Improved Security in Cloud Computer Networks Using RNN Deep Learning Techniques

Alaa Q. Raheema[1,*]

[1]Civil Engineering Department, University of Technology-Iraq, Baghdad, 10066, Iraq

40345@uotechnology.edu.iq

Abstract

DoS (denial of service) attacks address a remarkable new risk to cloud services and can really hurt cloud providers and their clients. DoS attacks can similarly achieve lost pay and security vulnerabilities due to system crashes, service power outages, and data breaks. Regardless, despite the fact that machine learning methods are the subject of assessment to distinguish DoS attacks, there has not been a ton of progress around here. In like manner, additional investigation is expected around here to make the best models for perceiving DoS attacks in cloud conditions. This change is proposed to search for a significant convolutional generative-arranged network as a significant learning model given further creating DoS attacks in the cloud. A proposed model of significant learning organizations (RNN) is used to fathom the spatiotemporal objects of organization traffic data, hence tracking down different models that show DoS attacks. Plus, to make RNN-LSTM all the more obvious for defending against attacks, it is acquired from a broad assortment of organization opportunity data. In addition, the model is dealt with by in reverse joint exertion and stochastic slope drop is the way into the current effortlessness of scaling among clear and saw traffic volumes. Test results show that the proposed model beats the latest particular attacks, relies upon denial of service, and undoubtedly shows misleading positive results.

Keywords: DOS Attack; Cloud Networks; Recurrence Neural Networks (RNN-LSTM); Attack Detection; Intrusion Detection System

1. Introduction

Monitoring cyber attacks has become an important matter due to the diversity of types of cyber attacks, their use of current and different programming, and the expansion of the scope of electronic breaks by cloud network programmers and computer programmers. However, DDoS attacks can be dealt with in two different ways. The basic procedure is to provide a directly comparable token and the resulting technique appears in the form of tokens. Direct attacks focus on any defect in the information systems layout, which causes damage and can potentially stop service. Also, malicious attacks attempt to search for different parts that are connected to parts of the system to attack and distort the flow and content of information [1-3]. The demand to produce improved security schemes for different practical implementations has increased and has been part of the utmost necessary and important to restrict internal with external intrusions and secure the institutions data and information which employ Internet and communications networks. To achieve these basic requirements, efficient algorithms are proposed that work with CLOUD networks to provide highly reliable detection and prevention of Cyber attacks by various means and methods. In fact, there are two central algorithms for cybersecurity aggregation and planning for cloud computing, called evaluation algorithms and control algorithms. The evaluation and control algorithms used in CLOUD networks are designed to achieve “utilitarian goals,” such as closed-loop security goals. In theory, the primary security goal focuses on achieving immunity against any malicious attacks on the electronic system. However, achieving the level of security also requires dealing with all variables and emergency circumstances. Also, when data and tags are collected from sensors of various computer network units including private information data which requires the application of security algorithms to ensure the authenticity of the data. The information network contains hundreds or thousands of compromised agents (bots, zombies or slave agents) which are more or less restricted by attacking one or more sections of the victim as shown in Figure 1 [2-5].

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

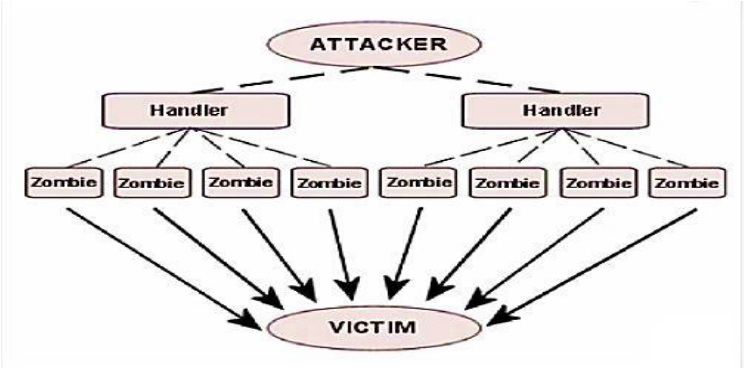


Figure 1. Schematic diagram showing the IDS system and its handling of several agents (bots or zombie) which attack one or more units of a computer network.

CLOUDs coordinate exercises and actual activities with exceptional projects and stages to communicate and introduce theoretical thoughts as well as displaying and plan, and incorporated examination strategies. It requires extraordinary interaction exercises between PCs, networks, and actual frameworks new plan as fundamental advances. As innovation depends on various trains like implanted frameworks, PCs, communications, and so on, with the product remembered for the equipment and its standard The primary component isn't just making computations, for instance, vehicles and clinical gadgets, logical devices, and intelligent transportation frameworks. The CLOUDs project is currently getting the interest of concerned analysts a lot right now [5-8]. Numerous modern districts, including power frameworks, shipment, downpour too medical care, give approved serious and significant improvements in schooling, control likewise pleasure over the last decagon, persuaded and out of dread and worries about manageability, proficiency and suitability, as this requires full similarity of frameworks, data, communications, and genuinely designed accounts, nitty gritty examination in the "examination and combination of cyber-actual frameworks, for example, of accomplishing the necessary norms for the ideal presentation and that the prerequisites for capacity, "maintainability" too confirmation, as the broad additionally brief presence of electronic things are many, and furthermore includes about undesired way to deal with such plans though, the broad with complicated existance of computerized units has underscored the feeling of dread toward undesirable path along several section towards like plans, as the material communication computerization demonstrated by ESCADA witness "supervisory control with information obtaining" to significant turns of events, which prompted a move against got, locked additionally cabled designs to structures. In this region, for the inductions of this examination, one allude to the "CLOUD" guarantee to present the insurance that is all right now utilized in an added substance highlight that is viable with protection against attacks and breaks, also provides adaptability, which is the characteristic of the framework that is viable with survival and recuperation after the assault or break [7-13]. Appropriated Denial of Service (DDoS) attacks are threatening preliminaries overpowered Online. In a DDoS assault, the organization's transmission capacity or the casualty's stores are depleted by communicating different bundles into an assigned server. DDoS assault programming has be present for quite a lengthy time, and various guard strategies are open for a conflict last exclusive-resource assaults. Subsequently, the stock of such assaults could be effectively obstructed or excused with the assist of further developed capacities. Although, intruders could choose through the immense proportion of powerless frameworks. Attackers utilize these frail hosts to begin an assault rather than using a solitary server, which is as of now not convincing today due to the remarkable improvement of Web use over the most recent decade. What's more, attacks by a solitary server may be effectively recognized. An aggressor controls various PC machines related with the Internet prior to starting an assault, such PC motor is named overseer, thus setting such PCs in an unfortunate spot. Then, by then, the assailant plants pernicious codes or apparatuses and other hacking strategies to exploit the weakness and shortcomings of such PCs and accept order through these apparatuses. This unfortunate engines are hence bargaining and afterward being " botnets." Quantities of botnets might be shown up at 100s or even 1000s [8-15]. Likewise, such tremendous catigories of freaks begin to shape a "zombies." The botnets degree concludes the step likewise satisfied of the assault's solidarity. A tremendous botnet accomplishes horrendous with serious assaults. DDoS gatecrashers have transformed towards a worldwide risk for the present Web. These intruders are specialists in nature and employ comparable techniques of regular DoS assaults against the exemption that the previous is done at a more prominent quality than the new through botnet. In general, it is recommended to employ a DDoS attack classification for IDS models, that effectively aggregates advanced classifications. This classification, which has four stages, is shown in Figure 2. The stages 1, 2, 3, and 4 intruders are classified in such investigation relied on the measure of computerization, counterability, also assault rate against effect driving, properly [9-15]..

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

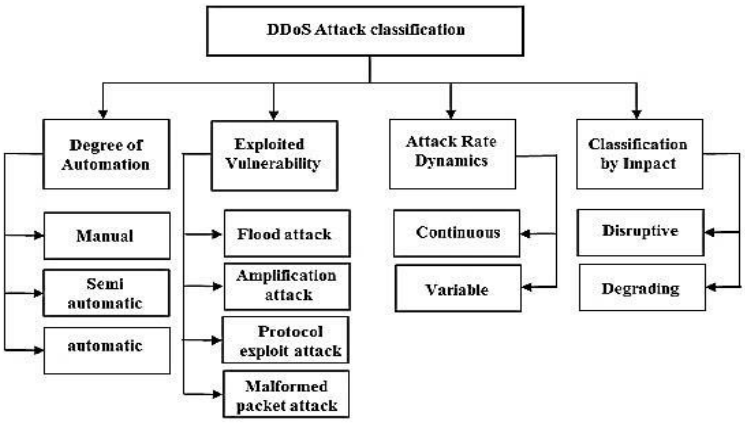


Figure 2. Classification DDoS attack in IDS system.

In fact, various types of cloud networks attacks available in literature such as, SYN stream assualt, internet control message protocol (ICMP) stream, user datagram protocol (UDP) stream assault, misuse attack and DoS attacks [8-20].

1.1 Defense Techniques of DDoS Assault

DDoS assaults are hard to decide. Basically, one of a kind DDoS attacks don't have typical elements along that they could being recognized. Besides, the scattered part of DDoS attacks makes them very difficult to go against or impact, and electronic program gadgets which spread DDoS attacks could being essentially accomplished. Invaders could additionally exploit IP mimicking to cover their personality and accordingly make the area of DDoS intrusions which is mind-boggling. In conclusion, machines related with the Web have deficient levels of wellbeing, with the web total against numerous security loopholes. Different experts have endorsed the usage of protection techniques to monitor victims with DDoS attacks. Figure 3 highlights the most inescapable factual and artificial intelligence draws near. In writing, various DDoS assault defense approaches have been suggested [10-15].

As illustrated from Figure 3, there are in general two main types of the DDoS defence techniques for cyber security systems (CSSs), which are; the statistical approaches, and the smart approaches which will be discussed in this study. Thus, the Cyber Security Systems (CSS) coordinate computing and messaging capabilities with scanning and controlling elements in the security world. These frameworks are generally created by a group of organized professionals, including: sensors, actuators, control processing units, and specialized tools.

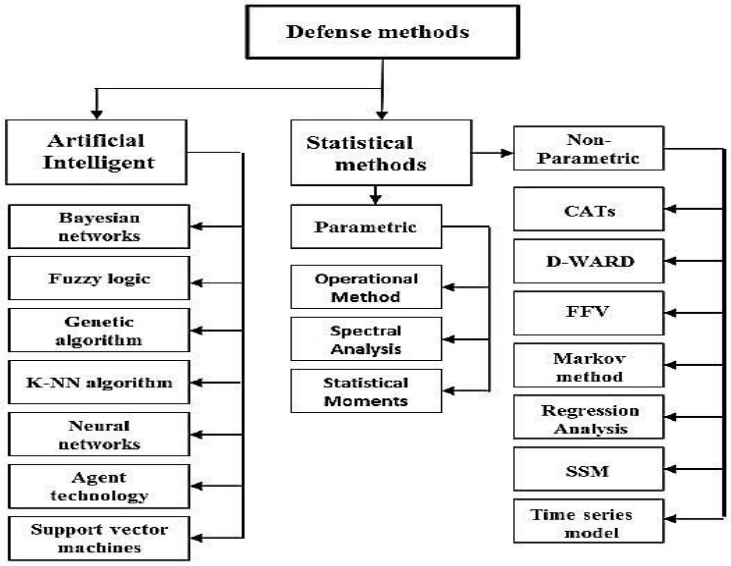


Figure 3. DDoS defense approaches using AI and statistical types.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

Anyhow, certain types of CSS are currently in use, the widespread development of remote implantable sensors and actuators is giving rise to a few new applications – in areas such as clinical tools, autonomous vehicles, and intelligent designs and extending the functionality of existing items [10-20].

1.2 The Statistical Defense Techniques

Actually, the statistical strategies, like entropy, correlation, and covariance, are the absolute utmost well known techniques for recognizing DDoS assults and breaking down and distinguishing anomalies in network stream. The statistical approach to DDoS intrusion detection works by extracting traffic statistics, which include the number of destination/source Internet Protocol (IP) addresses, Transmission Control Protocol (TCP) signals, packet sizes, flow rate, etc., to identify any abnormal behavior. Normal in traffic data flow [12-23]. Predictive models are used in statistics-based anomaly detection principles to detect intrusive malware and identify and control sophisticated exploit strategies. Such data models, which are collected within and around organizations, are being exploited to continually update and improve defenses. The statistical cyber-security bunch is creating information science strategies that empower huge dynamic PC networks to recognize intrusions and anomalous way of behaving and subsequently safeguard against cyber-attacks and false movement. Thus, the proportion of focal tendency and the proportion of scattering could depict the statistical appropriation of any event and gathering, yet they are not adequate to portray the idea of the circulation. For this reason, we utilize two other statistical measures that contrast the shape with the typical bend called Skewness and Kurtosis.Skewness and kurtosis are significant properties of conveyance that are concentrated on in elucidating measurements.

i) Skewness

Skewness is a statistical number that lets us know regardless of whether a dissemination is symmetrical. A dissemination is symmetric on the off chance that the right half of the conveyance is like the left half of the circulation. In the event that the appropriation is symmetric, the skewness esteem is 0. For instance, in the event that the appropriation is symmetric (typical dispersion): median = mean = mode, (skewness esteem is 0) On the off chance that the slant is more prominent than 0, it is called right slanted or the right tail is longer than the left tail. If the slant is under 0, it is called left slanted or the left tail is longer than the right tail [12-25].

The Skewness formula might be expressed as follows:

$$\text{Skewness } = \frac{\sum (X - \bar{X})^3}{(n-1).S^3} \qquad (1)$$

Such that, $\bar{X}$, represents the mean value, and S, denotes the standard deviation.

ii) Kurtosis

Kurtosis is a statistical number that lets us know whether a dissemination is longer or more limited than the typical circulation. On the off chance that the appropriation is like the typical circulation, the kurtosis esteem is 0. If the kurtosis is more noteworthy than 0, it means it has a higher pinnacle contrasted with the typical circulation. If the kurtosis is under 0, it is a level commonplace circulation. There are three sorts of disseminations: Leptokurtic: strongly crested circulation with fat tails and less unpredictability, Mesocortical: top mean conveyance, and Platykurtic: Level and exceptionally diffuse pinnacle dispersion [13-25].

Also, the Kurtosis equation could be oulined as below:

$$\text{Skewness } = \frac{\sum (X - \bar{X})^4}{(n-1).S^4} \qquad (2)$$

Where, , $\bar{X}$, denotes the mean value, and S, indicates the standard deviation.

iii) Autocorrelation

Autocorrelation alludes to the level of relationship between similar factors between two progressive time periods. It estimates the degree to which the slacked rendition of a variable's worth is connected with the first form of it in

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

a time series. Autocorrelation, as a statistical idea, is otherwise called sequential correlation. Autocorrelation is used to find out the extent to which the previous values of data affect its future values and the extent to which the current models are related and similar to the previous ones. Autocorrelation can help determine whether there is a similarity or difference in the data flow. Also, one of the most important uses of autocorrelation is to determine the extent of non-randomness of the data, as it gives an indication that the data is linked to the fact that it is free of randomness and vice versa.

Thus, the autocorrelation function might be expressed by the below formula:

$$R_{xx}(n) = \frac{1}{N}\sum_{i=0}^{N} x(i).x(i-n) \quad (3)$$

Therefore, these standards might be utilized in addition to other standards in conducting tests for statistical calculations, which are involved in detecting differences in the characteristics of the data and thus knowing whether it has been hacked or subjected to a cyber attack or not.

1.3 Deep Learning Defense Techniques

Deep learning procedures have arisen as section and because of machine learning strategies, that operate to mimic the human brain cells trying to address human reasoning way of behaving and program these methods by executing a system of preparing, practice, and variation dependent just upon the circumstance factors to be tended to. Deep preparation algorithms are recognized by their effectiveness and high accuracy in completing the errands expected of them, notwithstanding their proper expense and simplicity of programming, also their versatility also the chance of employing them in utmost complicated obstacles, for example, optimization, prediction object discovery, information mining, directing, following, and other significant and present day logical implementations. The main sorts of deep preparation algorithms will be evaluated in this section, and the idea of their study and inner construction will be studied.

A) Artificial Neural Networks

A regular neuron is an analytical value; it is represented as a structure of biological neuron. Regular neurons are primitive cells in a hidden neural system. Figure 8 presents the overall algorithm for a normal neuron [10-22]. The regular neuron which is illustrated in the above chart has n entries represented as $\{X_1,X_2,\dots,X_n\}$. Every direction which interfaces such improvements to the addition a weight is assigned to indicate the intersection as $\{W_1,W_2,\dots,W_n\}$. The nets data y_{in} might be represented as below:

$$yin = x_1.w_1 + x_2.w_2 + x_3.w_3 + \dots + x_n.w_n + b \quad (1)$$

The improvement function $F(a)$ is part of the essential remains of a neuron. A little starting abilities might become along of (restriction function, direct density, sigmoid function). With such section, a sigmoid function has been selected for its nonlinearity which consist of it probable to imprecise either quantity. Numerical structure of the formal neuron model presented in Figure 4.

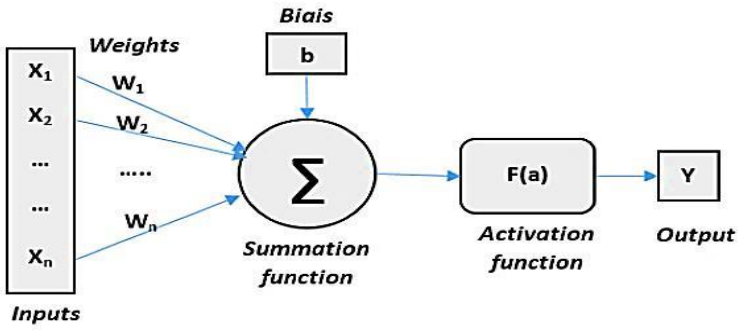


Figure 4. Numerical structure of the formal neuron model

Moreover, the result $\boldsymbol{y}$ of the neuron is provided in the hidden layer:

$$y = F(y_{in}) \sum w_i * x_i + b \quad (2)$$

Figure 5 displays a demonstration of the sigmoid function [12-23].

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

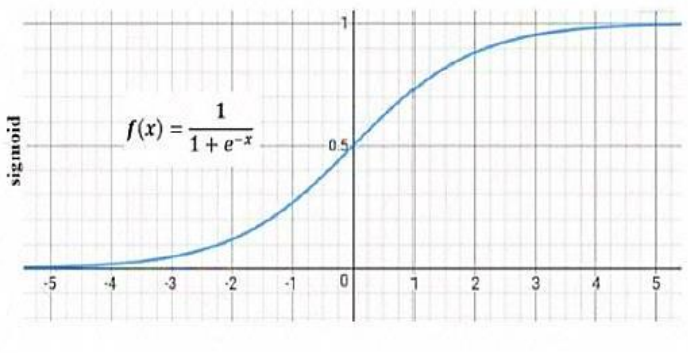


Figure 5. Demonstration of the sigmoid function.

Moreover, the multi-Layer-perceptron (MLP) is a class of feed-forward neural network that has somewhere near three layers of center points. It makes a lot of yields $\{y_1, y_2, \ldots, y_m\}$ along a lot of information sources $\{X_1, X_2, \ldots, X_n\}$. Except for the data center points, each center is a neuron that clients a nonlinear inception work. Figure 6 illustrates the construction of the multi-Layer-perceptron (MLP) model[13-25].

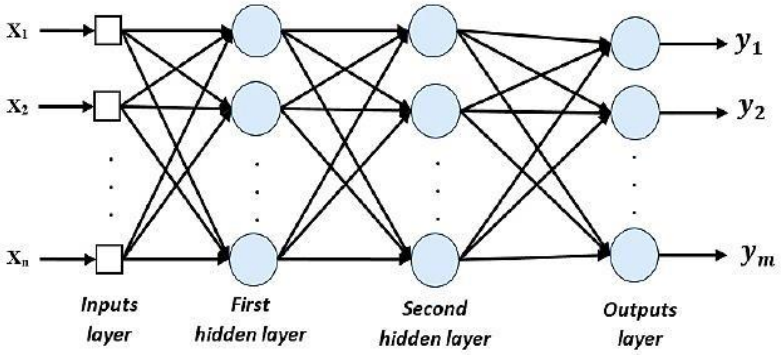


Figure 6. Construction diagram of the MLP scheme

A neural network is ready along data and objective pair plans against the limit of learning. MLP might seclude data that isn't straightforwardly conspicuous. It is especially arranged using a supervised learning strategy returned to proliferation (BP) technique, that objectives restricting the overall error assessed at the output layer by the association layer:

$$e(t) = y_d(t) - y_m(t) \quad (3)$$

$$E_g(t) = \frac{1}{2}\sum_{i=1}^{n}\left(y_{d,i}(t) - y_{m,i}(t)\right)^2 \quad (4)$$

Where $y_d(t)$ implies the best yield, and $y_m(t)$ the conscious result of the neuron. The BP algorithm uses an iterative supervised training framework, whereas the MLP is ready against a lot of predefined wellsprings of data and results. The overall misstep E_g not entirely set in stone by relation (4), this error might be restricted by the gradient descent method. There are a couple planning algorithms that could become used to prepare a MLP organization. In this review, we will present an emotional assessment between two getting ready algorithms: semi newton and structure slant. Wherein the used getting ready limits are independently train-LM: (Levenberg Marquardt (LM)) and train-SCG (Scaled Conjugate Gradient (SCG)) [13-25].

B) Recurrent Neural Network (RNN)

Researchers and interested parties conducted initial tests on distinguishing between fake images using machine learning. They proposed a statistical methodology to detect digital image forgery by analyzing false patterns to calculate image quality. Various procedures based on machine learning models that contain deep learning schemes such as discrete neural networks (RNNs) have been proposed to re-correct fake images. A feedforward brain network containing at least one hidden layers with what looks like a single connected circuit is referred to as a discontinuous network as shown in Figure 7 [13-25].

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

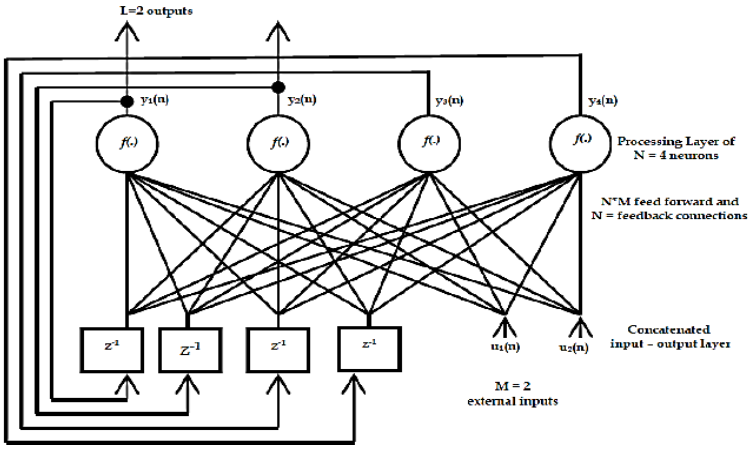


Figure 7. Recurrent Neural Networks, RNN schematic chart

As displayed in Figure 7, the feedback may be autonomic, or at least, the aftereffect of the activity of the not entirely set in stone by its approach of preparing. The feedback system include the implementation of defer unit parts with a few districts, prompting a non-linear dynamic way of conduct, as an intelligent lattice will be supposed to have backhanded units. Various elective sorts could fluctuate in the methodology of inner connecting, however they accomplish a similar point and wanted outcome, which is applying reiteration. Because RNNs have interior storage, they could deal with posted successions of fluctuating dimention with display physical kinetics. An illustration of a straightforward RNN design might be observed in Figure 8 [13-25]. Regarding the RNN algorithm design introduced in Figure 12, one might notice the common sections those have take entered marks aperture $Xt{-}w{:}t{-}1$ to estimates the advance instant print as result, $x'.t$. Recurrently, the entered arrangement is taken care of to the organization timestamp. In this manner, by employing the entered grouping $xt{-}1$ of the repetitive entity $ot{-}2$, using the enactment capability as $tanh$, the subsequent samples $x't$ is evaluated using the beneath expression:

$$x'_t = \sigma(W_{x'}, o_{t-1} + b_{x'}),$$
$$o_{t-1} = \tanh(W_{o.x_{t-1}} + U_o.o_{t-2} + b_h) \quad (5)$$

Where Wx', Wo, Uo, and b represent the components of the network. Repetition is achieved when the network uses the previous results as they were entered to perform recall and remembering operations for what was learned through training data, as explained during the previous procedures.

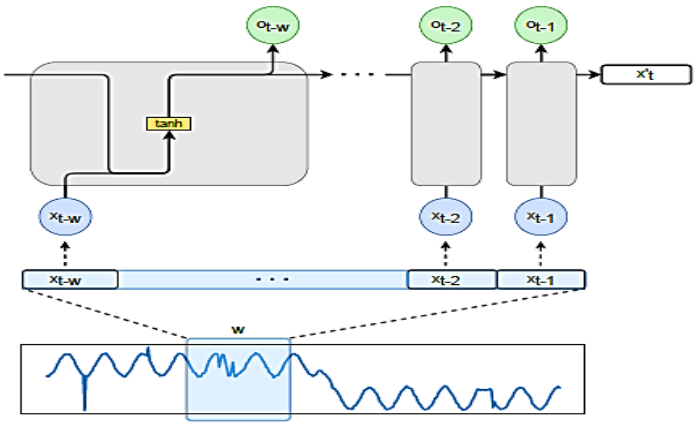


Figure 8. An example of a typical RNN structure

In fact, this is where the network of long- and short-term assumptions is learned and trained. RNNs include three types of main algorithms, namely (1) the long short-term memory (LSTM) algorithm, (2) the recurrent unit (GRU) algorithm, and (3) the recurrent neural network (RNN) algorithm, as presented in Figure 9 [14-30].

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

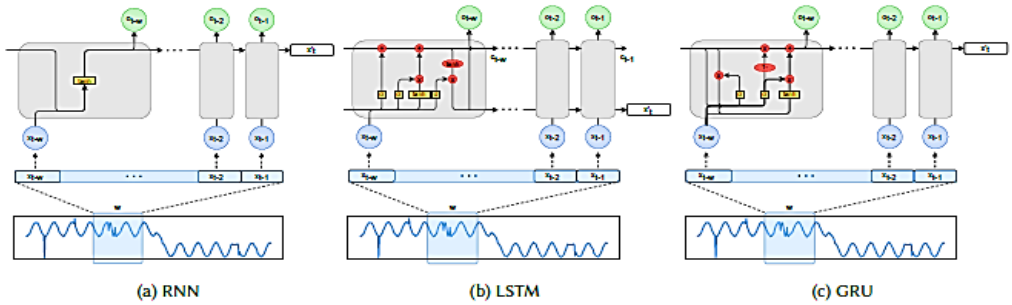


Figure 13. Determining relied models structure, (a) recurrent neural network (RNN), (b) long short-term memory (LSTM) unit, and (c) generalized recurrent unit (GRU)

2. Literature Review

This section offers a concentrated and definite review of various ways of managing recognizing and thwarting DDoS assaults, as shown by quantifiable and Artificial Intelligence (artificial intelligence) - based strategies that are conceivable at Open Systems Interconnection (OSI) network-layer level. A sum of 145 investigation paper and a few critical current papers are covered in this study. The overview segments DDoS assaults as shown by the class of weakness, the degree of robotization, impact, and components. These protection techniques use balance, area, as well as counteraction of DDoS assaults. What's more, this review integrates ordinary testing datasets and appraisal methods. The request for such DDoS assaults, a broad and significant viewpoint on a few DDoS protection methods, and tables of thinking are underlined. This review approach grants us to chip away at the augmentation and shape the heading of DDoS research. Dispersed Denial of Service (DDoS) attack has been generally around investigated and different systems have been recommended throughout the course of recent years to confront it. In any case, the ultimate of such examinations bases on the standard affiliation. Our center is coordinated into security cases about SDN-based foundation. Regardless of the way that SDN shares two or three relative contemplations as conventional affiliations, it has its stand-apart credits. Current undertakings to perceive DDoS attack can be extensively organized under two kinds of acknowledgment instruments, either dependent upon bunch overview or stream portions evaluation. In 2015, Li, S. et. al., [8] considered DDoS assaults as a critical risk defying web applications. They explored enormous assaults of DDoS which are again and again assigned at a couple of affiliations like eBay, Amazon, CNN, and Buy.com. The upsides of this study are; 1) realizing DoS assaults classifications that influence the web applications, 2) concentrating on the impacts of these assaults on different web applications like eBay, Amazon, CNN, and Buy.com, and 3) organizing these assaults as indicated by their threats to give the appropriate defense methodologies. The weaknesses of this study are; 1) the DoS didn't think about all web applications, and 2) there was a lack in the defense strategies conversation. In 2014, Prasad, K., et. al., [9] inspected kinds of DDoS attacks, that are two sorts characterized as weakness with flooding [8]. Flooding attacks contain the changing of the zombie's multitude with the interlopers to going after bundles that are going into their goal. Here is pointed toward growing the traffic to a sum that the person in question and his/her system can't deal with, in this manner achieving the crashing of the casualty's structure.

The benefits of this article are; 1) concentrating on DoS attack types known as weakness with flooding, and 2) concentrating on their construction and plan of attacking through the system to influence the casualty information. The weaknesses of this study are; 1) the lack of full numerical conditions, and 2) there was a lack in the defense strategies conversation. In 2015, Aggarwal, A., et. al., [10] presented arranged DDoS attacks In light of the procedure for assault, flooding attacks were called straightforward and incidental (along reflectors) DDoS. The upsides of this paper are; 1) introducing a survey of DDoS attacks organized in light of the assault methodology Immediate and accidental (along reversals) DDoS flood attacks are called DDoS, and 2) concentrating on their ideas of activities and plan of assorting through the system to influence the casualty information. The detriments of this article are; 1) the lack of adequate representation outlines, 2) pool of the defense methodologies conversation, and 3) the lack of full numerical conditions. In [11], Giotis et al. recommended an inconsistency-based distinguishing proof methodology, along the introduced framework basically looking at the stream areas and applying an entropy-based computation to take apart the assembled information. Subsequently, perceived surprising arrangements lead to discouraging the wellspring of the attack. The upsides of this examination are; 1) introducing an information classification and stream alignment defense strategy against different DoS attacks, and 2) the creators organized the introduced attacks like Application DDoS with Net DDoS spam attacks which makes greater ferocity. The drawbacks of this study are; 1) lack of analytical relations conversation, and 2) the lack of adequate delineation diagrams. In 2017, Somani, G., et. al., [12] presented another classification gave is that

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

introduced by [9], which described such attacks as subject to the protocol stage that is influenced; such makers organized them like Application DDoS with Net DDoS flooding attacks. Benefits of this examination are; 1) Another classification, which recognizes such attacks relying upon the impacted protocol stage, and 2) the creators organized the introduced attacks like Application DDoS with Net DDoS spam attacks which makes greater ferocity. The hindrances of this article are; 1) the lack of defense techniques conversation, and 2) the lack of adequate delineation charts. In [13], creators wanted to manage interruption and DDoS assaults in SDN environment by applying man-made intelligence techniques. Anyway, they just analyzed different man-made intelligence procedures, for instance, Support Vector Machine (SVM), feathery reasoning, decision tree, brain organizations, and Bayesian organizations, that may be used to perceive DDoS assaults in the systems organization structure without any explanation of how to perceive as well as reduce DDoS attack has been given. The benefits of this review are; 1) concentrating on interruption and DDoS assaults in SDN environment applying simulated intelligence systems, 2) applying classification and machine learning strategies for DDoS defense provision, and 3) the high exactness and accuracy in enemies of attacks activities. The burdens of this paper are; 1) high computational time for a bigger sum of flood assault information, 2) higher muddled than different methodologies, and 3) ongoing lake issues. Jankowski et al. [14] presented an interruption recognizable proof procedure using self-coordinated guides (SOM) as a Machine Learning (ML) technique. Such approach relies upon audit of stream areas, where eleven features isolated from stream entries delivered by various Virtual Machines (VM). Nevertheless, this approach zeros notwithstanding the features of streams, additionally, ignores incorporates that are related to the attack traffic. The upsides of this exploration are; 1) presenting an interruption recognizable proof procedure using self-coordinated guides (SOM) as a Machine Learning (ML) system, 2) high exactness due to executing Virtual Machines (VM), and 3) high organization in activity with assaults traffic. The inconveniences of this study are; 1) high computational time for bigger measures of assaults traffic information, and 2) bigger computational time than different methodologies. Wang et al. in [15] introduced the DDoS attack revelation model given an outline model. In this model, acknowledged attack plans are taken care of as a social outline among plans and their imprints to perceive normal and sporadic traffic.

At the point when the uncommon traffic is perceived, by then the wellsprings of the assaults are prevented. The upsides of this article are; 1) working of DoS attacks assaults with sporadic traffic, 2) great constant execution, and 3) high exactness, less intricacy, and less activity time with unpredictable traffic. The disservices of this examination are; 1) restricted to social outline model applications, and 2) lack of analytical conditions. Makers in [16] acquainted a procedure with perceive the DDoS attack that goals the SDN controller resources. The proposed plan relies upon analyzing the entropy assortment of the objective IP area with probability assessment in the midst of different hosts. Despite the fact that the proposed course of action endeavors to address attack acknowledgment, it presents extra vertical on the controller that could make it further defenseless against arranged DDoS assaults especially as there was no evasion remedial respected. The upsides of this study are; 1) the advantages of the entropy assortment of the objective IP area with probability assessment in the midst of different hosts, 2) better ongoing execution for SDN controller resources, and 3) endeavors to address attack acknowledgment. The hindrances of this examination are; 1) the lack of adequate outline charts, and 2) the lack of full numerical relations. Li et al. in [17] proposed a model considered Drawbridge which forms the clients to get involved with the ideal service given by ISPs to utilize the guidelines approved by the ISPs on their SDN transformations.

3. The Proposed methodology

In this section, the important design steps for implementing the proposed intrusion detection systems (IDS) security model to identify malware and identify network intrusions for Distributed Denial of Service (DDoS) flows through the use of artificial intelligence (deep learning) techniques will be explained and reviewed. The central concerns in our arrangement model are the informational indexes which ought to address two sorts of information, the first is the information (legitimate) informational indexes, and the second is the intrusion (malware) informational indexes. The approve web regions give many kinds of required information, and in this investigation, two critical objections were relied on for information handling, which are (kaggle.com, and github.com) as well as reenacting a couple of information using the useful elements of the MATLAB program.

3.1 The Implemented Dataset

According to the associated works, and late logical assessments concerning the subject of this proposition, the picked informational collections ought to be energetic, satisfactory, and flexible. Consequently, and as we as of late referred to the normal informational collections will be secluded towards two sorts; 1) the data (true) info, and 2) the intrusion (malware) informational collections. As a preliminary analysis of the information on this product provided through Kaggle.com, the information may be created by rearranging, organizing and preparing it appropriately. By developing a special methodology, the development of information will be changed from the entire CSV file to the DAT format (in the case of collecting information from the Internet), in addition to reducing

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

the amount of scattered data from the huge totals to vector numbers that will form the final data set. In this design, only two models will be selected out of over 2000 models. The basic protocol in the Internet protocol suite, which is the Transmission Control Protocol (TCP), will also be used. This rating is chosen as an Internet Protocol (IP) enhancement during core network testing. In this way, the data set will generally be referred to as TCP/IP modulation. A wave of octets (bytes) can be efficiently sent and passed over an IP network using TCP to later be mixed in with attack flows. TCP is used by critical Internet applications such as the Internet, email, remote link, and report transfer. The TCP data protocol will be handled by MATLAB m functions. Document code, to help TCP/IP information be processed into a virtual network structure in the code and analyzed programmatically." For this survey, we choose a specific type of information called TCP/IP for used (real) information datasets, while irregular (random) models are used) to represent intrusion (malware) data sets. The shapes of (real) information data sets are shown in Figure 10.

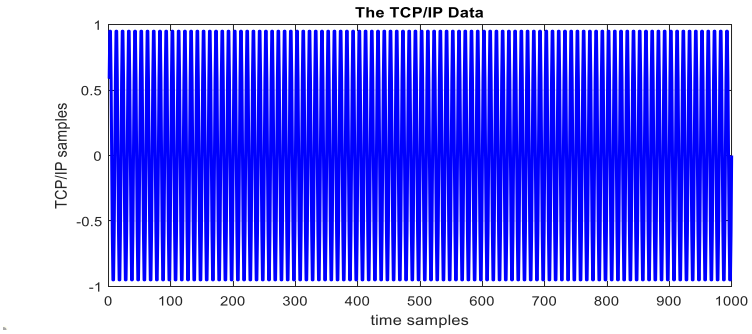


Figure 10. Demonstration graph of the TCP/IP data (true) datasets.

At the point when assault tests are created, they will deliver an irregular sign that taints or twists the state of the TCP/IP information. Figure 11 shows the DDoS arbitrary assault tests against time.

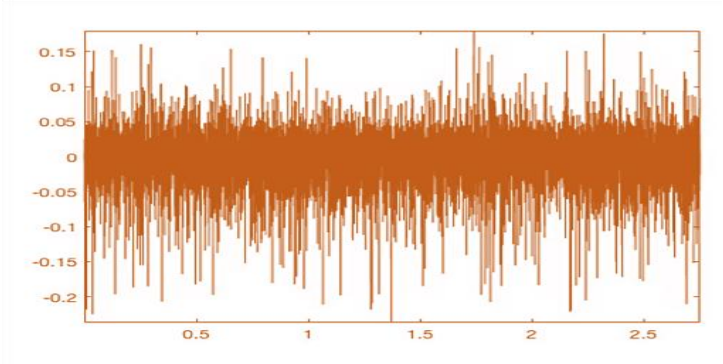


Figure 11. The DDoS arbitrary assaults time fragments.

Thus, the achieved corrupted (data plus DDoS assault) flood will be displayed in Figure 12.

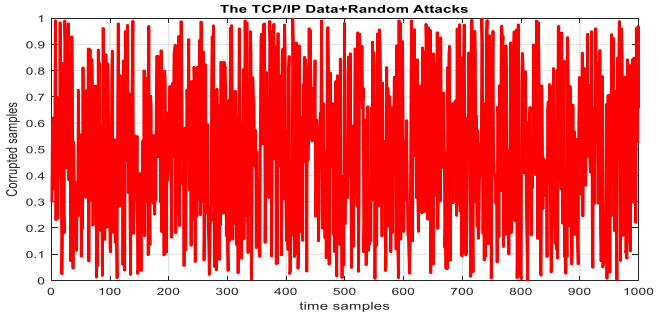


Figure 12. The obtained corrupted (data+ DDoS attack) flood samples.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

This data+ DDoS assault tests would be placed into the computer based intelligence algorithm to prepare its loads for perceiving the necessary true data and to dismiss the attacking data.

3.2 Design of Intrusion Detection Systems (IDS)

In this part, the Intrusion Detection Systems (IDS) will be introduced for detecting cyber attacks and identifying Denial of Service (DDoS) network intrusion executions with the assistance of an AI (PC-based intelligence) algorithm. The cybersecurity architecture will be equipped and secured using m-functions. Archive the script using MatLab2020b. It consists of the incoming units: 1) The input unit, that allows data and info to reach the network, 2) The verification point or control unit, which operates to verify the status of the information received into the network, 3) The statistical analysis and examination section, that provides the statistical evaluation and ranking of the information posted into the network, 4) The artificial intelligence (computer-based intelligence) algorithm unit, which works to manage the process of detecting security breaches from malware, random flows, attacks, and strange software information and isolates them from the data and information set, and 5) the final examination and verification unit, which operates to confirm and verify the The movement of information and data that passes through the network structure and ensuring that it is free from attack flows or any malicious programs. One can summarize the working of the suggested security architecture with all the modules described previous by the flow chart display in Figure 13.

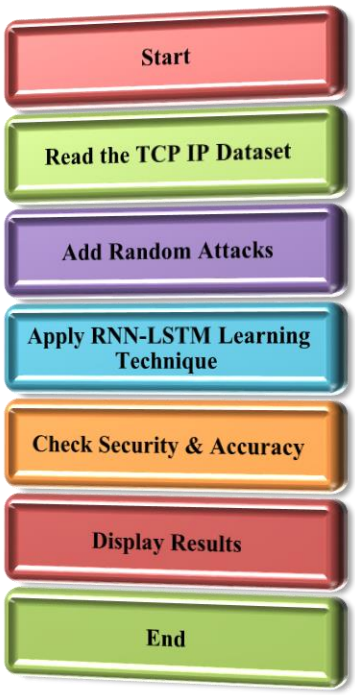


Figure 13. The proposed model methodology flow chart.

As one might observe from the proposed scheme flow chart presented in Figure 13, the suggested model will collect the important information data stream. There will be a checkpoint to choose if this pack is the referenced information package (non-hindering); in the event that it isn't, approach will be blocked; expecting it is, the posted information group will be transported off the model (i.e., it will not be obstructed). The entered information groups will be really investigated the going with advance toward check whether they contain an assault vector. The entered information will be taken care of and put aside as assault information, and access will be denied in the event that there is a positive assault vector check. The proposed model will be finished with pure information beyond assault designs if this isn't true. The information bundles will then, at that point, be appeared differently in relation to other standard activities for extra check. The information that went into the structure will in like manner be explored in the wake of beginning confirmation using statistical assessment systems (autocorrelation check, etc) and afterward passing dubious information to the artificial intelligence algorithm to get ready it and withdraw unfriendly and unwanted streams.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

As displayed in past works and review, specialists have dove into tests and examination in the field of assault and malware detection to identify and forestall DoS. The analysts talked about numerous classification as well as recognizing techniques, such as artificial intelligence algorithms. Among this large number of exploration and review, it worked out that the best strategies that have been utilized such a long ways in terms of effectiveness, speed, and accuracy of examination and detection are algorithms Artificial neural networks and their updates, which have demonstrated their "superb" execution in the area of classification, information testing, also fast recognition with extremely huge accuracy and proficiency. Such benefit is because of the versatile filters action in the design of such algorithms, that permit wide field of examination tasks.

To execute the possibility of data security in cloud correspondence networks with the assistance of deep learning strategies, a program was carried out that makes sense of a cyber data security network utilizing the Transmission Control Protocol (TCP) with the impact of a parcel assault and how to identify it. This assault was carried out utilizing deep learning algorithms versus statistical methods, for example, (Mean, standard deviation, kurtosis, skewness, and ACF). This software will likewise be utilized for boycott finding and assault anticipation innovation. The datasets utilized in this testing software comprise of Succeed records and varieties of standard information bundles required for preparing through the different cloud layers. Exhibited utilization of the RNN-LSTM algorithm as a deep learning method with a lower mean square error (MSE) while testing the prepared bundle with a superior capacity to distinguish the ongoing assault move through similar statistical estimations applied through standard learning algorithms. The blueprint of the data security model took on is displayed in Figure 14.

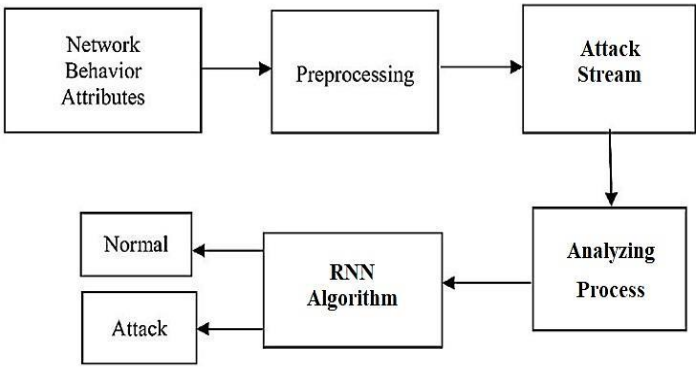


Figure 14. Block diagram of the trained RNN intrusion detection model.

The candidate program model describes the operation of the Recurrent Neural Network (RNN) algorithm based on the training data set by introducing (N = 2000 tests) to be distinguished to train the algorithm parameters to the extent that the security rates are appropriate and an appropriate MSE rate is reached. To understand the artificial neural network algorithm tool, data information represents the main data that is sent over the communication network. Such data are posted by collecting it into the the RNN algorithm input layer so that it is planned and ready for training. Such data is dealt with in classification techniques later providing it a basic fingerprint and then changing it by achieving it further encoding according to the basic name to advance classification precesion. The artificial neural network algorithm parameters (neurons) are trained, and their weights are updated by comparing the algorithm's outputs with the original data set and finding error flows. The resulting capacitive gains are then minimized by passing along the Relu layer, and such amounts are then collected in the pooling layer. Later to such procedures, the data are processed into the inner weight layers to prepare and update the algorithm layers to find the outcomes and deduce the amount of error and the best match. Finally, the settings and control parameters of the proposed RNN algorithm are shown in Table 1.

Table 1: The design specifications of the suggested WSN model.

Training Ratio	Neurons No.	Training Function	Max Epoch Counts
0.85	10	Gradient Descent	50
0.75	30	Bayesian Regulation	100
0.7	50	Levenberge Marquardt	200

According to the design specifications illustrated in Table 1, the proposed RNN-LSTM algorithm model will be employed using the MATLAB software that will be written to simulate the operation of the IDS model for intrusion detection and prevention.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

4 Results and Discussion

In this part, the proposed technology model for malware detection and network intrusion detection is implemented and tested to achieve security requirements with the help of artificial intelligence (deep learning) algorithms using MatLab2020b m. Text records. Scattered DDoS attack flows will also be represented using MATLAB randomization functions. This model shows the impact of DDoS packet attacks on a TCP/IP data set in a cloud network and how to handle and detect such intrusion using artificial intelligence methods and recurrent neural network (RNN) systems.

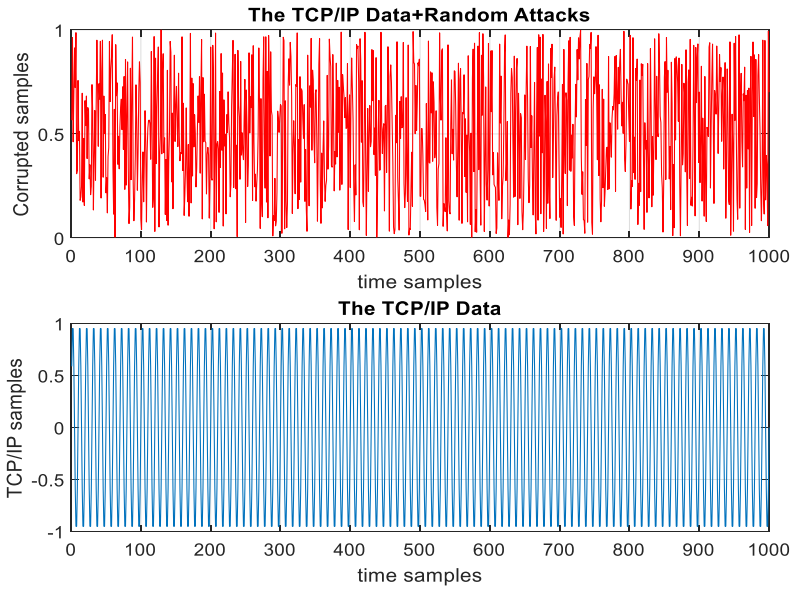
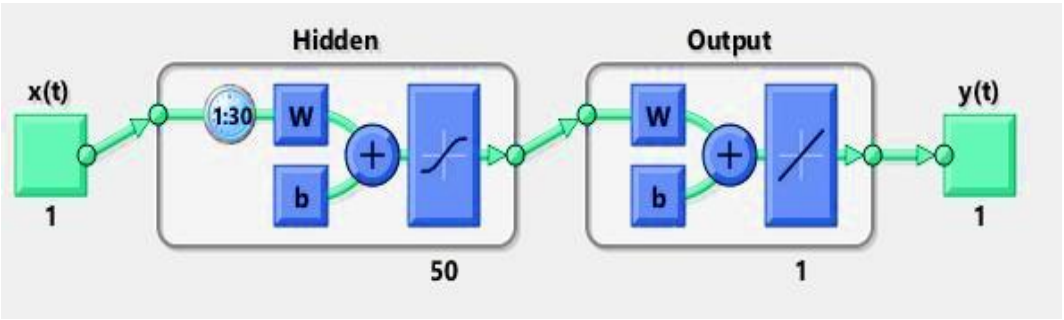


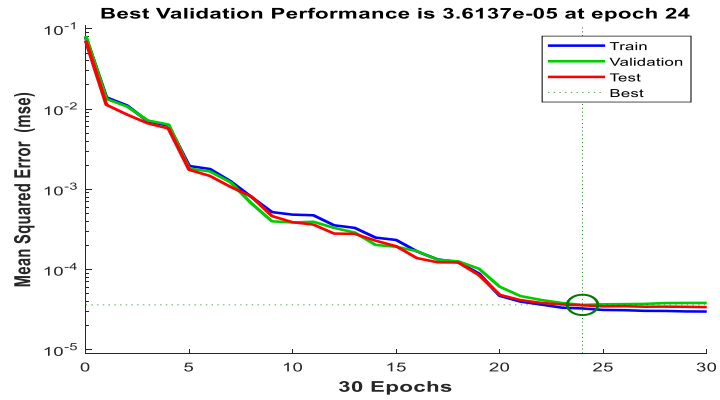
Figure 15. TCP/IP data sets against the intrusion attacks samples stacked to the model.

Taking a gander at Figure 15, one could notice the Abundance of the TCP/IP bundle stream with time tests showing up as various blended sinusoidal capabilities. The information TCP/IP data set bundle was introduced as a bar flood as displayed in Figure above. Likewise, the effect of the (arbitrary intrusion) flood is produced involving the random capability generator utility in MatLab2020 and introduced. As displayed here, the sufficiency of the assault packet is irregular dispersed against instant tested with a similar amount of parcel tests for the data set N = 1000. Such attack flood is graphed utilizing the bundle bar plot. Besides, the subsequent sign of summing the produced data sets with the arbitrary assault bundles has been shown. It is obvious from such chart that the irregular flood showed by the red-shaded examples has seriously adulterated the progression of the info data set examples. This activity will address a Denial of Service (DoS) occasion, and the subsequent dataset + attack flood will be dissected in our crossover hostile to assault scheme utilizing Profound Learning examination with RNN-LSTM algorithm innovation that addresses our Intrusion Detection Systems (IDS) cyber malware detection. Thus, by employing the RNN deep learning technology to the entered TCP-IP data stream corrupted with random attack floods, the results of the RNN DL training process are displayed in Figure 16.

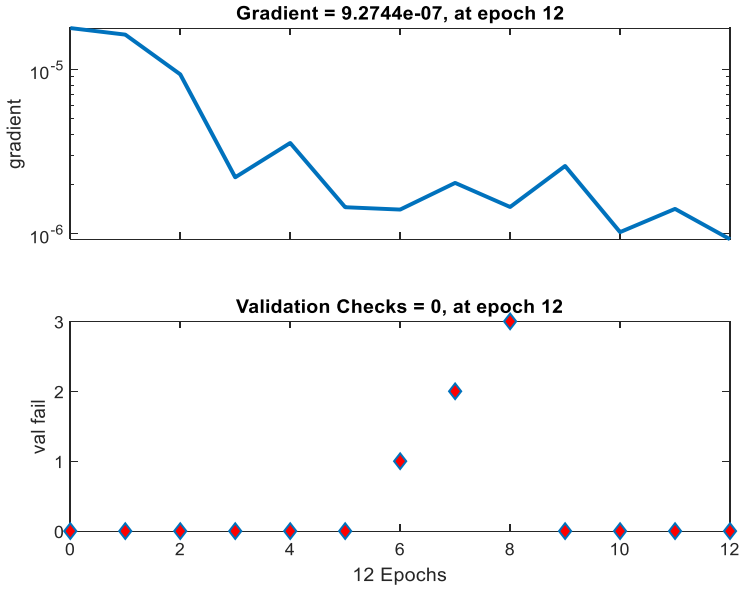


(a)

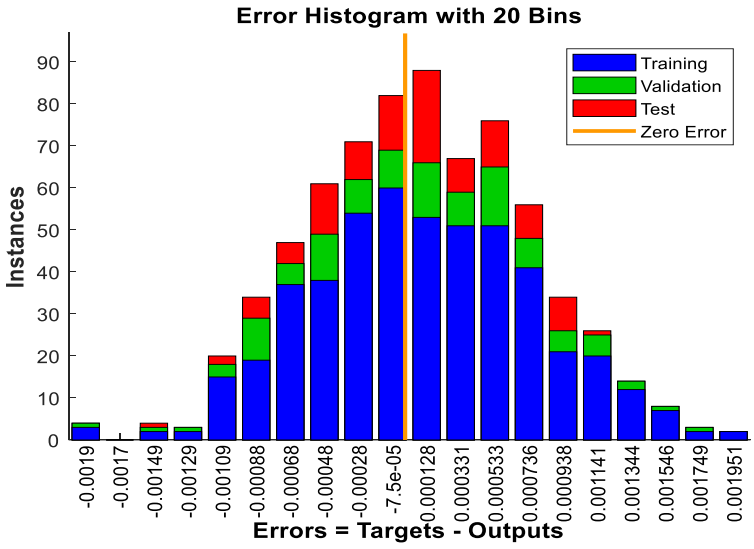
DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024



(b)

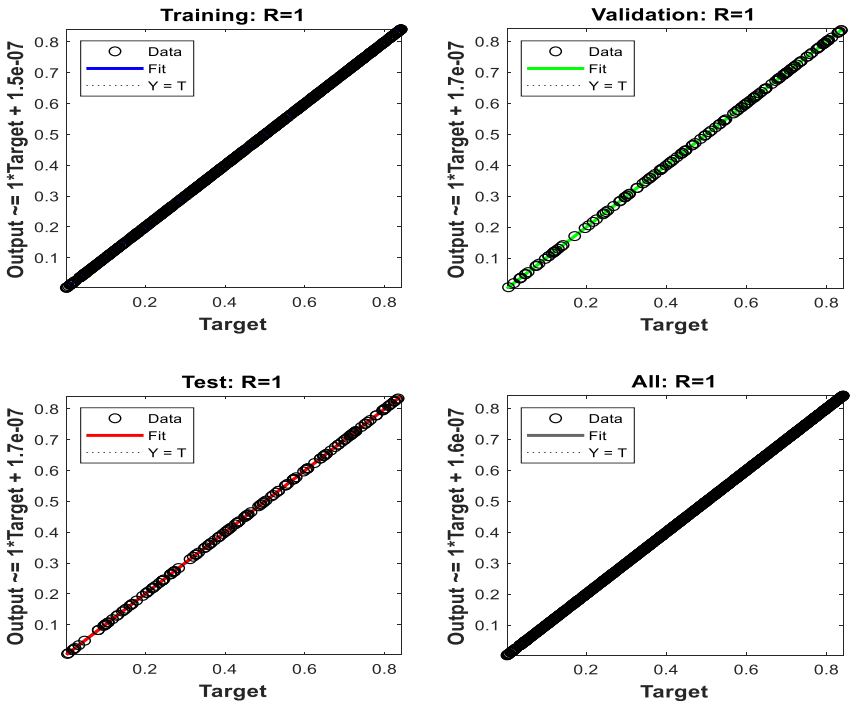


(c)



(d)

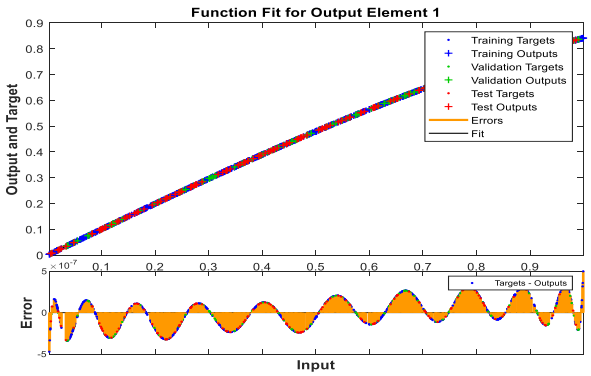
DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024



(e)

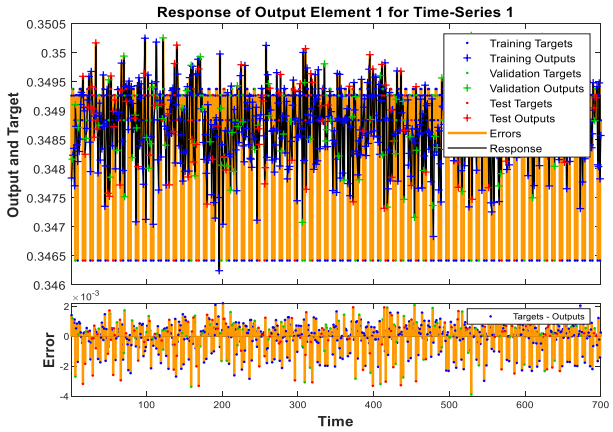
Figure 16. The results of the RNN-LSTM DL training process, (a) RNN model, (b) MSE performance, (c) Error histogram, (d) Training states, and (e) Regression (ROC) metrics.

In this way, unsettling Figure 16.(a), one could see that the accomplished RNN-LSTM model was planned by the changed boundaries with 50 neuron numbers for the secret layer. Likewise, with respect to Figure 16(b), the subsequent MSE execution of the approval, preparing, and testing tests has arrived at definite upsides of 3.614*10-5 error esteem at 24 age preparing tests which demonstrates an ideal detection and disposal of the intrusion (malware) parcel attacks happened in the mimicked IDS model. Likewise, in regards to the preparation states displayed in Figure 16(c), one could notice the slope with 9.274*10-7 qualities at 12 ages with approval check measure has been likewise assessed and recorded a worth of 0 at 12 age cycle tests, which further guarantees the reasonable RNN algorithm activity. Moreover, and as represented in Figure 16.(d), one could perceive the low upsides of error histogram records with just 20 containers and maximum error cases of 0.000378 at 90 cycle tests. Besides, the accomplished outcomes are displayed in Figure 16. (e), present reasonable regression estimations (likewise called receiver observing curve "ROC") for the preparation, approval, tried, and every one of the sums have been calculated and display an inclining (R=1) with ideal alignment amidst the objective with the result information. In reality, also as it is suggested by hypothetical ideas that the ideal equivalence among the results with the objective outcomes in the regression (ROC) estimations is gotten since R=1. Then, the time series reaction of the approval capability fit for the result elements has been additionally accomplished as presented in Figure 17.



(a)

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024



(b)

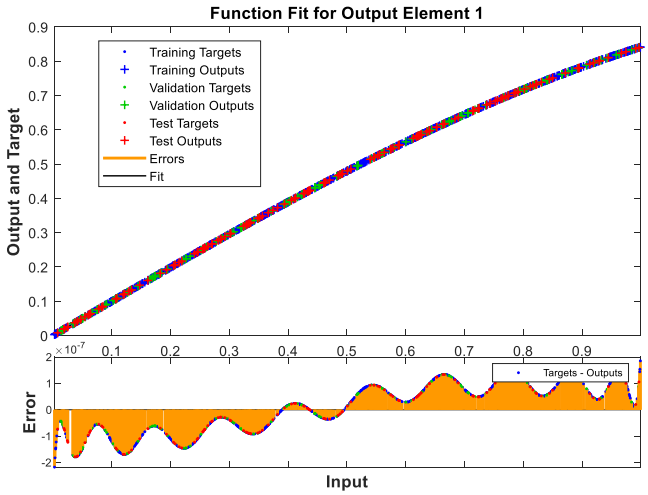
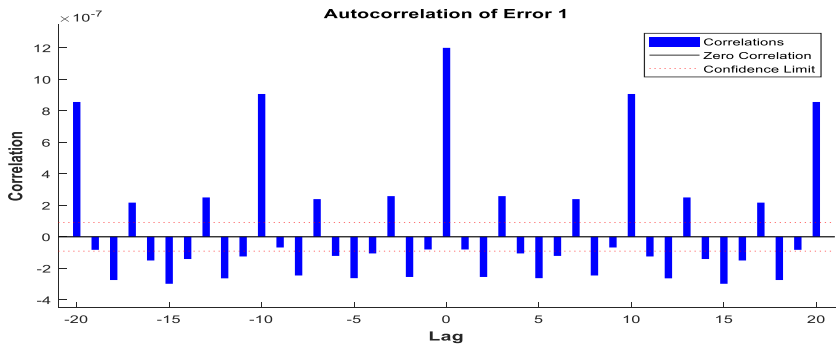


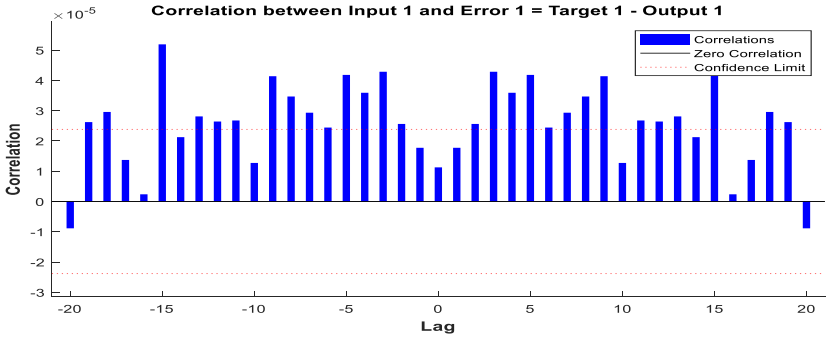
Figure 17. The time series response of the validation function fit for the output elements with various training functions, (a) Gradient decent, Bayesian regulation, and Levenberge Marquardt training function.

By concerning Figure 17, one might observe the time series response of validation function fit between the input and target dataset samples using different training functions applications. The correspondence between the results of the trained data (the output) and the required models (the target) might be observed after completing the training process of the intelligence algorithm and enabling it to extract data from data streams and basic sources according to the target function. Different types of training functions were used, each of which showed a high match with a low error rate, as shown in the figure. Moreover, the error auto correlation and cross correlation measurements have been obtained for the trained proposed DL algorithm as shown in Figure 18.



(a)

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024



(b)

Figure 18. The obtained correlation measurements for the trained proposed DL algorithm, (a) Error autocorrelation, (b) Error Cross correlation.

Figure 18 above shows that the autocorrelation consequence of the error created utilizing the proposed DL algorithm prepared demonstrates a comparability and little autocorrelation for the error signal 10-7 in Figure 18(a). Likewise, a little cross-connection of the error results, arriving at 10-5 as presented in Figure 18(b), shows the outcome of the preparation and empowers the proposed procedure to limit the surge of the assault tests. Accordingly, in this review, one could notice the activity of the proposed Intrusion Detection Systems (IDS) procedure which has been planned in view of the deep learning RNN-LSTM algorithm approach. The accomplished outcomes show an ideal detection for the intrusion (malware) going after bundle stream when they tainted the true tried TCP/IP informational index tests. A deep learning RNN algorithm model was applied to flow models and examined through the working mechanism described in this research. Table 2 has been created to illustrate the results achieved for effective detection and elimination of cyber attacks.

Table 2: The accomplished outcomes for productive cyber assault prevention and disposal IDS model utilizing RNN innovation.

Metrics	**Train**	**Validate**	**Test**	**Total**	**Samples Number**
EACF	2e-7	2.5e-7	2e-7	2e-7	2000
MSE	$3.614*10^{-5}$	$3.614*10^{-5}$	$3.614*10^{-5}$	$3.614*10^{-5}$	24
Gradiant	$9.274*10^{-7}$	$9.274*10^{-7}$	$9.274*10^{-7}$	$9.274*10^{-7}$	12
Error Histogram	0.000378 60	0.000378 75	0.000378 90	0.000378 90	 2000
Regression (ROC)	 1	 1	 1	 1	 2000

At long last, and by assessing the RNN algorithm assessment metric conditions made sense of in writing, we could accomplish the measurement values presented in Table 3.

Table 3: The accomplished RNN assessment metric outcomes.

Metric Values		Accuracy	Specifificity	Sensitivity	Precision	F score
TP	0.97989	98.194%	98.4%	98.39%	97.98%	98.19%
TN	0.98399					
FP	0.02011					
FN	0.01601					

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

By regarding the outcomes introduced in Table 3, it might be concluded that, the proposed DL RNN algorithm used for the IDS has provided a mailware intrution rejection with 98% accuracy for 2000 examination rounds.

5. Conclusion

In this study, a proposal is presented for models of DL algorithms used in achieving network security such as intrusion detection systems (IDS). The topic of achieving cybersecurity using intelligent hybrid technologies with the application of the RNN deep learning algorithm methodology is studied. Adversarial cybersecurity measures to follow up on detecting and blocking DoS flows were evaluated in this study with high efficiency using the proposed technique. The training and analysis results of the proposed RNN MSE algorithm model were obtained, showing an error performance of 3.614*10-5, with tolarance of 9.274*10-7, and an error correlation of 2*10-7 for 2000 attempts to evaluate the data set records and intermittent flood. Likewise, the regression metric, or ROC, scores between target and outcome and expected gains for all evaluation tests were 99% identical to prevent unwanted DDoS flows. Finally, A high detection and blocking efficiency of malicious flows, reaching 98%, was achieved by applying DL systems to confront various risks and attacks with a relatively low error rate of 0.12%.Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Agarwal, N.; Hussain, S. Z. (2018). A Closer Look at Intrusion Detection System for Web Applications. Security and Communication Networks, 2018, pp 1-27.
[2] Darch Abed Dawar, A. (2024). Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks. International Journal of Mathematics, Statistics, and Computer Science, 2, 183–198. https://doi.org/10.59543/ijmscs.v2i.9073
[3] Somani, G.; Gaur, M. S.; Sanghi, D.; Conti, M.; Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications 107, pp. 30-48..
[4] Firas Mahdi Muhsin Al-Salbi, “Investigation of QoS Multicast Routing Based on Intelligent Multiple Constrained”, www.ccsenet.org/cis Computer and Information Science Vol. 4, No. 4; July 2011, 64 ISSN 1913-8989 E-ISSN 1913-8997
[5] Deshpande, P.; Sharma, S. C.; Peddoju, S. K.; Junaid. S. (2018). HIDS: A host based intrusion detection system for cloud computing environment. International Journal of System Assurance Engineering and Management 9(3), pp. 567-576.
[6] Seyed Mohammad Mousavi and Marc St-Hilaire, (2019). Early detection of DDoS attacks against SDN controllers. In Computing, Networking and Communications (ICNC), 2019 International Conference on, pages 77–81. IEEE.
[7] Jun Li, (2018). Drawbridge: software-defined ddos-resistant traffic engineering. In ACM SIGCOMM Computer Communication Review, volume 44, pages 591–592. ACM.
[8] Li, S. H., Kao, Y. C., Zhang, Z. C., Chuang, Y. P., & Yen, D. C. (2015). A network behavior-based botnet detection mechanism using PSO and K-means, ACM Transactions on Management Information Systems (TMIS), 6(1), 3.
[9] Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2018). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. Global Journal of Computer Science and Technology.
[10] Aggarwal, A., & Gupta, A. (2015). Survey on data mining and IP traceback technique in DDoS attack. International Journal of Engineering and Computer Science, 4(06).
[11] Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30-48.
[12] Kostas Giotis, et. al., (2017). Combining openflow and sflow for an effective and scalable anomaly detection and mitigation mechanism on sdn environments. Computer Networks, 62:122–136, 2017.
[13] Javed Ashraf and Seemab Latif, (2018). Handling intrusion and DDoS attacks in software defined networks using machine learning techniques. In Software Engineering Conference (NSEC), National, pages 55–60. IEEE, 2014.
[14] Damian Jankowski and Marek Amanowicz, (2018). Intrusion detection in software defined networks with self-organized maps. Journal of Telecommunications and Information Technology.
[15] Bing Wang, et al (2019). Ddos attack protection in the era of cloud computing and softwaredefined networking. Computer Networks, 81:308–319.
[16] Hamid TABATABAEE, et al., (2019). Dynamic task scheduling modeling in unstructured heterogeneous multiprocessor systems, Journal of Zhejiang university – Science (Computers & Electronics) Vol.15, No.6, pp 423 – 434.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

[17] Uma Boregowda and Venugopal R Chakravarthy, (2018). A Hybrid Task Scheduler for DAG Applications on A Cluster of Processors, Fourth International Conference on Advances in computing and communications, Vol. 10, pp.143-146, August 2018.
[18] Jing Liu, et al. (2018). Minimizing system cost with efficient task assignment on heterogeneous multicore processors considering time constraint, IEEE Transactions on parallel and distributed systems, Vol.2, .No.8 ,August 2018.
[19] Vinaykumar, et al., (2019). A Novel Task Scheduling Algorithm for Heterogeneous computing, International Journal of Computer Applications, Vol.85, No.18, pp. January 2019.
[20] YAGOUBI Belabbas and KADRI Walid, (2019). Optimized Scheduling Approach for Scientific Applications Based on Clustering in Cloud Computing Environment, September 2019, Scalable Computing 20(3):527-540, DOI: 10.12694/scpe.v20i3.1548
[21] Wang, et al., (2019). Reliability-Driven Reputation Based Scheduling for Public-Resource Computing Using GA, Conference: The IEEE 23rd International Conference on Advanced Information Networking and Applications, AINA 2019, Bradford, United Kingdom, May 26-29.
[22] Nasr, et. al., (2018). Performance Enhancement of Scheduling Algorithm in Heterogeneous Distributed Computing Systems, June 2015 ,International Journal of Advanced Computer Science and Applications 06(05):88-96, DOI: 10.14569/IJACSA.2015.060514, License CC BY-NC-ND 4.0.
[23] Chronaki, Riko and Badia, (2015). Criticality-Aware Dynamic Task Scheduling for Heterogeneous Architectures, June 2015, DOI: 10.1145/2751205.2751235, Conference: the 29th ACM.
[24] David, et al., (2021).Detection of Denial of Service Attack (DOS), April 2021, Project: Detection of Denial of Service Attack.
[25] Mazhar Javed Awan, et al., (2021). Real-Time DDoS Attack Detection System Using Big Data Approach, Sustainability 2021, 13, 10743. https://doi.org/10.3390/su131910743, https://www.mdpi.com/journal/sustainability.
[26] Kushwah, G. S.; Ali, S. T. (2017). Detecting DDoS attacks in cloud computing using ANN and black hole optimization. In: 2nd International Conference on Telecommunication and Networks (TEL-NET), IEEE 2017, pp. 1-5.
[27] Ramin Fadaei Fouladi, et al., (2018). Statistical Measures: Promising Features for Time Series Based DDoS Attack Detection, Proceedings 2018, 2, 96; doi:10.3390/proceedings2020096 www.mdpi.com/journal/proceedings.
[28] D.J. Bernstein et al., (2020), Cryptographic Competitions, (DFG, German Research Foundation) under Germany's Excellence Strategy-EXC 2002 CASA 390781972 "Cyber Security in the Age of Large-Scale Adversaries", by the U.S. Na tional Science Foundation under grant 1913167, and by the Cisco University Research Program. "Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation" (or other funding agencies). Permanent ID of this document: b7af715576cc229aaf8c532ea89bb6acelc91a65. Date: 2020.12.25.
[29] Rajeev Singh and T. P. Sharma , (2020). Present Status of Distributed Denial of Service (DDoS) Attacks in Internet World, August 2019, International Journal of Mathematical, Engineering and Management Sciences 4(4):1008-1017.
[30] Zonayed Ahmed et al., (2017). Defense against SYN Flood Attack using LPTR-PSO: A Three Phased Scheduling Approach, January 2017, International Journal of Advanced Computer Science and Applications 8(9):433-441, DOI: 10.14569/IJACSA.2017.080957
[31] He, X.; Dai, H.; Ning, P. (2016). Faster learning and adaptation in security games by exploiting information asymmetry. IEEE Transactions on Signal Processing 64(13), pp. 3429-3443.
[32]Kajal, A.; Nandal, S. K. (2019). A Hybrid Algorithm using neural network and artificial bee colony for cyber security threats. International Journal of Innovative Technology and Exploring Engineering, 8(12), pp. 1-6.
[33] K. Igor and A. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms," International Journal of Computing vol. 4, pp. 113-123, 2014.
[34] K. Sharma and B. Gupta, "Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Present Era of Smartphone Devices, "International Journal of E-Services and Mobile Applications (IJESMA),"vol. 10, pp. 58-74, 2018.
[35] A. Saied, R. Overill and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," Neurocomputing, vol. 172, pp. 385-393, 2016.
[36] Abhishek Kajal, Sunil Kumar Nandal, "A Hybrid Approach For Cyber Security: Improved Intrusion Detection System Using ANN-SVM, August 2020, Indian Journal of Computer Science and Engineering 11(4): DOI:10.21817/indjcse/2020/v11i4/201104300.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024

[37] N. Z., Bawany, J. A., Shamsi & K. Salah, "DDoS attack detection and mitigation using SDN: methods, practices, and solutions ". Arabian Journal for Science and Engineering, 42(2), 425-441, 2017.
[38] J. Ye, Cheng, X., J. Zhu, L. Feng & L. Song, "A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018.
[39] Tsai C. F.; Hsu, Y. F.; Lin, C. Y.; Lin, W. Y. (2019). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), pp. 11994–12000.
[40] Lima F.; de, F. S.; Silveira, F. A.; Junior, A. D. M. B.; Solar, G. V.; Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks 2019.
[41] Watson, M. R.; Marnerides, A. K.; Mauthe, A.; Hutchison, D. (2018). Malware detection in cloud computing infrastructures. IEEE Transactions on Dependable and Secure Computing 13(2), pp. 192-205.
[42] Hosseini, S.; Azizi, M. (2019). The hybrid technique for DDoS detection with supervised learning algorithms. Computer Networks 158, pp. 35-45.
[43] Velliangiri, S.; Karthikeyan, P.; Kumar, V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. Journal of Experimental & Theoretical Artificial Intelligence, pp. 1-20.

DOI: https://doi.org/10.54216/JCIM.150129
Received: April 18, 2024 Revised: June 16, 2024 Accepted: August 20, 2024