A Comparative Study of Distributed Denial of Service Attacks On The Internet Of Things By Using Shallow Neural Network

Roheen Qamar[1,*], Baqar Ali Zardari[2], Aijaz Ahmed Arain[1], Zahid Hussain [2], Asadullah Burdi [3]

[1]Department of Computer Science, QUEST, Nawabshah, Pakistan
[2]Department of Information Technology, QUEST, Nawabshah, Pakistan
[3]Department of Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan
[*]Corresponding author: roheen.qamar04@yahoo.com

Abstract

The Internet of Things (IoT) is a term used to indicate a world in which objects are linked to the Internet. in some way, but not in the way that most people imagine. However, for the Internet of Things to be a success, computing must go beyond standard scenarios involving laptops and smartphones to include the networking of common intelligent Intelligence integration with the environment", "Smart homes, cities, and other wearable devices are examples. As a result, there will be new computing problems and features. Because of its variety, the Internet of Things has a difficult time guaranteeing universal privacy in areas like smart homes, smart hospitals, and so forth. Vulnerability can appear in a variety of forms. The internet of things has grown in popularity during the previous era. The internet of things (IoT), which may be characterized as a network of networked gadgets, has exploded in popularity during the last decade. Many elements of our lives have been fast-devoured by the Internet of Things (IoT). Smart homes, savvy cities, and other wearable devices are examples. IoT devices work to achieve their objectives, which include the building of a contemporary city. At the same time, there are a lot of security flaws in IoT devices that attackers could exploit. Distributed Denial of Service (DDoS) is the most common hazard to IoT security. The main goal of these assaults is to knock down victim computers and prevent legitimate people from accessing them using malicious software. The goal of this research is to provide compression of two algorithms 1. Scaled Conjugate Gradient (SCG) and 2. Levenberg–Marquardt algorithms (LMA) by training a Shallow neural network look into and assesses security vulnerabilities linked to DDoS attacks, as well as solutions like layered IoT device protection. In this research, it is discovered that the conjugant gradient algorithm has better accuracy as compared with Levenberg–Marquardt algorithm.

Keywords—Distributed Denial of Service, Internet of Things, and Internet of Things Security. Shallow Neural Network. Levenberg–Marquardt algorithm (LMA), Scaled Conjugate Gradient (SCG).

1 Introduction

Distributed Denial of Service (DDoS) refers to the use of multiple computers to launch DoS attacks. DDoS attacks coordinate the actions of many computers to deny users access to a victim machine's resources.DDoS attacks have evolved into an ongoing threat to the Internet. Even though this threat is well known, current countermeasures do not sufficiently reduce the volume, magnitude, or number of attacks. Arbour networks, on the other hand, reported an average of 1300 DDoS attacks per day in 2010. In 2017, the number of attacks increased to an average of 28,700 per day or nearly 20 per minute. The volume of DDoS traffic has increased, reaching terabytes of data per second in 2017. The number of people affected by DDoS attacks has steadily increased. In a Distributed Denial of Service (DDoS) attack, one of the major threats to any PC or Internet connection is phishing. In DDoS's early days, isolated servers would be disabled. Since 2007, entire countries have been deprived of the Internet. A DDoS attack is an attempt to render a system asset or a website unavailable for its authorized purpose. The Internet is powered by a large number of servers housed in server farms. When a server or its system is overburdened with client requests, the server or system ceases to function

ISSN: 2523-0379 (Online), ISSN: 1605-8607 (Print)
DOI: https://doi.org/10.52584/QRJ.2001.09

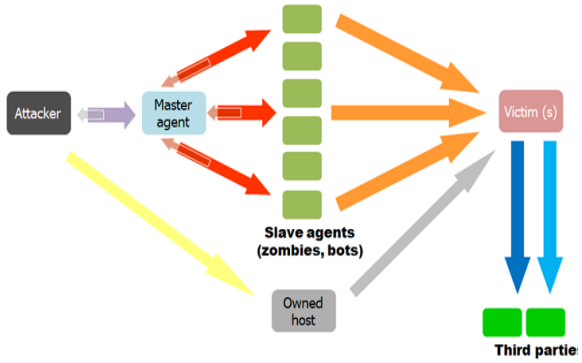


Fig. 1: Distributed Denial of Service Attack

properly and refuses to assist with legitimate demands [1, 2].

2 Distributed Denial-of-Service

Attackers utilize controller (inventor) machines to indicate the type of attack and the victim's address after creating and building the attack network. They then wait for the right moment to launch the attack, either remotely initiating the attack to "wake up" at the same time or programming ahead of time. The slave agent machines then start transmitting a stream of attack packets to the victim. The defendant's system is overburdened with meaningless data, depleting its resources. Due to a lack of resources, legitimate users are refused services. The DDoS attack is typically automated, with specially developed hacking tools, as shown in fig 1.

1) Attacker: Attackers send out a large number of packets or requests, eventually overwhelming the target system.
2) Master Agent: The master agent discovers other vulnerable devices and takes control of them.
3) Helvetica: Slave Agents: Slave agents, also known as attack servers, are in charge of directly attacking the victim.
4) Owned Host: own slaves' hosting checker tool gives detailed ownership and hosting information or attack to the victim.
5) Victim: A victim is a victimized target host.
6) Third Parties: The DDOS attack is transferred to the victim's system or devices. [3, 4] Figure 1 demonstrates the attack.

2.1 Attacks Used In Simulation DDOS

The Smurf attack targets a Web Communicate address with a large number of Web Control Message Convention (ICMP) ping signals. The response IP gives is a caricature of the expected hurt person. Instead of the IP used for the pings, all of the responses are provided to the injured person. Because of a single Web communication, a single ping is multiplied 255 times by a smurf assault, which may support up to 255 hosts. This slows down the system to the point where it becomes difficult to use. An intermediate IP broadcast network receives the request. This exploit impersonates an IP request and web server [5]. A massive volume of Internet Control Message Protocol (ICMP) echoes traffic sent by an attacker to several Internet Protocol (IP) broadcast addresses. ICMP echo packets contain the following information: The intended victim's source address (a spoofed address) is revealed [6]. Flooding in SYN Attack (SYN) works by saturating the unfortunate victim with fragmented SYN. This vulnerability may affect any machine that provides TCP-based network services. Half-open connections are used by attackers to force the server to consume all of its resources to keep track of all pending connections. The system would then crash or become unusable as a result [7, 8].

Perl Attack takes advantage of a flaw in some Perl implementations. It is a Perl modification that allows you to store the contents of your set client ID and set gathering ID. An adversary could use those contents to compromise the framework and get access [9].

Rootkit Attack is a collection of software tools that allow an attacker to get administrator access to a computer. A hacker often installs a rootkit on a victim's machine after gaining user-level access by exploiting a known flaw in the system or cracking a passcode [10].

Buffer Overflow Attack occurs when an attacker adjusts the support code with his own, thereby accelerating the attack. Strcpy (), strcat(), and sprint() are a few C functions that are vulnerable to this attack [11].

Attack on Load Modules is an attack on Sun OS 4.1 frameworks that use the x11 window system is known as a load module assault. Unauthorized users can gain root access on the local machine as a result of the effort in load module software [12].

Ipsweep Attack is a term used to describe a method of discovering who has been listening in on a system to locate vulnerabilities and breakout clauses [13].

Satan Attack RaaS is a simple type of ransomware that may be spread by anyone, even if they lack specialized knowledge. The way it works is that a skilled programmer creates the ransomware code and pitches it to others for implementation. The most current RaaS, dubbed "Satan," was discovered by a scientist known on the Dull Web as Xylitol. It allows anyone

to set up a record and create their version of Satan Ransomware. You don't have to pay a fee upfront; the virus designer is compensated by taking a 30% share of the installment payments made by unfortunate victims [14].

Teardrop Attack sends deformed IP addresses and larger-than-average data packets to the target PC, causing it to shut down or crash when it tries to understand them [15].

Spyware is a type of malware (sometimes known as "malevolent programming") that collects and distributes data about a computer or system without the consent of the user. It could be distributed as a hidden component of certified software bundles or through traditional malware channels such as deceptive advertisements, websites, emails, SMS, and direct document-sharing relationships. Spyware, unlike other types of malware, is widely used by criminal groups, as well as deceptive sponsors and companies, who use spyware to collect customer information without their consent. Regardless of its origins, spyware often escapes the client and is difficult to detect, but it can cause side effects such as distorted framework execution and a high recurrence of undesired behavior [16].

Password-guessing attacks on websites and web servers are fairly common. They are one of the most well-known vectors used to advertise discount sites. The technique is quite simple, and the attackers simply try numerous combinations of username and password until they find one that works. Once they've gotten in, they may employ malware, spam, phishing, or whatever else they want [17].

Client Warez Attack may be begin after the warez master assault has been completed. After a successful warez master assault, clients download unlawful warez programming [18].

Port Sweep Attack tries to determine what open ports are available on a computer on a host [13].

Nmap Attack is a communication over a network tool that uses several scanning protocols such as SYN, FIN, ACK, and others to determine which ports on a network are open and which are blocked [19].

Master Warez Attack takes advantage of a flaw in the FTP server. This attack occurs when the FTP server incorrectly grants compose permission to the system's clients [20].

PHF Attack occurs when an ineffectively written CGI script attempts to run instructions with the benefit of the http server [21], it is known as a PHF attack. An FTP_Write Attack occurs when an attacker takes advantage of a common puzzling FTP configuration error [22].

In Ping Of Death Attack, the attacker sends a message to the target. Twisted or larger-than-average packets via a standard ping path in an attempt to crash, destabilize, or solidify the targeted PC or administration. This sort of attack uses a simple ping request to provide distorted or unusually large packets to crash, destabilize, or damage the PC or organization center. IP social events are used in this attack to 'ping' a target structure with an IP address that exceeds the 65,535 byte limit. Because huge IP groupings are not permitted, the attacker areas the IP. IP addresses in groups This site is not permitted, so the attacker focuses on gathering IP addresses. When the target system is rebuilt, support floods and clustering occurrences may occur. When the target system reassembles the pack, support floods and clustered occurrences may occur. The use of a firewall that evaluates isolated IP packs for the maximum possible size can prevent the ping of death attacks [23].

Bandwidth Attacks can quickly deplete active and approaching transmission capacity by sending goods as quickly as without having to wait for a response The Smurf attack uses forgery to broadcast External IP ranges are flooded with bogus ICMP echo request packets. By sending massive amounts of ICMP echo reply packets from an intermediate site, these attacks cause network congestion or failures of a target. Ping can also be used to initiate an ICMP datagram-based attack. The attackers start the attack by sending a massive ICMP datagram using the ping command [24]. As a result, the system's transfer speed is reduced.

In an HTTP attack, the attacker attacks a web server or application with ostensibly legal POST or GET HTTP requests To capture an online targeted server in an HTTP strike. The attacker mishandles actual HTTP GET or POST sales. HTTP flood is a sort of DDoS assault in which the attacker modifies HTTP GET or POST sales to target a web server or application [25].

Peer to Peer attacks shared cyber-attacks take advantage of the texture of observing technologies to carry out attacks. For interruption, the assailant does not need to speak with the clients [26].

3 Internet of Things

The Internet of Things (IoT) is the linking of the world wide web-connected smart objects or things over wireless networks. The Web has grown in popularity in recent years (IoT) has emerged as a viable technology option for connecting a varied variety of heterogeneous things all around the world. The Internet of Things (IoT) allows us to access, operate, and manage these

devices in several scenarios, including smart homes, smart healthcare, smart transportation, smart industrial, and so on. It can assist us in automating device control to make device usage easier, provide individuals with comfort and convenience, and increase their well-being. [27] Illustrates this.

3.1 Layout of Internet of Things

The three-layer design defines the central concept of the Internet of Things.

1) Conception Level: This layer collects all physical world facts and information, such as temperature, speed, time, and humidity. A sensor network is composed of several detectors.
2) 2. Networking Level: The Networking Layer is an intermediary layer that handles data and information processing as well as data broadcasting. Among other things, data [28].
3) 3. Applicability Level: All programs that use IoT technology or have IoT implemented in them are defined by the application layer. Smart homes, smart cities, smart health, animal tracking, and other IoT applications are all viable. It is in charge of providing apps with services [29].

3.2 IoT Devices' Security Problems

Information security is a technology segment devoted to the protection of connected devices and networks in the internet of things (IoT). IoT entails connecting a system of interconnected computing devices, mechanical and digital machines, objects, animals, and/or people to the internet. Each "thing" is given a unique identifier and the ability to transfer data automatically across a network. [30].

3.3 The Internet Of Things Needs A Wide Range Of Security Services

The following are the numerous security services that are required for IoT.

1) Security: Messages moving from source to destination can easily be intercepted by an attacker, putting the content at risk. As a result, all relay nodes should be unaware of the message, meaning that secure end-to-end communications are required for IoT. For device storage, the same technique can be applied. The encryption and decryption approach is a straightforward solution. [31].
2) Significance: The integrity of a message should not be jeopardized as it travels from source to destination; it should arrive at the receiver's end in the same state as it left the sender's end. No intermediate should change the content of the communication while it is being passed on. [31]
3) Ease of access: Services offered by devices must always be available and in a continuous state of operation for the IoT to continue operating and accessing data whenever it is needed. As a result, detecting and preventing breaches is critical to uptime [31].
4) Uniqueness: End users should be able to recognize one another identities to ensure that they are dealing with the same entities that they claim to be [31].

3.4 DDoS Attacks on IoT: A Taxonomy

The Internet of Things has three major layers: TCP/IP, the Access Layer, and the Observational Layer [32]. And DDoS attacks differ depending on which layer is targeted.

1) RFID is a technology for receiving and retrieving data from sensors embedded in devices that use the Internet of Things but don't have direct access to the internet for human interaction, and • DDoS on the Observation Layer, where assaults such as jamming, kill command attacks, and so on are possible. In the first layer, rely on ambiguity to prohibit network service.
2) Distributed Denial of Service at the Subnet (DDoS): The network layer is the most vulnerable to attacks that use data pumping to target both wired and wireless networks. The system that receives the data continues to try to delay responses to requests to gather the necessary resources until there are no direct connections left, at which point the service is terminated. ICMP flood and SYN flood attacks are examples of network layer attacks [33].
3) DDoS Attacks on the Protocol Stack: It functions through apps in the implementation phase that provide the user interface in its most basic form (smart governments, smart cities, smart gadgets, mobile applications, and the web). There are two types of attacks that can happen in this stratum. In a denial-of-service attack, use path-based reprogramming [33].

3.5 DDoS Attack on Internet-Connected Devices

When IoT devices are connected, a perfect setting for the foundation for distributed denial-of-service (DDoS) assaults has been laid, which is why malware (bots and zombies) can spread quickly.

1) Use Mirai to infect Linux systems.

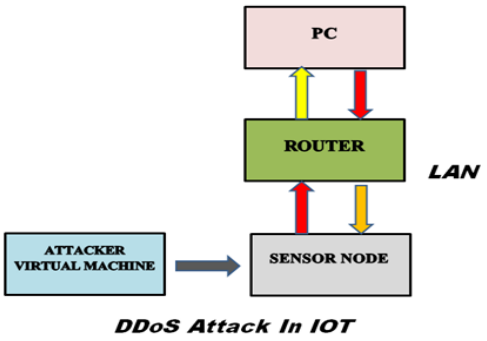


Fig. 2: IoT Device Environment

2) Use Wirex to infect Android devices. Google remedied the situation by eliminating a huge number of apps from the Play Store.
3) The bot can search major firms such as Cisco and Linksys that have been impacted by weaknesses in smart objects.
4) Torii is an entirely new character. It can objectively assess the majority of today's most modern computers, cellphones, and other electronic devices, such as tablets with architectures such as (64-bit), x86, ARM, MIPS, and others. [33]. Figure 2 depicts an IoT DDoS threat.

4 Literature Review

Kranz et al. [29] investigated a wireless system that employs smartphones but lacks Internet control functionality, in which things were physically attached to Bluetooth sub-controllers, and the smartphone was subsequently controlled using built-in Bluetooth connections. However, because of restrictions in the system's range of operations, it was unable to cope with mobility and could only be used close to the device. Researchers have also tried to employ house gateways to offer As seen in the Internet of Things, highlights include remote access and network interoperability, which can be used to manage home appliances and gadgets, as well as challenges and risks.

According to Evans et al. [34], the Internet of Things has progressed to the point that different sensors and networks must connect and communicate using common standards, and this effort is required. It is necessary and will necessitate collaboration from academics, standards bodies, governments, and corporations. The study looks at what has to happen for the Internet of Things to gain public acceptance, as well as the impact of service providers offering apps that add value to the Internet of Things.

Elsayed, Mahmoud et al. [35] propose DDoSNet, an intrusion detection system for DDoS attacks in SDN environments, in this paper. This method is based on the Deep Learning (DL) technique, which combines the Recurrent Neural Network (RNN) with an autoencoder. We test our model using the newly released dataset CICDDoS2019, which contains a wide range of DDoS attacks and fills gaps in existing datasets. When compared to other benchmarking methods, we obtain a significant improvement in attack detection. As a result, this model provides high confidence in the security of these networks.

Zhang et al. [36] propoes a lightweight defensive technique for DDoS assaults across IoT network settings is presented in this study. It is suggested and tested against multiple situations to dissect the interactive communication among various types of network nodes. The proposed defensive algorithm could successfully assist functioning nodes in an IoT network in distinguishing between malicious and legal requests and processing them differently.

Tuptuk , N. et al. [37] explore the challenges that those attempting to secure smart manufacturing systems face. Lessons from history show that attempts to retrofit security on systems whose primary driver was the development of functionality result in unavoidable and costly breaches. Indeed, over the last few years, today's manufacturing systems have begun to experience this. However, the integration of complex smart manufacturing technologies vastly increases the scope for attack from adversaries aiming at economic espionage and disruption. The potential consequences of these attacks range from economic damage and lost production to injury and loss of life, as well as catastrophic national-level effects. They discuss the security of existing industrial and manufacturing systems, existing vulnerabilities, potential future cyberattacks, the weaknesses of existing measures, levels of awareness and preparedness for future security challenges, and why security must play a key role in the development of future smart manufacturing systems in this article.

Ge et al. [38] suggested a unique anti-malware solution for IoT networks that classifies data flow using deep learning principles Using a recently available IoT data collection, the author derived general characteristics extracted from field data at the packet level The author created a feed-forward neural network model for binary and multi-class classification of IoT device threats such as denial of service, distributed denial of service, reconnaissance, and data theft. The suggested system has high classification accuracy, according to the results of its evaluation using the processed large

dataset. Kim, Daniel E. et al. [39] found that neural networks can provide a useful, self-learning approach to threat detection for network intrusion. Researchers confirm previous researchers' findings that shallow neural networks are better suited for network intrusion detection than deep neural networks after testing a variety of simple shallow and deep neural networks on the well-known NSL-KDD dataset, which consists of 148,000 observations and 41 features with 22 specific attacks. Shallow networks were able to classify network data more accurately and with lower error rates than deep networks.

Altwaijry Najwa et al. [40] propose two deep learning-based models, BDNN and MDNN, for binary and multiclass classification of network attacks, respectively, in this paper. On the well-known NSL-KDD dataset, we evaluate the performance of our proposed models and compare them to similar deep-learning approaches and state-of-the-art classification models. The experimental results show that our models perform well in terms of accuracy and recall.

According to Gaglio and Lo [41], there is a shift away from meaningless and cold items and toward enticing home apps, in which customers compete for control, and gadgets and apps serve as bargaining chips. Because of the vast frameworks and architecture required in the IoT, many IoT technologies will require governmental, business, household, and individual cooperation and consent to function. Individual benefits can be driven by societal and organizational benefits, however, the importance of leisure and entertainment in guaranteeing technology acceptability should not be neglected. Concurrently, the decision's ramifications and suitability.

Anne H. Ngu et al. [42] demonstrate the need for IoT middleware by demonstrating an IoT application for real-time blood alcohol level prediction utilizing smartwatch sensor data. Following that, a survey of existing IoT middleware capabilities was conducted. We also examine the obstacles and enablement technologies associated with designing IoT software. Experts also investigate the issues and supporting technologies involved in designing IoT middleware that embraces the heterogeneity of IoT devices while providing the needed composition, flexibility, and security in an IoT context. Madakam, Somayya et al. [43]] provide an overview of the Internet of Things, architecture, and key technologies, as well as how they are used in our daily lives. As a result, the present investigation conducts a systematic analysis of scholarly research publications, business white papers, expert interviews, and online resources to analyze topics connected to the Internet of Things.

According to Miorandi et al. [44], the IoT is a broad statement that represents the level to which the web and the Internet have invaded the physical environment, with globally distributed devices widely spread and associated with physical goods for identification via greater actuation and sensing capabilities. The Internet of Things (IoT) idea envisions a future in which physical and digital things are all connected, resulting in a new generation of services and applications that make use of relevant and appropriate information systems.

According to Tan and Wang et al. [45], as a consequence, communication will change from mostly between people to predominantly between humans. And objects, ushering in a new era of ubiquitous communications and computers that will drastically transform our way of life. RFID and other sensing technologies that enable effective recognition are widely regarded as essential parts of the approaching Internet of Things revolution.

Tufail, et al. [46] compared two machine learning techniques for detecting DDOS assaults; logistic regression and shallow neural network (SNN) were used in this investigation (SNN). In logistic regression, we achieved 98.63 percent accuracy and 99.85 percent accuracy in SNN. However, our study shows that SNN training takes significantly longer than logistic regression.

Kim, Daniel E., et al. [47] confirm previous researchers' findings that shallow neural networks are better suited for network intrusion detection than deep neural networks after testing a variety of simple shallow and deep neural networks on the well-known NSL-KDD dataset, which consists of 148,000 observations and 41 features with 22 specific attacks. When it came to identifying network data, shallow networks were more accurate and had lower error rates than deep networks.

5 Artificial Neural Network

An artificial neural network is a nonlinear data simulation system in which models or patterns are organized into intricate interactions between inputs and outputs (ANN). The learning capacities of neural networks are better. They are frequently used for more complicated tasks like handwriting and face recognition. A neural network is sometimes known as a "training algorithm." It debuted in the early 1940s. They have only recently emerged as a critical component of artificial intelligence [48-49]. Many different types of artificial neural networks are used in machine learning; however, this study used shallow

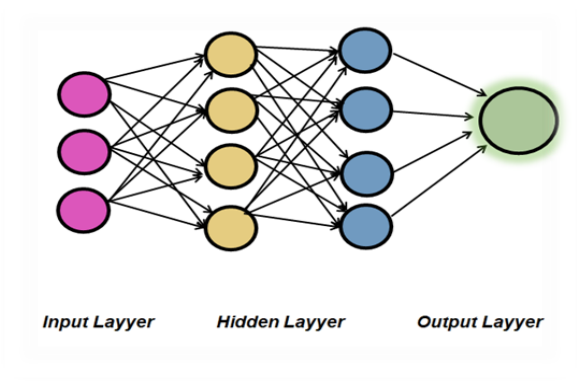


Fig. 3: Architecture of Artificial Neural Network

neural networks to detect DDoS attacks. Figure 3 displays the architecture of an artificial neural network.

5.1 Shallow Neural Networks

In brief, "shallow" neural networks have only one hidden layer, as opposed to "deep" neural networks, which have several hidden layers of varying sorts. Shallow neural networks are neural networks with a few layers, usually just one hidden layer. A simple neuron with R inputs is depicted in the diagram below. Each input is assigned a weight of w. The total of the weighted inputs plus the bias comprises the input to the transfer function b. Neurons can generate output using any differentiable transfer function b, [50]. As seen in fig 4.

6 Training Algorithm

6.1 Scaled Conjugate Gradient Algorithm

The scaled conjugate gradient (SCG) approach is based on conjugate directions, but unlike previous conjugate gradient strategies, it raises the processing cost of the system. Putting a supervised algorithm with a linear convergence rate into action (Scaled Conjugate Gradient). The study is based on numerical analytic methods from the class of conjugate gradient optimization. Any network may be trained using Trainscg's weight, net input, and transfer function derivative functions. The performance derivatives for weight and bias variables are calculated via backpropagation [51].

Moller's scaled conjugate gradient (SCG) method relies on conjugate directions, and then it does not require a line search at each iteration, unlike other conjugate gradient algorithms. Increasing the computing expense of the system. SCG was created to eliminate the time-consuming line search. "Training" is a MATLAB network training function that updates weight and bias variables using the scaled conjugate gradient approach. It can train any network using derivative weight, net input, and transfer functions. The step size in the SCG approach is determined by a quadratic approximation of the error function, making it more robust and free of user-defined factors. [51].

6.2 Levenberg–Marquardt algorithm

The Levenberg–Marquardt algorithm (LMA or simply LM), also known as the controlled least squares (DLS) technique, is used to solve non-linear least-squares problems. These minimization challenges are very common in least-squares curve fitting. The LMA interpolates between the Gauss-Newton and gradient descent algorithms [52].

7 Simulation Results

The MATLAB R2021a tool was applied in this research. To begin, clean the NSL-KDD (knowledge discovery data-base) data set and assign values to protocols, assaults, and flags. Then, using a shallow neural network, they create a network model and train it on the KDD data set. The neural networks were tested and prototyped on the same system, which ran the Windows 10 Pro operating system. MATLAB 2021 b was used as the development platform for the experiments and data collection. The Neural Network Toolbox and visualization features in MATLAB were heavily used. The NSL-KDD dataset was chosen as the main dataset on which the experiment is based. A total of 21 attacks were employed in training. Both shallow and deep neural networks go through the same experimental steps: data preprocessing, network training and testing, and result gathering. We received the results of DDoS assaults after completing the training. The Scaled conjugate algorithm and the Levenberg–Marquardt algorithm were employed in this study to train a shallow neural network that changes weight and bias values.

7.1 Training of Scaled Conjugate Gradient Algorithm

The graph demonstrates that the network's error values are disproportionately concentrated in the lowest possible values, closer to zero, with only a minor fraction in the subsequent error ranges. The figure depicts the shallow network training process by graphing gradient changes and validation check occurrences. Six validation checks resulted in the training process's terminating circumstances. The top graph in the picture

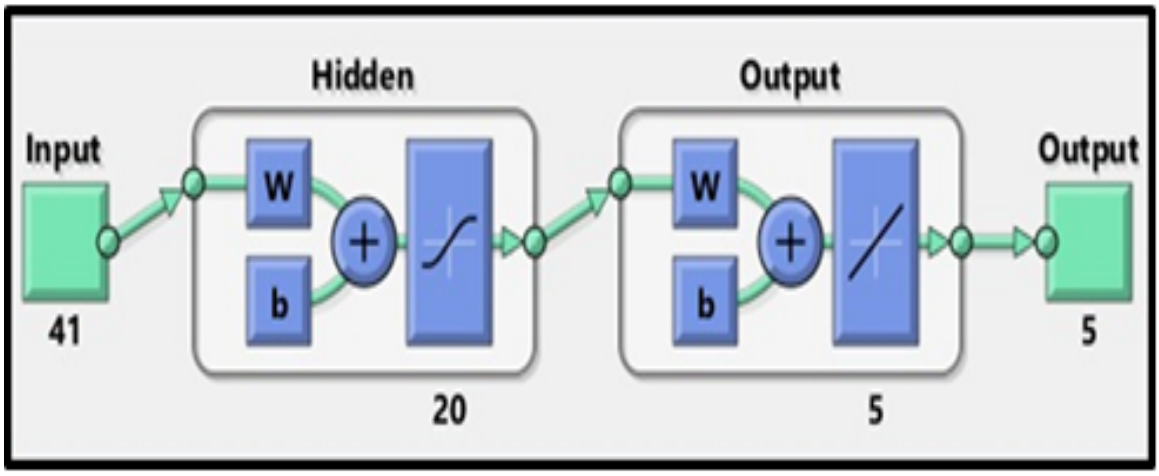


Fig. 4: Shallow Neural Network, Where W Represents Weights and B Represents the Bias

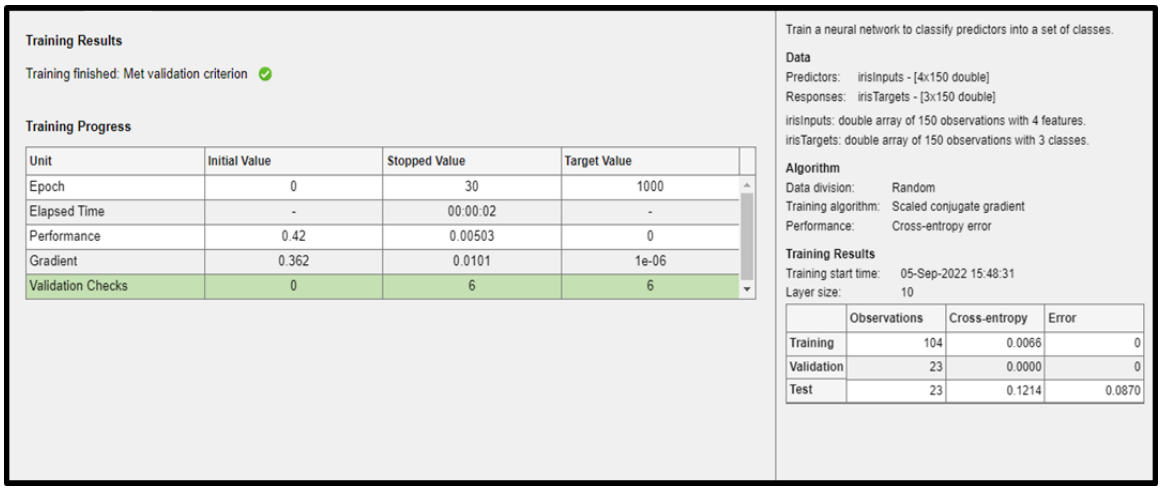


Fig. 5: Training Results of Scaled Conjugate Gradient Algorithm

depicts the constant downward trend of the gradient fall, with the largest drop in the gradient occurring in the first few epochs and learning then slowing until six validation checks were achieved in the bottom graph at the 41st epoch. as shown in fig 6.

The neural network training state map is depicted in Figure 7. At epoch 35, it also shows a validation check. The shallow neural network's performance demonstrates that validation is concerned with optimizing the threshold. Figure 7 depicts the performance curve created by the network throughout training, testing, and validation. The best validation performance is obtained with 0.028934 epochs. 41.

The majority of errors occurred at the third position (horizontal axis), and errors steadily decreased as one moved away from the zero point. This demonstrates that ANN correctly predicts with appropriate error distributions, as seen in Fig. 8.

Fig. 9 shows the ANN model regression plot: Upper left: training data; lower left: test data; upper right: validation data; and lower right: regression results

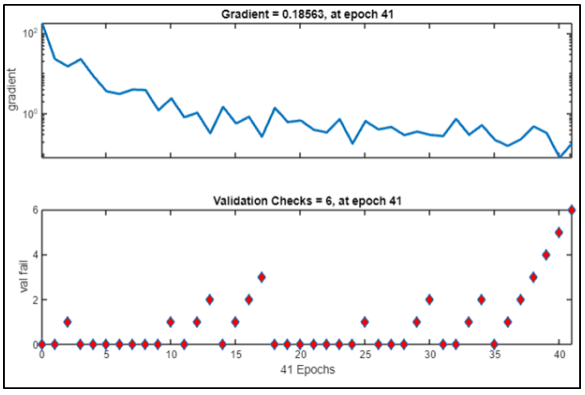


Fig. 6: Training State Graph Showing Gradient, Mean Deviation, And Validation Check

As shown in fig 10 Fitness against reference solution

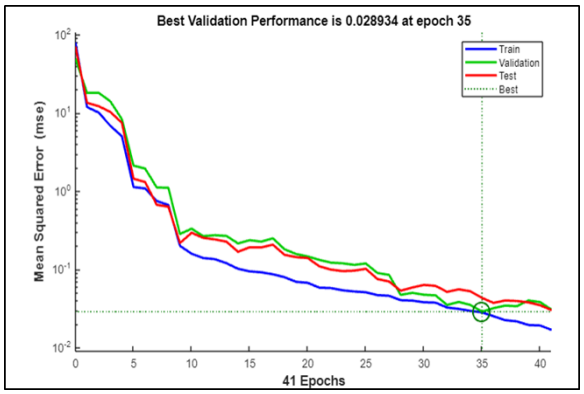


Fig. 7: The Efficacy of the Shallow Neural Network Reveals That Validation Continues While Reducing The Threshold.

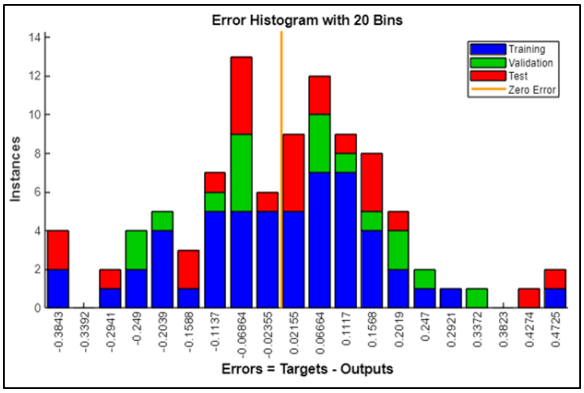


Fig. 8: Demonstrates The Network's Error Histogram, Which Depicts The Network's Error Distribution.

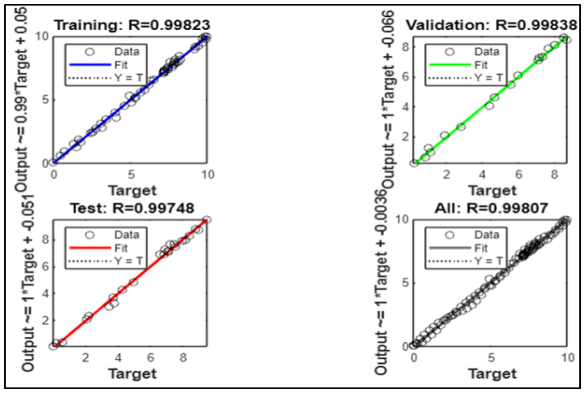


Fig. 9: Regression Graph Showing The Roc Curve

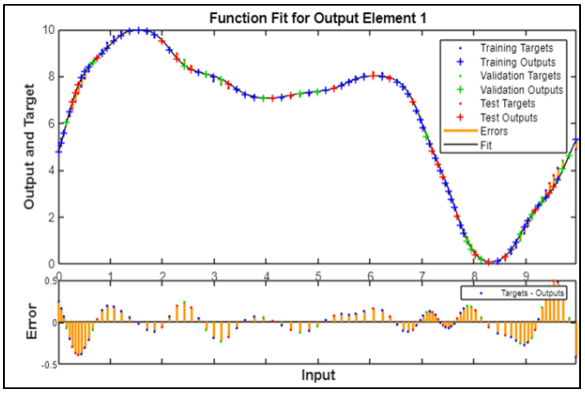


Fig. 10: Provide Plot Supervised Learning.

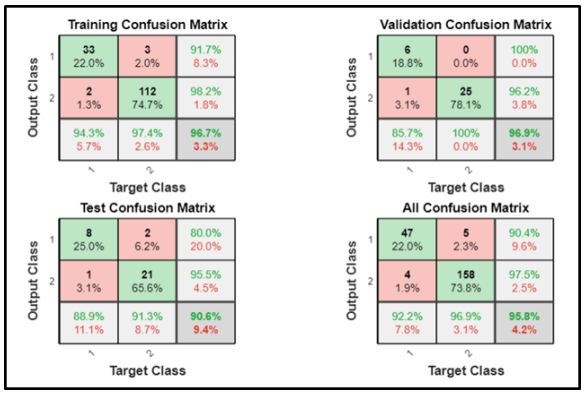


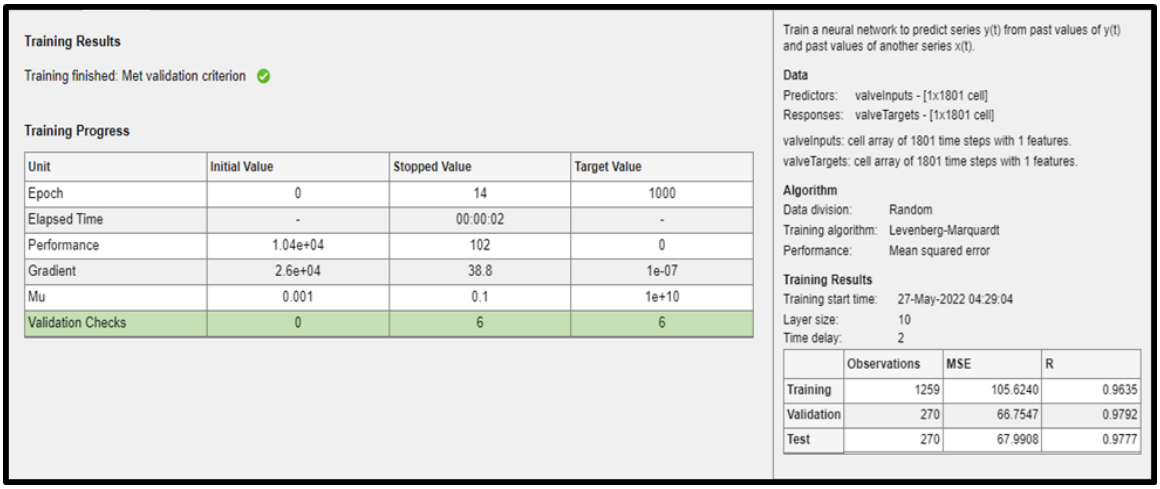
Fig. 11: Confusion Matrix Scaled Conjugate Gradient Algorithm

detecting of DDoS outcomes for each type of capillary transport model scenarios.

7.2 Training of Levenberg–Marquardt Algorithm

The graph demonstrates that the network's error values are disproportionately concentrated in the lowest possible values, closer to zero, with only a minor fraction in the subsequent error ranges. The figure depicts the shallow network training process by graphing gradient changes and validation check occurrences. Six validation checks resulted in the training process's terminating circumstances. The top graph in the picture depicts the constant downward trend of the gradient fall, with the largest drop in the gradient occurring in the first few epochs and learning then slowing until six validation checks are achieved in the bottom graph at the 35th epoch, as shown in fig 13.

Figure 14 shows the performance of the network calculated by the cross entropy performance function, with peak performance shown at the intersection of the dotted lines, which stops just short of the last epoch of 29. Training performance in the MATLAB simulator and NSL The KDD datasets Blue represents



Training Results

Training finished: Met validation criterion

Training Progress

Unit	Initial Value	Stopped Value	Target Value
Epoch	0	14	1000
Elapsed Time	-	00:00:02	-
Performance	1.04e+04	102	0
Gradient	2.6e+04	38.8	1e-07
Mu	0.001	0.1	1e+10
Validation Checks	0	6	6

Train a neural network to predict series y(t) from past values of y(t) and past values of another series x(t).

Data

Predictors: valveInputs - [1x1801 cell]
Responses: valveTargets - [1x1801 cell]

valveInputs: cell array of 1801 time steps with 1 features.
valveTargets: cell array of 1801 time steps with 1 features.

Algorithm

Data division: Random
Training algorithm: Levenberg-Marquardt
Performance: Mean squared error

Training Results

Training start time: 27-May-2022 04:29:04
Layer size: 10
Time delay: 2

	Observations	MSE	R
Training	1259	105.6240	0.9635
Validation	270	66.7547	0.9792
Test	270	67.9908	0.9777

Fig. 12: Training Results of Levenberg–Marquardt Algorithm

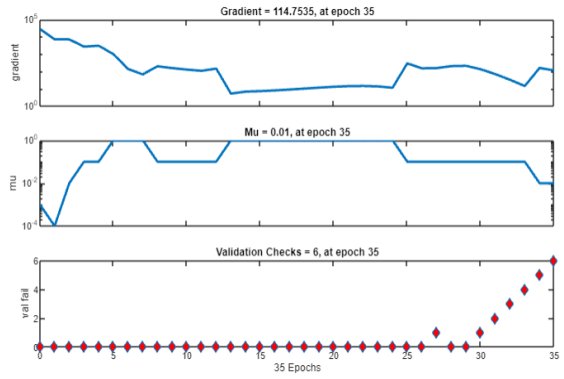


Fig. 13: Gradient, Mean-Variance, and Validity Check Training State Graph

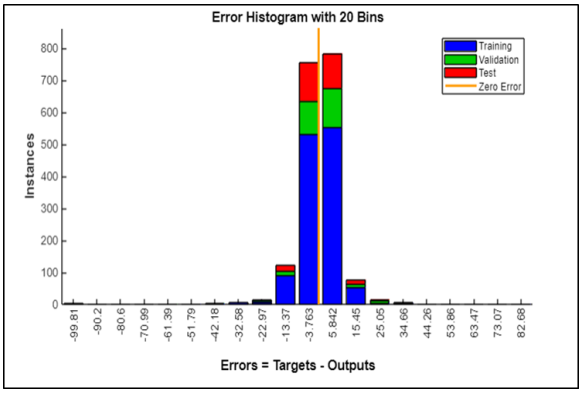


Fig. 15: Error Histogram Of Shallow Neural Network

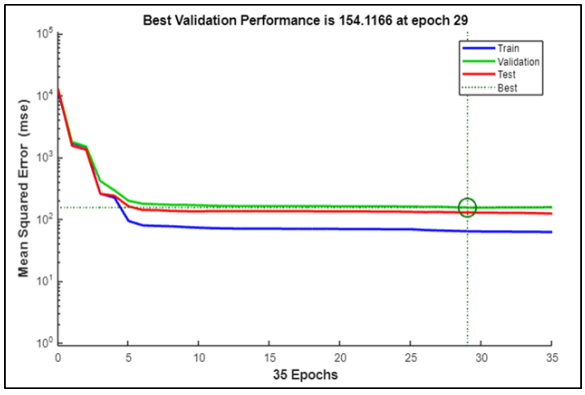


Fig. 14: The Shallow Neural Network's Test Demonstrates That Validation Continues While Adjusting The Cutoff point.

training, green represents validation, red represents testing, and the circle represents the greatest validation performance.

As shown in Fig. 15, an error histogram depicted the differences between target and forecast values after training a shallow neural network with 20 bins.

Scatter plots of experimental data for training, validation, and testing are provided as can be seen in this figure 16, the values of R in the training, validation and testing periods are 0.99768, 0.99637, and 0.99661, respectively

As shown in fig 17 the detection of suggested DDOS is analyzed using error histogram illustrations, and the results are graphically displayed.

Fig 18 shows the classification value of the neural network which is 94.9% and miss classification 5.1%.

8 Conclusion

This article discusses DDoS threats as well as security solutions for each IoT tier. It demonstrates that attackers exploit different vulnerabilities at each tier. Possible network security solutions are also highlighted, enhancing the security of the IoT network. To create a solid safe framework, we must address security concerns at all levels, not just one. To put

TABLE 1: Scale of the level of occurrence and level of significance

S#	Neural Networks	Algorithm	Validation Performance	Number of Epochs	Best Validation Performance	Success Rate	Classification
1.	Shallow Neural Network	Scaled Conjugate Gradient (SCG) Algorithm	0.018563	41	0.028934	95.8%	4.2%
2.		Levenberg–Marquardt Algorithm	11.47535	35	154.5566	94.9%	5.1%.

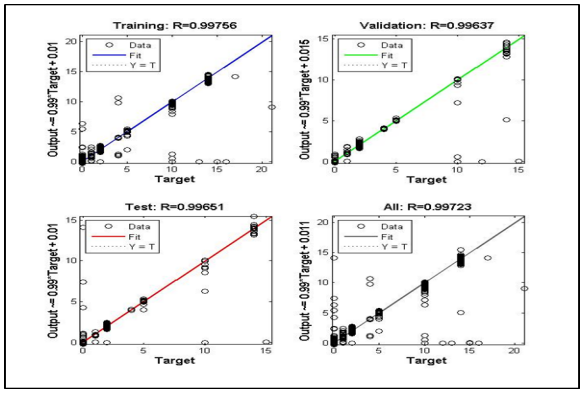


Fig. 16: ROC Plot for Neural Network Training, Testing, and Validation States

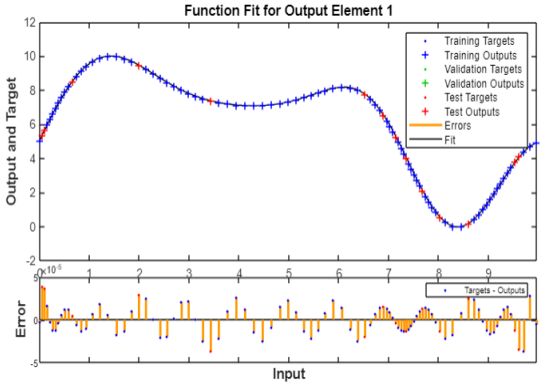


Fig. 17: Training and Testing Result Of Plotted

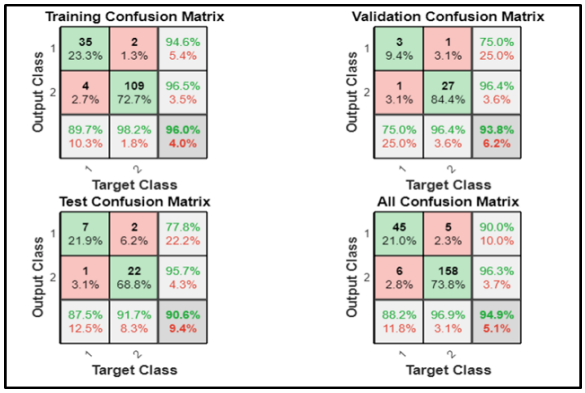


Fig. 18: Confusion Matrix Levenberg–Marquardt Algorithm

it another way, simply securing the application layer will not prevent attackers from hacking the network layer. Despite the large number of DDoS avoidance mechanisms described in the literature, all of them require extensive research and refinement. The industry is changing rapidly as a result of IoT applications. There is a significant need to use technologies such as machine learning and artificial intelligence to create unified solutions for a variety of scenarios that include heterogeneous devices, networks, and protocols. Furthermore, application users must be aware of the importance of using strong passwords and credentials, as well as regularly updating software. This research aimed to identify the best algorithm according to accuracy and training time. The shallow neural network was trained to check the accuracy and detection of DDoS attacks. The result shows that the "Scaled conjugate gradient algorithm" provides better results in a short training duration with good precision performance (95.8 percent accuracy) as compared to the "Levenberg–Marquardt Algorithm". In the future, various techniques, models, and neural networks may be used for deep learning and machine learning. In the future, different algorithms and neural networks can be used to detect which neural network and algorithm are best for the detection of DDoS IOT attacks.

References

[1] Brooks, Richard R., Lu Yu, Ilker Ozcelik, Jon Oakley, and Nathan Tusing. "Distributed denial of service (DDoS): a history." IEEE Annals of the History of Computing 44, no. 2 (2021): 44-54.

[2] Chadd, Anthony. "DDoS attacks: past, present and future." Network Security 2018, no. 7 (2018): 13-15.

[3] He, Qiang, Cheng Wang, Guangming Cui, Bo Li, Rui Zhou, Qingguo Zhou, Yang Xiang, Hai Jin, and Yun Yang. "A game-theoretical approach for mitigatingedge ddos attack." IEEE Transactions on Dependable and Secure Computing (2021).

[4] Acharya, Saket, and Nitesh Pradhan. "DDoS Simulation and Hybrid DDoS Defense Mechanism." International Journal of Computer Applications 163, no. 9 (2017).

[5] ARIEF, MUHAMMAD, and Ahmad Heryanto. "DETEKSI SERANGAN SMURF ATTACK MENGGUNAKAN ALGORITMA RANDOM FOREST." PhD diss., Sriwijaya Universiy, 2021.

[6] Bouyeddou, Benamar, Fouzi Harrou, Benamar Kadri, and Ying Sun. "Detecting network cyber-attacks using an integrated statistical approach." Cluster Computing 24, no. 2 (2021): 1435-1453.

[7] Nashat, Dalia, and Fatma A. Hussain. "Multifractal detrended fluctuation analysis based detection for SYN flooding attack." Computers Security 107 (2021): 102315.

[8] Dimolianis, Marinos, Adam Pavlidis, and Vasilis Maglaris. "SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering." In 2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pp. 126-133. IEEE, 2021.

[9] Sabri, Shima, Noraini Ismail, and Amir Hazzim. "Slowloris DoS Attack Based Simulation." In IOP Conference Series: Materials Science and Engineering, vol. 1062, no. 1, p. 012029. IOP Publishing, 2021.

[10] Nadim, Mohammad, Wonjun Lee, and David Akopian. "Characteristic features of the kernel-level rootkit for learning-based detection model training." Electronic Imaging 2021, no. 3 (2021): 34-1.

[11] Lee, Jongmin, and Gunjae Koo. "Restore Buffer Overflow Attacks: Breaking Undo-Based Defense Schemes." In 2022 International Conference on Information Networking (ICOIN), pp. 315-318. IEEE, 2022.

[12] Iliaee, Nahal, Shichao Liu, and Wei Shi. "Non-Intrusive Load Monitoring based Demand Prediction for Smart Meter Attack Detection." In 2021 International Conference on Control, Automation and Information Sciences (ICCAIS), pp. 370-374. IEEE, 2021.

[13] Chen, Lei, Shao-En Weng, Chu-Jun Peng, Hong-Han Shuai, and Wen-Huang Cheng. "Zyell-nctu nettraffic-1.0: A large-scale dataset for real-world network anomaly detection." In 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 1-2. IEEE, 2021.

[14] Iliyasu, Auwal Sani, Usman Alhaji Abdurrahman, and Lirong Zheng. "Few-shot network intrusion detection using discriminative representation learning with supervised autoencoder." Applied Sciences 12, no. 5 (2022): 2351.

[15] Alharbi, Yasser, Ali Alferaidi, Kusum Yadav, Gaurav Dhiman, and Sandeep Kautish. "Denial-of-service attack detection over ipv6 network based on KNN algorithm." Wireless Communications and Mobile Computing 2021 (2021).

[16] Al Arafat, Abdullah, Zhishan Guo, and Amro Awad. "Vr-spy: A side-channel attack on virtual key-logging in vr headsets." In 2021 IEEE Virtual Reality and 3D User Interfaces (VR), pp. 564-572. IEEE, 2021.

[17] Al-Shareeda, Mahmood A., Mohammed Anbar, Selvakumar Manickam, and Iznan H. Hasbullah. "Password-Guessing Attack-Aware Authentication Scheme Based on Chinese Remainder Theorem for 5G-Enabled Vehicular Networks." Applied Sciences 12, no. 3 (2022): 1383.

[18] Khan, Suleman, Kashif Kifayat, Ali Kashif Bashir, Andrei Gurtov, and Mehdi Hassan. "Intelligent intrusion detection system in smart grid using computational intelligence and machine learning." Transactions on Emerging Telecommunications Technologies 32, no. 6 (2021): e4062.

[19] Saputro, Elang Dwi, Yudha Purwanto, and Muhammad Faris Ruriawan. "Medium interaction honeypot infrastructure on the internet of things." In 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), pp. 98-102. IEEE, 2021.

[20] Duraisamy, A., and M. Subramaniam. "Attack Detection on IoT Based Smart Cities using IDS Based MANFIS Classifier and Secure Data Transmission Using IRSA Encryption." Wireless Personal Communications 119, no. 2 (2021): 1913-1934.

[21] Jat, M. Tech Scholar Rakesh, and Sumit Sharma. "Survey on Cloud Attack Types and Detection Techniques." traffic 5 (2021): 6.

[22] Slamet, Slamet, and Izzeldin Ibrahim Mohamed Abdelaziz. "An enhanced classification framework for intrusions detection system using intelligent exoplanet atmospheric retrieval algorithm." Bulletin of Electrical Engineering and Informatics 11, no. 2 (2022): 1018-1025.

[23] Walad, S. Iswandi, Muhammad Zarlis, and M. IT Syahril Efendi. "Analysis of denial of service attack on web security systems." In Journal of Physics: Conference Series, vol. 1811, no. 1, p. 012127. IOP Publishing, 2021.

[24] Mishra, Anupama, Neena Gupta, and B. B. Gupta. "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller." Telecommunication systems 77, no. 1 (2021): 47-62.

[25] Muraleedharan, N., and B. Janet. "A deep learning based HTTP slow DoS classification approach using flow data." ICT Express 7, no. 2 (2021): 210-214.

[26] Daniel, Erik, and Florian Tschorsch. "IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks." IEEE Communications Surveys Tutorials 24, no. 1 (2022): 31-52.

[27] Yu, Shanshan, Jicheng Zhang, Ju Liu, Xiaoqing Zhang, Yafeng Li, and Tianfeng Xu. "A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN." EURASIP Journal on Wireless Communications and Networking 2021, no. 1 (2021): 1-21.

[28] Shaikh, Asma, and Preeti Gupta. "Real-time intrusion detection based on residual learning through ResNet algorithm." International Journal of System Assurance Engineering and Management (2022): 1-15.

[29] Kranz, Matthias, Paul Holleis, and Albrecht Schmidt. "Embedded interaction: Interacting with the internet of things." IEEE internet computing 14, no. 2 (2009): 46-53.

[30] Vishwakarma, Ruchi, and Ankit Kumar Jain. "A survey of DDoS attacking techniques and defence mechanisms in the IoT network." Telecommunication systems 73, no. 1 (2020): 3-25.

[31] Strous, Leon, Suné von Solms, and André Zúquete. "Security and privacy of the Internet of Things." Computers Security 102 (2021): 102148.

[32] Chopra, Amardeep, Sunny Behal, and Vishal Sharma. "Evaluating machine learning algorithms to detect and classify DDoS attacks in IoT." In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 517-521. IEEE, 2021.

[33] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, and Rakesh Tripathi. "A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing." Transactions on Emerging Telecommunications Technologies 32, no. 6 (2021): e4112.

[34] D. Evans. "The Internet Of Things: How The Next Evolution Of The Internet Is Changing Everything", 2014, Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed 24 March, 2022]

[35] Elsayed, Mahmoud Said, Nhien-An Le-Khac, Soumyabrata Dev, and Anca Delia Jurcut. "Ddosnet: A deep-learning model for detecting network attacks." In 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pp. 391-396. IEEE, 2020.

[36] Zhang, Congyingzi, and Robert Green. "Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network." In Proceedings of the 18th symposium on communications networking, pp. 8-15. 2015.

[37] Tuptuk, Nilufer, and Stephen Hailes. "Security of smart manufacturing systems." Journal of manufacturing systems 47 (2018): 93-106.

[38] Ge, Mengmeng, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, and Antonio Robles-Kelly. "Deep learning-based intrusion detection for IoT networks." In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC), pp. 256-25609. IEEE, 2019.

[39] Kim, Daniel E., and Mikhail Gofman. "Comparison of shallow and deep neural networks for network intrusion detection." In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 204-208. IEEE, 2018.

[40] Altwaijry, Najwa, Ameerah ALQahtani, and Isra AlTuraiki. "A deep learning approach for anomaly-based network intrusion detection." In International Conference on Big Data and Security, pp. 603-615. Springer, Singapore, 2019.

[41] Gaglio, Salvatore, and Giuseppe Lo Re. Advances onto the Internet of Things. Vol. 349. Springer, 2014.

[42] Ngu, Anne H., Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng. "IoT middleware: A survey on issues and enabling technologies." IEEE Internet of Things Journal 4, no. 1 (2016): 1-20.

[43] Madakam, Somayya, Vihar Lake, Vihar Lake, and Vihar Lake. "Internet of Things (IoT): A literature review." Journal of Computer and Communications 3, no. 05 (2015): 164.

[44] Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. "Internet of things: Vision, applications and research challenges." Ad hoc networks 10, no. 7 (2012): 1497-1516.

[45] Tan, Lu, and Neng Wang. "Future internet: the internet of things. Advanced Computer Theory and Engineering (ICACTE)." In 2010 3rd International Conference on, vol. 5, pp. V5-V376. 2010.

[46] Tufail, Shahid, Shanzeh Batool, and Arif I. Sarwat. "A Comparative Study Of Binary Class Logistic Regression and Shallow Neural Network For DDoS Attack Prediction." In SoutheastCon 2022, pp. 310-315. IEEE, 2022.

[47] Kim, Daniel E., and Mikhail Gofman. "Comparison of shallow and deep neural networks for network intrusion detection." In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 204-208. IEEE, 2018.

[48] Pineda-Jaramillo, Juan D. "A Shallow Neural Network approach for identifying the leading causes associated to pedestrian deaths in Medellín." Journal of Transport Health 19 (2020): 100912.

[49] Oymak, Samet, and Mahdi Soltanolkotabi. "Toward moderate overparameterization: Global convergence guarantees for training shallow neural networks." IEEE Journal on Selected Areas in Information Theory 1, no. 1 (2020): 84-105.

[50] Zhou, Baohua, Zifan Li, Sunnie Kim, John Lafferty, and Damon A. Clark. "Shallow neural networks trained to detect collisions recover features of visual loom-selective neurons." Elife 11 (2022): e72067.

[51] Esfe, Mohammad Hemmat, Mohammad Hasan Kamyab, and Davood Toghraie. "Statistical review of studies on the estimation of thermophysical properties of nanofluids using artificial neural network (ANN)." Powder Technology (2022): 117210.

[52] Shakibjoo, Ali Dokht, Mohammad Moradzadeh, Seyed Zeinolabedin Moussavi, Ardashir Mohammadzadeh, and Lieven Vandevelde. "Load frequency control for multi-area power systems: A new type-2 fuzzy approach based on Levenberg–Marquardt algorithm." ISA transactions 121 (2022): 40-52.