REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

COMPUTER NETWORK INTRUSION DETECTION USING CASCADE BACK PROPAGATION NEURAL NETWORK

Sarah Alfitouri Mohamed ELGETAIT

Master's Thesis

Supervisor

Asst. Prof. Dr. Oğuz ATA

Istanbul, 2022

COMPUTER NETWORK INTRUSION DETECTION USING CASCADE BACK PROPAGATION NEURAL NETWORK

Sarah Alfitouri Mohamed ELGETAIT

Information Technologies

Master’s Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled COMPUTER NETWORK INTRUSION DETECTION USING CASCADE BACK PROPAGATION NEURAL NETWORK prepared by SARAH ALFITOURI MOHAMED ELGETAIT and submitted on 16/05/2022 has been **accepted unanimously** for the degree of Master of Science in Information Technologies.

Asst. Prof. Dr. Oğuz ATA

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Oğuz ATA	Faculty of Engineering and Architecture, Altınbaş University	
Asst. Prof. Dr. Doğu Çağdaş ATİLLA	Faculty of Engineering and Architecture, Altınbaş University	
Asst. Prof. Dr. Aytuğ BOYACI	Air Force Academy, National Defence University	

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

Submission date of the thesis to the Graduate Education Institute: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Sarah Alfitouri Mohamed ELGETAIT

Signature

ABSTRACT

COMPUTER NETWORK INTRUSION DETECTION USING CASCADE BACK PROPAGATION NEURAL NETWORK

Elgetait, Sarah Alfitouri Mohamed

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Oğuz ATA

Date: May/2022

Pages: 57

Security over the internet network is demanded, protecting the personal data and governing the users access so that privacy level is maintained. This task is more complicated since the internet is a public network that gives access to everyone, even to those users with malicious activities hence an attacker may steal a users' credentials, allowing them to access the server without being recognized. Wide expansion on computer and internet network increases the chances of network intrusion where hacking a malicious activity are more likely to exists. Internet is considered as public network where all the parties required to exchange the data need to share it over the internet through a server or cloud. The data being available in servers or clouds; its safety is limited to the strength of cloud, server, etc. Firewalls which prevent attacks to happen, but the advancement of software technology made the available firewalls weaken to face overwhelmed attacks activities. Prediction of attack is made using deep learning paradigms namely: Cascade Feed Forward Back Propagation (CFFBP), Feed Forward Back Propagation (FFBP) and Layer Learning Neural Network (LLNN). Using the dataset named ADFA-LD. In this study we proposed an automatic attack prediction approach using deep learning technology. The proposed models are trained to detect six types of denial

of service attacks and the best achieved accuracy of attack prediction is corresponding to 82.7586207 percent.

Keywords: ADFA-LD, CASCADE, Intrusion Detection, Attack, Performance.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

ADFA-LD	:	Australian Defense Force Academy- Linux Dataset
CFFBP	:	Cascade Feed Forward Back Propagation
FFBB	:	Feed Forward Back Propagation
LLNN	:	Layer Learning Neural Network
ML	:	Machine Learning
DL	:	Deep Learning
VPN	:	Virtual Private Network
QOS	:	Quality of Service
IP	:	Internet Protocol
MAE	:	Mean Absolute Error
RMSE	:	Root Mean Square Error
MSE	:	Mean Square Error
DOS	:	Denial of Service
SSI	:	Secure Sockets Layer
IDS	:	Intrusion Detection System

LIST OF SYMBOLS

Ci : Correct detections of the attacks.

Ti : Total number of attacks existed.

E : Errors that are calculated in the error vector.

n : Is the summation of total column elements.

1. INTRODUCTION

1.1 OVERVIEW

Computer network is increasingly expanded at the last twenty years especially after the emerging of new communication technologies as well as handsets advancement. [4][5] Internet network development has allowed data to steam in large quantity all over the world. This data is variating in type and nature, including personal data, banking data, companies and business-related data, etc. In order to participate the internet network and gaining the advantages of networking, data in all types needed to be presented over the internet. Internet development and mobile communication expansion made thousands of users share plenty of data with personal and business content through the internet (public networks). Therefore, virtual personal networks were designed to work as a tunnel containing the channels (connections) taking place between particular nodes [6][7] .

The outbreak of security systems and their expansion is inspired by the necessity of privacy for sensitively natured data, especially over the cloud servers[8]. Such kind of data imposed the need for solid firewalls to prevent any stolen or snooping attempt[9]. Generally, attacks detection technology has come into the image as a way of security enforcement over data networks. The need for such a technique has gained extended interest in technology providers due to its outstanding performance in tackling the privacy threats on the networks [10]. Different types of computer attacks are being observed so far and hence different prevention tasks are made to prevent the so-called attack. Most of those attacks are working to interrupt the smooth process of the network by receiving the data from one node and then dropping where the actual receiver as well as the sender will keep waiting to complete the delivery process. Upon the delay, network will fall into stage call denial of service stage where new requests to this network cannot be attended unless the current request is getting clear, and as name implies, this attack is called as denial of service attacks (DoSs).

Research Terminologies:

Network Security:

New data privacy and security challenges are posed due to the vast expanse of networks and enlargement of the subscribers' number[11]. Data being shared over the network may reach

the node of the source into the destination node without interruption. However, the expansion of the internet and computing technologies raised the challenges of data snooping and hacking. Those malicious processes are performed by other network subscribers intending to perform malicious attacks on particular data[12].

The intensions of malicious attackers might steal the data or damage the data where both are unpleasant events and need to be combated. The idea of network security was made initially to ensure the access of only authorizers to the network[13]. It is imposed after defining the internet of things and electronic commerce, and internet banking. Operations like the mentioned are susceptible to malicious operations and required to be protected from any third-party access. On the other hand, the development of mobile applications and internet capabilities made tones of personal orientated transactions to be conducted over the internet. The privacy of such data is essential[14].

Channel Impact:

For any network to operate, a path for exchanging data is mandatory so that the network terminal can send and receive its payloads. The path used for carrying network traffics is termed a channel. Two types of a channel can be recognized in the network context: wire channel and wireless channel. Wire channel is subdivided into three categories: copper coaxial channel, copper twisted pair channel, and optical fibber channel.

Data Packets:

Packet switching networks are made to tackle the problems of path noise observed in circuit switching networks. The data stream is broken down into smaller blocks called packets; each packet may pave its way towards the destination node using a different path, destination will then have packets from various paths. Upon packets reaches the destination, the original form of data will be recovered using the sequence number and packet identification number attached to the packet frame overhead [15]. Data packets are generated in the source node, where the packet overhead can be added to each packet. The overhead information integrated into the packet frame[16] can be used to route the packet through the network. Routing protocols are used in packet switching networks for sending the packets from the source into the destination. The main task of routing protocols is to establish the path between node pairs that give minimum delay and maximum throughput. As a result, packet switching networks are less susceptible to data loss as the data packets reach the destination through different

paths. If the noise attacked any path in the network, only the packet of that particular path would be affected, and other packets will be delivered to the destination [17][18].

On the other hand, Data can be transmitted between nodes in the network using circuit switching technology. This technology is used to transmit the data from a particular node in the network into another node by establishing a specific path between those nodes. Path establishment between any pair of nodes may remain constant, so the connection of those particular pairs will be dedicated only to their traffic. The path may remain idle if there is no traffic between the nodes. Circuit switching technology can be used for those applications which are required a slight time delay. On the other hand, if any noise impacts the path, all data transmitted using this technology will be susceptible to loss [19] [20].

Packets Transmission:

Data generated in the source node is heading towards its destination node in the form of packets where the source node itself will define the destination node identification number and the paths that each packet needs to use to flee towards that destination. The path selection mechanism may be identified using the shortest-path-to-go theory, where each node needs to reveal its location and the status of its queuing process by broadcasting a piece of signalling information. The broadcast of such messages also depends on network infrastructure [19] [20].

In the seven-layer-TCP/IP network, each node reveals the traffic and location information to the concerned node using an encrypted Hello message where only the concerned node may receive this requirement and accordingly reply (respond) for it. On the other hand, networks like Adhoc networks merely broadcast a HELLO message for all the nodes sharing the location and traffic status; the concerned node and the other nodes will receive that information. In normal conditions, the concerned node only will respond to the HELLO message unless any malicious node is present[21][22].

The request back response will be sent from the destination node back to the source node, intimating that this node is open and available to receive the payload, and it may ask for sending the packets. However, the source node will be sharing the first packet with the specific sequence number to the destination node. In addition, the source node will be expecting to receive an acknowledgement from that node as the packet was successfully

delivered. Accordingly, the source node may wait for a nominated time until receiving the acknowledgement from the destination node [23][24][25].

Hence, two scenarios are to be anticipated, which are as follow: either the destination node will reply during the defined waiting time to the destination node with the acknowledgement number of which acts as a confirmation of successful delivery packet and seeking for the next possible packet. On the other hand, an acknowledgement may not be generated from the destination node or even delayed (generated after the configured waiting time). In this case, the source node will consider failed delivery and will retransmit the packet once more.

1.2 PROBLEM DEFINITION

Chances of data loss or privacy breaching has then increased since the internet is public network, and anyone can gain the access by simply having an active connection. The hiking and non-legitimate activity on the internet is also increased which made it more susceptible to privacy breaching and data intrusion.

Data servers and clouds were established to accommodate the said data while it is presented over the internet network. In every server or cloud, certain level of security is being built in order to maintain the data privacy and to protect the data from the unauthorized accesses. Due to the advancement of software technology, hacker was able to crack many famous/ popular networks security and stolen their data in last twenty years. Network undergoing the denial of service is having economical losses as well if we considered the delay in the sensitive data delivery i.e. banking data, business data and so on.

In order to clear those attacks, it is essential to discover the attack type, in other word, the denial of service (DoS) attacks are classified according to their target type i.e. the attack that is targeting HTTP protocol, attack that is targeting MAC layer, attack that is targeting network layer, etc. This means that denial of service attack nature can be vary according to the target and hence it is difficult to design a common attack detection program with high compatibility using the traditional approaches.

1.3 RESEACH OBJECTIVES

In order to tackle the challenges mentioned in the above section and enhance the current trends on network security, the following objectives are to be fulfilled.

a) monitoring the inward data of each connection requested on the general-purpose network by analysing the routing information obtained from the log data.

b) implementation of smart, robust and rapid anti-intrusion paradigm using the deep learning to predict the malware activity.

c) providing a solution for the other network performance metrics such as throughput, time delay, and packet losses in the presence of the proposed anti-intrusion paradigm. In other words, learn through the impacts of the proposed approach on the other performance metrics apart from the security enhancement.

d) effective data pre-processing model is to be developed to address the challenges in dataset alike number of columns in every entry in the log data and data normalization. That can be done using the MATLAB programming language.

1.4 THESIS STRUCTURE

This thesis report involves six technical chapters that illustrate hereinafter: Chapter one (Introduction): Provides a briefing information about the data technology impact on the data transmission and demonstrates the problem statement along with the objectives of this research. Chapter Two (Literature Review): Illustrates the previous research activities that conducted in the interest of the security alternatives and discuss the strength of each research in order to define the problem statement and the works guidelines of this study. Chapter Three (Methodology): Illustrates the underlaying technologies used to develop the entire study and Illustrates the proposed model. Chapter Four (Results and Discussion): Demonstrates the outcomes and discusses it in details and interprets the results in various graphical representations. Chapter Five (Conclusion): Concludes and highlights the outcomes obtained from this study. The thesis report will be terminated by mentioning the references and books that have been used to construct this report.

2. LITRATURE REVIEW

Due to the outstanding role of the virtual private network in assuring the privacy of data over the standard networks, comprehensive researches have been conducted in the interest of virtual private networks performance enhancement[26].

At [10], the author stated that several popular service providers such as skype and Secure Shell deploy virtual private network technologies in their infrastructures. Therefore, the main goal of this study is to find the proper protocol for different types of network activities. Furthermore, it was mentioned that protocol recognition in a virtual private network is vital for the success of the security objectives.

However, the standard traditional virtual private networks have played an essential role in security and privacy control over the internet network[27]. The increased traffic through the internet due to the data revolution in the current years have led to the performance of conventional security norms for re-evaluation. The extended traffic through the networks and the increments of the regular payloads in network nodes have made the conventional security programs fail in tackling the data threats[28].

At[29], various traffic over the networks, such as internet protocol traffic and relay traffic, has led to more data types such as multimedia traffic into virtual private network design consideration. In addition, voice over IP has an essential impact on the internet payload. Therefore, in this study, the importance of virtual private networks for addressing the various data nature is an add-on point for their performance.

The study[30] mentioned that virtual private networks had been grappled with the attention of large retail companies worldwide due to their easy to establish and relatively low cost and their noteworthy performance. However[31], some of those applications are looking for real-time, very short latency in data transmission, while others seek a high throughput network that can deliver high-quality data without dropping the packets. In order to fulfil such demands over the virtual private network, another methodology is to be adopted by the network service providers. This study suggests using of various nature switches labelled for different kinds of traffic where all those switches are to be gathered on a centralized switch unit. This kind of network topology is demonstrated in Figure 2.1.

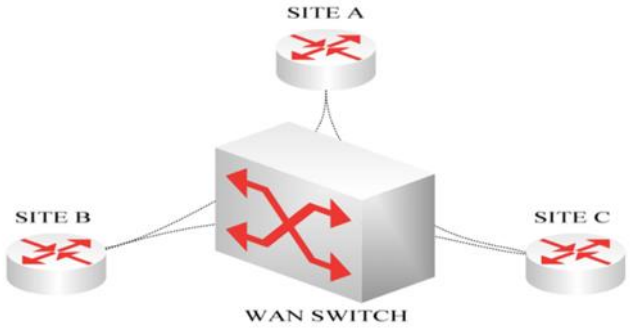

Figure 2.1: Wide area network topology for virtual private network structure.

At [32], a new study was proposed to ensure a high level of security over the intranet networks such as inter-building networks, college networks and school networks. Authors have done a new experiment using the network structure in school wherein the virtual private network can be integrated into the structure. The virtual private network is made in another approach in this study using unlikely the conventional approach of a software-defined virtual private network.

The authors suggested chips in order to incorporate the virtual private network on the hardware of the school's network. This approach would enable a high level of security on the intranet networks using microcontrollers and ensure a safe data transmission between particular pairs only with no chance for changing this connection or hiking it by any malware activity. However, the cost of adopting such a network is slightly higher than the conventional software-defined virtual private network.

At[33], it used hardware gateways as an alternative way to incorporate the virtual private network. However, the functionality of the virtual private network can be implemented using unique microcontrollers, and that can be incorporated in network design where a permanent safe connection can be produced.

At [34], organizations such as colleges and universities that are likely willing to be merged under one organization face the problem of merging their networks under one centralized network. However, this study was made given several network interconnections and the possibility of security violating. Therefore, the authors suggested using IP Security protocol as one of the most robust virtual private network protocols to ensure safety over data sharing between the different blocks of the bigger origination.

The authors mentioned that IP security protocol is outperformed for latency tackling as well as good throughput preservation. Figure 2.2 demonstrates the structure of the proposed network used in this study[1]. The study had taken place over a campus where several colleges are set to be connected in one network.

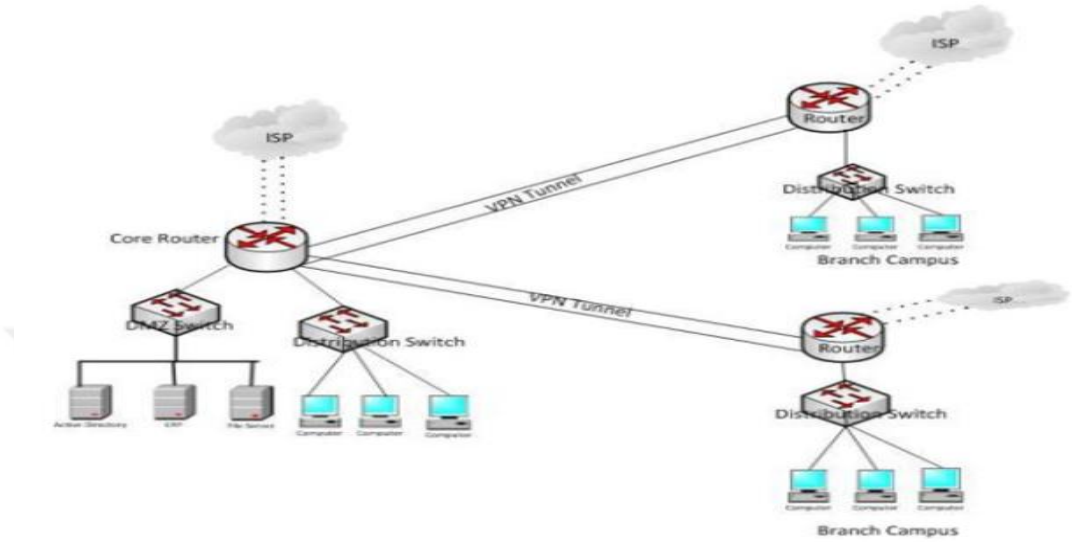

Figure 2.2: Interconnection of several colleges at one campus using the concept of virtual private network[1].

At [35], in a review of multiple scenarios of virtual private networks, observations are made likely loads can be fluctuated by different nodes or even on the same node for the connection period. Thus, load from each node is required to be under the so-called load balancing in order to enhance the network's performance[36]. Additionally, the researchers in[37] propose an algorithm that balances the load inside the network by anticipating the future coming load from each node.

This anticipation is taking place by conducting a statistical calculation using the probability theory. Each node might change the load or data payload every time during the connection time. Thus, load balancing is to be conducted. The proposed algorithm considers the conduction of load calculation as the first step in virtual private network server assignment[37].

In order to assign a particular node for some virtual private network server, a scheduling server is made[38], which takes the information of anticipation of load and calculates which

server of the virtual private network will fit those load requirements[39]. This technology plays a crucial role in addressing the delay and enhancing the throughput over the network.

At [40], the article mentioned the importance of a virtual private network in securing users via the internet. The author stated that the internet is not a safe network without security norms and authentication algorithms existence[41]. However, the author has made the so-called network data rates focal of the research.

The data rate[42] is an essential consideration in designing the virtual private network as security is the main point in such network for ensuring the privacy of users' data via a wide network accessed by the public. Restriction of access is the only solution to prevent unauthorized access to user's data. Access could be restricted using private networking algorithms, which enabled the network and service providers to configure a software-defined private network for security maintenance. However, the data rate is also another point to consider. As this kind of network is used to prevent malfunctioning access, it must facilitate the exchange of high data rates according to the users' needs. In other words, data rate facilities should not be violented by the security enforcement algorithms via a virtual private network.

At [43], virtual private network applications such as using the college library network has gained more interest over the academic professionals. Usually, each college or research Centre preserves unique access for some electronic resources such as requested journals and electronic books providers. Furthermore, services related to student academics, such as conducting the assignments and online submitting their homework, are usually dedicated to those getting access from inside the campus. In contrast, people who are not able to access from the campus cannot access from elsewhere.

That is due to making the network recognize the IP addresses only from the inter-campus and block any incoming request from other IP addresses. In this study, the author stated that inter-campus access might discomfort the researchers and delay many researchers' work. However, using the virtual private network can be a good solution for access to intra-campus requests and prevent the problems raised due to geographical access restrictions[44].

At [45], a new study was conducted to provide remote access for the academic professions to the campus services, including the digital library, electronic books, etc. A virtual private network was earlier proposed to support the demand for secure access for academic professionals to campus services.

In this approach, a virtual private network is being used to implement secure access for those users who are willing to access the campus network from out of the campus.

For doing so, IP security protocol is used over the virtual private network in cooperation with internet service providers companies. The security network architecture is implemented using the IPSec protocol over the virtual private network[46].

The network was instructed to permit the internet request coming from particular internet service providers. This technology was proposed to allow outsider communication with campus networks without physical presenting on the campus. It is also considered a cost-efficient means of intra-campus access networking[47].

At [48], some communications networks that dedicated to particular tasks such as the monitoring process. Those networks are responsible for transferring the sensing information from the sites (the device or machines under surveillance) to the remote site where the data is recorded and processed. For example, power monitoring systems[49] are usually transferred through the so-called wide-area measurement system. Electrical power components such as transformers, transmission lines, and other equipment are more susceptible to faults (errors) due to various reasons such as environmental changes.

Those errors can cause a significant economic disadvantage as that equipment is very costly. As a sort of solution, protection systems are found to prevent fault occurrences. Protection systems involve a group of sensors for different tasks. Those sensors can learn about the parameter fluctuations that lead to faults.

Each sensor produces a signal that reveals the current situation of the particle being monitored. Like the networks, a wide-area measurement system (WAMS) is used as a backbone to transmit those signals to the end system. In addition, server or end monitoring system might act according to the received information and reply to the control device to change the status of the machine (e.g. switching off the machine, changing the power feeder,

and so on); this information; being transmitted, is vital for the safety of the power network (the so-called smart grid)[50]. Therefore, virtual private networks are proposed in this study to secure the information transmission between the power network nodes.

At [51], another approach to digitizing the content of the schools and colleges campuses is proposed in this article. The author mentioned the necessity of making the school content such as libraries, departments, offices, and administration work in electronic format. This way enables students and the facility members to log in and get the required service. Virtual private network impact in such application is necessary to secure the information transferred among the facilities and safeguard the digital sources such as books and researchers from unauthorized accesses.

The author mentioned that IPsec is the best option in the virtual private network protocols to perform this task. Other details were found in this article, more likely, the methods used to digitize the content of the entire campus. Figure 2.3 demonstrates the process of the IPsec paradigm.

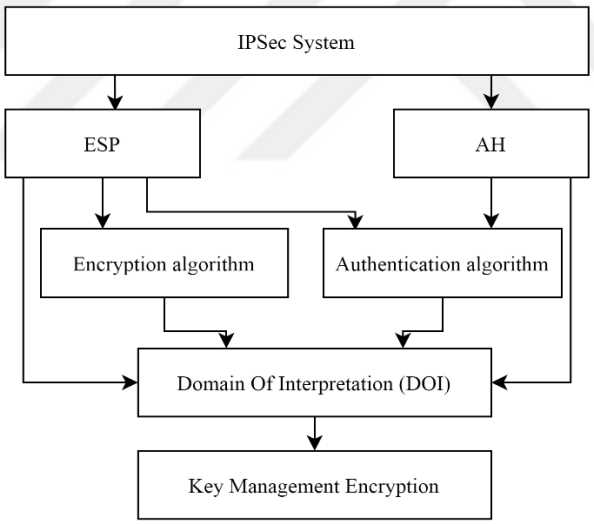

Figure 2.3: Internet protocol security in school based virtual private network.

At [52], the realization of mobile internet is made in this study and concluded that migration from the stationary internet service in conventional devices into the mobile internet had imposed huge amounts of data to be exchanged between the host and the servers. However, this data preserves private content where security is the key feature of mobile internet services. Therefore, this article proposed using IPsec protocol in the virtual private network to impose the required security between the hosts of the mobile network. The mobile network

integration with the virtual private network begins with a vehicles-based network where the two cars can communicate with each other using the virtual private network tunnel to ensure the privacy as well as security of the being shared data.

At [53], cloud service has drawn an enormous contribution in data auditing service, data over the cloud has made a considerable advantage in the technologies over cloud services more likely, most of the computing service had been updated on the cloud, and hence the so-called cloud computing has largely emerged. In addition, services such as getting access to particular software which is not easy to access from the computer have made noticeable advantages.

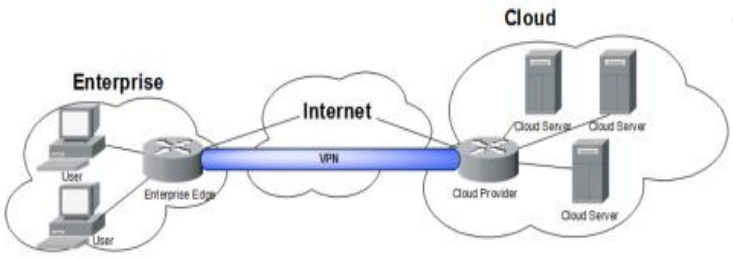

Figure 2.4: Cloud based virtual private network[2].

However, the advancement of cold computing enabled the big companies to get cloud services so that each company will have an on-cloud server with the same capability as the physical server. Virtual servers have been established over the clouds. Thus, each user can be allotted those services upon his subscription to the cloud provider. Furthermore, (in Figure 2.4)[2], a virtual private network has gained its role to provide security to the data being transmitted over the cloud.

At [54], the virtual private network is found to impose privacy and security over the data being transmitted via public networks. Internet is an extensive public network where anyone can get access and initiate any type of service over this extensive network. Therefore, the virtual private network has outperformed as security enforcement means over the internet. On the other hand, some services like susceptible services that require special access from the users into the servers. For example, servers like government servers or sensitive administration work like tax department or banking work have required another enhancement.

SSL certificate is being provided to those uses where the user can download this certificate from the server before it connects to that server. This certificate enhances the job of the virtual private network, especially where the user is part of a home network or office network so, an SSL certificate can prevent any other computer access by any means to this server apart from the computer with an SSL certificate. This task significantly correlates with firewalls on both host and server sides.

At [55], Risks of system security of library network information face two kinds: external and internal. This internal risk contains software, hardware, management and technical. In contrast, viruses and hackers are external ones. Lacking control over the first kind of risk will foray the external risk and opportunities. Therefore, managing internal risk on digital library and network security is a prerequisite and cornerstone. Through VPN technology for the tunnel, encryption, and QOS approaches, the technology of VPN can assist us in maximizing the usage of the network, public network, lowering costs, improving efficiency, and improving network security.

At [56], As the industry criterion, SSL protocol determines between two specific layers, namely transport and application layer in the reference model TCP/IP. Therefore, the architecture of this layering protocol is divided into two layers. The record protocol is in a lower layer, and three parallel protocols are in the upper layer: alert, handshake and change cipher spec protocol.

Power utilities, whose objective is to deliver a secure and reliable electricity supply, have higher safety needs for enterprises' information systems than regular enterprises. In addition, demand for data sharing among a diversity of the remote terminals of wireless and Intranet is increasing as power utility informatization progresses. How to ensure the wireless remote access's security in power utilities has emerged as a significant issue. The authors[56] have analysed existing SSL VPN technology besides designing a new secure platform for wireless remote access depends on SSL VPN for power utilities, which gives a novel solution for safe wireless in distance access in it, based on the characteristics and particular demands of power utilities.

3. RESEARCH METHODOLOGY

3.1 INTRUSION DETECTION

The intrusion detection system (IDS) is a tool that is used to monitor network traffic so that the network can protect itself from potential intrusions. To grantee its confidentiality, availability, as well as integrity. The classification of it is presented in figure 3.1 below[3]. Although many studies have been conducted, IDS still encounter challenges in increasing detection accuracy while decreasing false alarm rates, as well as in detecting novel intrusions. Recently, like machine learning (ML), deep learning (DL) systems[57] have been deployed as potentiality solutions in order to detect intrusion across the network in an efficient way[3].

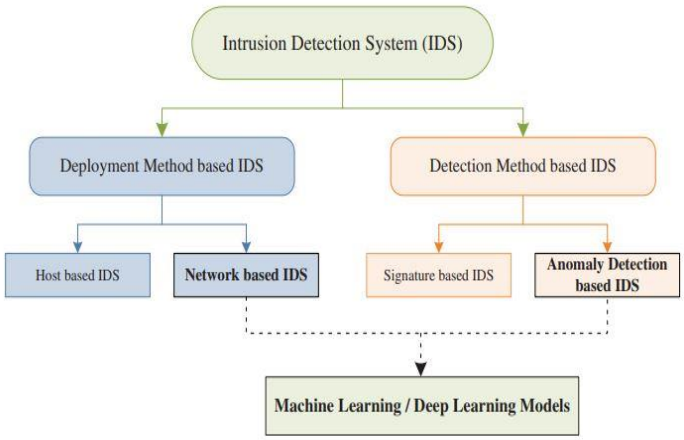

Figure 3.1: The classification of intrusion detection[3].

3.2 NEURAL NETWORK MODEL

Artificial neural network is one of the classification tools that proven reliable performance in addressing of numerous problems in sciences and technology. This model is structured of three parts namely input layers, hidden layers and output layers as showed in figure 3.2. Each layer is responsible for particular task that to be applied on input data in order to perform the required mapping or classification. According to the number of hidden layers, the said neural network model complexity is measured. The denser of hidden layers may lead to undesired occurrences such as large training time and computational complexity that required high processing power which applies cost of hardware adaptation. In this work, three type of neural networks are adopted with the structed made in Table 3.1.

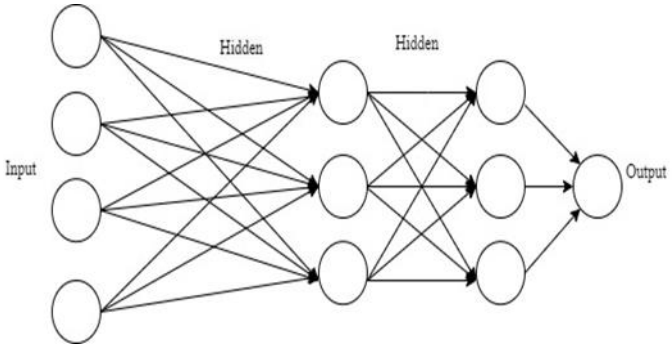

Figure 3.2: Neural Network Overview

Table 3.1: Neural network structure and parameters.

Parameter	Details
General structure	Three layers
Hidden structure	Single layer
Algorithm of training	LM
Targeted training performance	MSE
Targeted performance value	1e-33
Data portions	80 % training, 20 % testing

The proposed neural network models are mentioned in hereinafter:

3.2.1 Cascade Feed Forward Back Propagation (CFFBP)

In this model, the structure detailed in Table 3.1 are used so the final structure given in Figure 3.3 is established. The training of the model is made using the backpropagation model and thus results are determined. The model is containing of multiple feed forward backpropagation models connected in cascade style.

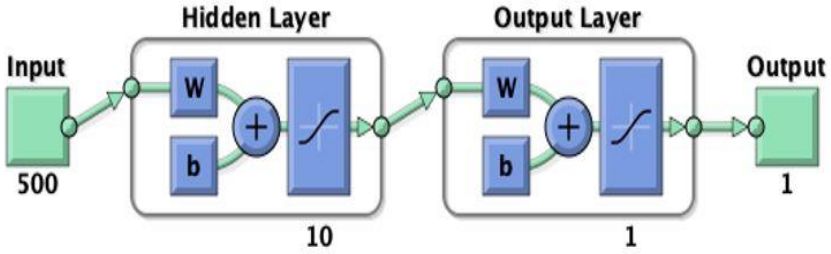

Figure 2.3: Layer structure of Cascade Feed Forward Back Propagation (CFFBP)**.**

3.2.2 Feed Forward Back Propagation (FFBP)

In this model, the structure detailed in Table 3.1 are used so the final structure given in Figure 3.2 is established. The training of the model is made using the backpropagation model and thus results are determined. The model is containing of single feed forward backpropagation models connected using feedback loop. Two weights coefficients are included in the output layer of this model.

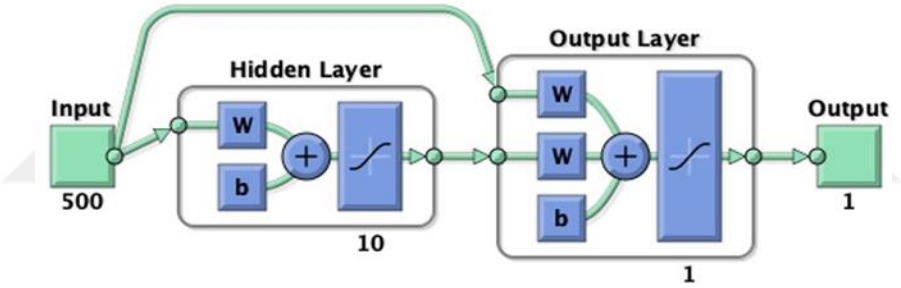

Figure 3.4: Layer structure of Feed Forward Back Propagation (FFBP)**.**

3.2.3 Layer Learning Neural Network (LLNN)

This model is consisting of single backpropagation model with three parameters one is called bias coefficients and two groups of weights coefficients at the hidden layer. Model is demonstrated in Figure 3.5.

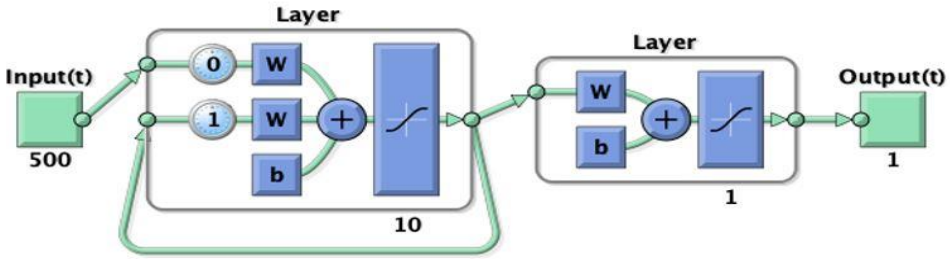

Figure 23.5: Layer structure of Layer Learning Neural Network (LLNN)**.**

3.3 WORK OVERVIEW

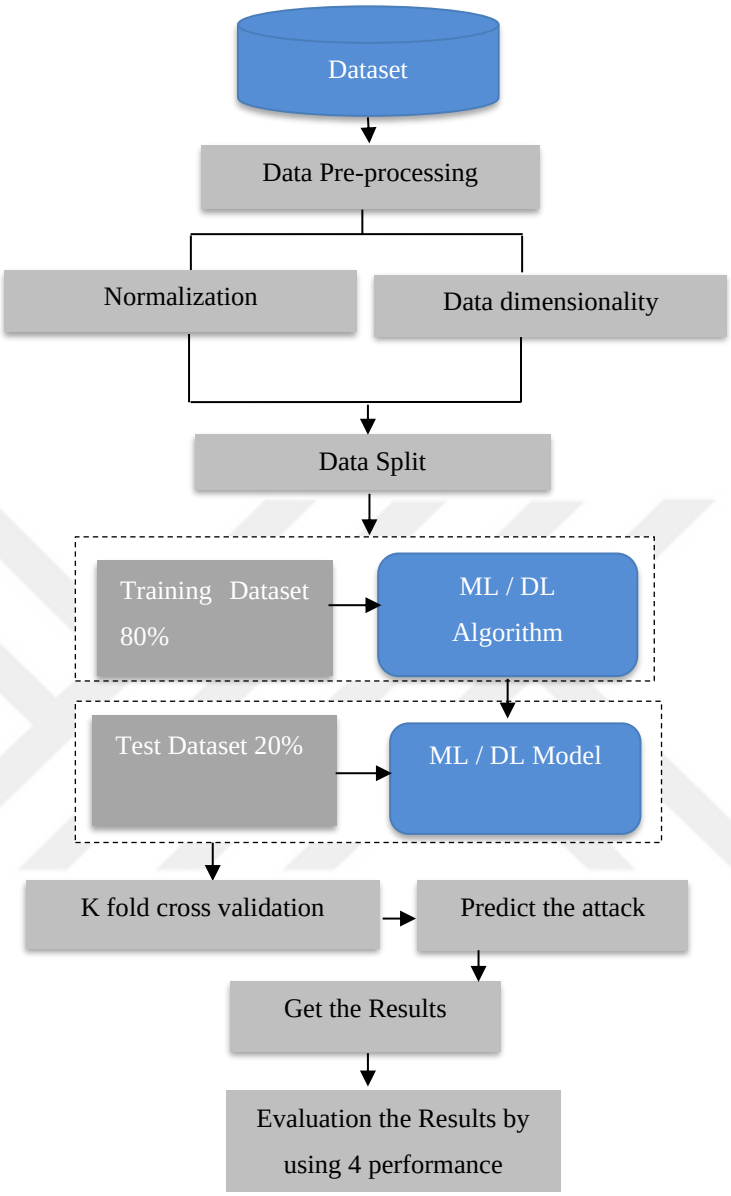

Figure 3.6: The generalization of the proposed work

3.3.1 Dataset Description

The dataset about intrusion attacks named ADFA-LD is referred to from the GitHub respiratory. This data is not actually labelled; Thus, the labelling process of the data lines is performed at the commencing stage of processing. The data is divided into six classes that represent the following six types of intrusion attacks on the web/cloud network:

a. Add_user
b. Hydra_FTP
c. Hydra_SSH
d. Java_Meterpreter
e. Meterpreter
f. Web_Shell

Table 3.2: The generation of ADFA-LD attack dataset using attack vectors[58].

Attack	Payload/Effect	Vector
Hydra-FTP	Password brute force	FTP by Hydra
Hydra-SSH	Password brute force	SSH by Hydra
Add user	Add new superuser	Client-side poisoned executable
Java-Meterpreter	Java based Meterpreter	TikiWiki vulnerability exploit
Meterprete	Linux Meterpreter Payload	Client-side poisoned executable
Web shell	C100 Web shell	PHP remote file inclusion vulnerability

The process that made in the next phase is data normalization where every row of the said data is being normalized by dividing the row elements by the maximum row element value. One more operation is performed on the said row data which is related to data dimensionality. It was realized that attacks base data in every row are not in identical count hence that presented a serious training error. The error is being rectified by extending the less length rows with zeros so that equal number of elements is made in every row of this database.

3.3.2 K-fold Cross Validation

In this stage dataset is being divided into ten folds using the 10-fold cross validation algorithm, every fold itself is divided into 80 percent and 20 percent portions that stands for training set and testing set. This stage is deployed here in order to investigate the performance of every algorithm with different data structures.

3.4 PERFORMANCE METRICS

In order to examine the performance of every model used in this study, four performance metrics are defined here:

1. Accuracy: stands for the percentage of the correct detections of the attacks (Ci) to the total number of attacks existed in the dataset (Ti) and can be represented as in equation 3.1.

$$Accuracy = \frac{Ci}{Ti} * 100\% \quad (3.1)$$

2. Mean Square Error (MSE): stands for the averaging the square error values that are calculated in the error vector as following:

$$Error = [E1, E2, E3, \ldots, En]$$

$$MSE = \frac{\sum E^2}{n} \quad (3.2)$$

3. Root Mean Square Error (RMSE): stands for the natural root of the mean square error metric results and given in the equation 3.3.

$$RMSE = (MSE)^{0.5} \quad (3.3)$$

4. Mean Absolute Error (MAE): stands for the averaging the absolute value of errors that are calculated in the error vector as following:

$$MAE = \frac{\sum |E|}{n} \quad (3.4)$$

4. RESULTS AND DISCUSSIONS

In this section each algorithm is designed in order to do the claustration of the attack, hence, it can be predicted in advance. Four performance metrics have been used to evaluate the performance of each algorithm and the results that have been obtained are presented below.

4.1 CASCADE FEED FORWARD BACK PROPAGATION (CFFBP)

Accuracy of attack prediction using Cascade Feed Forward Back Propagation (CFFBP) algorithm is determined using tenfold cross validation. Data is divided into tenfold and every fold is then used to train the algorithm/ model in 80:20 portions. Thus, ten accuracies are determined for the same dataset as in Table 4.1, the same is demonstrated in Figure 4.1. from the other hand, other performance metrics alike mean square error (MSE) (see Table 4.2 and Figure 4.2), mean absolute error (MAE) (see Table 4.3 and Figure 4.3), and root mean square error (RMSE) (see Table 4.4 and Figure 4.4) are determined. It has been found that best accuracy of attack prediction is 74.13 percent.

Table 4.1: Accuracy of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Fold number	Accuracy %
1	72.4137931034483
2	63.7931034482759
3	56.8965517241379
4	29.3103448275862
5	13.7931034482759
6	8.62068965517242
7	20.6896551724138
8	62.0689655172414
9	74.1379310344828
10	44.8275862068966

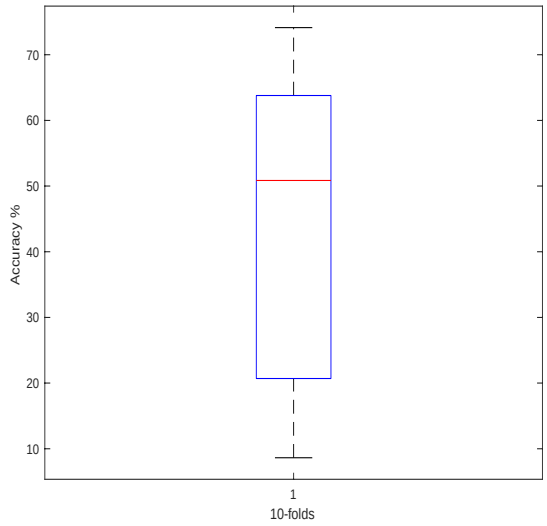

Figure 4.1: Demonstration of Accuracy of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Table 4.2: MSE of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Fold number	MSE
1	1.37931034482759
2	1.39655172413793
3	1.67241379310345
4	2.39655172413793
5	6.87931034482759
6	5.34482758620690
7	5
8	1.18965517241379
9	1.41379310344828
10	1.50000000000000

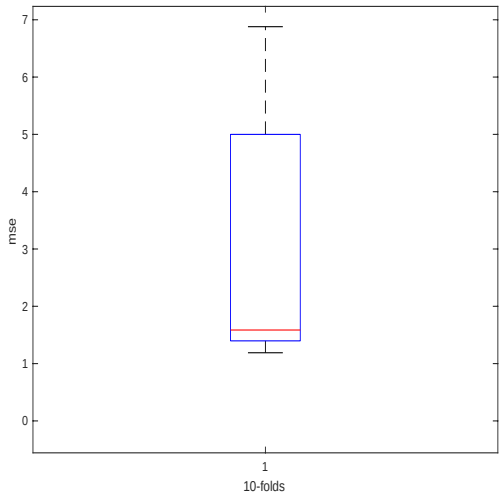

Figure 4.2: Demonstration of MSE of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Table 4.3: MAE of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Fold number	MAE
1	0.517241379310345
2	0.603448275862069
3	0.706896551724138
4	1.15517241379310
5	2.15517241379310
6	2
7	1.68965517241379
8	0.568965517241379
9	0.517241379310345
10	0.810344827586207

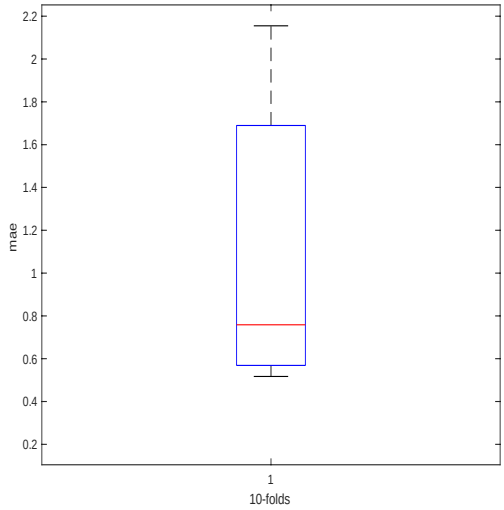

Figure 4.3: Demonstration MAE of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Table 4.4: RMSE of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

Fold number	RMSE
1	1.17444043902941
2	1.18175789573750
3	1.29321838569650
4	1.54808001218862
5	2.62284394214135
6	2.31188831611886
7	2.23606797749979
8	1.09071314854722
9	1.18903032065977
10	1.22474487139159

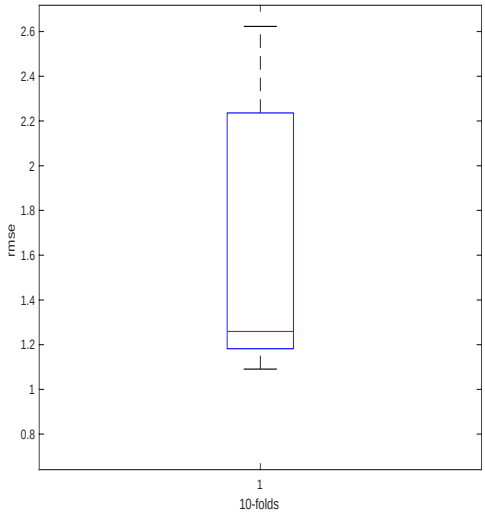

Figure 4.4: Demonstration of RMSE of Cascade Feed Forward Back Propagation (CFFBP) algorithm after 10 folds cross validation.

4.2 FEED FORWARD BACK PROPAGATION (FFBP)

Accuracy of attack prediction using Feed Forward Back Propagation (FFBP) algorithm is determined using tenfold cross validation. Data is divided into tenfold and every fold is then used to train the algorithm/ model in 80:20 portions. Thus, ten accuracies are determined for the same dataset as in Table 4.5, the same is demonstrated in Figure 4.5. from the other hand, other performance metrics alike mean square error (MSE) (see Table 4.6 and Figure 4.6), mean absolute error (MAE) (see Table 4.7 and Figure 4.7), and root mean square error (RMSE) (see Table 4.7 and Figure 4.7) are determined. It has been found that best accuracy of attack prediction is 82.75 percent.

Table 4.5: Accuracy of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Fold number	Accuracy %
1	15.5172413793103
2	48.2758620689655
3	25.8620689655172
4	15.5172413793103
5	18.9655172413793
6	27.5862068965517
7	10.3448275862069
8	82.7586206896552
9	67.2413793103448
10	75.8620689655172

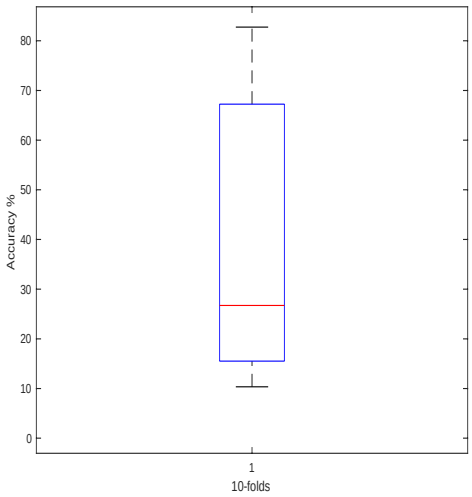

Figure 4.5: Demonstration of Accuracy of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Table 4.6: MSE of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Fold number	**MSE**
1	6.46551724137931
2	3.20689655172414
3	4.39655172413793
4	7.74137931034483
5	3.62068965517241
6	5.13793103448276
7	7.98275862068966
8	0.706896551724138
9	2.48275862068966
10	1.08620689655172

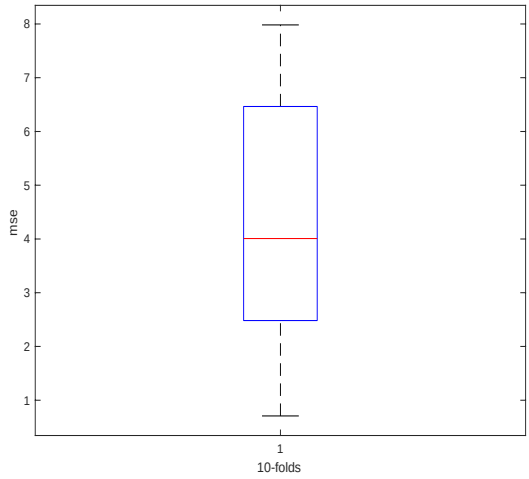

Figure 4.6: A demonstration of MSE of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Table 4.7: MAE of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Fold number	**MAE**
1	2.01724137931034
2	1.13793103448276
3	1.56896551724138
4	2.22413793103448
5	1.51724137931034
6	1.72413793103448
7	2.32758620689655
8	0.327586206896552
9	0.827586206896552
10	0.465517241379310

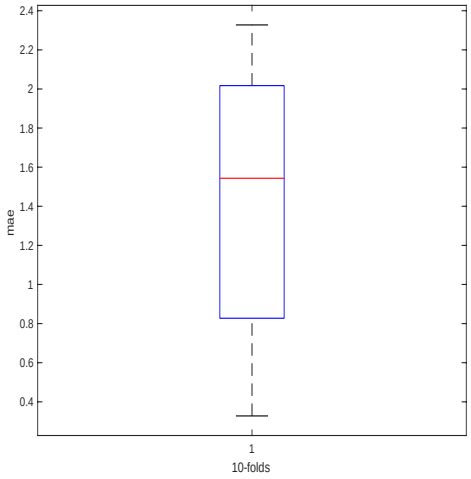

Figure 4.7: A demonstration of MAE of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Table 4.8: RMSE of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

Fold number	RMSE
1	2.54273813857804
2	1.79078098932397
3	2.09679558472874
4	2.78233342903844
5	1.90281098776847
6	2.26670047304066
7	2.82537760674386
8	0.840771402774939
9	1.57567719431667
10	1.04221250066948

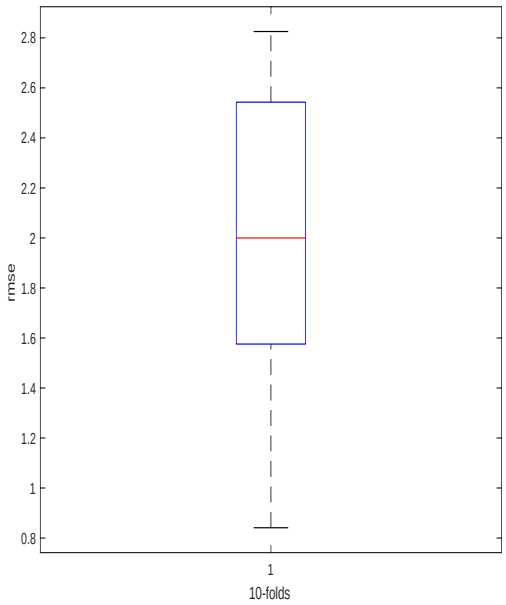

Figure 4.8: A demonstration of RMSE of Feed Forward Back Propagation (FFBP)algorithm after 10 folds cross validation.

4.3 LAYER LEARNING NEURAL NETWORK (LLNN)

Accuracy of attack prediction using Layer Learning Neural Network (LLNN) algorithm is determined using tenfold cross validation. Data is divided into tenfold and every fold is then used to train the algorithm/ model in 80:20 portions. Thus, ten accuracies are determined for the same dataset as in Table 4.9, the same is demonstrated in Figure 4.9. from the other hand, other performance metrics alike mean square error (MSE) (see Table 4.10 and Figure 4.10), mean absolute error (MAE) (see Table 4.11 and Figure 4.11), and root mean square error (RMSE) (see Table 4.12 and Figure 4.12) are determined. It has been found that best accuracy of attack prediction is 81.76 percent.

Table 4.9: Accuracy of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Fold number	Accuracy %
1	12.0689655172414
2	58.6206896551724
3	39.6551724137931
4	51.7241379310345
5	29.3103448275862
6	56.8965517241379
7	81.7675206000052
8	25.8620689655172
9	46.5517241379310
10	56.8965517241379

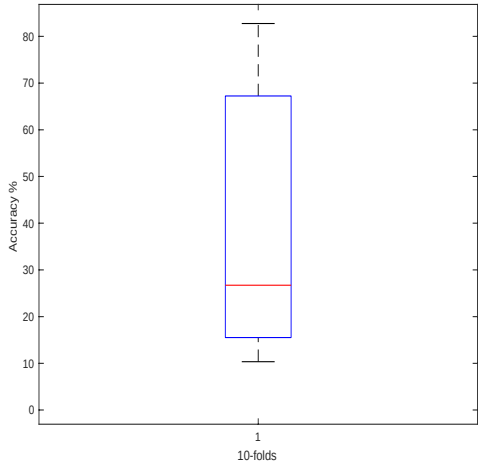

Figure 4.9: A demonstration of Accuracy of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Table 4.10: MSE of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Fold number	MSE
1	8.75862068965517
2	1.17241379310345
3	2.13793103448276
4	0.948275862068966
5	1.51724137931034
6	1.67241379310345
7	0.982758620689655
8	2.51724137931034
9	1.27586206896552
10	1.67241379310345

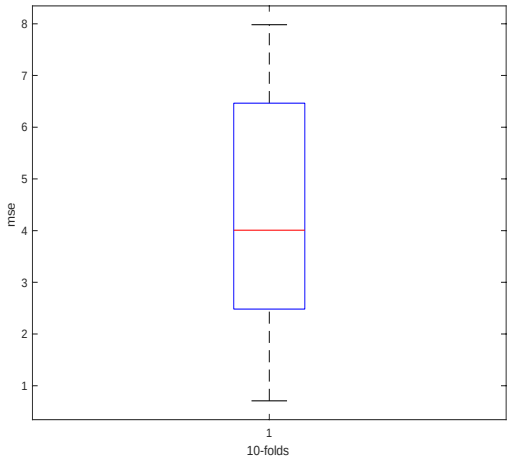

Figure 4.10: A demonstration of MSE of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Table 4.11: MAE of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Fold number	**MSE**
1	2.51724137931034
2	0.620689655172414
3	1
4	0.603448275862069
5	0.931034482758621
6	0.741379310344828
7	0.327586206896552
8	1.20689655172414
9	0.724137931034483
10	0.706896551724138

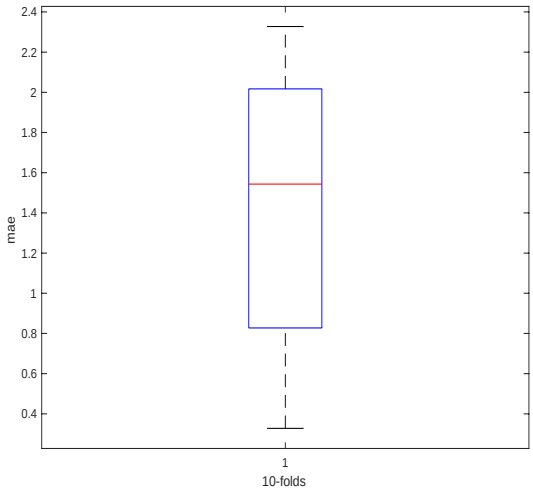

Figure 4.11: A demonstration of MAE of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Table 4.12: RMSE of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation.

Fold number	**RMSE**
1	2.95949669532763
2	1.08278058400742
3	1.46216655497339
4	0.973794568720203
5	1.23176352410288
6	1.29321838569650
7	0.991341828376900
8	1.58658166487274
9	1.12954064511443
10	1.29321838569650

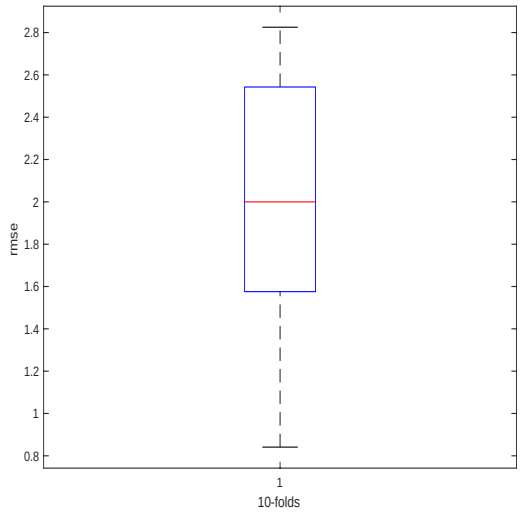

Figure 4.12: A demonstration of RMSE of Layer Learning Neural Network (LLNN) algorithm after 10 folds cross validation**.**

4.4 PERFORMANCE COMPARISON

The performance comparison of each algorithm is based on:

4.4.1 Accuracy Metrics

The accuracies of the three proposed algorithms are being compared and results are tabbed in Table 4.13 and demonstrated in Figure 4.13. The best accuracy is achieved when Feed Forward Back Propagation (FFBP) is used corresponding to 82.758 percent. Similarly, MSE (Table 4.15, Figure 4.15), MAE (Table 4.16, Figure 4.16) and RMSE (Table 4.17, Figure 4.17) are found minimum in when Feed Forward Back Propagation (FFBP) is used for attack prediction.

Table 4.13: Comparison between accuracies in the proposed methods.

Algo.	Accuracy %
CFFBP	74.137931
FFBP	82.7586207
LRNN	81.7675206

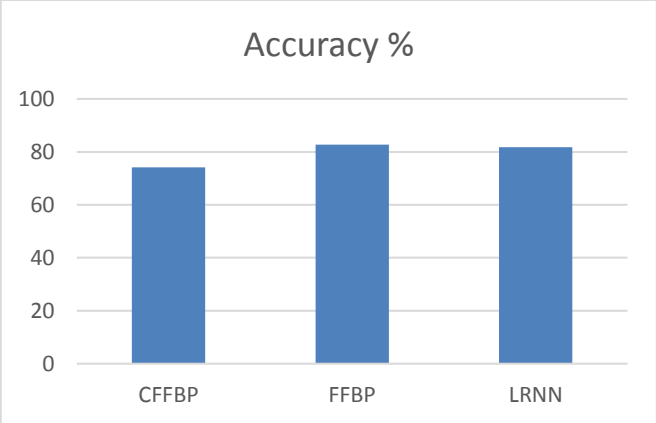

Figure 4.13: A demonstration of Comparison between accuracies in the proposed methods.

4.4.2 MSE METRIC

This section presented the results that have been obtained regard to the MSEs of each algorithm.

Table 4.14: Comparison between MSEs in the proposed methods.

Algo.	MSE
CFFBP	1.18965517
FFBP	0.70689655
LRNN	0.98275862

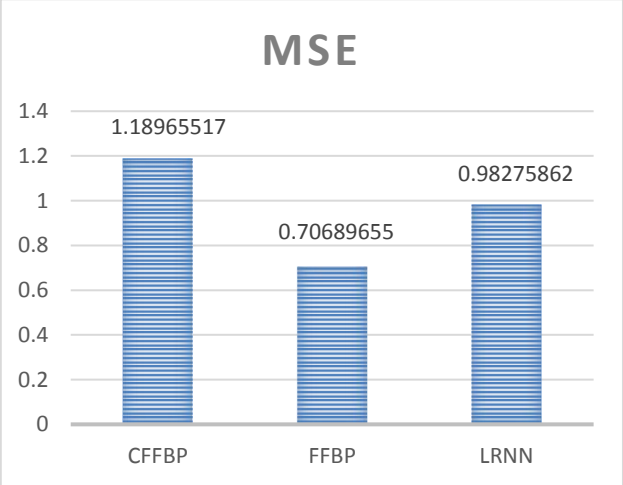

Figure 4.14: A demonstration of Comparison between MSEs in the proposed methods.

4.4.3 MAE METRIC

This section presented the results that have been obtained regard to the MAEs of each algorithm.

Table 4.15: Comparison between MAEs in the proposed methods**.**

Algo.	**MAE**
CFFBP	0.51724138
FFBP	0.32758621
LRNN	0.32758621

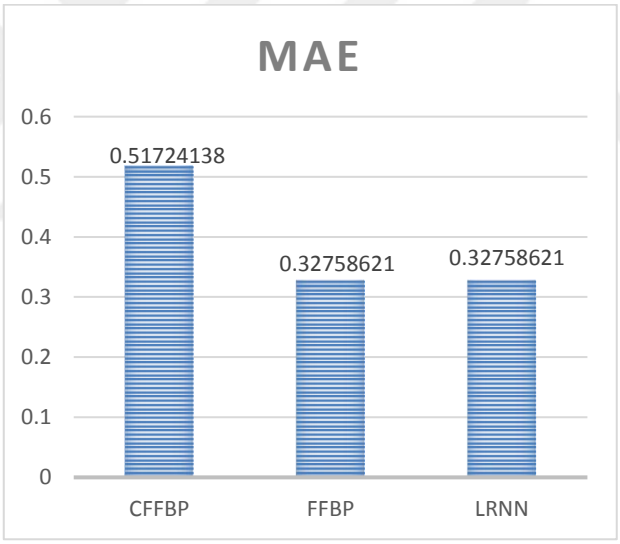

Figure 4.15: A demonstration of Comparison between MAEs in the proposed methods.

4.4.4 RMSE Metric

This section presented the results that have been obtained regard to the RMSEs of each algorithm.

Table 4.16: Comparison between RMSEs in the proposed methods.

Algo.	RMSE
CFFBP	1.18903032
FFBP	0.8407714
LRNN	0.99134183

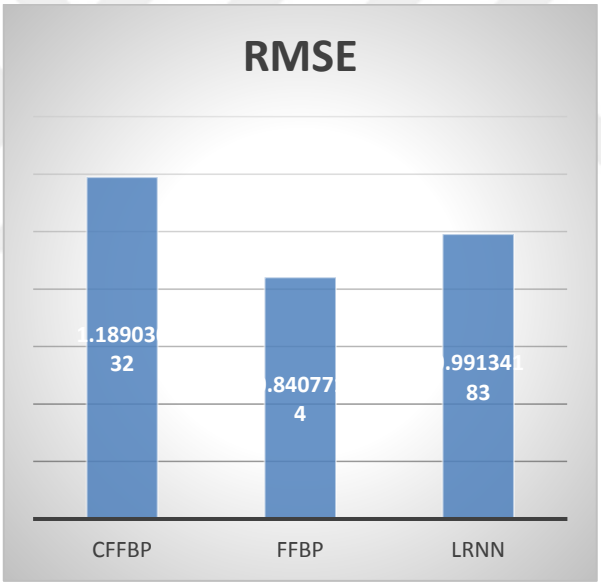

Figure 4.16: A demonstration of Comparison between RMSE in the proposed methods**.**

4.5 THE COMPARASION OF PROPOSED METHOD WITH PREVIOUS STUDIES

In[59] two algorithms on ADFA-LD dataset have been used namely "k-nearest neighbour(kNN) as well as k-means clustering (kMC)". They used a frequency-based paradigm to represent the data also reduced the feature vector's dimension using "principal component analysis (PCA)". Hence, the accuracy that they achieved is 60% with 20% of FPR. In[60] the abnormal system detects anomalies using a CNN-based model, which has a small detection rate that is 60.18% and high FAR. On the same dataset in[61], a one-class SVM they used associated with a short sequence-based-technique. The maximum accuracy that they achieved is 70% using a single-class SVM. In [62] the authors proposed the DeepIDEA and the result that had obtained is 45.31%. In[63] presented a novel lightweight IDS relying on a representation of vector space associated with a Multilayer Perceptron(MLP) and the result was 94%. In[64] WOA and Genetic Algorithms has DR that is 94.44% in detection the attach except DOS attacks. They analysed the performance of the classifier depend on FN,TN,FP FN rates as well the execution time for the training dataset was high so it still needs to be decreased. In[65] to get a good accuracy which is 80%, they utilize CNN to grabs local liaison within trace files as well as RNN to learn sequential liaison correlation despite this result their Model is extremely complex, as the proper amount of hyperparameter regard to CNN and RNN-based modules must be defined. It knows that the accuracy scores of all approaches implies the proposed in this study has a good result, as it is illustrated in table 4.17.

Table 4.17: Comparison of the proposed methodology results with other methodologies from the literature.

Approach	**Performance**
KNN+ KMC[59]	60%
one-class SVM[61]	70%
DeepIDEA[62]	45.31%
CNN[60]	61.18%
MLP[63]	94%
CNN+RNN[65]	80%
WOA+ Genetic Algorithm[64]	94.44%
Proposed (FFBP)	82.7586207 %

5. CONCLUSION

Malicious attack prediction is vital for the security of computer networks, thus various types of attack prediction are developed in the literature. Automatic attack prevention by automatic attack detection is used in this study. Prediction of attack is made using deep learning paradigms namely: Cascade Feed Forward Back Propagation (CFFBP), Feed Forward Back Propagation (FFBP) and Layer Learning Neural Network (LLNN). Using the dataset descripted in the chapter 3, all those algorithms are trained for the attack prediction task and hence every algorithm performance is examined using four performance metrics namely: accuracy, means square error (MSE), mean absolute error (MAE) and Root mean square error (RMSE). The best algorithm that yielded the best attack prediction performance is the Feed Forward Back Propagation (FFBP) with accuracy of 82.7586207. with the proposed work, the performance of this model is compared with other studies from the literature and the results are listed in Table 4.17.

Future Work:

Intrusion detection in cloud servers and computer networks involves evaluating the authenticity of the inward connections; however, the current research work involves improving the performance of evolution of the techniques used for performing the same by automatic sensing of the inward connections. Future work might be conducted using parallel programming (hardware-based deep learning), i.e. using FPGA devices where more doors of performance optimization are available.

REFERENCES

[1] M. N. Bin Ali, M. E. Hossain, and M. M. Parvez, "Design and Implementation of a Secure Campus Network," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 5, no. 7, pp. 370–374, 2015.

[2] C. Huang, Z. Sun, and P. Smith, "Secure Network Solutions for Enterprise Cloud Services," in *Handbook of Research on Demand-driven Web Services: Theory, Technologies and Applications*, 1st ed., no. September, Z. Sun and J. Yearwaord, Eds. United States: IGI-Global, 2014, pp. 222–244.

[3] Z. Ahmad, "Network intrusion detection system : A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, no. September 2020, pp. 1–29, 2021, doi: 10.1002/ett.4150.

[4] P. Jain, M. Gyanchandani, and N. Khare, "Enhanced Secured Map Reduce layer for Big Data privacy and security," *J. Big Data*, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0193-4.

[5] N. Olinder, K. Fedyakin, and E. Korneeva, "Personal Data Protection in the Internet of Things," in *Proceedings of the 1st International Scientific Conference "Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development" (LARDER 2020)*, 2021, vol. 171, no. Larder 2020, pp. 227–232, doi: 10.2991/aebmr.k.210318.037.

[6] K. Dubey and S. C. Sharma, "An extended intelligent water drop approach for efficient VM allocation in secure cloud computing framework," *J. King Saud Univ. - Comput. Inf. Sci.*, 2020, doi: 10.1016/j.jksuci.2020.11.001.

[7] W. Gan and X. Yin, "Research on high security of IP tunnel in virtual private network," *J. Phys. Conf. Ser.*, vol. 1856, no. 1, 2021, doi: 10.1088/1742-6596/1856/1/012014.

[8] I. Kunz, A. Schneider, and C. Banse, "Privacy smells: Detecting privacy problems in cloud architectures," in *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 2020, pp. 1324–1331, doi: 10.1109/TrustCom50675.2020.00178.

[9] R. Alsaqour, A. Motmi, and M. Abdelhaq, "A Systematic Study of Network Firewall and Its Implementation 1 1," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 4, pp. 199–208, 2021, [Online]. Available: http://paper.ijcsns.org/07_book/202104/20210424.pdf.

[10] H. Habibzadeh and E. Al, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, pp. 0–42, 2019, doi: 10.1016/j.scs.2019.101660.

[11] N. Gerber, V. Zimmermann, and M. Volkamer, “Why johnny fails to protect his privacy,” *Proc. - 4th IEEE Eur. Symp. Secur. Priv. Work. EUROS PW 2019*, pp. 109–118, 2019, doi: 10.1109/EuroSPW.2019.00019.

[12] S. Kumar and D. Agarwal, “Hacking Attacks, Methods, Techniques And Their Protection Measures Article in International Journal of Advance Research in Computer Science and Management,” *Int. J. Adv. Res. Comput. Sci. Manag.*, vol. 4, no. 4, pp. 2252–2257, 2018, [Online]. Available: https://www.researchgate.net/publication/324860675_Hacking_Attacks_Methods_Techniques_And_Their_Protection_Measures%0Awww.ijsart.com.

[13] M. V. Pawar and J. Anuradha, “Network security and types of attacks in network,” *Procedia Comput. Sci.*, vol. 48, pp. 503–506, 2015, doi: 10.1016/j.procs.2015.04.126.

[14] S. Rathore, P. K. Sharma, V. Loia, Y. S. Jeong, and J. H. Park, “Social network security: Issues, challenges, threats, and solutions,” *Inf. Sci. (Ny).*, vol. 421, pp. 43–69, 2017, doi: 10.1016/j.ins.2017.08.063.

[15] Kamesh and N. Sakthi Priya, “A survey of cyber crimes Yanping,” *Secur. Commun. Networks*, vol. 5, no. June, pp. 422–437, 2012, doi: 10.1002/sec.

[16] M. Carmo, J. S. Silva, E. Monteiro, P. Simões, and F. Boavida, “Ethernet QoS Modeling in Emerging Scenarios,” in *In Proceedings of 3rd International Workshop on Internet Performance, Simulation, Monitoring and Measurement (IPS-MoMe 2005*, 2005, pp. 90-96.

[17] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, “On the vital areas of intrusion detection systems in wireless sensor networks,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013, doi: 10.1109/SURV.2012.121912.00006.

[18] A. H. Farooqi and F. A. Khan, “A survey of intrusion detection systems for wireless sensor networks,” *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 9, no. 2, pp. 69–83, 2012, doi: 10.1504/IJAHUC.2012.045549.

[19] C. Kiennert, Z. Ismail, H. Debar, and J. Leneutre, “A survey on game-theoretic approaches for intrusion detection and response optimization,” *ACM Comput. Surv.*, vol. 51, no. 5, 2018, doi: 10.1145/3232848.

[20] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, “The impact of rank attack on network topology of routing protocol for low-power and lossy networks,” *IEEE Sens. J.*, vol. 13, no. 10, pp. 3685–3692, 2013, doi: 10.1109/JSEN.2013.2266399.

[21] W. Xie *et al.*, “Routing loops in DAG-based low power and lossy networks,” *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 888–895, 2010, doi: 10.1109/AINA.2010.126.

[22] A. Dvir, T. Holczer, and L. Buttyan, “VeRA - Version number and rank authentication in RPL,” in *Proceedings - 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2011*, 2011, pp. 709–714, doi: 10.1109/MASS.2011.76.

[23] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Proc. 1st IEEE Int. Work. Sens. Netw. Protoc. Appl. SNPA 2003*, pp. 113–127, 2003, doi: 10.1109/SNPA.2003.1203362.

[24] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, “An intrusion detection framework for energy constrained IoT devices,” *Mech. Syst. Signal Process.*, vol. 136, no. 0888–3270, p. 106436, 2020, doi: 10.1016/j.ymssp.2019.106436.

[25] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, “6LoWPAN fragmentation attacks and mitigation mechanisms,” *WiSec 2013 - Proc. 6th ACM Conf. Secur. Priv. Wirel. Mob. Networks*, pp. 55–66, 2013, doi: 10.1145/2462096.2462107.

[26] K. Kuldeep, V. V Singh, and H. Gupta, “A NEW APPROACH FOR THE SECURITYOF VPN CCS Concepts Security and privacy → Formal Security Models,” pp. 1–5, 2016, [Online]. Available: http://dx.doi.org/10.1145/2905055.2905219.

[27] R. R. Jadhav and P. S. Sheth, “VPN: Overview and Security Risks,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 7, no. 1, pp. 305–309, 2021, doi: 10.48175/ijarsct-1649.

[28] S. Ndichu, S. McOyowo, H. Okoyo, and C. Wekesa, “A Remote Access Security Model based on Vulnerability Management,” *Int. J. Inf. Technol. Comput. Sci.*, vol. 12, no. 5, pp. 38–51, 2020, doi: 10.5815/ijitcs.2020.05.03.

[29] F. Bensalah, N. El Kamoun, and A. Bahnasse, “Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP,” *IJCNS Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 4, pp. 361–369, 2017.

[30] A. Z. Bhat, D. K. Al Shuaibi, and A. V. Singh, “Virtual private network as a service-A need for discrete cloud architecture,” *2016 5th Int. Conf. Reliab. Infocom Technol. Optim. ICRITO 2016 Trends Futur. Dir.*, no. September, pp. 526–532, 2016, doi: 10.1109/ICRITO.2016.7785012.

[31] H. H. Song, “Testing and evaluation system for cloud computing information security products,” in *Procedia Computer Science*, 2020, vol. 166, pp. 84–87, doi: 10.1016/j.procs.2020.02.023.

[32] I. Lodha, L. Kolur, K. S. Hari, and P. Honnavalli, “Secure Wireless Internet of Things Communication Using Virtual Private Networks,” *Lect. Notes Electr. Eng.*, vol. 637, pp. 735–742, 2020, doi: 10.1007/978-981-15-2612-1_70.

[33] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, “Internet of Things: Evolution and technologies from a security perspective,” *Sustain. Cities Soc.*, vol. 54, no. July 2019, p. 101728, 2020, doi: 10.1016/j.scs.2019.101728.

[34] V. Hashiyana, T. Haiduwa, N. Suresh, A. Bratha, and F. K. Ouma, “Design and Implementation of an IPSec Virtual Private Network: A Case Study at the University of Namibia,” *2020 IST-Africa Conf. IST-Africa 2020*, no. October, 2020.

[35] P. Kumar and R. Kumar, “Issues and challenges of load balancing techniques in cloud computing: A survey,” *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–35, 2019, doi: 10.1145/3281010.

[36] S. K. Mishra, B. Sahoo, and P. P. Parida, “Load balancing in cloud computing: A big picture,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 2, pp. 149–158, 2020, doi: 10.1016/j.jksuci.2018.01.003.

[37] S. Manaseer, M. Alzghoul, and M. Mohmad, “An advanced algorithm for load balancing in cloud computing using MEMA technique,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 3, pp. 36–41, 2019.

[38] S. Afzal and G. Kavitha, “Load balancing in cloud computing – A hierarchical taxonomical classification,” *J. Cloud Comput.*, vol. 8, no. 1, pp. 1–24, 2019, doi: 10.1186/s13677-019-0146-7.

[39] Y. T. H. Hlaing and T. T. Yee, “Static Independent Task Scheduling on Virtualized Servers in Cloud Computing Environment,” *2019 Int. Conf. Adv. Inf. Technol. ICAIT 2019*, pp. 55–59, 2019, doi: 10.1109/AITC.2019.8920865.

[40] J. Pacheco and S. Hariri, “IoT security framework for smart cyber infrastructures,” *Proc. - IEEE 1st Int. Work. Found. Appl. Self-Systems, FAS-W 2016*, pp. 242–247, 2016, doi: 10.1109/FAS-W.2016.58.

[41] A. Z. Bhat, D. K. Al Shuaibi, and A. V. Singh, “Virtual private network as a service-A need for discrete cloud architecture,” in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions*, 2016, no. July 2020, pp. 526–532, doi: 10.1109/ICRITO.2016.7785012.

[42] D. Benzid and M. Kadoch, “Virtual private network over wireless mesh networks,” in *Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014*, 2014, no. October, pp. 340–345, doi: 10.1109/FiCloud.2014.60.

[43] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[44] Z. Zhou and T. Huang, “Open VPN Application under Campus Network,” *J. Phys. Conf. Ser.*, vol. 1865, no. 4, 2021, doi: 10.1088/1742-6596/1865/4/042014.

[45] S. Liu, T. Zeng, Y. Chao, and H. Wang, “Application of VPN Based on L2TP and User’s Access Rights in Campus Network,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10989 LNAI, pp. 676–686, 2018, doi: 10.1007/978-3-030-00563-4_66.

[46] H. Dhall, D. Dhall, S. Batra, and P. Rani, “Implementation of IPSec protocol,” *Proc. - 2012 2nd Int. Conf. Adv. Comput. Commun. Technol. ACCT 2012*, pp. 176–181, 2012, doi: 10.1109/ACCT.2012.64.

[47] V. G. Nguyen and Y. H. Kim, “SDN-based enterprise and campus networks: A case of VLAN management,” *J. Inf. Process. Syst.*, vol. 12, no. 3, pp. 511–524, 2016, doi: 10.3745/JIPS.03.0039.

[48] W. A. Gould, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks,” *IEEE Commun. Surv. TUTORIALS.*, vol. 16, no. 1, pp. 266–282, 2014, doi: 10.1533/9781845696146.3.419.

[49] M. A. A. Sufyan, M. Zuhaib, and M. Rihan, “An investigation on the application and challenges for wide area monitoring and control in smart grid,” *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 580–587, 2021, doi: 10.11591/eei.v10i2.2767.

[50] R. Gore and M. Kande, “Analysis of Wide Area Monitoring System architectures,” in *Proceedings of the IEEE International Conference on Industrial Technology*, 2015, vol. 2015-June, no. June, pp. 1269–1274, doi: 10.1109/ICIT.2015.7125272.

[51] H. Debar, M. Dacier, and A. Wespi, “Towards a taxonomy of intrusion-detection systems,” *Comput. Networks*, vol. 31, no. 8, pp. 805–822, 1999, doi: 10.1016/S1389-1286(98)00017-6.

[52] G. Meng, Y. Liu, J. Zhang, A. Pokluda, and R. Boutaba, “Collaborative Security,” *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1–42, 2015, doi: 10.1145/2785733.

[53] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, “Kalis - A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 656–666, 2017, doi: 10.1109/ICDCS.2017.104.

[54] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, “A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks,” *IEEE Trans. Emerg. Top. Comput.*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.

[55] K. Dai, “Secure digital library technology research based on VPN,” *Proc. - 2011 Int. Symp. Intell. Inf. Process. Trust. Comput. IPTC 2011*, no. 3, pp. 165–168, 2011, doi: 10.1109/IPTC.2011.49.

[56] K. Wu, J. He, and T. Ding, “Secure wireless remote access platform in power utilities based on SSL VPN,” *Proc. - 2011 6th IEEE Jt. Int. Inf. Technol. Artif. Intell. Conf. ITAIC 2011*, vol. 1, pp. 93–97, 2011, doi: 10.1109/ITAIC.2011.6030159.

[57] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electron.*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.

[58] B. Borisaniya and D. Patel, "Evaluation of Modified Vector Space Representation Using ADFA-LD and and ADFA-WD Datasets," *J. Inf. Secur.*, vol. 6, no. July, pp. 250–264, 2015.

[59] M. Xie, J. Hu, X. Yu, and E. Chang, "Evaluating Host-Based Anomaly Detection Systems : Application of the Frequency-Based Algorithms to ADFA-LD," pp. 542–543, 2014.

[60] N. N. Tran, R. Sarker, and J. Hu, "An approach for host-based intrusion detection system design using convolutional neural network," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 235, pp. 116–126, 2018, doi: 10.1007/978-3-319-90775-8_10.

[61] M. Xie, J. Hu, and J. Slay, "Evaluating Host-based Anomaly Detection Systems : Application of the One-class SVM Algorithm to," pp. 978–982, 2014.

[62] B. Dong, H. W. Wang, A. S. Varde, D. Li, and B. K. Samanthula, "Cyber Intrusion Detection by Using Deep Neural Networks with Attack-sharing Loss," *arXiv Prepr. arXiv*, 2021.

[63] B. S. Khater, A. W. B. A. Wahab, M. Y. I. Bin Idris, M. A. Hussain, and A. A. Ibrahim, "A lightweight perceptron-based intrusion detection system for fog computing," *Appl. Sci.*, vol. 9, no. 1, pp. 1–21, 2019, doi: 10.3390/app9010178.

[64] R. Vijayanand and D. Devaraj, "A Novel Feature Selection Method Using Whale Optimization Algorithm and Genetic Operators for Intrusion Detection System in Wireless Mesh Network," *IEEE Access*, vol. 8, no. 3, pp. 56847–56854, 2020, doi: 10.1109/ACCESS.2020.2978035.

[65] A. C. B, B. Lee, S. Fallon, and P. Jacob, "Host Based Intrusion Detection System with Combined CNN/RNN Model," *Springer*, no. 11329, pp. 149–158, 2019, doi: 10.1007/978-3-030-13453-2.

[66] https://github.com/verazuo/a-labelled-version-of-the-ADFA-LD-dataset.