QATAR UNIVERSITY

COLLEGE OF ENGINEERING

A DEEP LEARNING BASED APPROACH TO DETECT COVERT CHANNELS ATTACKS AND ANOMALY IN NEW GENERATION INTERNET PROTOCOL IPV6

BY

FELWA RASHID ALSENAID

A Thesis Submitted to

the Faculty of the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Computing

June 2020

COMMITTEE PAGE

The members of the Committee approve the Thesis of
Felwa Rashid AlSenaid defended on 05/05/2020.

Dr. Somaya Ali S A Al-Maadeed
Thesis/Dissertation Supervisor

Dr. Mohsen Guizani
Committee Member

Dr. Ammar Belatreche
External Examiner

Dr. Hasan Mehrjedee
Committee Member

Approved:

Khalid Kamal Naji, Dean, College of Engineering

ABSTRACT

ALSENAID, FELWA RASHID Masters: June : 2020:, Masters of Science in Computing

Title: A Deep Learning Based Approach To Detect Covert Channels Attacks and Anomaly In New Generation Internet Protocol IPv6

Supervisor of Thesis: Somaya, Al-Maadeed.

The increased dependence of internet-based technologies in all facets of life challenges the government and policymakers with the need for effective shield mechanism against passive and active violations. Following up with the Qatar national vision 2030 activities and its goals for "Achieving Security, stability and maintaining public safety" objectives, the present paper aims to propose a model for safeguarding the information and monitor internet communications effectively. The current study utilizes a deep learning-based approach for detecting malicious communications in the network traffic. Considering the efficiency of deep learning in data analysis and classification, a convolutional neural network model was proposed. The suggested model is equipped for detecting attacks in IPv6. The performance of the proposed detection algorithm was validated using a number of datasets, including a newly created dataset. The performance of the model was evaluated for covert channel, DDoS attacks detection in IPv6 and for anomaly detection. The performance assessment produced an accuracy of 100%, 85% and 98% for covert channel detection, DDoS detection and anomaly detection respectively. The project put forward a novel approach for detecting suspicious communications in the network traffic.

DEDICATION

To my parents, For their support and

partnership for success in my life.

.

ACKNOWLEDGMENTS

I would like to express my special appreciation, thanks and gratitude to my supervisor Prof. Somaya Al-maadeed for encouraging and guiding throughout the research journey. Her enthusiasm and mentorship have been invaluable to engage me in this academic scholarship. I would like to extend my deepest gratitude to my parents, who supported me with love and understanding. Without their support I could never have reached this current level of success. I also acknowledge everyone who played a role in my academic accomplishments.

Finally, this work was made possible by NPRP grant # [NPRP11S-0113-180276] from the Qatar National Research Fund (a member of Qatar Foundation). The findings achieved herein are solely the responsibility of the author.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

The dramatic growth of the internet in the 1980s raised dire warning of internet address exhaustion. As a consequence, Internet Engineering Task Force (IETF) lead the development of robust, efficient and secure internet protocol, IPv6. This enhanced protocol not only improves the performance but also offers a structured and productive approach for packets handling. Although, IPv6 improvise and rationalize the internet protocol, it raises a number of several security challenges. The topic has attracted the attention of many researchers, striving to address the cyber security concerns. On the other hand, with the emergence of new technologies, hackers and cyber criminals are actively targeting the exploitation of possible vulnerabilities. In the early days of IPv6 implementation, Kelin, an independent security researcher, explored the security vulnerabilities and defects in IPv6. Using a dedicated tool, the researcher created covert channels which can bypass firewalls and intrusion detection systems. This tool has warned the security experts of the need for a convenient mitigation technology. Kelin added that, as the adoption of IPv6 expands, more deformities and security flaws will be disclosed [1]. With the rapid expansion and prevalence of IPv6 networks, the number of threats and defects are growing on a large scale.

The ever-increasing demand for security countermeasures opens up a new research arena among academics and network security enthusiasts. The current paper analyzes a number of serious security threats in IPv6 such as covert channels, distributed denial of service (DDoS) and anomaly detection.

1.1 Background and Motivation

Network security specialists are increasingly challenged with novel security threats and information loss. The intruders are leveraging the security drawbacks of IPv6 through attacks and cyber security violations. IPv6 is susceptible to different forms

of attacks such as covert channels, DoS, man in the middle attacks [2]. Covert channels, an unconventional security threat, have been evolving over four decades with the rise of the concept in the early 1970s [3]. The covert channel emphasizes secrecy and hidden communication between two IP addresses. Most commonly, the covert channels can be achieved by exploiting shared network resources intended for different communication purposes. Such exploited and alternate communication path considered as a violation of network security policies. Another term used to express the concept of these illegitimate communications is network steganography. It has been noticed that certain fields in TCP/IP protocol layers such as network layer, internet layer, transport layer and application layer are exploited to establish covert channels. Further to field exploitation, certain types of attacks manipulated the relationship between TCP/IP layers by crafting packets and creating gaps between headers. With the proliferation of internet applications and social media, covert channel attacks also emerged with new approaches and modes. Like for instance, stealing user cookies and using the Facebook wall as pipe are some of the latest techniques of covert channel attacks [4]. Although covert channel attacks have been discussed widely in IPv4, very few studies addressed the concept in IPv6. With the increase in the number of networks adopting IPv6, the need for an appropriate and efficient countermeasure to mitigate covert channels communications arises. There exists a potential for robust, accurate, and less false-alarming covert channel detection approach.

Artificial intelligence has a wide variety of useful applications. Due to the powerful capabilities of artificial intelligence approaches in classification problems, it can be considered as a valuable component in network security. Recently, a large number of studies exposed the efficacy of machine learning and deep learning applications in the detection of attacks. Therefore, it can be employed for the

identification of abnormalities in network traffic. The scarcity of deep learning approach for anomaly detection in IPv6, pointing to the need for more research and development in the field. By addressing the identified research gap, the present paper investigates a machine learning solution for intrusion detection in IPv6 based network.

1.2 Research Objectives

The current research proposes a deep learning-based approach for the detection of attacks in the new generation of the internet protocol IPv6. The paper primarily addresses the following objectives:

- Propose a new feasible framework utilizing a deep learning technique for IPv6 anomaly detection.
- Assess the performance of the proposed model for the detection of covert channels, DDoS attacks and anomaly in IPv6.
- Compare the efficiency of the suggested model against existing frameworks.

1.3 Solution Overview

The present study put forward a new framework for ensuring increased security in the internet protocol version 6 based on the concept of artificial intelligence and machine learning. The proposed framework implements the underlying notion of deep learning to analyze internet packets and detect abnormalities in the network system. The concept of machine learning in IPv6 has been previously assessed only to a minimal extent. This gap in the literature, especially for storage based covert channels, demands a new mechanism for analysis and classification. Such that the current research deeply explores the application of deep learning technique to the aspect of covert channel and DDoS attacks detection. The paper also examines the effectiveness and performance of the network traffic analysis.

CHAPTER 2: LITERATURE REVIEW

2.1 Internet Protocol Version 6 (IPv6)

The proliferation of internet based technologies and communication channels raises the need for effective security protocols and mechanisms. IPv6, a successor of IPv4, is also known as IPng (Internet Protocol next generation) facilitating a revolutionary upgrade to internet protocol. IPv6 was introduced with a 128-bit address field which essentially allows for the steady growth of the internet. Advantageously, the larger address field in IPv6 has overcome the much-feared challenges of "Internet addressing shortage" in the late 1980s. The adoption of IPv6 has gained more all-inclusive popularity due to its advantages to the network world. The percentage of global IPv6 deployment as of this writing (May 2020) is estimated to be around 30% [5]. Some of the most prominent benefits are reduction in processing time, sub-block processing, and Internet Protocol Security support [6]. More importantly, the concept of ICMPv6, which combines the neighbor discovery and router advertisement, also make the IPv6 a much robust protocol to use in the ever-growing connected world. However, the lack of cryptographic protection in IPv6 makes the protocol vulnerable against hidden channel and DDoS attacks.

To the best of knowledge, IPv6 is not particularly new and has been used for many years in the field, the deployment of IPv6 has been increasing at an enormous scale. Essentially, the header format of IPv6 is the facilitating feature in enabling this as a flexible entity. By increasing the length from 20 bytes in IPv4 to 40 bytes in IPv6 enables it to have abundant address lines and other optional features. The general structure of the IPv6 header format according to the RFC 2460 standard is shown in Figure 1 and will be discussed in the subsequent section.

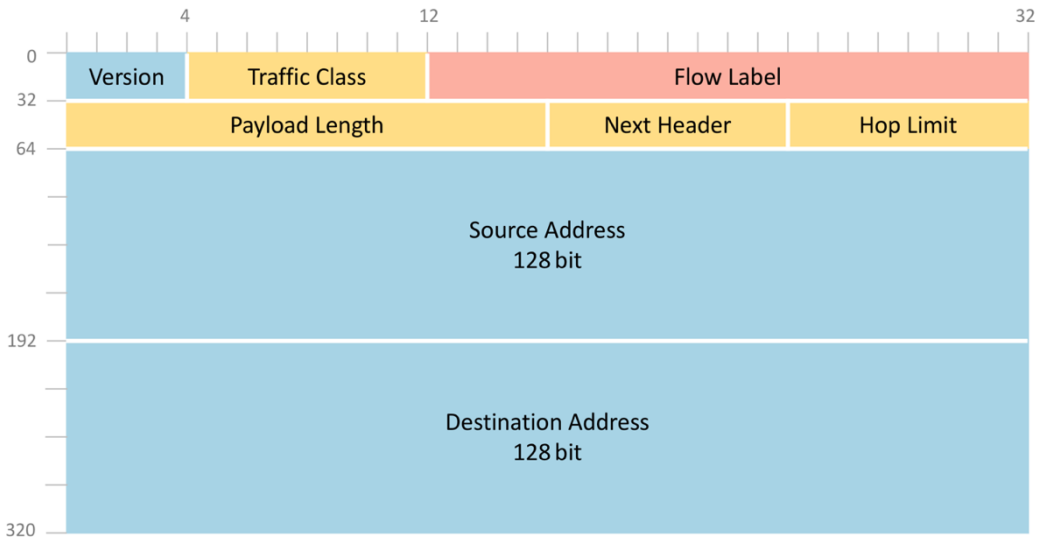

Figure 1: IPv6 Header Format

The Version field of IPv6 header holds a 4-bit data to recognize the internet protocol version similar to the version field of IPV4 header. The traffic Class is an 8-bit field where the first six-bit indicate the differentiated services (DS) and the last two bits refers to the explicit congestion notification (ECN). The Flow Label field is a 20-bit field, supplemented in IPv6 as opposed to IPv4 which facilitates tracking the flow of internet packets. The field following the IPv6 header is a 16-bit Payload Length field denotes the same purpose as that of IPv4. The payload field essentially represents the payload length of the data packets. The 8-bit Next header field symbolizes an upper layer protocol like TCP, UDP, or an optional extension header. Following the Next header field is a Hop limit field stating the number of intermediate routers the internet packets will traverse through. The Hop limit field is serving the same functionality as that of Time-to-live field in IPV4. The source and destination address field identify the sender and receiver of the IPV6 packets. The source and destination address field carry 128-bit address fields, thus enabling to address a broader range of devices and information units.

The internet protocol is not highly reliable, demanding additional mechanisms to report problems and communicate necessary information. The Internet Control Message Protocol (ICMPV6) is an essential part of modern Internet protocols to communicate information on network connectivity issues to the source of transmission specially used by network devices like routers. The role of ICMPV6 in internet protocol goes beyond error reporting to processing packet datagrams, diagnostics and other interlayer functions. It is worth to note that the use of ICMP in IPV6 has significant modifications as compared to the implementation of ICMP in IPV4. In IPv6, the ICMP will be called for the value of 58 in the header field "Next header".

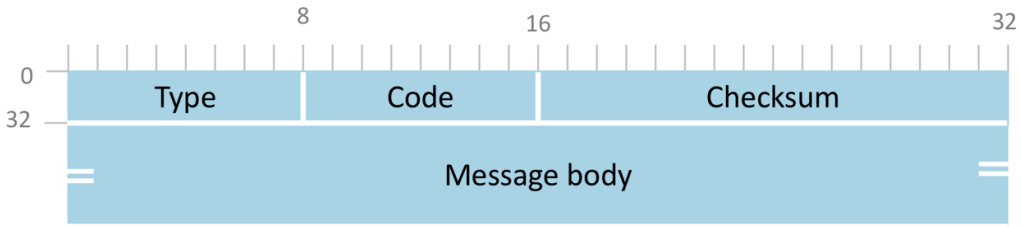

Figure 2. ICMPv6 Header Format

Figure 2 illustrates the ICMP header format for IPV6 as per RFC 4443. The first field, Type is an 8-bit field to specify the nature of messages such as error and informational messages. The Destination Unreachable, Time exceeded, parameter problems, and echo request are some of the examples of ICMPV6 messages. The subsequent field, Code, is again an 8-bit field which provide some additional details of the message type according to the Type field value. In order to validate the ICMPV6 message and IPV6 header for any discrepancies, a 16-bit checksum field is employed.

The last part of ICMP is of a varying length field, carries the message content based on the values of both Type and Code field. Consequently, the overall size of the ICMP packet should not exceed 1280 byes, which is the minimum IPV6 MTU.

2.2 Features of IPv6

Internet addressing shortage was one of the biggest concerns of information scientist in the later 1990s. This adverse situation directs to IEFT (Internet Engineering Task Force) to initiate the development of internet protocol version 6 with robust address and security features. Extended addressing features of IPv6 is considering as one of the significant expansion of the modern internet world. IPv6 offers an address range of 128 bits which is quite large as compared to the existing 32-bit address range of IPv4. Primarily, IPv6 can accommodate about 3.4×10^{38} addresses which are adequate for addressing the exponential growth of network connected devices [7, 8]. Another commendable feature of IPv6 is its simplified header format with a fixed size. IPv6 propose a 40 bytes fixed header size with eight fields whereas IPv4 has a varying header format and size. These particular features enable dynamic routing of IPv6 due to the predetermined fields and field values. In a nutshell, IPv6 eradicates the use of some of the non-essential fields such as checksum, fragment, protocol, options, and "Time to live" [9]. Nevertheless, IPv6 introduced "hop limit" and "Next header type" fields for powerful synchronization and packet organization.

A large number of existing studies in the broader literature have examined network security as an enhancement in IPv6 [10-12]. With the mandatory enforcement of IPsec in IPv6, as compared to the optionality in IPv4, provides data integrity, confidentiality, and authentication as a built-in feature of IPv6. The enhanced security features are employed through two security headers, Authentication Header (AH) and Encapsulating Security Payload (ESP). Both AH and ESP applied conjointly with the

security key exchange, IPSec offers access control to all connected system and services at the IP layers. Furthermore, IPSec facilitates superior security through connectionless integrity, data origin authentication, and packet counter mechanism [13].

Quality of networks and internet services plays a significant role in the reliability of the communications. IPv6 was introduced with dedicated features to overcome the quality of services (QoS) challenges in IPv4 [14]. It is imperative that IPv6 emphasizes on the QoS through flow label field in the packet header. The flow label values extend an effective mechanism for packet labelling, flow identification and its state lookup through effective management of peculiarities like bandwidth, reliability controlled jitter and latency [15, 16]. More recently, the IETF has proposed and standardized a number of QoS architectures such as Integrated Services (IntServ) and Differentiated Services (DiffServ) [15]. In essence, the IPv6 flow label field eases the provisions for applying QoS. Another significant feature of IPv6 in comparison to the previous protocol is its flexibility in supporting options and extensions. The immense size of the address field and other scalable features of IPv6 opens up plentiful innovative and collaborative possibilities. Through a robust Dynamic Host Configuration protocol version 6 (DHCPv6), IPV6 proposes a relatively lighter auto configuration mechanism for interfaces connected to the network. This enhanced node automatic configuration mechanism relieves the network from contacting the server from time to time, to configure their IP addresses as opposed to IPV4. As such, the server required to store the configuration information for each requested device [7]. The node to node addressing improves not only the connectivity but also provides increased transparency and efficiency.

Having said that, IPV6 introduced an efficient mechanism for managing routing tables. IPV4 faced adverse challenges in managing and storing routing tables for a more

substantial number of devices. Mobile nodes connected with IPV4 required to re-establish its connection with location changes due to the lack of support in handover and mobility in IPv4. However, IPv6 is equipped to overcome the mobility support through its sophisticated extension headers and support systems. Recent research highlights the scalability of IPv6 protocol with IPv6 extension header to provide a better authentication, handover and more agile routing mechanisms [7, 17].

2.3 Security Vulnerabilities of IPv6

The latest release of the internet protocol was addressing the growth of reliance on the internet and technology by expanding the addressing capabilities. The latest release came along with a sophisticated enhancement on the performance and security. Although the IPv6 considered several security issues, the design was mostly inherited from the previous generation of IPv4. Recent studies reported a number of numerous pressing vulnerabilities and threats associated with the IPv6. More specifically, the national vulnerability database identified 402 vulnerabilities related to IPv6 [18] Similarly, [19] presented a high level overview of the IPv6 associated security concerns and possible threats. Despite the enforcement of IPSec to strengthen the security in IPv6, there exist several shortcomings and security vulnerabilities. It is worth noting, IPv6 inherit some of the security challenges of IPv4 as similar to that of format inheritance. IPv6 address field heavily depends on the Media Access Control (MAC) raises a more significant security threat. The MAC addresses primarily facilitate address spoofing thus enable identification and track devices which intrinsically affecting the user's privacy. With the release of IPv6, attackers adapted hacking tools like THC and Scapy to explore IPv6 and to misuse its features. Due to the larger address size, the concept of applying port scanning is not anymore a reasonable option in IPv6. Due to the absence of identification token in OSI architecture and the IPv6

characteristics of assigning multiple addresses, there arises a higher challenge in updating the filtering rules of the firewalls and access control list [7, 8]. This poses a series of security threats at the access control level.

Although IPv6 extension header provides supplementary information for passing and processing internet packets, there is a higher potential for malicious use. Attackers can manipulate the extension header of variable size with padding a series of extension headers. The packet manipulation would lead to a Denial of service (DoS) and bypassing the firewall policies and intrusion detection systems. These manipulated extension headers circumvent the security policies and facilitate covert channel communication. In IPv6, packet fragmentation is performed at the source and destination nodes, not by intermediate routers, the presence of fragmentation at the nodes enables the attackers to perform the attack in the form of small fragments and evading the filtering and detection [20]. The security flaws in IPv6 poses a significant threat to communication and demands novel approaches for mitigation.

2.4 Distributed Denial of Service Attacks (DDoS)

Distributed DoS attacks are one of the most common forms of attacks against IPv6 protocol. The DDoS attacks are essentially disturbing legitimate communications among network connected devices. The intruder disrupts the normal traffic of a network or server thus making the resource unavailable. In essence, DDoS attacks are performed through exhaustion of a device in a network by overloading it with a large sequence of packets leading to the device unavailability. This kind of attacks are violating the fundamental principles of information security, commonly known as CIA Triad. When the DoS is executed from multiple distributed computers or botnets, it is referred as DDoS attack [21]. The unique characteristics of IPv6 opened up new ways of performing DDoS flooding attacks exploiting the new types of extension header,

ICMPv6 messages and the dependency on multicast addresses. For instance, the Hop by Hop option header contains optional information that should be reviewed by every node in the packet path. One possible scenario to trigger DoS attacks is by sending a large number of packets with the Hop by Hop option header attached with irregular or duplicate options. Upon identifying the irregularity at the hop-by-hop option header, the intermediary nodes will send ICMP error messages back to the sender. These multiple ICMP error messages and packet examinations at every node would significantly impact the performance of the network [22]. What's more, DDoS attack are often performed with dual purpose, where the first attack hits the system to install a ransomware or malware which eventually leads to significant disruption in the long run [23]. Although, IPv4 intrusion detection systems are feasible for IPv6, the characteristics and structure of IPV6 raise challenge to apply the same technique of IPv6 attack detection [24]. The new uncertainty mandates for novel DDoS attack detection techniques in IPv6.

2.5 Covert Channels Attacks

The concept of covert channel was first introduced by Butler Lampson to address channels not intended for information transfer [25]. The concept has gained much popularity among academics and information professionals which was mostly addressing the unconventional and secure data transfer. A wider accepted definition to covert channel is coined by Gligor and Virgil [26] which emphasizes the denial of policy and adoption of property. More recently, Lucena, et al. [27] defined covert channel as the communication path which facilitates the transmission of information through a nontraditional, illicit, and unconventional method that “violates a system security policy”. Piscitello [28] compares covert channel to a secret compartment in a brief case to carry sensitive documents or materials through a secured medium.

Interestingly, the concept of covert channel is different from any encrypted tunnels or channels due to the unobserved nature of data transmission.

Covert channels form an invisible channel to transfer information secretly by manipulating packets information and the timing of the packets. Based on this manipulation it classified into two forms: storage based covert channels (CSC) and covert timing channels (CTC). The concept of storage based covert channel primarily encapsulates the secret data into a shared storage medium like the protocol header, thus facilitating asynchronous encoding and decoding. However, the timing based covert channels are synchronous in nature, essentially achieved by manipulating the inter packet gaps to encode information [29].

2.6 Implications of Covert Channels

The optimal goal of attackers while using covert channels is to circumvent and bypass the security policies. Covert channels are mainly used to exfiltrate and infiltrate data out of and into a network in an unauthorized hidden manner. Perhaps, it may be used to leak sensitive information leading to serious consequences. Usually most of the attacks are launched through covert channels evading the firewalls and security policies. Delivery of malicious codes could be performed through such hidden channels. Though covert channels have some beneficial use like increased security of the critical connection, the darker side is not ignorable. Often covert channels are used for establishing connections which are prohibited or controlled by the regional communication policies. Primarily covert channels would be a threat to information privacy where the communication may remain undetected [30].

Furthermore, controlling the botnets robots could be easily achieved by illicit signaling, leading to a DoS attacks affecting network resources. Recently, the concept of covert channel has gained increased attention in image steganography where

information is hidden within images. Attackers are suspect to use graphics to obscure data in websites as a form of unrecognized communication [31]. The wider possibilities of covert channel are its ability in hiding the presence of data as opposed to encryption methods. The application of covert channels opened up a new era of research and study in the modern network technology.

2.7 Related Work

Recent literature has been investigating the vulnerabilities of the new generation protocol IPv6 and possible mitigation approaches. The scarcity of reliable IPv6 dataset challenges the research community for developing a convenient detection system. Multiple algorithms have been proposed utilizing machine learning based classifiers. Deep learning, a subset of machine learning, found numerous problem-solving applications in speech and image recognition. The practical applications of deep learning grow beyond to network traffic analysis and internet security in the recent years. There have been several researches addressing the practicality of using deep learning techniques in intrusion detection.

2.7.1 Use of Deep Learning in Networks Packets Analysis

With the rapid growth of internet and network technologies, the network traffic classification has gained more importance than ever before. Though there have been several approaches discussed in the literature, most techniques are focusing on classification based on predefined features. Deep learning enables to automate the process by facilitating the integration of feature extraction and classification into one system. Lotfollahi, et al. [32] proposed an approach to analyze network packet using a deep learning-based technique, called Deep Packets, for classifying the network traffic. The research argues that the Deep Packets outperform all pre-existing models on traffic dataset. Similarly, Brun, et al. [33] and McDermott, et al. [34] discussed the use of deep

learning technique for addressing network security attacks through packet analysis. A deep neural network model for intrusion detection for Software Defined Network (SDN) was developed for identifying and overcoming the possible security threat. The SDN based model was later tested using the basic six features of data records in NSL-KDD dataset [35]. The research in the field are emphasizing on capturing the data packets and extracting packet level matrices for assessing the presence of attacks. The underlying concept behind packet analysis is the extraction of packet features and its efficient classification.

2.7.2 IPv6 Attacks Detection

A network intrusion is defined as the forcible or unauthorized activity on a network. The network intrusion often leads to endangering both the network and the data. As such, network Intrusion detection systems play a vital role in securing networks, while providing defense and monitoring traffic for possible attacks. Intrusion detections systems are typically categorized into two types as signature based and anomaly based intrusion detection systems. The signature based detection approaches are based on simple pattern matching techniques which compare a captured event with a set of predefined patterns. On the other hand, anomaly based detection is a behavioral analysis approach, it extracts the behavior of normal and malicious network activities [36]. Roesch [37] proposed a lightweight rule based intrusion detection and prevention system named snort for small networks. Snort is principally a signature based approach, performs packet sniffing, traffic logging, and traffic analysis for scrutinizing pattern matching and consequently detecting attacks. The major drawback of this kind of signature based approach is its inability to inspect encrypted packet parts, and detecting zero day or new forms of attacks. Besides, Li, et al. [38] suggested a fuzzy rule based model for attack detection in IPv6. The model was evaluated by employing a set of data

obtained from IPv6 based China Education and Research Network (CERNET2). Experimental results of the aforementioned approach showed a high accuracy, and low false alarm rates. The model outperformed the detection capabilities of the previously discussed snort IDS. Nevertheless, this model lacks the capability to detect user to root (U2R) related kind attacks. More recently, a machine learning based approach for IPv6 has been proposed for detecting router advertisement based flooding attacks. This new approach leverages Principal Component Analysis and information gain ratio for feature selection while employing a Support vector machine (SVM) for anomaly detection. The SVM effectively utilizes the result of the feature selection process to train the prediction model for anomaly detection. The performance model had been evaluated using a dataset obtained from the National Advanced IPv6 Center of Excellence (NAv6). The experimental results of their proposed technique resulted in a testing accuracy of 98% and high precision rate [24] . A novel flow-based network intrusion detection system (NIDS) has been introduced by Elejla, et al. [39] for detecting the presence of IPv6 DDoS attacks. This new approach evaluated the extracted features and the flow representation by applying a number of classification techniques using WEKA platform for classifiers such as C4.5 decision tree, Support vector machine (SVM), Naive Bayes, k-nearest neighbors (KNN), Random forest trees, and Conjunctive rules. The commendable part of the research is the introduction of a new ICMPv6 DDoS dataset created through a number of simulations. Further, the performance assessment of the proposed intrusion detection system exhibited acceptable accuracies and low false positive rates. The flow based IDS has shown significant performance improvement as compared to the packet based IDS.

2.7.3 IPv6 Covert Channels Detection Techniques

Machine learning exhibited wider acceptance in packet analysis. Network analyst and researchers have been experimenting with various artificial intelligence techniques for machine learning in both IPv4 and IPv6. A notable research in the field of IPV6 storage covert channel proposes an intelligent heuristic algorithm for detection. The particular approach is based on a supervised Machine Learning naive Bayesian classifier along with a feature selection algorithm. The naive Bayes classifier is a probabilistic classifier focus on the relationship between the attributes and the class. Additionally, the C 4.5 decision tree algorithm was employed to derive the most prominent features to reduces the computation complexity at the processing phase. For the purpose of training the developed model, a primary dataset was created through a number of simulated covert channel attacks. The proposed approach analyses the header fields of every IPv6 data packets for examining the presence of any manipulations. A 10 fold cross validation was performed to assess the performance efficiency of the model and resulted in 94% accuracy [40]. Following the supervised approach, Salih, et al. [41] proposed a rule-based technique for detecting storage based covert channels using the advanced fuzzy logic concept. The concept was essentially analyzing ipv6 and icmpv6 header fields for detection. This new technique used a genetic algorithm to function as an optimization method for enhancing the fuzzy rules. Their work was trained and tested using the primary dataset as similar to that of their previous work. The experimental tests on the proposed framework resulted a detection rate of 95% pointing to its efficiency in terms of computational complexity.

Chourib [42] proposed a covert channel detection model based on three machine learning algorithms SVM, k-NN, and deep neural networks. The model adopted real-life network traffic along with generated benchmark dataset for training and testing the

proposed framework. The dataset was created by employing 11 distinct covert channel tools and each data record was represented using 20 features. The author evaluated the model applying three-fold cross-validation. The research highlighted the commendable performance of k-NN over both SVM and DNN. The K-NN model produced an accuracy and precision of 90% and 96% while the false positive stay very less as one percentage. The review of works of literature demonstrates the inclination of research to protocol or pattern specific covert channel detection approaches. Conversely, Ayub, et al. [43] proposed a protocol-independent approach for the detection of a storage-based covert channel in IPV4. This autonomous approach fundamentally used a supervised machine learning algorithm to detect covert channels in IP, TCP, and DNS protocol. The model was trained and tested using a primary dataset developed through the application proposed by Rowland [44] for the generation of storage covert channel at the TCP/IP stack. Also, the research employed DNS2TCP tool for bringing out DNS based covert channel datasets. The methodology of the research comprises a preprocessing phase where the packets have employed for feature extraction. Following the feature extraction, the obtained values are fed into kNN, Decision tree, logistic regression, SVM (Linear kernel) and SVM (Gaussian Kernel) machine learning classifiers. Essentially, the covert channel was encoded in fields such as the IP identification field, TCP sequence number field, and DNS query and response names fields. The performance assessment of this protocol-independent model illustrates that SVM with Gaussian kernel was the most efficient classifiers in IP and TCP protocols. Nonetheless, the decision tree outperformed the rest of the machine learning techniques in the detection of the covert channel at the application layer (DNS).

CHAPTER 3: METHODOLOGY

The present study utilizes the underlying concept of deep learning technique for the covert channel detection in IPV6 network. The proposed model principally employed the concept of convolution neural network (CNN), a subset of deep neural networks. CNN has been used for sophisticated data processing tasks due to its ability to classify and abstract features from both row and processed data effectively. Essentially deep learning models facilitate to learn and represent features of data by assessing the nature of data in contrast to human intervened classification. The present research is principally based on a supervised machine learning classification technique. The issue addressed in the research is essentially a binary classification, where a set of captured network packets are classified to two categories as normal and abnormal covert communication. The subsequent section will provide a brief overview of CNN and the proposed CNN architectures.

3.1 Convolutional Neural Network

The Convolution Neural network (CNN) were first coined by a computer science researcher Fukushima through a neocognition research [45]. CNN is a deep learning model which is capable to accept inputs and differentiate or classify various objects within the input for further processing. Due to the ability to perform feature engineering independently, the technique has been applied extensively in image classifications and data processing. LeCun's investigation on deep learning argues the advantages of CNN over other approaches for classification, especially due to its unique characteristics and suitability to handle certain type of data. CNN performs the best for data following structure such as data in form of multiple arrays, data with strong local correlation, and data with invariant features to translation and distortion. More importantly, the one dimensional CNN (1D-CNN) is suitable for sequential data or

natural language processing whereas 2D-CNN can be employed to classify traffic images and network traffic classification. Recently, network security research is utilizing this CNN based concept for traffic analysis and malware classification. Nevertheless, network traffic is often considered as sequential data with one dimensional byte flow with hierarchical structure. In comparison to the natural language processing (NLP) technique, the byte, packets, and session are similar to that of word, character, and sentence respectively [46]. For instance, recent studies investigating the application of CNN in NLP employed a 1D-CNN for performing text classification and sentiment analysis.

3.2 Proposed CNN Architecture

Research demonstrates the evolution of CNN and deep learning models for serving different purposes in network analysis. The present research adopted a model as illustrated in Figure 3 which constitutes three convolutional layers. The proposed model enables the classification and features extraction without human intervention. The first layer is the input layers which accept the data ready to be processed and fed into the subsequent convolution layer. The convolution layer performs the mathematical operations for extracting the features of the captured data and fed the data into a max pooling for size reduction and repeat the process for two remaining convolution max pooling layers. The first convolution layers performed the operation with 256 filters each with size 2 and resulted in feature maps. Whereas the second and third convolution layers produces 128 and 64 feature maps respectively. The three convolution layers in the model employ a sigmoid activation function for activating nodes. Each convolution layer is followed by a max pooling layer to produce an abstract representation of the parameters thus reducing the computational cost. A dropout layer with dropout rate of 50% is included in the architecture to avoid any overfitting and

enhancing robustness of the model. Lastly, a dense layer was designed to perform classification on extracted features maps from preceding layers. This layer utilizes ReLu and sigmoid activation function for performing the classification. The two activation functions and convolutional layers filter sizes are selected based on a series of experiments. The process of implementing the proposed CNN model consist of four phases. In the first phase, the hyperparameters were selected and trained the CNN model in the second phase. In each epoch, the performance of the training is validated. Lastly the performance of the resulted model is evaluated. The process will continue to phase one forming a circular pattern optimal model is obtained.

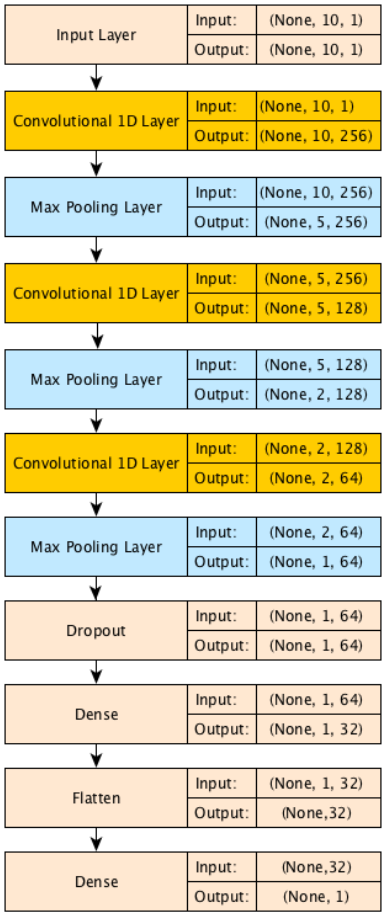

Figure 3. The proposed CNN architecture

3.3 Performance Evaluation Metrices

Evaluating the performance of proposed algorithm is an inevitable part of machine learning model development. There exist numerous evaluation metrics varying based on tasks such as classification, clustering, ranking, and regression. Nevertheless, the current research measures for binary classification using the notation such as accuracy, precision, recall, F1 score to evaluate and judge the performance of the proposed model.

3.3.1 Accuracy

Accuracy is the most common and less complex measures. The accuracy evaluation metric primarily assesses the effectiveness of a classification model in terms of ratio of acceptably classified samples to the total number of samples. In another word, accuracy can be termed as the degree of accurate prediction of any model.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

3.3.2 Precision

The evaluation measure precision pointing to the fraction of detected positive which are truly correct. In essence, precision compares results from both positive and negative trials and estimate the total posterior probability. It is the ratio of correct positive results to the number of classifier predicted positive results**.**

$$Precision = \frac{TP}{TP + FP}$$

3.3.3 Recall

The measure of recall indicates the proportion of actual positives predicted as positive. In contrast to the precision value, recall is not about identifying all positives, rather about capturing all positives as positives. Whereas, precision is about being precise and capture the correct value.

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

3.3.4 F1 score

F1 score is required when there is a need to balance between precision and recall value. It is fundamentally a harmonic mean between precision and recall holding a value range of [0,1]. F1 score helps to determine the preciseness and robustness of a classifier.

$$F1\ score = 2.\ \frac{Precision\ \times\ Recall}{recision + Recall}$$

3.4 Dataset

Research processes require efficient dataset to train and test the proposed models. The present research adopts four distinct datasets for assessing the performance of the developed model. The first dataset is a new dataset created for the purpose of testing the viability of the proposed model in the detection of covert channel attacks in IPv6. The second and third datasets are obtained from an open-source platform, which are utilized for evaluating the performance of the proposed model in packet analysis. Lastly, the fourth was based on a network flow based representation of ICMPv6 DDoS attacks. The subsequent sections will provide a brief overview of the utilized datasets and the conducted experiments.

3.4.1 IPV6 covert channel dataset

Considering the scarcity of IPv6 based covert channel dataset, a new dataset has been created through a number of covert channel attack simulations on a controlled network topology developed using oracle virtual GNS3 platform [47]. The simulated network topology basically consists of two Local Area Network (LAN)s each is compromised of a victim and an attacker. Covert channel attacks were triggered using Scapy and THC-IPv6 toolkits through manipulation of IPv6 and ICMPv6 fields [48,

49]. A sample scapy code for covert channel generation illustrates the manipulation of ICMPv6 code and type field is given below.

#scapy>>>send(IPv6(dst="fe80::3c79:6d52:d355:9381")/ICMPv6EchoRequest(type=129,code=99))

Further, the manipulated packets were captured using Wireshark to create a number of covert channel instances. Figure 4 demonstrate a packet representation of the previously generated covert channel captured using Wireshark. Correspondingly, the features of the captured packets are extracted by employing a C program. The extracted features are then converted into numerical formats in order to make it compatible for processing using the proposed model. The resulted dataset has been used for detecting and testing covert channel attacks in IPV6. Each record is a representation of IPv6 and ICMPv6 header fields, described by 9 attributes, as illustrated in Table 1. In addition, the instances will have a class label to identify the existence of covert communication. Table 2 illustrates a sample of the generated dataset which consist of both normal and abnormal records in binary representation.

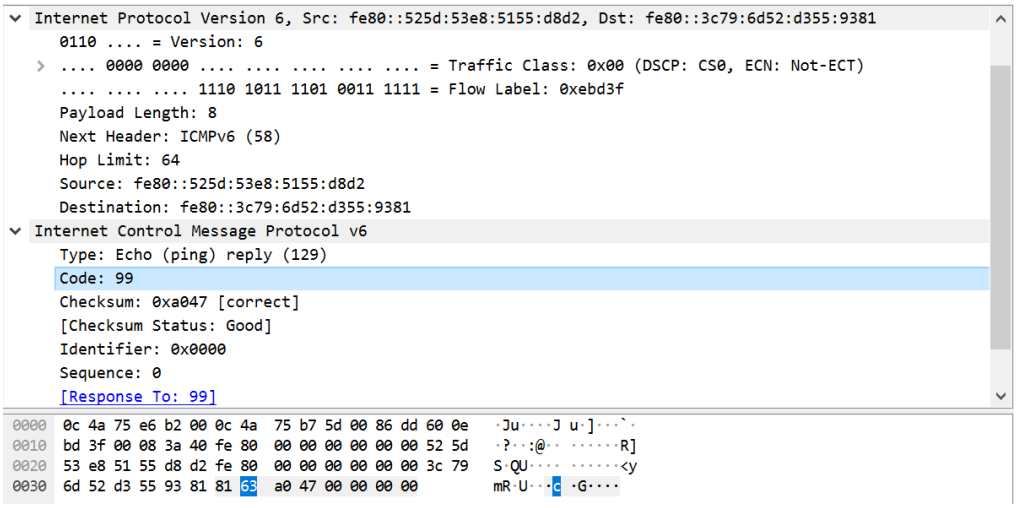

Figure 4. Encoding a random value in the ICMPv6 code field using scapy

Table 1. Covert channel dataset's features

Category	No.	Attribute Name
IPv6 header	1	Traffic_class
	2	Flow_label
	3	Payload_length
	4	Next_header
	5	Source_address
	6	Destination address
ICMPv6 header	7	ICMPv6_Type
	8	ICMPv6_Code
	9	ICMPv6_Payload

Table 2. Sample of the covert channel dataset

Traffic Class	Flow label	Payload length	Next header	Src. add	Dst. add.	ICMP Type	ICMP Code	ICMP Payload	Class
0	0	8	58	2	1	255	0	0	0
0	0	8	58	1	2	129	87	0	1
0	0	8	58	1	2	128	197	0	1
0	0	8	58	4	3	129	0	0	0
0	0	8	58	3	4	1	227	0	1
0	0	8	58	1	2	0	222	0	1
0	0	8	58	4	3	128	0	0	0
0	0	8	58	3	4	1	77	0	1
0	0	8	58	1	2	129	190	0	1

3.4.2 NSL-KDD Dataset

The NSL KDD set is an open-source dataset, from the Canadian Institute of cybersecurity, employed in the current research for detecting attacks in IPV6. This dataset principally used for testing the efficiency and performance of the proposed model in attacks detection. The aforementioned dataset consists of 41 features representing the traffic with a label to portray the malicious communication. It has been observed that 11 features, comprising some of the primary features and time-relevant features of those instances, are standard for both IPv6 and IPv4. Having said that, the

proposed model considers 11 features as demonstrated in Table 3 for testing the presence of attacks [50].

Table 3. NSL-KDD dataset features

Category	No.	Attribute Name
Basic feature	1	Protocol type
	2	Service
	3	Flag
	4	Src bytes
	5	Land
Content related feature	6	Logged in
Time related features	7	Count
	8	Srv count
	9	Same srv rate
	10	Diff srv rate
	11	Srv diff host rate

3.4.3 DARPA 1999 Dataset

The present study performs a comparative analysis with existing covert channel detection models like Enhanced Naïve Bayes classifier (NBC) and New intelligent Heuristic algorithm (NIHA) [40, 51]. The aforementioned models were practicing the attacks detection by means of the benchmark DARPA dataset. Although, this dataset is limited with IPV6 attack records, both present and previous research utilized this dataset to evaluate the performance of the classifiers. The DARPA 1999 dataset is a simulation based dataset, consist of various normal and malicious network traffic records represented in an IPv4 packet based format. The data records constitute of 41 features representing the basic, time, contents and host based network traffic attributes. The DARPA dataset is essentially a predecessor to the NSL KDD dataset. Primarily, the Covert channel detection can be applied through inspecting the session data of

network communication [52]. As such, the DARPA dataset consisting of a number of session-based records, which further facilitate in extracting the characteristics of benign and malicious communications.

3.4.4 Flow based DDoS attacks dataset

DDoS attacks found to be the most common form of attacks against ipv6 networks [2]. Primarily, the DDoS attacks dependence on ICMP demands the need for an explicit dataset to test the performance in IPv6. The present research adopted a flow based dataset of ICMPv6 based DDoS attacks developed by a group of researchers from the university of Saint Malaysia. The dataset consists of a combination of normal and abnormal traffic records collected from a real IPv6 network and a virtual environment respectively. Further, the dataset includes around 92,000 records, each consist of 11 features as illustrated in Table 4 and a class label [53].

Table 4: Flow based DDoS dataset features

No.	Attribute Name	Description
1	ICMPv6 Type	Type of the ICMPv6 message
2	Packets Number	Number of packets send within the flow
3	Transferred Bytes	Number of bytes sent from the source to the destination node
4	Duration	Length of the flow
5	Ratio	Ratio of bytes transferred in the flow
6	Length	Standard deviation of the packets length
7	Flow label	Standard deviation of the Flow labels of the flow packets
8	Hop limit	Standard deviation of the Hop limits of the flow packets
9	Traffic Class	Standard deviation Traffic classes of the flow packets
10	Next Header	Standard deviation of the next headers of the flow packets
11	Payload length	Standard deviation of the packets payload lengths

3.5 Experimental Setup

The proposed model was trained and tested using a Mac workstation (Mac OS 10.12.6), with a 2.6 GHz Intel Core i7 processor and 16 GB RAM. The deep learning model was developed using the python programming language. The broader choice of libraries in Python encouraged the use of Python for machine learning and artificial intelligence in recent times. Scikit-learn, Pandas, TensorFlow, and Keras are libraries which were used in conjunction with python 3.6 for implementing the proposed CNN architecture.

CHAPTER 4: RESULTS AND DISCUSSION

4.1 Cross Validation

The Cross-validation is a commonly used technique for evaluating the performance of machine learning models. In cross-validation, a portion of the sample is allocated for training while the remaining will be used for testing the model. K-fold cross-validation is a popular model which ensures the availability of data samples in both training and testing through various iterations. The underlying concept of K-fold cross-validation is that the data sample will be divided into K equal parts, where a specific number of folds are allocated for training and testing. The choice to administer a new set of test data on every iteration makes the technique suitable for estimating the behavior of machine learning models. As such, the current study practices a 10 fold cross-validation model for training and testing the proposed covert channel attack detection algorithm. To be more specific to the present scenario, one portion or 10% of the sample is employed for testing and the remaining 90% for training the model.

4.2 Detection Results

The performance of the desired model was evaluated in terms of accuracy, precision, recall, and F1 score using ten-fold cross-validation. The detection testing was

carried out through two experiments and are described in the subsequent sections.

4.2.1 IPv6 covert channel detection

The covert channel detection experiments were performed on the primary dataset. The experimental results are illustrated in

Figure 5 and Figure 6, which represents the accuracy versus number of epochs and loss versus number of epochs, respectively. Figure 6 exhibits a reduction in loss with the increase of epochs, pointing to a significant decline in the false detection or classification error. Similarly,

Figure 5 demonstrates the improvement in accuracy with an increment in epoch for both testing and training phases. The experimental evaluation uncoiled a value of 100% for accuracy. Correspondingly, both precision and recall hold a value of 100% indicates the favorable performance of the developed model. It is also worth noting that F1 score for the experiments signified an overall improved functioning of the model through a value of one as presented in Table 5. The results of the covert channel detection experiment are revealed in Figure 7. The illustrations and evaluation metrics are pointing out the efficiency and feasibility of the proposed scheme in covert channel attack detection.

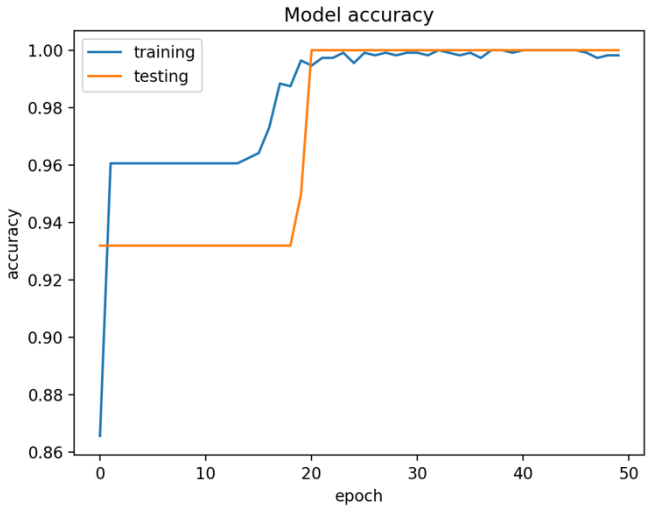

Figure 5. IPv6 covert channel detection accuracy

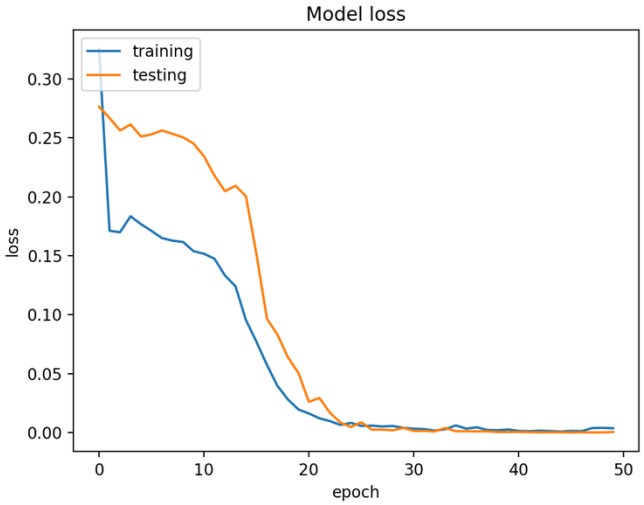

Figure 6. IPv6 covert channel detection loss

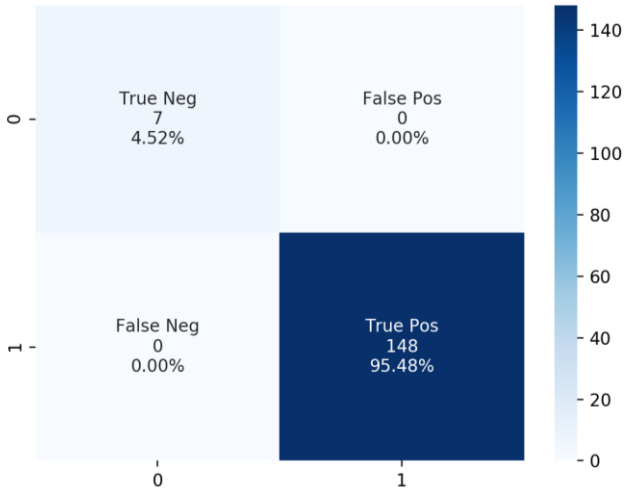

Figure 7. Covert channel detection results

4.2.2 IPv6 network anomaly detection

Using the NSL KDD open-source dataset, a network security attack detection was launched using the proposed model. The experimental results for the training phase as depicted in Figure 8 and Figure 9 reveal the variation of both accuracy and loss with the rise of epoch for IPv6 anomaly detection. The curve in Figure 9 demonstrate the commendable drop in loss with the increment of the epoch. However, Figure 8 instantiates the strengthening of accuracy with the increment of the epoch. The evaluation metrics have proven a higher degree of efficacy in network anomaly detection with a value of 98% for accuracy, precision, and recall, as provided in Table 5. Accordingly, the model shows a commendable performance potency with 98% for F1 score. The summary of network anomaly detection is depicted in Figure 10. The model has proven to be very beneficial in terms of both anomaly detection and covert channel detection in IPv6. The evaluation matrix has shown a remarkable performance efficacy disclosing the practical use of the model in a real-time network setting.

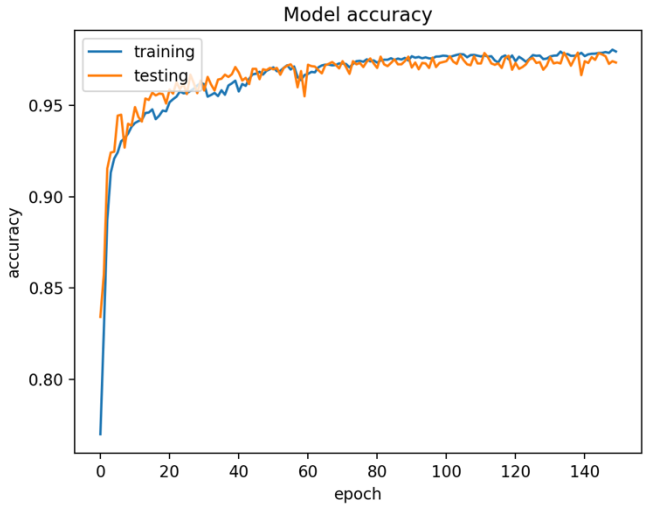

Figure 8. IPv6 anomaly detection experiemnt accuracy

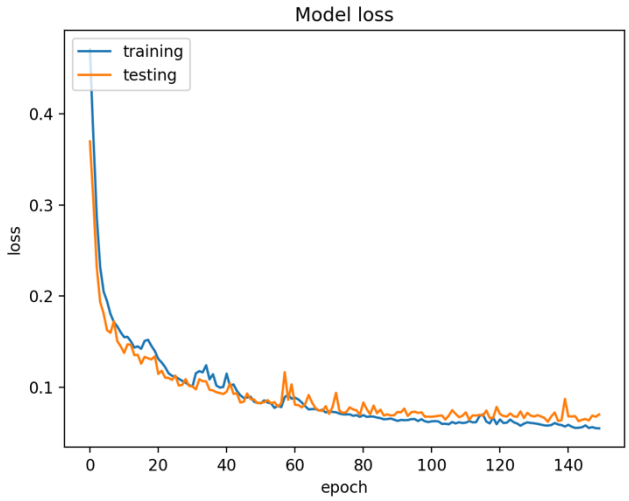

Figure 9. IPv6 anomaly detection experiemnt loss

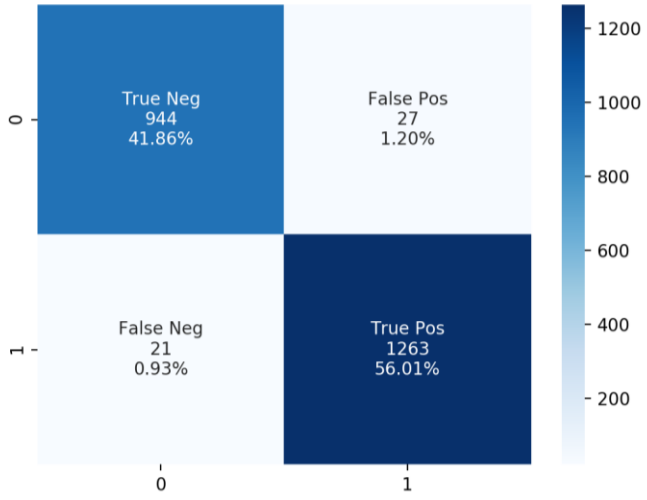

Figure 10. Anomaly detection results

Table 5. Experimental results of anomaly detection

Experiment	Accuracy	Precision	Recall	Loss	F1 Score
IPv6 covert channel detection	**1**	**1**	**1**	**0**	**1**
Anomaly detection in IPv6 network	0.98	0.98	0.98	0.05	0.98

4.2.3 Comparative analysis

The third phase of experimental evaluation addresses a comparative study of classifiers performance. This comparison examines the existing covert channel detection models like Naïve Bayes classifier, Enhanced NBC, and NIHA. The graphical representation of both accuracy and loss for the detection performance using DARPA dataset is provided in Figure 11 and

Figure 12 respectively. The model illustrates a significant increase in performance with the increase in epoch for both training and testing phases. Likewise, the illustration of loss indicates a considerable decrease in value with the increase in epoch. The rate of accuracy and loss are pointing to the outstanding efficiency of the proposed model. Figure 13 indicate the low false alarm rate of the classifier. The comparative study results of the proposed solution as depicted in Figure 14 demonstrate a superior performance in precision and accuracy with a value of 99%. Nonetheless, both enhanced NBC [41] and NIHA [40] indicates an accuracy of 96% and precision of 98%, which is relatively lower than the suggested model. Similarly, the Naïve Bayes classifiers results shows a noteworthy difference in performance with accuracy and precision as 80% and 90% correspondingly. These results indicate the significant efficiency of the current model in network packet analysis.

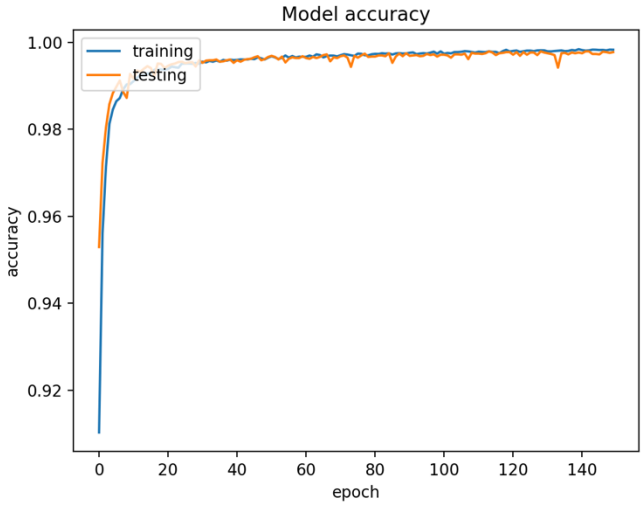

Figure 11. Accuracy of the proposed model using DARPA dataset

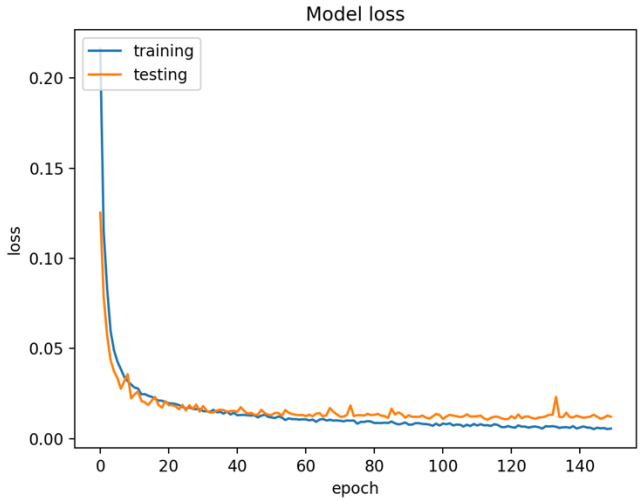

Figure 12. Loss of the proposed model using DARPA dataset

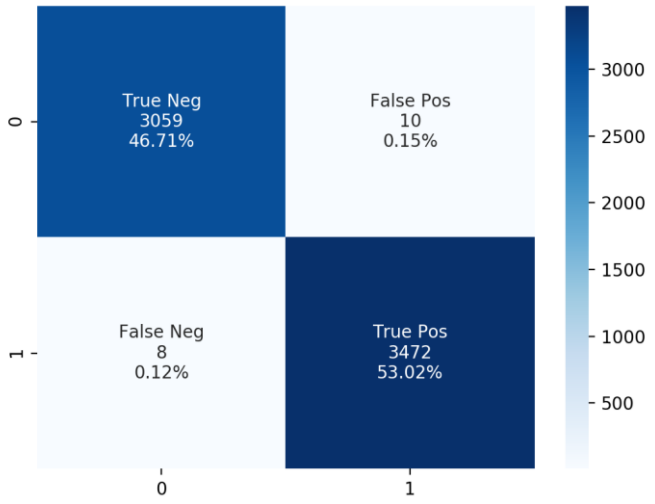

Figure 13. Results of attacks detection using DARPA dataset

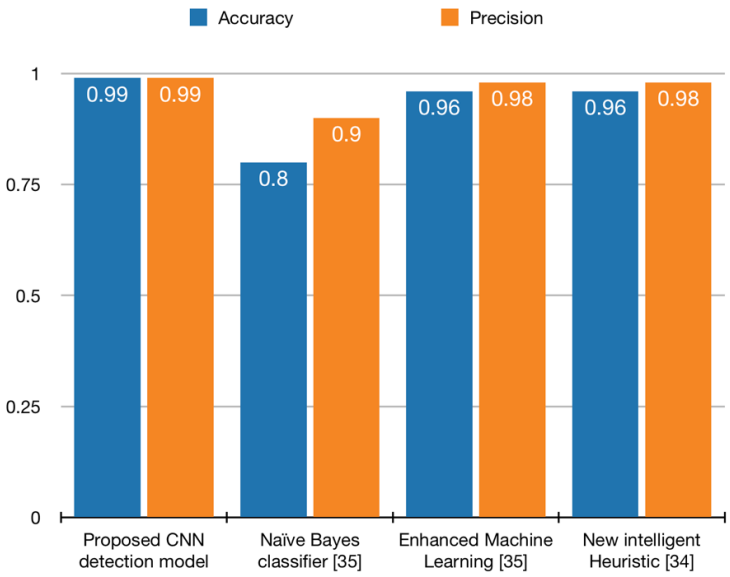

Figure 14. Comparative analysis of the accuracy and precision

4.2.4 IPv6 based DDoS Attacks Detection

DDoS is one of the most challenging network security risks associated with IPv6. The proposed model was assessed using the ICMPv6 based DDoS attacks dataset, which essentially evaluates the detection efficacy for DDoS attacks. In order to enhance the performance for DDoS detection, the model has been customized with minor modification at the layers level. The testing results indicate an accuracy of 85% with precision and recall as 99% and 68% respectively. Further the F1 score results in 81% pointing to the commendable performance of the model in the detection. Figure 17 summarizes the testing results obtained for the DDoS attacks detection. A comparison of proposed model's with a model drawn from literature, both utilizing the same dataset, pointing to the acceptable performance of the current model. Although both the models are addressing the same dataset, the current project has got access to the dataset with 8K missing records. However, the performance did not deteriorate where the previous model produced about 85.66% while the present model met 85% accuracy [39].

Figure 15 illustrates the model accuracy which further show the increase of accuracy with the increase in epoch. Similarly, the model loss has presented through Figure 16, pointing to the significant decrease in values with the increase in epoch. The model loss plot highlights the performance efficacy of the current model.

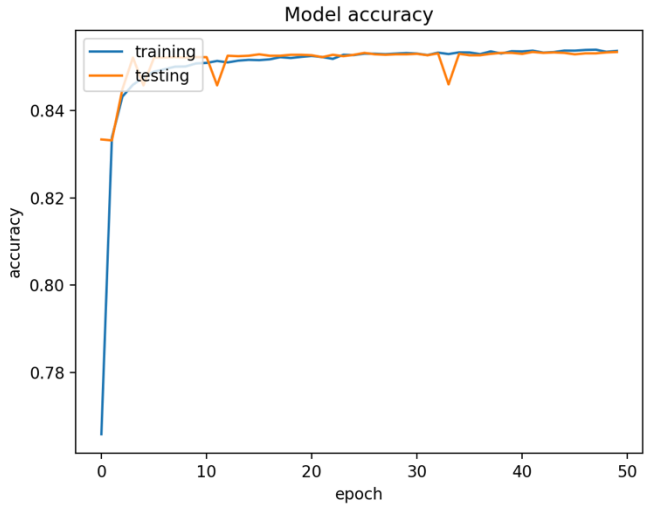

Figure 15. Accuracy of the proposed model in DDoS detection

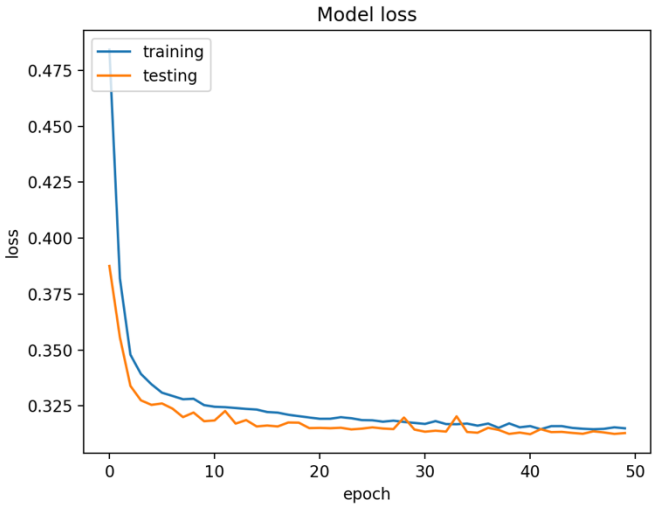

Figure 16. Loss of the proposed model in DDoS detection

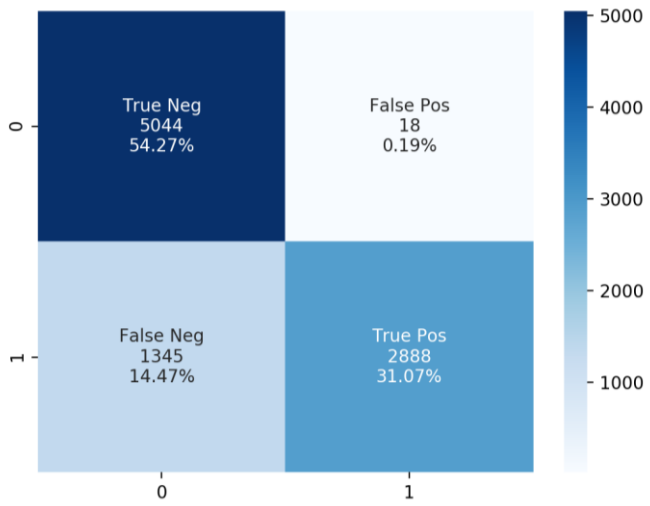

Figure 17. Results of DDoS attacks detection

CHAPTER 5: CONCLUSION

With the increasing dependency on internet-based technologies and the emergence of novel security threats demands rigorous research in network anomaly detection techniques. The covert channel, a method for embedding and hiding information, has been exploited in recent years for launching various form of attacks. Principally, the covert channel could be encoded using unused or reserved bits in the packet headers calls for the complexity in its detection's schemes. Most importantly, such attack challenges detection by the traditional mitigation principles and rules like firewalls. The current circumstances raise the need for advanced anomaly detection technique. The present research aimed to study and propose a new, feasible framework for intrusion detection in IPV6 using a deep learning technique. The proposed model was leveraging the underlying concept of convolutional neural network in packet analysis and classification. The aforementioned model was developed in python programming language and performed a series of experiments using mainly three datasets. The assessment results of the proposed model proved to have an accuracy of 100% for IPv6 covert channel attack detection, 98% for anomaly detection, and 85% for DDoS attacks. That being said, the reduced computational cost, minimal error rate, and higher accuracy make this model applicable to implement in the real-time network environment.

5.1 Future Research Directions

Deep learning-based approach, explicitly using CNN and RNN based techniques are growing importance with the successful adoption and feasible application in complex problem-solving. The present research faced challenges with obtaining an open-source dataset for IPV6, specifically for covert channel attacks. There exists a demand for contributing to the development of an open-source dataset, which would further facilitate the research community for engaging in IPV6 security research. Besides, CNN has proven to be a convenient approach for image processing and pattern recognition. Leveraging the effectiveness of CNN in image processing, the current paper recommends the possibility of implementing a graphical representation of network data packets. Such graphical representation can further extend to analyze with CNN for covert channel or network anomaly detection in IPv6.

REFERENCES

[1] R. Lemos. "Covert channel tool hides data in IPv6." https://www.securityfocus.com/news/11406 (accessed 4 Jan, 2020).

[2] J. B. Ard, "Internet Protocol version Six (IPv6) at UC Davis: Traffic Analysis with a Security Perspective," University of California, 2012.

[3] J. S. Thyer, "Covert Data Storage Channel Using IP Packet Headers," SANS Institute, 2008. [Online]. Available: https://www.sans.org/reading-room/whitepapers/covert/covert-data-storage-channel-ip-packet-headers-2093

[4] J. Selvi, "Covert Channels Over Social Networks," SANS Institute, 2012. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/covert-channels-social-networks-33960

[5] "Google IPv6 Statistics." https://www.google.com/intl/en/ipv6/statistics.html (accessed 11 May, 2020).

[6] P. Membrey, D. Hows, and E. Plugge, "IPv6: Implications and Concepts," in *Practical Load Balancing: Ride the Performance Tiger*, P. Membrey, D. Hows, and E. Plugge Eds. Berkeley, CA: Apress, 2012, pp. 225-234.

[7] C. Caicedo, J. Joshi, and S. Tuladhar, "IPv6 Security Challenges," *Computer*, vol. 42, no. 2, pp. 36-42, 2009, doi: 10.1109/MC.2009.54.

[8] H. A. Dawood, "IPv6 Security Vulnerabilities," *International Journal of Information Security Science* vol. 1, no. 4, pp. 100-105, 2012.

[9] E. Durdağı and A. Buldu, "IPV4/IPV6 security and threat comparisons," *Procedia - Social and Behavioral Sciences*, vol. 2, no. 2, pp. 5285-5291, 2010, doi: 10.1016/j.sbspro.2010.03.862.

[10] C. A. Shoniregun, "Internet Protocol Versions 4 (IPV4) and 6 (IPV6)," in *Synchronizing Internet Protocol Security (SIPSec)*. Boston, MA: Springer US,

2007, pp. 75-106.

[11] S. Szigeti and P. Risztics, "Will IPv6 bring better security?," in *Proceedings. 30th Euromicro Conference, 2004.*, Sep 3, 2004, pp. 532-537, doi: 10.1109/EURMIC.2004.1333418.

[12] P. Nikander, A. Gurtov, and T. R. Henderson, "Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks," *IEEE Communications Surveys & Tutorials,* vol. 12, no. 2, pp. 186-204, 2010, doi: 10.1109/SURV.2010.021110.00070.

[13] D. Žagar, K. Grgić, and S. Rimac-Drlje, "Security aspects in IPv6 networks – implementation and testing," *Computers & Electrical Engineering,* vol. 33, no. 5, pp. 425-437, 2007/09/01/ 2007, doi: 10.1016/j.compeleceng.2007.05.008.

[14] O. J. S. Parra, A. P. Rios, and G. L. Rubio, "IPV6 and IPV4 QoS mechanisms," presented at the Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services, Ho Chi Minh City, Vietnam, 2011. [Online]. Available: https://doi.org/10.1145/2095536.2095631.

[15] S. K. Sharma and S. Sharma, "IPv4 Vs IPv6 QoS: A challenge in MANET," *International Journal of Science and Applied Information Technology,* vol. 3, no. 4, pp. 7-11, 2014.

[16] *IPv6 Flow Label Specification, Request for Comments: 6437,* S. Amante, B. Carpenter, S. Jiang, and J. Rajahalme, 2011.

[17] A. Shiranzaei and R. Z. Khan, "A Comparative Study on IPv4 and IPv6," *International Journal of Advanced Information Science and Technology,* vol. 4, no. 1, 2015, doi: 10.15693/ijaist/2015.v4i1.9-16.

[18] NIST. National Vulnerability Database [Online] Available: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=ipv6&search_type=all

[19] A. Turiel, "IPv6: New technology, new threats," *Network Security*, vol. 2011, 2011, doi: 10.1016/S1353-4858(11)70085-X.

[20] C. Caicedo, A.Rawal, S. Gopal, R. Kamat, and J. Bejar, *Study of IPv6 Security Vulnerabilities*. 2014.

[21] S. Yu, "An Overview of DDoS Attacks," *Distributed Denial of Service Attack and Defense*New York, NY: Springer, 2014.

[22] J. Kim, H. Cho, G. Mun, J. Seo, B. Noh, and Y. Kim, "Experiments and Countermeasures of Security Vulnerabilities on Next Generation Network," presented at the Future Generation Communication and Networking (FGCN 2007), 2007, 559-564.

[23] A. Chadd, "DDoS attacks: past, present and future," *Network Security*, vol. 2018, no. 7, pp. 13-15, 2018, doi: 10.1016/S1353-4858(18)30069-2.

[24] M. Anbar, R. Abdullah, B. N. Al-Tamimi, and A. Hussain, "A Machine Learning Approach to Detect Router Advertisement Flooding Attacks in Next-Generation IPv6 Networks," *Cognitive Computation*, vol. 10, no. 2, pp. 201-214, 2018/04/01 2018, doi: 10.1007/s12559-017-9519-8.

[25] B. W. Lampson, "A note on the confinement problem," *Communications of the ACM*, vol. 16, no. 10, pp. 613-615, 1973, doi: 10.1145/362375.362389.

[26] Gligor and Virgil, "A Guide to Understanding Covert Channel Analysis of Trusted Systems," 1993.

[27] N. B. Lucena, G. Lewandowski, and S. J. Chapin, "Covert Channels in IPv6," Berlin, Heidelberg, 2006: Springer Berlin Heidelberg, in Privacy Enhancing

Technologies, pp. 147-166.

[28] D. Piscitello. "What Is an Internet Covert Channel?" https://www.icann.org/news/blog/what-is-an-internet-covert-channel (accessed 6 Sep, 2019).

[29] Y. Qian, T. Sun, J. Li, C. Fan, and H. Song, "Design and analysis of the covert channel implemented by behaviors of network users," *Security and Communication Networks,* vol. 9, no. 14, 2016, doi: 10.1002/sec.1503.

[30] C. Cilli, "Understanding Covert Channels of Communication," ed, 2017.

[31] K. Reiland, W. Oblitey, S. Ezekiel, and J. Wolfe, "Steganography and Covert Channels," presented at the PACISE conference, Bloomsburg, 2005.

[32] M. Lotfollahi, M. J. Siavoshani, R. S. H. Zade, and M. Saberian, "Deep packet: a novel approach for encrypted traffic classification using deep learning," *Soft Computing,* vol. 24, no. 3, pp. 1999-2012, 1 Jan, 2020, doi: 10.1007/s00500-019-04030-2.

[33] O. Brun, Y. Yin, and E. Gelenbe, "Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-connected Home Environments," *Procedia Computer Science,* vol. 134, pp. 458-463, 1 Jan, 2018, doi: https://doi.org/10.1016/j.procs.2018.07.183.

[34] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *2018 International Joint Conference on Neural Networks (IJCNN),* pp. 1-8, 2018.

[35] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM),* pp. 258-263, 2016.

[36] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16-24, 1 Jan, 2013, doi: https://doi.org/10.1016/j.jnca.2012.09.004.

[37] M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," presented at the Proceedings of the 13th USENIX conference on System administration, Seattle, Washington, 1999.

[38] Y. Li, Z. Li, and L. Wang, "Fuzzy Anomaly Detection System for IPv6 (FADS6): An Immune-Inspired Algorithm with Hash Function," Berlin, Heidelberg, 2006: Springer Berlin Heidelberg, in Intelligent Computing, pp. 553-562.

[39] O. E. Elejla, M. Anbar, B. Belaton, and B. O. Alijla, "Flow-Based IDS for ICMPv6-Based DDoS Attacks Detection," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7757-7775, 1 Dec, 2018, doi: 10.1007/s13369-018-3149-7.

[40] A. Salih, X. Ma, and E. Peytchev, "New Intelligent Heuristic Algorithm to Mitigate Security Vulnerabilities in IPv6," *International Journal for Information Security (IJIS)*, vol. 4, 2015.

[41] A. Salih, X. Ma, and E. Peytchev, "Detection and classification of covert channels in IPv6 using enhanced machine learning," presented at the Proceedings of the International Conference on Computer Technology and Information Systems (ICCTIS) Dubai, UAE, 2017.

[42] M. Chourib, "Detecting Selected Network Covert Channels Using Machine Learning," presented at the International Conference on High Performance Computing & Simulation (HPCS 2019), Dublin, Ireland, 2019.

[43] M. A. Ayub, S. Smith, and A. Siraj, "A Protocol Independent Approach in Network Covert Channel Detection," in *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, New York, USA, 2019, doi: 10.1109/CSE/EUC.2019.00040.

[44] C. H. Rowland, "Covert Channels in the TCP/IP Protocol Suite," *First Monday*, vol. 2, no. 5, 1997.

[45] K. Fukushima, "Neocognitron: A hierarchical neural network capable of visual pattern recognition," *Neural Networks*, vol. 1, no. 2, pp. 119-130, 1 Jan, 1988, doi: https://doi.org/10.1016/0893-6080(88)90014-7.

[46] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436-444, 1 May, 2015, doi: 10.1038/nature14539.

[47] G. J, M. B, G. C, and E. A. "Gns3 graphical network simulator." https://www.gns3.com/ (accessed 19 Dec, 2019).

[48] H. M. "THC IPv6 attack tool kit." https://www.aldeid.com/wiki/THC-IPv6-Attack-Toolkit (accessed 19 Dec, 2019).

[49] P. Biondi. "Scapy." https://scapy.net/ (accessed 19 Dec, 2019).

[50] B. Vrat, N. Aggarwal, and S. Venkatesan, "Anomaly Detection in IPv4 and IPv6 networks using machine learning," in *2015 Annual IEEE India Conference (INDICON)*, 17-20 Dec, 2015, pp. 1-6, doi: 10.1109/INDICON.2015.7443752.

[51] A. Salih, X. Ma, and E. Peytchev, "Implementation of Hybrid Artificial Intelligence Technique to Detect Covert Channels Attack in New Generation Internet Protocol IPv6," presented at the Leadership, Innovation and Entrepreneurship as Driving Forces of the Global Economy Springer

Proceedings in Business and Economics, Dubai, UAE, 2016.

[52] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems," *Applied Sciences,* vol. 9, no. 20, 2019, doi: 10.3390/app9204396.

[53] O. Elejla, M. Anbar, B. Belaton, and S. Hamouda, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," *Neural Computing and Applications,* vol. 31, no. 8, pp. 3629 - 3646, 2018, doi: 10.1007/s00521-017-3319-7.