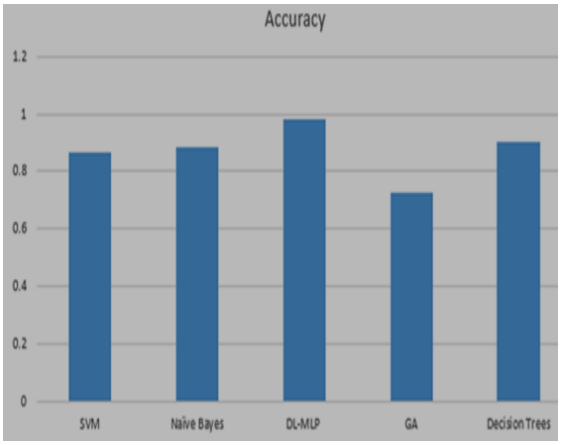

Figure 14. Accuracy of all models

To show the effectiveness of the proposed model in identifying application-layer DDoS attacks using deep learning neural networks, we compute the ROC curve for all classified classes. We also compare our results with the results of the other classifier. The comparison is shown in Table 3 and visual representation in figure 11-14. According to the obtained results, the overall performance of our proposed deep learning multi-layer perceptron model is much better than other classifiers.

CONCLUSION

In this paper, we propose a deep learning neural network that uses feed-forward architecture using eight hidden layers for classifying malicious users and legitimate users. The proposed approach protects services from application-layer DDoS attacks by using profiling the malicious user and legitimate user through the proposed system and detecting malicious behavior. It can also detect malicious behavior from packets if an entirely new malicious pattern is being used. Those patterns would serve as a secondary data set to train the neural networks in the proposed system. The proposed approach is evaluated using the generate benchmark dataset. The experimental results demonstrate the accuracy in terms of Accuracy Rate (AR), Detection Rate (DR), Sensitivity, specificity, (ROC) curve, our proposed model can detect the DDoS attack with accuracy is 0.983, sensitivity is 0.999 and specificity is 0.0561. The paper is limited only to application-layer DDoS attack detection. However, its prevention mechanism is not illustrated in the paper.

In future work, we will investigate further to improve the accuracy of detection and how to separate a layer seven DDoS attacks from a flash event through an analysis of their different accessing behaviors, and also extend our work to detect network layer DDoS attack.

REFERENCES

1. Singh, Karanpreet, Paramvir Singh, and Krishan Kumar. "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges."Computers& Security 65 (2017): 344-372.
2. Behal, Sunny, and Krishan Kumar. "Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review." IJ Network Security 19, no. 3 (2017): 383-393.
3. Jiang, Muhui, Chenxu Wang, Xiapu Luo, MiuTung Miu, and Ting Chen. "Characterizing the Impacts of Application Layer DDoS Attacks." In Web Services (ICWS), 2017 IEEE International Conference on, pp. 500-507. IEEE, 2017.
4. Yusof, Mohd Azahari Mohd, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus. "Detection and Defense Algorithms of Different Types of DDoS Attacks." International Journal of Engineering and Technology 9, no. 5 (2017).
5. Jazi, Hossein Hadian, Hugo Gonzalez, Natalia Stakhanova, and Ali A. Ghorbani. "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling." Computer Networks 121 (2017): 25-36.
6. Diovu, R. C., and J. T. Agee. "A cloud-based openflow firewall for mitigation against DDoS attacks in smart grid AMI networks." In PowerAfrica, 2017 IEEE PES, pp. 28-33. IEEE, 2017.
7. Behal, Sunny, Krishan Kumar, and Monika Sachdeva. "D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events."Journal of Network and Computer Applications 111 (2018): 49-63.
8. Kesavamoorthy, R., and K. Ruba Soundar. "Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system." Cluster Computing (2018): 1-8.
9. Thomas, Arun, T.Gireesh Kumar, and Ashok Kumar Mohan. "Neighbor Attack Detection in Internet of Things." In Advanced Computational and Communication Paradigms, pp. 187-196. Springer, Singapore, 2018.
10. Prasad, K. Munivara, A. Rama Mohan Reddy, and K. Venu Gopal Rao. "An Experiential Metrics-Based Machine Learning Approach for Anomaly Based RealTime Prevention (ARTP) of App-DDoS Attacks on Web." In Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 99-112. Springer, Singapore, 2018.
11. Rezaei, Hamed, Yaghoub Farjamib, and Mohammad Hossein Yektae. "A Novel Framework for DDoS Detectionin Huge Scale Networks, Thanksto QoS Features." arXiv preprint arXiv:1801.02300 (2018).
12. Hassan, Inzimam Ul, and Amandeep Kaur. "Prevention and detection of DDoS attack on WSN." 2018 (2018): 245-249.
13. Bharot, Nitesh, Priyanka Verma, Sangeeta Sharma, and Veenadhari Suraparaju."DistributedDenial-of-Service Attack Detection and Mitigation Using Feature Selection and Intensive Care Request Processing Unit." Arabian Journal for Science and Engineering 43, no. 2 (2018): 959-967.
14. Ali, Yasir, Yuanqing Xia, Liang Ma, and Ahmad Hammad. "Secure design for cloud control system against distributed denial of service attack." Control Theory and Technology 16, no. 1 (2018): 14-24.
15. Monisha, S., and K. Anitha. "Identification of Peer-to-Peer Botnets in DDOS Attacks." (2018).

16. Girma, Anteneh, Mosses Garuba, and Rajini Goel. "Advanced Machine Language Approach to Detect DDoS Attack Using DBSCAN Clustering Technology with Entropy." In Information Technology New Generations, pp. 125-131. Springer, Cham, 2018.
17. Koay, Abigail, Aaron Chen, Ian Welch, and Winston KG Seah. "A new multiclassifier system using entropy-based features in DDoS attack detection." In Information Networking (ICOIN), 2018 International Conference on, pp. 162-167. IEEE, 2018.
18. Zare, Hossein, Mojgan Azadi, and Peter Olsen. "Techniques for Detecting and Preventing Denial of Service Attacks (a Systematic Review Approach)." In Information Technology-New Generations, pp. 151-157. Springer, Cham, 2018.
19. Singh, Karanpreet, Paramvir Singh, and Krishan Kumar. "Fuzzy-based User Behavior Characterization to Detect HTTP-GET Flood Attacks." (2018).
20. Rais, Helmi Md, and Tahir Mehmood. "Dynamic Ant Colony System with Three Level Update Feature Selection for Intrusion Detection." International Journal of Network Security20, no. 1 (2018): 184-192.
21. Keshtgary, M., and N. Rikhtegar. "Intrusion Detection based on a Novel Hybrid Learning Approach." Journal of AI and Data Mining 6, no. 1 (2018): 157-162.
22. Nur, Abdullah Yasin, and Mehmet Engin Tozal. "Record route IP traceback: Combating DoS attacks and the variants." Computers & Security 72 (2018): 13-25.
23. Wang, Chenxu, Tony TN Miu, Xiapu Luo, and Jinhe Wang. "SkyShield: A Sketch-Based Defense System Against
24. Demir, Kubilay, Ferdaus Nayyer, and Neeraj Suri. "MPTCP-H: A DDoS attack resilient transport protocol to secure wide area measurement systems." International Journal of Critical Infrastructure Protection 25 (2019): 84-101.
25. Dimolianis, Marinos, Adam Pavlidis, Dimitris Kalogeras, and Vasilis Maglaris. "Mitigation of Multi-vector Network Attacks via Orchestration of Distributed Rule Placement." In 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 162-170. IEEE, 2019.
26. Dong, Shi, Khushnood Abbas, and Raj Jain. "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments." IEEE Access 7 (2019): 80813-80828.
27. DORON, Ehud, B. E. N. Yotam, and David Aviv. "System and method for out of path ddos attack detection." U.S. Patent Application 16/212,042, filed June 13,2019.
28. Prasad, K. Munivara, V. Samba Siva, J. Nagamuneiah, and Siddaiah Nelaballi. "An Ensemble Framework for Flow-Based Application Layer DDoS Attack Detection Using Data Mining Techniques." In ICT Analysis and Applications, pp. 9-19. Springer, Singapore, 2020.
29. Sharma, Ankita, and Anshu Bhasin. "Critical Investigation on Application Layer-DDoS Attacks: Taxonomy and Parameter Efficacy." In Proceedings of ICETIT 2019, pp. 921-934. Springer, Cham, 2020.[30] Singh, Aman Kumar, and Raj K. Jaiswal. "DDoSify: Server Workload Migration During DDOS Attack In NFV." In Proceedings of the 2020 9th International Conference on Software and Computer Applications, pp. 364-369. 2020.
30. Saxena, Utkarsh, J. S. Sodhi, and Yaduveer Singh. "An Analysis of DDoS Attacks in a Smart Home Networks." In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 272-276. IEEE, 2020.
31. Parra, Gonzalo De La Torre, Paul Rad, Kim-Kwang Raymond Choo, and Nicole Beebe. "Detecting Internet of Things attacks using distributed deep learning." Journal of Network and Computer Applications (2020): 102662.
32. M.Zolotukhin, T.Hämäläinen, T.Kokkonen and J. Siltanen, "Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic," 2016 23rd International Conference on Telecommunications (ICT),Thessaloniki,2016,pp.16,doi:10.1109/ICT.2016.7500408.
33. X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning,"2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong,2017,pp.18,doi:10.1109/SMARTCOMP.2017.7946998.
34. S.Yadav and S.Subramanian, "Detection of Application Layer DDoS attack by feature learning using Stacked Auto Encoder," 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, 2016,pp.361-366,doi: 10.1109/ICCTICT.2016.7514608.
35. C. Ye, K. Zheng and C. She, "Application layer ddos detection using clustering analysis," Proceedings of 2012 2nd International Conference on Computer Science and Network Technology, Changchun, 2012, pp. 1038-1041, doi: 10.1109/ICCSNT.2012.6526103.
36. H.Lin, S. Cao, J. Wu, Z. Cao and F. Wang, "Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices," in IEEE Access, vol. 7, pp. 164480-164491,2019,doi: 10.1109/ACCESS.2019.2950820.
37. M. Shtern, R. Sandel, M. Litoiu, C. Bachalo and V. Theodorou, "Towards Mitigation of Low and Slow Application DDoS Attacks," 2014 IEEE International Conference on Cloud Engineering, Boston, MA, 2014, pp. 604-609, doi: 10.1109/IC2E.2014.38.
38. J. Wang, X. Yang and K. Long, "Web DDoS Detection Schemes Based on Measuring User's Access Behavior with Large Deviation,"2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Houston, TX, USA, 2011, pp. 1-5, doi: 10.1109/GLOCOM.2011.6133798.
39. Jin Wang, Xiaolong Yang and Keping Long, "A new relative entropy based app-DDoS detection method," The IEEE symposium on Computers and Communications, Riccione,2010,pp.966-968,doi: 0.1109/ISCC.2010.5546587.
40. Bavani, K., M. P. Ramkumar, and Emil Selvan GSR. "Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined Network." In 2020

6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 380-385. IEEE, 2020.
41. Idhammad, Mohamed, Karim Afdel, and Mustapha Belouch. "Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest." Security and Communication Networks 2018 (2018).
42. Li, Saifei, Yunhe Cui, Yongfeng Ni, and Lianshan Yan. "An effective SDN controller scheduling method to defence DDoS attacks." Chinese Journal of Electronics 28, no. 2 (2019): 404-407.
43. Sree, Thankaraja Raja, and Somasundaram Mary Saira Bhanu. "HAP: detection of HTTP flooding attacks in cloud using diffusion map and affinity propagation clustering." IET Information Security 13, no. 3 (2018): 188-200.
44. Selvarajan, Shitharth, Masood Shaik, Sirajudeen Ameerjohn, and Sangeetha Kannan. "Mining of intrusion attack in SCADA network using clustering and genetically seeded flora-based optimal classification algorithm." IET Information Security 14, no. 1 (2019): 1-11.
45. Yue, Meng, Zhijun Wu, and Jingjie Wang. "Detecting LDoS attack bursts based on queue distribution." IET Information Security 13, no. 3 (2019): 285-292.
46. Ingham, Max, Jims Marchang, and Deepayan Bhowmik. "IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN." IET Information Security (2020).
47. Rongrong, Xi, Yun Xiaochun, and Hao Zhiyu. "Framework for risk assessment in cyber situational awareness." IET Information Security 13, no. 2 (2018): 149-156.
48. Lanotte, Ruggero, Massimo Merro, Andrei Munteanu, and Luca Viganò. "A formal approach to physics-based attacks in cyber-physical systems (extended version)." arXiv preprint arXiv:1902.04572 (2019).
49. Kwon, Donghyun, Hayoon Yi, Yeongpil Cho, and Yunheung Paek. "Safe and efficient implementation of a security system on ARM using intra-level privilege separation." ACM Transactions on Privacy and Security (TOPS) 22, no. 2 (2019): 1-30.
50. Jin, Hongyu, and Panos Papadimitratos. "Resilient privacy protection for location-based services through decentralization." ACM Transactions on Privacy and Security (TOPS) 22, no. 4 (2019): 1-36.
51. Powell, Brian A. "Malicious overtones: Hunting data theft in the frequency domain with one-class learning." ACM Transactions on Privacy and Security (TOPS) 22, no. 4 (2019): 1-34.
52. Vemulapalli, Chaitanya, Sanjay Kumar Madria, and Mark Linderman. "Security Frameworks in Mobile Cloud Computing." In Handbook of Computer Networks and Cyber Security, pp. 1-41. Springer, Cham, 2020.
53. Manasrah, Ahmed M., M. A. Shannaq, and M. A. Nasir. "An Investigation Study of Privacy Preserving in Cloud Computing Environment." In Handbook of Computer Networks and Cyber Security, pp. 43-61. Springer, Cham, 2020.
54. Jouini, Mouna, and Latifa Ben Arfa Rabai. "Towards New Quantitative Cybersecurity Risk Analysis Models for Information Systems: A Cloud Computing Case Study." In Handbook of Computer Networks and Cyber Security, pp. 63-90. Springer, Cham, 2020.
55. Kale, Rahul Vishwanath, Bharadwaj Veeravalli, and Xiaoli Wang. "A Practicable Machine Learning Solution for Security-Cognizant Data Placement on Cloud Platforms." In Handbook of Computer Networks and Cyber Security, pp. 111-131. Springer, Cham, 2020.
56. Vázquez-Ingelmo, Andrea, Á. M. Moreno-Montero, and Francisco José García-Peñalvo. "Threats Behind Default Configurations of Network Devices: Wired Local Network Attacks and Their Countermeasures." In Handbook of Computer Networks and Cyber Security, pp. 133-172. Springer, Cham, 2020.
57. Roy, Moumita, Chandreyee Chowdhury, and Nauman Aslam. "Security and Privacy Issues in Wireless Sensor and Body Area Networks." In Handbook of Computer Networks and Cyber Security, pp. 173-200. Springer, Cham, 2020.
58. Jain, Rachna, Nikita Jain, and Anand Nayyar. "Security and Privacy in Social Networks: Data and Structural Anonymity." In Handbook of Computer Networks and Cyber Security, pp. 265-293. Springer, Cham, 2020.
59. Ferrag, Mohamed Amine, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." Journal of Information Security and Applications 50 (2020): 102419.
60. Ma, Mimi, Debiao He, Shuqin Fan, and Dengguo Feng. "Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare." Journal of Information Security and Applications 50 (2020): 102429.
61. Hasan, MGM Mehedi, and Mohammad Ashiqur Rahman. "A signaling game approach to mitigate co-resident attacks in an IaaS cloud environment." Journal of Information Security and Applications 50 (2020): 102397.