AN INTRUSION DETECTION SYSTEM FOR DDOS FLOODING ATTACKS ON IPV6 NETWORKS USING DEEP LEARNING TECHNIQUES

AHMED MARWAN IDREES ALEESA

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

STATUS CONFIRMATION FOR THESIS
DOCTOR OF PHILOSOPHY

AN INTRUSION DETECTION SYSTEM FOR DDOS FLOODING ATTACKS ON IPV6 NETWORKS USING DEEP LEARNING TECHNIQUES

ACADEMIC SESSION: 2020/2021

I, **AHMED ALEESA**, agree to allow this Thesis to be kept at the Library under the following terms:

1. This Thesis is the property of the Universiti Tun Hussein Onn Malaysia.
2. The library has the right to make copies for educational purposes only.
3. The library is allowed to make copies of this Thesis for educational exchange between higher educational institutions.
4. The library is allowed to make available full text access of the digital copy via the internet by Universiti Tun Hussein Onn Malaysia in downloadable format provided that the Thesis is not subject to an embargo. Should an embargo be in place, the digital copy will only be made available as set out above once the embargo has expired.
5. ** Please Mark (√)

☐ CONFIDENTIAL (Contains information of high security or of great importance to Malaysia as STIPULATED under the OFFICIAL SECRET ACT 1972) *Title and Abstract only*

☐ RESTRICTED (Contains restricted information as determined by the Organization/institution where research was conducted) *Title, Abstract and Introduction only*

☐ EMBARGO _________ until _________
(date) (date)

√ FREE ACCESS

Approved by,

(WRITER'S SIGNATURE)
AHMED MARWAN ALEESA

(SUPERVISOR'S SIGNATURE)
TS. DR. NAN BIN MAD SAHAR

Permanent Address:
AL-MUROR NEIGHBORHOOD,
MOSUL, NINEVEH, 41002, IRAQ

Date : 19/02/2021

Date: 19/02/2021

NOTE:

** If this Thesis is classified as CONFIDENTIAL or RESTRICTED, please attach the letter from the relevant authority/organization stating reasons and duration for such classifications.

This thesis has been examined on date 26 November 2020
and is sufficient in fulfilling the scope and quality for the purpose of awarding the Degree of Doctor of Philosophy in Electrical Engineering.

Chairperson:

ASSOC. PROF. DR. SITI ZARINA BINTI MOHD MUJI
Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

Assistant Chairperson:

MR. HAZWAJ BIN MHD POAD
Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

Examiners:

PROF. DR. IMAD FAKHRI TAHA Al SHAIKHLI
Department of Computer Science
Head of Research at the Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

PROF. DR. JIWA BIN ABDULLAH
Department of Electronic Engineering
Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

AN INTRUSION DETECTION SYSTEM FOR DDOS FLOODING ATTACKS ON IPV6 NETWORKS USING DEEP LEARNING TECHNIQUES

AHMED MARWAN IDREES ALEESA

A thesis submitted in
fulfillment of the requirement for the award of the
Doctor of Philosophy in Electrical Engineering

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

MARCH 2021

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Student : ……………………………………………………………
AHMED MARWAN ALEESA

Date. : ……………………………………………………………..

Supervisor : ……………………………………………………………
DR. NAN BIN MAD SAHAR

This thesis is dedicated:

- To the sake of Allah, my Creator, and my Master, my great teacher and messenger, Prophet Muhammed (may the peace and blessings of Allah be upon him, his family, his Companions and all those who follow him exactly till the Day of Judgement), who taught us the purpose of life.
- To my great parents, who never stop giving of themselves in countless ways.
- To my beloved brother and sisters; particularly my dearest brother, Radwan, who stands by me when things look bleak.
- To my love, soulmate and wife who has been a constant source of love, support and encouragement. I am truly thankful for having you in my life
- To my supervisors who were with me during my PhD journey
- To all my family, the symbol of love and giving.
- To my friends who encourage and support me.
- To all the people in my life who touch my heart.

I dedicate this research.

ACKNOWLEDGEMENT

First and foremost, I must acknowledge my limitless thanks to Allah, the Ever-Magnificent; the Ever-Thankful, for His help and bless. I am sure that this work would have never become truth, without His guidance.

I also would like to express my wholehearted thanks to my family for the generous support they provided me throughout my entire life and particularly through the process of pursuing the master's and PhD's degree. Because of their unconditional love and prayers, I have the chance to complete this thesis. I owe a deep debt of gratitude to my parents for allowing me to study and support me emotionally and financially since the first day I came to Malaysia. I always knew that they believed in me and wanted the best for me. I would like to express my sincere appreciation to my main supervisor Dr Nan Bin Mad Sahar and my co-supervisors Dr Bilal Bahaa Zaidan and Associate Professor Dr Aws Alaa Zaidan for his thoughtful insights, helpful suggestions and continued support in the form of knowledge, enthusiasm, and guidance throughout the duration for this research. towards the compilation of this thesis. they showed me what it means to be dedicated, each in his unique way particularly to my best supervisors ever, who were teachers, leaders, brothers, and friends. who were always advised, motivate, and support me during all phases of my research.

I would like to take this opportunity to say warm thanks to all my beloved friends, who have been so supportive along the way of doing my thesis. Also, my deepest thanks go to all people who took part in making this thesis real. Finally, I would like to express my gratitude and appreciation to the Malaysian Government and Universiti Tun Hussein Onn Malaysia for the facilities and support. Thank you

ABSTRACT

The news about distributed denial of service (DDoS) attacks is rapidly increased around the world. Many services of companies and/or governments are victims of the attack. The main purpose of DDoS attacks is to overload the service for a long time, rather than to steal money or data from the targets. Since the user might not re-use services jammed by crackers, a company attacked by the crackers will lose many benefits.

Major challenges are faced by the researchers are the unavailability of the dataset such as "no labelled DDoS attacks for IPv6, no data available online for download or use, few datasets on the internet but the security institutes or researchers who own it are kept private even for the research purposes". In this research, I developed a DDoS-IPv6 dataset from real attacks traffic that contains 96 extracted features, the generated IPv6-DDoS dataset where had been collected by capturing attacks packets can be converted into network flows that contain rich metadata about the statistics of each flow, which are composed of the captured packet data. These flows are structured in the form of tabular data and contain both continuous and categorical features. Then deployed deep learning technique as intrusion detection system on the developed dataset, moreover optimised deep learning hyperparameters (i.e. the number of hidden layers/neurons, etc.) in order to find the optimal deep learning model, and check if the optimisation of layers/neurons would contribute to improving the accuracy.

Accordingly, the result of the optimal deep learning technique for the four models with the developed dataset DDoS-IPv6 are between 99.79% and 99.996% and losses are between 0.0014% and 0.781%. I found that all the techniques succeeded to classify/detect IPv6 attacks and this will lead to new further research that needs to be developed in this area.

ABSTRAK

Berita mengenai serangan Penafian Perkhidmatan (DDoS) telah pesat meningkat di seluruh dunia. Banyak perkhidmatan Syarikat dan/atau kerajaan adalah mangsa serangan. Tujuan utama serangan DDoS adalah untuk sarat Perkhidmatan untuk masa yang lama, dan bukannya untuk mencuri wang atau data dari target. Oleh kerana pengguna mungkin tidak menggunakan semula perkhidmatan yang sesak oleh keropok, sebuah syarikat yang diserang oleh keropok akan kehilangan banyak faedah.

Cabaran utama yang dihadapi oleh penyelidik untuk membangunkan penyelidikan itu sendiri dan ketiadaan Dataset seperti "Tiada serangan DDoS yang dilabelkan untuk IPv6, tiada data yang ada dalam talian untuk muat turun atau penggunaan, beberapa set data di internet tetapi institusi keselamatan atau penyelidik yang memiliki ia disimpan swasta walaupun untuk tujuan penyelidikan. Dalam kajian ini, kami membangunkan DDoS-IPv6 Dataset daripada lalu lintas serangan sebenar yang mengandungi 96 ciri yang diekstrak, IPv6 yang dihasilkan-DDoS Dataset di mana telah dikumpulkan oleh paket serangan yang dilakukan boleh ditukar kepada aliran rangkaian yang mengandungi metadata kaya tentang statistik setiap aliran, yang terdiri daripada data paket yang ditangkap. Aliran ini distruktur dalam bentuk data tabulus dan mengandungi ciri yang berterusan dan berbentuk kategori. Kemudian dikerahkan dalam teknik pembelajaran mendalam sebagai sistem pengesanan pencerobohan pada Dataset yang dibangunkan, lebih-lebih lagi dioptimumkan dalam pembelajaran hiperparameter (iaitu bilangan lapisan tersembunyi/neurons dan lain-lain) untuk mencari model pembelajaran mendalam yang optimum, dan memeriksa jika pengoptimuman lapisan/neuron akan menyumbang untuk meningkatkan ketepatan.

Oleh itu, hasil daripada teknik pembelajaran mendalam yang optimum bagi empat model yang dibangunkan Dataset DDoS-IPv6 adalah antara 99.79% dan 99.996% dan kerugian adalah di antara 0.0014% dan 0.781%. Kami mendapati bahawa semua teknik berjaya mengelaskan/mengesan serangan IPv6 dan ini akan membawa kepada penyelidikan lanjut baru perlu dibangunkan di kawasan ini.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AE	-	Autoencoder
AI	-	Artificial Intelligence
ANN	-	Artificial Neural Network
APTs	-	Advanced Persistent Threats
ATM	-	Automated Teller Machines
BPNN	-	Back-Propagation Neural Network
CNN	-	Convolutional Neural Network
CPU	-	Central Processing Unit
CIFAR	-	Canadian Institute for Advanced Research
CDBN	-	Conditional Deep Belief Networks
DBN	-	Deep Belief Network
DDoS	-	Distributed Denial of Service Attack
DL	-	Deep Learning
DNN	-	Deep Neural Network
DNS	-	Domain Name System
DoS	-	Denial of Service Attack
DT	-	Decision Tree
FDI	-	False Data Injection
GAN	-	Generative Adversarial Network
GMM	-	Gaussian Mixture Model
GPU	-	Graphical Processing Unit
GUI	-	Graphical User Interface
HDLN	-	Hybrid Deep Learning Network
HTTPS	-	Hypertext Transfer Protocol Secure
ICMP	-	Internet Control Message Protocol
IDS	-	Intrusion Detection System
IEEE	-	Institute of Electrical and Electronics Engineers
IPS	-	Intrusion Protection System
IPSec	-	Internet Protocol Security

IPv4/ IPv6	-	Internet Protocol version 4/Internet Protocol version 6
JSON	-	JavaScript Object Notation
LCS	-	Learning Classifier System
LSTM	-	Long Short-Term Memory
MITM	-	Man-In-The-Middle
ML	-	Machine Learning
MLD	-	Multicast Listener Discovery
MNIST	-	Modified National Institute of Standards and Technology
MTU	-	Maximum transmission unit
NB	-	Naïve Bayes
NIDS	-	Network Intrusion Detection System
NN	-	Neural Network
PCA	-	Principal Component Analysis
PCAP	-	Packet Capture
PNN	-	Probabilistic Neural Network
QoE	-	Quality Of Experience
QoS	-	Quality Of Service
RAM	-	Random Access Memory
RF	-	Random Forest
ReLu	-	Rectified linear unit
RNN	-	Recurrent Neural Network
RNTN	-	Recursive Neural Tensor Network
RBM	-	Restricted Boltzmann Machine
RD	-	Router Advertising
SAE	-	Stacked Autoencoder
SDA	-	Stacked Denoising Autoencoder
SoC	-	State-Of-Charge
SVM	-	Support Vector Machine
TCP	-	Transmission Control Protocol
UDP	-	User Datagram Protocol
UTHM	-	Universiti Tun Hussein Onn Malaysia
WoS	-	Web of Science

CHAPTER 1

INTRODUCTION

1.1 Introduction

In past years, there is a rapid rise globally on news about the distributed denial of service (DDoS) attack. Most private and/or government departments have become targets. A hacker group developed tools to execute DDoS attacks very easily and sell them to many people. As a result, DDoS attacks became one of the most harmful attacks in network security.

DDoS attacks are primarily to jam the services for a long time instead of taking money or data from the targets. Since a user might not re-use services jammed by crackers, a company attacked by the crackers will lose many benefits. A DDoS attack can be initiated from many computers hijacked by crackers, and then every computer will send large numbers of packets to the target server simultaneously. The server attempts to respond to all the packets, but its bandwidth gets exhausted very quickly and the service stops. A cracker who has hijacked many computers only sends some attack commands to the hijacked computers. These computers can be connected to multiple bots either directly or through a botnet. Consequently, detecting a cracker is extremely difficult. Hence, it seems that the right strategy is to detect DDoS attacks rather than crackers.

Intrusion detection systems are strategically placed on a network to detect threats and monitor packets. The intrusion detection system (IDS) accomplished this by collecting data from different systems and network sources, then analysing the data for possible threats [1]. The functions of the IDS include offering information on threats, taking corrective steps when it detects threats, and recording all important events within a network [2]. Different researchers have developed different classification representations [3-7], researchers have previously presented intrusion detection surveys and taxonomies [4, 8]. This research builds upon their work and introduces deep learning networks techniques which are void of references. With the increasing value of big data, deep learning networks are an important element to capture a DDoS attack in an IDS. the taxonomy presented within this thesis provides a fine-grained overview of the different machine learning techniques for intrusion detection systems. The detection mainly depends on the source of data and intrusion technique used. The source of data is the nodes that gather the information for analysis.

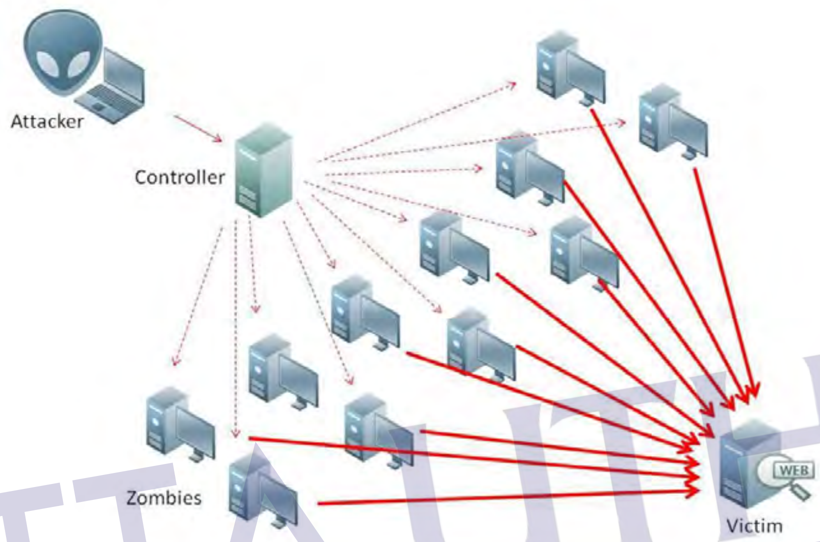

Figure 1.1: DDoS Architecture [9]

Two typical methods are commonly used in IDS such as clustering and classification. It is difficult and costly to obtain the bulk of labelled network connection records for supervised training in the first stage. The clustering analysis has emerged as an anomaly intrusion detection approach in recent years [8]. Clustering is an unsupervised data exploratory technique that partitions a set of unlabelled data patterns into groups or clusters such that patterns within a cluster are similar to each other but dissimilar to another clusters' pattern. Meanwhile, classification is a supervised method to distinguish benign and malicious traffics on the basis of provided data which usually comes from clustering results as shown in Fig.1.2. The clustering and classification can be easily implemented by various machine learning methods.

Deep Learning is a branch of machine learning on the basis of a set of algorithms that attempt to model high-level data abstractions. Deep learning is also known as Neural Networks (NN) as it’s inspired by the human brain’s functionality to learn and identify objects e.g. vision. The human brain processes raw data which is populated through our sensory inputs i.e. eyes and learns the features on its own by nature. Likewise, in deep learning, raw data is provided as input through the deep neural networks, which learns to identify the object and its features on which it is trained by algorithms. In Machine Learning, it requires manual inputs for selecting which features to process through the machine learning modules. Hence, the machine learning process is a bit slower and the result's accuracy may be affected by human errors. Deep learning's sophisticated, self-learning capability and intelligence results in higher accuracy and faster processing as compared to machine learning. Deep learning is also called deep machine learning, hierarchical learning, or deep structured learning. It can be unsupervised or supervised learning from the collected data on the basis of multiple layered models.

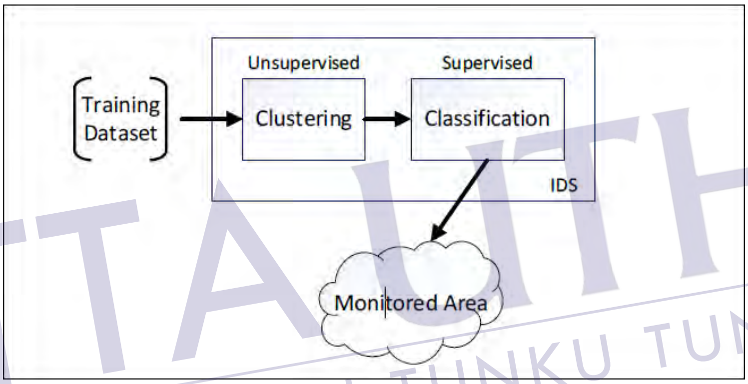

Figure 1.2: Common IDS approach [10]

there may be confusion about how to adopt deep learning in IDS applications properly since the different approaches have been adopted by previous work. Several types of research use deep learning methods in a partial sense only while the rest still uses conventional neural networks. The complexity of the deep learning method may be one of the reasons. Besides, the deep learning method requires a lot of time to train properly. Nonetheless, there are several researchers that adopted the deep learning method in their IDS research to compare the IDS performance among them. I claim that deep learning is very useful in IDS, especially for feature extraction. The feature extraction is a process of transforming raw data into features that are better represented for the underlying problem of the predictive models, resulting in improved model accuracy on unseen data. To support our claim, to provide future challenges and directions to employ deep learning in IDS accordingly. concluded that the deep learning method is suitable for pre-training or feature engineering/extraction, not as the classifier. Finally, deep learning methods can enhance future research on unknown attack detection.

1.2 Problem Statement

The distributed nature of DDoS attacks tends to make it very difficult to defend against. The main aim of such an attack is to degrade networks, deplete network resources, and to prevent legitimate users from having access to network resources [11]. Furthermore, From the related works in section 2.4.1 and section 2.5.3 the major challenges have shown that facing researchers to develop the researches and challenges of the dataset such as (“no labelled DDoS attacks for IPv6, no data available online for download or use, few datasets on the internet but the security institutes or researchers who own it are kept private even for the research purposes).

Accordingly, accuracy analysis of Deep Learning techniques in IPv4 found that the accuracy rate that been reached between 60% to 99.92% as been explained in section 2.6. this raises a question that is, do deep learning will maintain similar/less or even better accuracy in DDoS IPv6 classification/detection?

Nevertheless, deep learning hyperparameters (i.e. number of hidden layers, number of neurons, etc.) would contribute to improving the accuracy. In other words, is there any positive/negative correlation between the accuracy/loss and other evaluation metrics when the architecture of the neural is changed? Another side question related to the types of deep learning deployed and the data pre-processing is yet to be figured out and/or discussed in the academic literature.

- Accuracy of Deep Learning techniques in IPv4 between 60% to 99.92%, this raises a question that is, does deep learning will maintain similar/less or even better accuracy in DDoS IPv6 classification/detection?
- Challenges of the dataset such as (“no labelled DDoS attacks for IPv6, no data available online for download or use, few datasets on the internet but the security institutes or researchers who own it are kept private even for the research purposes”).
- No available IPv6 dataset there would be no developed deep learning models for such type of dataset as shown in section 2.5.3. does deep learning will be a success as an intrusion detection system in IPv6

- Deep Learning Hyperparameters (i.e. the number of hidden layers, number of neurons etc.) would contribute to improving the accuracy. In other words, is there any positive/negative correlation between the accuracy/lose and other evaluation metrics when the architecture of the neural is changed?

1.3 Research Question

i. What are the Deep Learning models that been used as Intrusion detection systems?
ii. What are the available datasets for DDoS attacks in IPv6?
iii. How to generate and collect DDoS IPv6 Dataset?
iv. What are the features of DDoS IPv6 attacks?
v. What is the best deep learning model to classify DDoS ipv6 attacks?
vi. What is the optimal design for deep learning models on DDoS IPv6 classification attacks?
vii. How accurate the detection/classification of deep learning models on the developed dataset?

1.4 Objectives

The research objectives can be identified as follows

i. To investigate the deep learning models as an intrusion detection system.
ii. To generate and collect dataset for anomaly DDoS flooding attack in real-time IPv6 environment. Then extract and prepare the features of the collected dataset towards creating a DDoS-IPv6 dataset.
iii. To develop deep learning models as based DDoS detection and classification models using developed dataset in objective (ii) on different deep learning models. Then optimize deep learning models' parameters (layers and neurons) using different model configurations towards identifying the optimal neural network design.
iv. To evaluate, compare, and validate the proposed DDoS flooding attacks detection technique identified in objective (iii) and (iv) using the available evaluation metrics.

1.5 Thesis Scope

i. The most common DDoS attacks such as (Smurf, TCP-SYN, Router Advertisement Flooding Attack, and Various DDoS Attacks) on IPv6 have been used to develop our dataset.
ii. The number of packets included was 1.2 million packets.
iii. Used five personal computers.
iv. Software used in our thesis, (python programming language, THC-IPv6, Ostinato, and Wireshark).
v. The deep learning models utilized in this study are ANN, DNN, SAE, and CNN.
vi. Used IPv6 environment due to the lack of research articles in this area (during the development of the literature, non-reviewed articles utilized deep learning models with DDoS IPv6).
vii. The programming language used was a python, attacks system was Linux, the attacking tool was THC-IPv6 tool, and the monitoring software was Wireshark.

1.6 Research Outline

The layout of this research as Chapter two will include the systematic literature review with analysis and review principles been used in this research. Whereas Chapter three explains the methodological part been followed to fulfil the objective. In addition, Chapter four will present the method followed to generate and pre-process the IPv6 dataset. Chapter five will show the outcomes of our research. Lastly, Chapter six contains the discussion and future work of our research.

1.7 Summary

This chapter presents an introduction to our research and showing the problem statement, and objectives. Although it represents the research mapping and how the research conducted.

CHAPTER 2

LITERATURE REVIEW

2.1 Background

This chapter investigates the deep learning that been used as an intrusion detection system through a systematic literature review, then present a taxonomy in this area with an explanation for each class and subclasses. Moreover, discuss challenges, recommendations, and motivations in the related work. Additionally, a methodological aspect, critical analysis problem background and deep learning architecture are shown with an analysis for the latest related work in this field. Lastly, finalise the findings in section research gaps and present a summary for the chapter. The structure of the literature review and the purpose of each section is presented in the table below:

Table 2.1: Literature Review Sections and Their Purpose

SECTION	PURPOSE
2.2 Systematic review protocol	To choose the set of studies to review and analyse it. The protocol explains selection procedures such as inclusion, exclusion, resources, and the procedure of selection. Consequently, select the most relevant resources for our research.
2.3 Taxonomy	To identify the themes of selected studies towards selecting the path of our research and ease gaps identification.
2.4 Discussion	To identify the current challenges in the previously selected studies and the recommendations of the authors for future research. In addition to that the motivation behind their work. These elements can help to draw the shape of our problem statement and help to answer the question of why this research is important.

Table 2.1: Literature Review Sections and Their Purpose (Continued)

SECTION	PURPOSE
2.5 Methodological Aspect	To justify the configuration of our research. In addition to that the statistics configuration in the selected studies.
2.6 Critical Analysis	This section aims to narrow down the focus into a set of studies close to our research. Through the section, the result and the accuracy have been achieved in the selected studies.
2.7 Problem Background	four major challenges which are challenges related to DDoS attacks, Challenges of DDoS in IPv6, is the challenges faced by researchers in IPv6 Dataset, and lastly, challenges on IDS in IPv6
2.8 Deep Learning Layer With DDoS	To review the current researches done as an intrusion detection system on the basis of deep learning technique. In addition to that review under which network-layer DDoS attacks are classified and established.
2.9 Deep Learning Models	The section presents the architecture of deep learning models that been used in this research
2.10 Related Works Analysis Update	This section showing the latest related work with their analysis in this research field
2.11 Research Gaps	This section showing gaps and challenges in the related works that will be our objectives in this research
2.12 summary	This section summarises the findings of this chapter

2.2 Systematic Review Protocol

'Deep learning' DL is the most significant phrase in the scope of this study. Other artificial intelligence models that are not used as DL models are eliminated. For example, CNN, Deep Neural Network (DNN), and Autoencoder (AE) are used to develop intrusion detection systems (IDSs). I consider all areas related to intrusion detection and limit our scope to the English literature. Moreover, I use intruder and attacker as general categories.

2.2.1 Information sources

I proceed with the research on target articles and select the following digital databases:
(1) Web of Science (WoS) is an extensive database indexed as cross-disciplinary research. This database is selected to provide a comprehensive assessment of scientists' endeavours with an extensive view and to cover relevant technical literature.
(2) The ScienceDirect database provides an entry to journals and technical and science articles.
(3) The Xplore database of the Institute of Electrical and Electronics Engineers (IEEE) contains technical literature in electrical engineering, electronics, computer science, and other related fields.
(4) Scopus is the largest abstract database of peer-reviewed literature (i.e. scientific journals and conference proceedings).

2.2.2 Study selection

Study collection consists of two phases of scanning and filtering to search for literature resources. The first phase involves skimming titles and abstracts to exclude irrelevant articles and duplicates. The second phase involves reading the complete form of the selected manuscripts.

2.2.3 Search

This study started at the beginning of December 2017 through the advanced search boxes in the WoS, ScienceDirect, IEEE Xplore, and Scopus databases. I used a combination of diverse variations of keywords that consisted of 'deep learning,' 'intrusion' and 'attack' to perform our study. These keywords were combined with 'OR' and 'AND' operators. Figure 2.1 illustrates the exact query texts used in this study. I focused on two types of articles, namely, journal and conference articles, and used the preferences in each search engine to eliminate other types of reports and book chapters. In our survey on this emerging trend of intrusion detection, I assumed that the two areas consist of the latest and related scientific studies.

2.2.4 Eligibility criteria

Figure 2.1 lists the criteria that each article must satisfy. The initial goal was to plan the research on DL into an overall and coarse-grained taxonomy with three sets. I used Google Scholar and derived the categories from a pre-survey of related studies without limitations to obtain an initial perception of the background and directions of related papers. If the eligibility criteria were unsatisfied in the remaining articles after the initial removal of duplicates, then they were excluded from filtering and screening the articles. The exclusion criteria included having the objective of intrusion detection technology rather than non-DL models and not being written in English. A single Excel file with a complete list of all the articles from numerous resources with their equivalent initial categories was used to simplify the subsequent processing steps of data collection. I accomplished several full-text readings, and thus obtained a running classification of articles into a refined taxonomy and a large collection of highlights and comments on the surveyed studies. The major findings followed the processes of tabulation, description, and summarization. Excel and Word files were used to maintain a set of relevant information, including the source databases, their complete list of articles, description tables and summaries, categorization tables on the basis of attack type, review sources, objectives, number of features, and model used to develop DL, in addition to certain related information.

2.2.5 Results and statistical information of articles

The preliminary query resulted in 1,861 articles in the four databases: 1,203 in Scopus, 117 in IEEE Xplore, 477 in ScienceDirect, and 64 in WoS. This study grouped the filtered articles that were published from 2015 to 2018 into four categories. After scanning the titles and abstracts, the number of articles decreased to 179 from all the categories, and the duplicate articles were 59 out of 179. The final full-text reading and review excluded 52 papers. A total of 68 articles remained in the final set given the different topics related to DL as an intrusion detection technique.

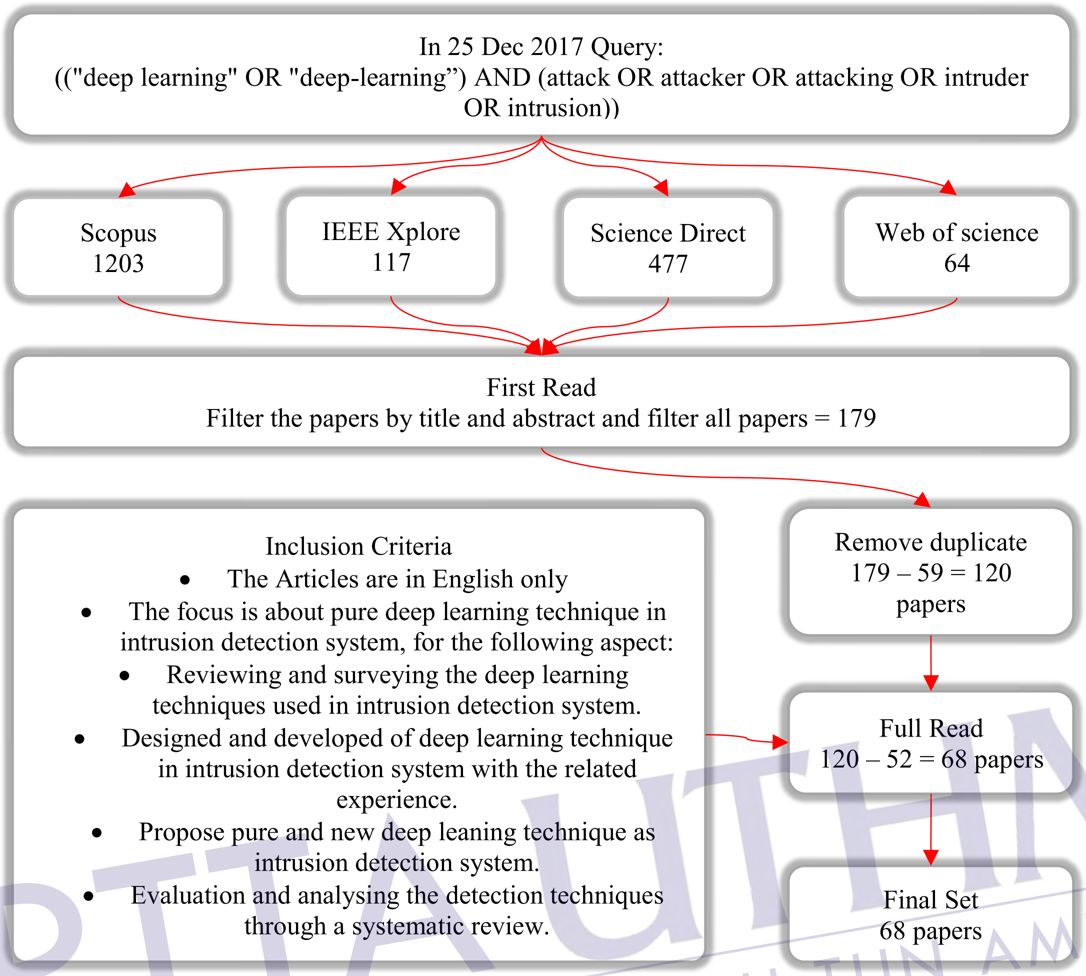

Figure 2.1: Flowchart Of Study Selection, Including The Search Query And Inclusion Criteria

2.3 Taxonomy

The classification suggests different classes and subclasses. Figure 2.2 illustrates the taxonomy of an IDS; it shows an inclusive improvement of several studies and applications. The first class includes articles associated with the objectives of this study. The second class includes articles on the number of techniques used as single or hybrid techniques to develop DL techniques to be used in IDSs. The third class comprises the artificial intelligence techniques used as DL techniques in IDSs. The largest proportion (72.06%; 49/68) relates to articles that develop an approach for evaluating or identifying intrusion detection techniques using the DL approach. The second-largest proportion (22.06%; 15/68) relates to studying/applying articles to the DL area, IDSs, or other related issues. The third-largest proportion (5.88%; 4/68) discusses frameworks/models for running or adopting IDSs. The taxonomy of the literature presented in Figure 2.2 identifies several subcategories from the main classes.

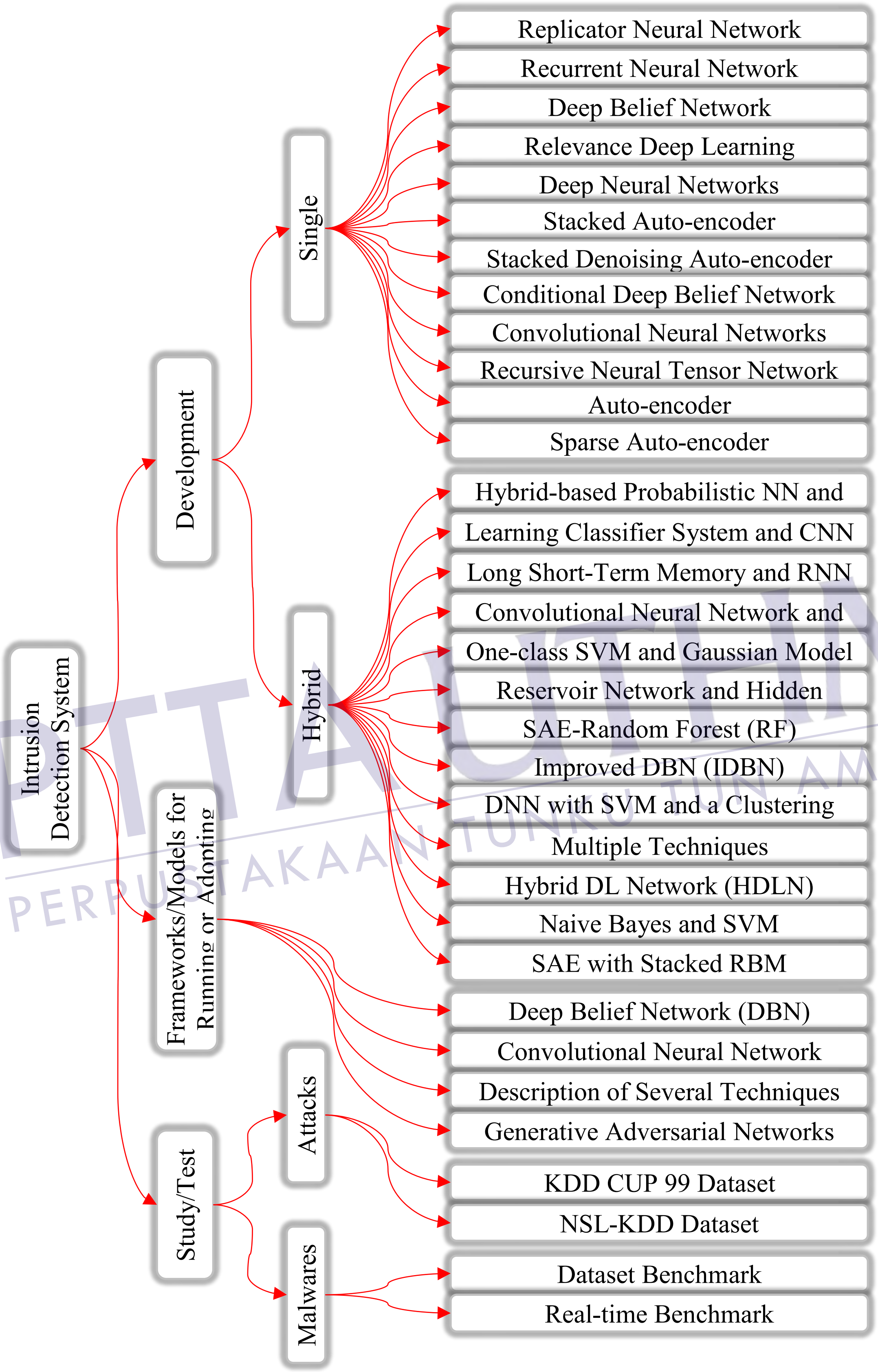

Figure 2.2: Taxonomy Of Literature On Intrusion Detection System On the basis of Deep Learning

2.3.1 Development

The first subsection in the classification of our taxonomy is divided into two sections, namely, single and hybrid techniques: -

2.3.1.1 Single Technique

This class is divided into 12 subclasses on the basis of the type of technique used to develop the DL technique.

A. Replicator Neural Networks

Replicator NNs, such as Autoencoders and NNs, are specific. These networks have been initially proposed as compression techniques that are trained to replicate the given input as an output. Compression can be achieved by using input units that are more than the units in the intermediate layer [12]. The principal component analysis (PCA) dimensionality reduction technique has confirmed that this compression process belongs to replicator NNs. An anomaly intrusion detection on the basis of DL that used replicator NNs was presented in [13]. Unsupervised dimensionality reduction was performed by the hidden layer between an encoder and a decoder. Therefore, the presented technique is on the basis of a decoder and an encoder, and this network corresponds to PCA. However, the proposed method did not exhibit accuracy when evaluated.

B. Recurrent neural network

This technique has a unique feature that is identical to a human brain process. That is, it can adopt the inner memory to process random sequences of inputs, and thus perform complex tasks, such as unsegmented and pattern recognition; moreover, this technique is ideal for handling real-time learning tasks given its capability to handle time-series data [14]. The following articles have adopted RNNs to build their DL technique.

<u>Attack intrusion detection</u>: An IDS on the basis of RNN was proposed in [15] by classifying the collected data. In the experiments, different hidden node numbers and learning rate values were utilised for binary and multiclass classification. A realistic performance was accomplished by this technique, and computational processing was high. The authors of [16] developed a DL algorithm by using the preceding technique with Hessian-free optimisation to detect intrusions; the output exhibited relatively better performance in this technique than in the previous model. The false alarm rate was only 2.1%, and the detection rate was 95.37%. The authors of [17] suggested a system called DeepDefense, which adopts a DL-based distributed denial-of-service (DDoS) attack detection technique. The authors transformed packet-based DDoS detection to window-based detection and formulated DDoS detection as a series of classification problems to improve the performance in identifying DDoS attack traffic. The results confirmed that the models' performance depends on the dataset size, which does not depend on the system used for training.

Intruder behaviour detection: To predict the behaviour of users in Tor networks, the authors of [18] applied deep RNNs combined with kernel PCA and long short-term memory (LSTM)-RNN; their method consists of feature extraction, attack detection, and data pre-processing. Better performance than those of previous strategies was achieved by using this proposed threat analysis strategy. In another study, a framework was suggested to perform intruder detection and analysis using DL networks and association rule mining [14]. This framework can predict future intruder operations that may occur and the locations where these operations may be generated; then, it will show the progress of intruder attacks.

Malware detection: The authors of [19] proposed a natural language modelling that is similar to learning the language of malware spoken through the extraction of robust and executed instructions by using time-domain features. During the projection stage when features were extracted, the authors used RNNs to conduct experiments on malicious or benign files.

C. Deep Belief Network

A DBN is a Deep Neural Network model generated by a stacked Restricted Boltzmann machine (RBM), and the input of an RBM is the result of earlier RBMs, Between RBMs layers the information has become available on the system. Whole layers provide a unidirectional connection, except for the two top layers, which provide a two-way connection. DBNs have been used as follows.

Android malware detection: A framework called 'Deepsign' was presented in [20] to detect malware automatically using a signature generation method on the basis of DBN. Registry entries, web searches, and port accesses formed the dataset on the basis of the behaviour logs of application programming interface (API) calls. The logs were converted into a binary vector in a sandbox. The result showed that using DBN for classification can achieve an accuracy of 98.6%. The authors of [21] proposed 'DroidDeepLearner,' an approach that uses a DL algorithm to address the current requirement for malware detection to become more autonomous at learning to solve problems with minimal human intervention for Android malware characterisation and identification. In their experiments, the DBN model performed better than various SVM models. The authors of [22] proposed 'DroidDetector,' an online DL-based Android malware detection engine that can detect whether an app is a malware or works automatically by using DL techniques to correlate the features from a static analysis with other features from dynamic analysis of the characterised malware and Android apps. Traditional (i.e. ML) techniques were outperformed, with a detection accuracy of 96.76%. The authors of [23] developed 'DroidDelver,' a programmed Android malware DS that utilises a DL structure that considers a DBN. From a small code extract, API call block features maintain an inherent relationship that exists within API calls.

Attack intrusion detection: An intelligent communication middleware was proposed to complement the conventional quality of service (QoS) evaluation that utilises the quality of experience (QoE) metrics in [24]. Communication infrastructure and data acquisition systems are crucial technologies for maintaining system economic reliability and efficiency. The proposed middleware effectively utilised traditional QoS criteria to detect and defend against potential congestion that attacks QoE evaluation from the operators of a power system. The authors of [25] used DBN to propose a NIDS for the security of in-vehicular networks. Detection accuracy was improved compared with those of earlier methods.

D. Relevance Deep Learning

The authors of [26] proposed a network intrusion detection technique on the basis of relevance DL, which learned a principle of deep relevance and the training algorithm of RBM. Relevance DL was applied to a NIDS to analyse the principle of feasibility in the NIDS. This technique was also applied to network intrusion detection technology and obtained high detection accuracy. The ratio of intrusion detection to normal data detection was 10:1. The average detection of a high-speed ultrahigh bandwidth network was greater than 50%, and the error rate was approximately 1.5%. These results indicated the effectiveness of the relevant DL algorithm in network intrusion detection.

E. Deep Neural Networks

DNNs, which provide powerful instruments to automatically produce high-level abstractions of complex multimodal data, have recently attracted considerable attention from industry and academia. DNNs learn features themselves, and thus the learning process becomes increasingly accurate; DNNs are verified to be more efficient and accurate than shallow learning [27]. The use of DNNs is presented as follows.

Attack intrusion detection: The authors of [27] proposed a high-level feature extraction capability of Internet of things systems that can be a resilient mechanism for novel attacks or small mutations. The compression capabilities and self-taught DL architecture are key mechanisms for hidden pattern discovery from the training data; hence, attacks are discriminated from benign traffic. The authors of [28] suggested a DNN with 3 hidden layers that use 41 features. The outcomes were mixed, i.e. those with more classes were less accurate than those that focused on fewer classes. The authors of [29] investigated the influence of fault injection attacks on DNNs. Through a fault injection attack by modifying the parameters used in DNNs, a specified input pattern was misclassified into an adversarial class that was attempted by attackers. The authors proposed two types of fault injection attacks to achieve these objectives. The first type was a single-bias attack that requires modifying only one parameter in the DNN for a misclassification on the basis of the observation outputs of the DNN that may linearly depend on several parameters. The second type was a gradient descent attack that aims to reserve classification accuracy on input patterns other than the targeted one to force stealthy misclassification. Moreover, the manual burden placed on Department of Défense investigators was reduced by using the ML application in the early triage of security warnings that were reviewed as a case study in [30]. The triage tool prototype, called federated analysis security, was implemented in this study. Numerous daily events/alerts were summarized, categorized, and highlighted using the FAST prototype. The NN achieved a high classification accuracy of 98% and a log loss below 0.0001. Fivefold cross-validation obtained a result calculated from sample data.

Malware detection: A new adversary-resistant technique that prevents attackers from constructing influential adversarial samples by randomly nullifying features within data vectors was proposed in [31]; the accuracy of this technique was 73.59% in the Canadian Institute for Advanced Research (CIFAR) dataset and 98.43% in the Modified National Institute of Standards and Technology (MNIST) dataset. A malware detector that uses static features was proposed in [32] to deploy DNNs. The accuracy results of any previously published detection engine that used exclusively static features were less than those of this proposed approach. However, in the case of obfuscated binaries, static analysis may not provide satisfactory input for classification, and the authors did not consider dynamic analysis results in their research.

Spam detection: The authors of [33] proposed a novel technique on the basis of DL techniques. This technique constructed a binary classifier on the basis of the preceding representation dataset for the syntax of each tweet that will be learned through the Word Vector training phase. Performance evaluation was conducted from a 10-day ground-truth dataset with more than 600 million real-world tweets after the technique collected a part of the labelled data (376,206 spam and 73,836 no spam tweets). The data were pre-processed and converted into high-dimensional vectors by utilising the Word Vector technique.

F. Stacked Auto-encoder

Autoencoder layers and a logistic regression layer were used to construct SAE. SAE was built by stacking additional unsupervised feature learning layers through greedy methods for each additional layer and could be trained. I trained the new hidden layer by training a standard supervised NN with one hidden layer. SAE was used as follows.

Attack intrusion detection: A three-layer Wi-Fi impersonation attack detection system was developed in [34]. In the original dataset, SAEs firstly performed feature extraction through SAE and then feature selection through SVM, decision tree (DT), or artificial NN (ANN) on the newly extracted features and the original data. An ANN was used for the final classification. The proposed system results presented a 0.012% false-positive rate and a 99.918% detection rate. The deep features of an application-layer DDoS attack on the basis of a DL architecture that consisted of more than three layers were proposed in [35]. The concept of an Autoencoder was applied to the proposed work. The DL architecture aimed to receive high-level features using SAE. The proposed architecture achieved an average false positive rate of 1.27% and an average detection rate of 98.99%. The authors of [36] proposed various denial-of-service (DoS) attacks with timely detection against a computer or a network system on the basis of SAE. Their research focused on detecting application-layer DoS attacks by applying an anomaly detection-based approach to statistics extracted from network packets to utilize encrypted protocols. A classification scheme using a DL approach and a solution on the basis of anomaly detection was presented in [37]. The capability to perform attack classification accurately and the features necessary to detect network anomalies were self-learned in the DL approach. The overall accuracy of 98.6% was achieved through the SAE architecture frameworks formed on two and three hidden layers. The proposed frameworks can detect multipliable attacks in an IEEE 802.11 network. This network has high overall accuracy, considers novel attacks, and can perform four-class classification. A leveraged SAE was proposed in [38] to improve impersonation detection and classification by using weighted feature learning from shallow machine learners.

Android malware detection: The authors of [39] used a Linux-kernel system, called a graph-based DL framework, to propose an Android malware detection system on the basis of DL architecture with the SAE model. A DeepMalDroid method was developed for dynamic analysis, rather than depending on a random event generator or user interactions.

G. Stacked Denoising Autoencoder

SDA, which is a development of traditional SAEs, introduces the structure and relevant terminology of a denoising Autoencoder [40]. A session-based network intrusion detection model using DL architecture was proposed in [31]. Researchers obtained relatively impressive results by applying an SDA-based DL architecture to detect botnet traffic.

H. Conditional Deep Belief Networks

CDBNs are extended versions of DBNs and have been presented to model temporal data by treating previously observed data through the implementation of an autoregressive data-modelling scheme and additional input to model temporal data. Real-time measurement data from geographically distributed phasor measurement units (PMUs) leverage physical coherence in power systems and are analysed using CDBNs to stabilise performance, probe and detect a data corruption scheme, verify the validity of lead agents' PMU data and estimate their true values [41]. The authors of [42] proposed a real-time detection technique. DL techniques on the basis of CDBN used historical measurement data and revealed features to detect false data injection (FDI) attacks in real-time and recognise the behaviour patterns of FDI attacks.

I. Convolutional Neural Network

The CNN process is similar to that of traditional ANNs, i.e. it consists of self-optimisation through learning neurons. Each neuron will operate and receive an input, such as a nonlinear function as a basis for countless ANNs [43]. CNNs are used as follows.

<u>Hardware cybersecurity detection:</u> This scheme was proposed as a CNN technique for securing the automated teller machines (ATMs) of banks because customers are prohibited from wearing a helmet whilst using ATMs. Google's inception model was used for this purpose. The use of ATM surveillance camera feed can help improve security significantly as a form of automated helmet detection. The model achieved an accuracy of 95.3% whilst training on a proprietary ATM surveillance dataset [44].

Attack intrusion detection: The authors of [42] proposed a CNN that automatically learns the features of a graphic NSL-KDD dataset transformation by using a graphic conversion technique as an image conversion method for the dataset. The proposed technique is performed effectively and can be used as an anomaly detection classifier. A novel poisoning algorithm on the basis of the concept of back-gradient optimisation, i.e. to compute the gradient of interest through automatic differentiation, was proposed by the authors of [45] to extend the definition of poisoning attacks to multiclass problems and significantly reduce attack complexity whilst reversing the learning procedure. Their approach can target a wide class of learning algorithms compared with current poisoning strategies, including NN and CNN architectures that are trained with gradient-based procedures.

Android malware detection: The proposed CNN operation conducts classification along the sequence. The convolution window slides down the sequence to learn sequential patterns for each location and construct high-level features from small local features. CNN architecture uses multiple CNN layers. CNN is a natural choice for sequential data because its performance is considerably better than that of LSTM [46].

J. Recursive Neural Tensor Network

An RNTN, which is a development of RNN, is a tree-structured network similar to RNN that uses a tensor to improve its performance. A tensor is used to calculate a high-order composition of input features in RNTN after being enabled. On the basis of network behaviour, a technique was proposed in [47] to determine whether a dynamic analysis must be suspended to intensely and efficiently collect malware communication. Two characteristics of malware communication were focused on using the proposed technique, namely, the common latent function and the change in communication purpose. Overall, the proposed method reduced analysis time by 67.1% and avoided a complete analysis of 80.2% of the malware samples.

K. Auto-Encoder

Autoencoders aims to transform input into output with the least possible amount of distortion; they are considered a plain learning technique. Although they are theoretically simple, Autoencoders play an important role in ML. A three-stage algorithm was proposed in [48]. The first stage was a standardised dataset. The second stage produced a regression function by using DL depending on an Autoencoder model. The third stage produced a classifier function using a memetic. The system successfully classified 90.72% of the records. The authors of [49] proposed an Autoencoder technique for the real-time detection of cyber-physical attacks on water distribution systems. A test dataset that features several classes of plausible attacks was used to evaluate detection performance. The authors of [50] presented a new approach to network intrusion detection and classification for cybersecurity on an energy-efficient neuromorphic hardware platform by using DL algorithms on the basis of an Autoencoder. This Autoencoder was evaluated on IBM's True North Neurosynaptic CPU with less than 50 mow computation energy. The results achieved a classification rate of approximately 81.31% and an accuracy of nearly 90.12% for intrusion detection.

L. Sparse Auto-Encoder

The authors of [51] proposed a DL approach that depends on a sparse Autoencoder to implement a flexible and effective NIDS. A feature-learning task was realised completely unsupervised by using a Sparse Autoencoder. The result achieved a classification accuracy rate of over 98%.

2.3.1.2 Hybrid Technique

This class is divided into 13 subclasses on the basis of the type of hybrid techniques used to develop the following DL techniques.

A. Hybrid-based Probabilistic NN (PNN) and Deep Belief Network (DBN)

An intrusion detection strategy that utilises DBN and a probabilistic neural system was provided in [52]. Firstly, the major attributes of raw data were maintained to convert them into low-dimensional data through the nonlinear learning capability of DBN. Secondly, the number of hidden-layer nodes for each layer was increased by using a swarm optimisation algorithm to obtain optimal learning performance which reached 99.31%. Lastly, researchers of low-dimensional data who used PNN were categorised.

B. Learning Classifier System (LCS) and Convolutional Neural Network (CNN)

The authors of [53] proposed the convolutional neural-LCS (CN-LCS), which is a hybrid system that uses LCS and CNN for an IDS. CN-LCS can classify high-dimensional and sparse feature vectors of queries from data by using the automatic feature selection capability of convolution–pooling processes and a genetic algorithm. The model result achieved 94.64% accuracy.

C. Long Short-Term Memory (LSTM) and Recurrent Neural Network (RNN)

One work proposed a classifier for IDSs following the DL approach. Among six optimisations for the LSTM RNN model used as IDS, Nadam's optimiser was suitable for the LSTM RNN model in detecting intrusions. This classifier achieved a detection rate of 98.95% and a false alarm rate of 9.98%; these results indicated that this classifier demonstrated better performance than the other classifiers [54]. Another IDS model with the DL approach was on the basis of the LSTM architecture with RNN. This model achieved an attack detection percentage of 98.8%, an average false alarm rate of 10.03%, and normal instances of 10% [55].

D. Convolutional Neural Network (CNNs) and Stacked Autoencoders (SAEs)

A novel network intrusion model with the DL approach on the basis of stacked dilated convolutional Autoencoders was proposed in [56]. This method was evaluated on two new intrusion detection datasets. This network intrusion detection model merged the advantages of SAEs and CNNs. It can automatically learn additional unlabelled raw network traffic data that contain real-world traffic from botnets and important features from large-scale data, such as advanced persistent threats (APTs), normal traffic, scans, web-based malware, and exploits. The binary classification result achieved an accuracy rate between 97.91% and 98.62%%.

E. One-class SVM (OC-SVM) and Gaussian Mixture Model (GMM)

This framework was built on the basis of two models to form a clustering model that can discover new anomalies [56]. The architecture obtained the capability to detect new anomalies. Multi-cluster anomalies were sorted using word2vec and subspace spectral ensemble clustering. These anomalies will be ignored by most unsupervised anomaly detection methods. The authors used weblogs to extract features manually and perform unsupervised anomaly detection by applying the features extracted by GMM and OC-SVM. The model outcome achieved approximately 0.8691 Rn and 0.8321 NMI. The model was 28 times faster than other techniques. The results validated that their model can cluster anomalies into correct categories.

F. Reservoir Network and Hidden Markov Model

Automatic identification is a type of integrity attack that affects cyber-physical systems; an innovative framework called ‘IDAS’ was proposed to address this issue [57]. The technique’s architecture is on the basis of two models, namely, the reservoir network and the hidden Markov model, for a specific application scenario. The pattern recognition algorithms of different modelling properties were customised to learn their distribution, and a feature set was designed in the spectrum by capturing the characteristics of each attack. With regard to handling hidden attacks, a novel detection element was integrated. In terms of the future usage of the structure and

REFERENCES

[1] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," *arXiv preprint arXiv:1701.02145,* 2017.

[2] S. hafez Amer and J. A. hamilton Jr, "Intrusion detection systems (ids) taxonomy-a short review," *This is a paid advertisement. STN 13-2 June 2010: Defensive Cyber Security: Policies and Procedures 2,* p. 23, 2010.

[3] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," in *Annales des télécommunications*, 2000, pp. 361-378.

[4] S. J. C. U. o. T. G. Axelsson, Sweden, "Intrusion Detection Systems: A Survey and Taxonomy. 2000," 2005.

[5] S. hafez Amer, J. A. J. T. i. a. p. a. S.-J. D. C. S. P. hamilton Jr, and P. 2, "Intrusion detection systems (ids) taxonomy-a short review," p. 23, 2010.

[6] C. Xenakis, C. Panos, I. J. C. Stavrakakis, and Security, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks," vol. 30, pp. 63-80, 2011.

[7] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, K.-Y. J. J. o. N. Tung, and C. Applications, "Intrusion detection system: A comprehensive review," vol. 36, pp. 16-24, 2013.

[8] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. J. a. p. a. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," 2017.

[9] A. N. Jaber, M. F. Zolkipli, H. A. Shakir, and M. R. Jassim, "Host based intrusion detection and prevention model against DDoS attack in cloud computing," in *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2017, pp. 241-252.

[10] E. Aminanto and K. Kim, "Deep learning in intrusion detection system: An overview," in *2016 International Research Conference on Engineering and Technology (2016 IRCET)*, 2016.

[11] S. T. Zargar, J. Joshi, D. J. I. c. s. Tipper, and tutorials, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," vol. 15, pp. 2046-2069, 2013.

[12] R. Hecht-Nielsen, "Replicator neural networks for universal optimal source coding," *Science,* vol. 269, pp. 1860-1863, 1995.

[13] C. G. Cordero, S. Hauke, M. Mühlhäuser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using Replicator Neural Networks," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, 2016, pp. 317-324.

[14] A. Thilina, S. Attanayake, S. Samarakoon, D. Nawodya, L. Rupasinghe, N. Pathirage, *et al.*, "Intruder detection using deep learning and association rule mining," in *Computer and Information Technology (CIT), 2016 IEEE International Conference on*, 2016, pp. 615-620.

[15] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access,* vol. 5, pp. 21954-21961, 2017.

[16] J. Kim and H. Kim, "Applying recurrent neural network to intrusion detection with hessian free optimization," in *International Workshop on Information Security Applications*, 2015, pp. 357-369.

[17] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," in *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2017, pp. 1-8.

[18] T. Ishitaki, R. Obukata, T. Oda, and L. Barolli, "Application of Deep Recurrent Neural Networks for Prediction of User Behavior in Tor Networks," in *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on*, 2017, pp. 238-243.

[19] R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, "Malware classification with recurrent networks," in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*, 2015, pp. 1916-1920.

[20] O. E. David and N. S. Netanyahu, "Deepsign: Deep learning for automatic malware signature generation and classification," in *Neural Networks (IJCNN), 2015 International Joint Conference on*, 2015, pp. 1-8.

[21] Z. Wang, J. Cai, S. Cheng, and W. Li, "DroidDeepLearner: Identifying Android malware using deep learning," in *Sarnoff Symposium, 2016 IEEE 37th*, 2016, pp. 160-165.

[22] Z. Yuan, Y. Lu, and Y. Xue, "Droiddetector: android malware characterization and detection using deep learning," *Tsinghua Science and Technology,* vol. 21, pp. 114-123, 2016.

[23] S. Hou, A. Saas, Y. Ye, and L. Chen, "Droiddelver: An android malware detection system using deep belief network based on api call blocks," in *International Conference on Web-Age Information Management*, 2016, pp. 54-66.

[24] Y. Wu, G. J. Mendis, Y. He, J. Wei, and B.-M. Hodge, "An Attack-Resilient Middleware Architecture for Grid Integration of Distributed Energy Resources," in *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on*, 2016, pp. 485-491.

[25] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one*, vol. 11, p. e0155781, 2016.

[26] L. Jing and W. Bin, "Network Intrusion Detection Method Based on Relevance Deep Learning," in *Intelligent Transportation, Big Data & Smart City (ICITBS), 2016 International Conference on*, 2016, pp. 237-240.

[27] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761-768, 2018.

[28] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced Intrusion Detection System," in *Emerging Technologies and Factory Automation (ETFA), 2016 IEEE 21st International Conference on*, 2016, pp. 1-8.

[29] Y. Liu, L. Wei, B. Luo, and Q. Xu, "Fault injection attack on deep neural network," in *Proceedings of the 36th International Conference on Computer-Aided Design*, 2017, pp. 131-138.

[30] S. McElwee, J. Heaton, J. Fraley, and J. Cannady, "Deep learning for prioritizing and responding to intrusion detection alerts," in *Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE*, 2017, pp. 1-5.

[31] Q. Wang, W. Guo, K. Zhang, A. G. Ororbia II, X. Xing, X. Liu*, et al.*, "Adversary resistant deep neural networks with an application to malware detection," in *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2017, pp. 1145-1153.

[32] J. Saxe and K. Berlin, "Deep neural network based malware detection using two dimensional binary program features," in *Malicious and Unwanted Software (MALWARE), 2015 10th International Conference on*, 2015, pp. 11-20.

[33] T. Wu, S. Liu, J. Zhang, and Y. Xiang, "Twitter spam detection based on deep learning," in *Proceedings of the Australasian Computer Science Week Multiconference*, 2017, p. 3.

[34] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 621-636, 2018.

[35] S. Yadav and S. Subramanian, "Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder," in *Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on*, 2016, pp. 361-366.

[36] M. Zolotukhin, T. Hämäläinen, T. Kokkonen, and J. Siltanen, "Increasing web service availability by detecting application-layer DDoS attacks in encrypted

traffic," in *Telecommunications (ICT), 2016 23rd International Conference on*, 2016, pp. 1-6.

[37] V. L. Thing, "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach," in *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*, 2017, pp. 1-6.

[38] M. E. Aminanto and K. Kim, "Detecting impersonation attack in WiFi networks using deep learning approach," in *International Workshop on Information Security Applications*, 2016, pp. 136-147.

[39] S. Hou, A. Saas, L. Chen, and Y. Ye, "Deep4maldroid: A deep learning framework for android malware detection based on linux kernel system call graphs," in *2016 IEEE/WIC/ACM International Conference on Web Intelligence Workshops (WIW)*, 2016, pp. 104-111.

[40] P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P.-A. Manzagol, "Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion," *Journal of machine learning research,* vol. 11, pp. 3371-3408, 2010.

[41] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Joint Workshop on*, 2016, pp. 1-6.

[42] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, "Intrusion detection using convolutional neural networks for representation learning," in *International Conference on Neural Information Processing*, 2017, pp. 858-866.

[43] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *arXiv preprint arXiv:1511.08458,* 2015.

[44] A. Mathew, J. Mathew, M. Govind, and A. Mooppan, "An Improved Transfer learning Approach for Intrusion Detection," *Procedia Computer Science,* vol. 115, pp. 251-257, 2017.

[45] L. Muñoz-González, B. Biggio, A. Demontis, A. Paudice, V. Wongrassamee, E. C. Lupu, *et al.*, "Towards poisoning of deep learning algorithms with back-gradient optimization," in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*, 2017, pp. 27-38.

[46] R. Nix and J. Zhang, "Classification of Android apps and malware using deep neural networks," in *Neural Networks (IJCNN), 2017 International Joint Conference on*, 2017, pp. 1871-1878.

[47] T. Shibahara, T. Yagi, M. Akiyama, D. Chiba, and T. Yada, "Efficient dynamic malware analysis based on network behavior using deep learning," in *Global Communications Conference (GLOBECOM), 2016 IEEE*, 2016, pp. 1-7.

[48] S. Mohammadi and A. Namadchian, "A New Deep Learning Approach for Anomaly Base IDS using Memetic Classifier," *International Journal of Computers, Communications & Control,* vol. 12, 2017.

[49] R. Taormina and S. Galelli, "Real-time detection of cyber-physical attacks on water distribution systems using deep learning," in *World Environmental and Water Resources Congress 2017*, 2017, pp. 469-479.

[50] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security on neuromorphic computing system," in *Neural Networks (IJCNN), 2017 International Joint Conference on*, 2017, pp. 3830-3837.

[51] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, 2016, pp. 21-26.

[52] G. Zhao, C. Zhang, and L. Zheng, "Intrusion detection using deep belief network and probabilistic neural network," in *Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on*, 2017, pp. 639-642.

[53] S.-J. Bu and S.-B. Cho, "A hybrid system of deep learning and learning classifier system for database intrusion detection," in *International Conference on Hybrid Artificial Intelligence Systems*, 2017, pp. 615-625.

[54] J. Kim and H. Kim, "An Effective Intrusion Detection Classifier Using Long Short-Term Memory with Gradient Descent Optimization," in *Platform Technology and Service (PlatCon), 2017 International Conference on*, 2017, pp. 1-6.

[55] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *Platform Technology and Service (PlatCon), 2016 International Conference on*, 2016, pp. 1-5.

[56] G. Yuan, B. Li, Y. Yao, and S. Zhang, "A deep learning enabled subspace spectral ensemble clustering approach for web anomaly detection," in *Neural Networks (IJCNN), 2017 International Joint Conference on*, 2017, pp. 3896-3903.

[57] S. Ntalampiras, "Automatic identification of integrity attacks in cyber-physical systems," *Expert Systems with Applications,* vol. 58, pp. 164-173, 2016.

[58] P. V. Dinh, T. N. Ngoc, N. Shone, A. MacDermott, and Q. Shi, "Deep learning combined with de-noising data for network intrusion detection," in *Intelligent and Evolutionary Systems (IES), 2017 21st Asia Pacific Symposium on*, 2017, pp. 55-60.

[59] Y. Liu and X. Zhang, "Intrusion detection based on IDBM," in *Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C*, 2016, pp. 173-177.

[60] T. Ma, Y. Yu, F. Wang, Q. Zhang, and X. Chen, "A Hybrid Methodologies for Intrusion Detection Based Deep Neural Network with Support Vector Machine and Clustering Technique," in *International Conference on Frontier Computing*, 2016, pp. 123-134.

[61] H. Maghrebi, T. Portigliatti, and E. Prouff, "Breaking cryptographic implementations using deep learning techniques," in *International Conference on Security, Privacy, and Applied Cryptography Engineering*, 2016, pp. 3-26.

[62] F. K. Lodhi, S. R. Hasan, O. Hasan, and F. Awwadl, "Power profiling of microcontroller's instruction set for runtime hardware Trojans detection without golden circuit models," in *Proceedings of the Conference on Design, Automation & Test in Europe*, 2017, pp. 294-297.

[63] R. Yan, X. Xiao, G. Hu, S. Peng, and Y. Jiang, "New deep learning method to detect code injection attacks on hybrid applications," *Journal of Systems and Software,* vol. 137, pp. 67-77, 2018.

[64] Y. Shi, Y. Sagduyu, and A. Grushin, "How to steal a machine learning classifier with deep learning," in *Technologies for Homeland Security (HST), 2017 IEEE International Symposium on*, 2017, pp. 1-5.

[65] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using deep learning," in *System Science and Engineering (ICSSE), 2017 International Conference on*, 2017, pp. 210-214.

[66] R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluating effectiveness of shallow and deep networks to intrusion detection system," in *Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on*, 2017, pp. 1282-1289.

[67] F. Martinelli, F. Marulli, and F. Mercaldo, "Evaluating convolutional neural network for effective mobile malware detection," *Procedia Computer Science,* vol. 112, pp. 2372-2381, 2017.

[68] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing,* vol. 234, pp. 11-26, 2017.

[69] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *Proc. IEEE ICCSN*, 2016, pp. 581-585.

[70] Y. Harel, I. B. Gal, and Y. Elovici, "Cyber Security and the Role of Intelligent Systems in Addressing its Challenges," *ACM Transactions on Intelligent Systems and Technology (TIST),* vol. 8, p. 49, 2017.

[71] U. Fiore, A. De Santis, F. Perla, P. Zanetti, and F. Palmieri, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection," *Information Sciences,* 2017.

[72] L. Deng and D. Yu, "Deep learning: methods and applications," *Foundations and Trends® in Signal Processing,* vol. 7, pp. 197-387, 2014.

[73] S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. Krishna, "A deep learning based artificial neural network approach for intrusion detection," in *International Conference on Mathematics and Computing*, 2017, pp. 44-53.

[74] X. Zhang and J. Chen, "Deep learning based intelligent intrusion detection," in *Communication Software and Networks (ICCSN), 2017 IEEE 9th International Conference on*, 2017, pp. 1133-1137.

[75] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in *Big Data and Smart Computing (BigComp), 2017 IEEE International Conference on*, 2017, pp. 313-316.

[76] P. Aggarwal and S. K. Sharma, "Analysis of KDD dataset attributes-class wise for intrusion detection," *Procedia Computer Science,* vol. 57, pp. 842-851, 2015.

[77] 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," in *Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on*, 2016, pp. 258-263.

[78] R. Rahul, T. Anjali, V. K. Menon, and K. Soman, "Deep learning for network flow analysis and malware classification," in *International Symposium on Security in Computing and Communication*, 2017, pp. 226-235.

[79] I. Rosenberg, G. Sicard, and E. O. David, "DeepAPT: nation-state APT attribution using end-to-end deep neural networks," in *International Conference on Artificial Neural Networks*, 2017, pp. 91-99.

[80] T. Vanderbruggen and J. Cavazos, "Large-scale exploration of feature sets and deep learning models to classify malicious applications," in *Resilience Week (RWS), 2017*, 2017, pp. 37-43.

[81] A. Jones and J. Straub, "Using deep learning to detect network intrusions and malware in autonomous robots," in *Cyber Sensing 2017*, 2017, p. 1018505.

[82] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid,* vol. 8, pp. 2505-2516, 2017.

[83] Y. Yu, J. Long, and Z. Cai, "Network intrusion detection through stacking dilated convolutional autoencoders," *Security and Communication Networks,* vol. 2017, 2017.

[84] N. A. s. Networks, "14th Annual Worldwide Infrastructure Security Report," 2019.

[85] E. B. Oleg Kupreev, Alexander Gutnikov, "DDoS attacks in Q4 2019," *Secure list,* 2020.

[86] N. A. s. Network, "NETSCOUT Arbor’s 13th Annual Worldwide Infrastructure Security Report," 2018.

[87] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. J. C. n. Das, "The 1999 DARPA off-line intrusion detection evaluation," vol. 34, pp. 579-595, 2000.

[88] K. J. U. h. w. k. o. k.-c. v. k.-c.-D. Cup, "Data (1999)," 1999.

[89] O. E. Elejla, M. Anbar, B. Belaton, S. J. N. C. Hamouda, and Applications, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," pp. 1-18, 2018.

[90] O. E. Elejla, A. B. JANTAN, A. A. J. J. o. T. AHMED, and A. I. Technology, "THREE LAYERS APPROACH FOR NETWORK SCANNING DETECTION," vol. 70, 2014.

[91] M. W. G. J.-.-h. m. w. a. jp/mawi, "MAWI Working Group traffic archive," ed, 2012.

[92] D. Barrera and P. C. Van Oorschot, "Security visualization tools and IPv6 addresses," in *2009 6th International Workshop on Visualization for Cyber Security*, 2009, pp. 21-26.

[93] C. Team, "The Cooperative Association for Internet Data Analysis," ed: Mar, 2009.

[94] M. D. Gray, "Discovery of IPv6 router interface addresses via heuristic methods," Naval Postgraduate School Monterey United States2015.

[95] M. Fomenkov and K. Claffy, "Internet measurement data management challenges," 2011.

[96] M. Zulkiflee, N. Haniza, S. Shahrin, and M. J. I. R. C. S. Ghani, "A framework of ipv6 network attack dataset construction by using testbed environment," vol. 9, pp. 1434-1441, 2014.

[97] M. Zulkiflee, M. Azmi, S. Ahmad, S. Sahib, and M. J. W. T. C. Ghani, "A framework of features selection for ipv6 network attacks detection," vol. 14, pp. 399-408, 2015.

[98] R. Saad, S. Manickam, E. ALOMARI, M. ANBAR, P. J. J. o. T. SINGH, and A. I. Technology, "DESIGN & DEPLOYMENT OF TESTBED BASED ON ICMPv6 FLOODING ATTACK," vol. 64, 2014.

[99] F. Najjar and M. M. Kadhum, "Reliable behavioral dataset for ipv6 neighbor discovery protocol investigation," in *2015 5th International Conference on IT Convergence and Security (ICITCS)*, 2015, pp. 1-5.

[100] O. E. Elejla, M. Anbar, B. Belaton, S. J. N. C. Hamouda, and Applications, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," vol. 31, pp. 3629-3646, 2019.

[101] M. Tavallaee, N. Stakhanova, A. A. J. I. T. o. S. Ghorbani, Man,, and P. C. Cybernetics, "Toward credible evaluation of anomaly-based intrusion-detection methods," vol. 40, pp. 516-524, 2010.

[102] S. Raghavan and E. Dawson, *An investigation into the detection and mitigation of denial of service (dos) attacks: critical information infrastructure protection*: Springer Science & Business Media, 2011.

[103] S. D. Kotey, E. T. Tchao, and J. D. J. T. Gadze, "On Distributed Denial of Service Current Defense Schemes," vol. 7, p. 19, 2019.

[104] A. Abhishta, R. van Rijswijk-Deij, and L. J. J. A. S. C. C. R. Nieuwenhuis, "Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers," vol. 48, pp. 70-76, 2019.

[105] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in *Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, 2002, pp. 1530-1539.

[106] P. J. Criscuolo, "Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319," California Univ Livermore Radiation Lab2000.

[107] S. Kumar, "Smurf-based distributed denial of service (ddos) attack amplification in internet," in *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, 2007, pp. 25-25.

[108] K. M. Elleithy, D. Blagovic, W. K. Cheng, and P. Sideleau, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison," 2005.

[109] F. O. Catak and A. F. Mustacoglu, "Distributed denial of service attack detection using autoencoder and deep neural networks," *Journal of Intelligent & Fuzzy Systems*, vol. 37, pp. 3969-3979, 2019.

[110] K. He, X. Zhang, S. Ren, and J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," in *Proceedings of the IEEE international conference on computer vision*, 2015, pp. 1026-1034.

[111] S. Ioffe and C. J. a. p. a. Szegedy, "Batch normalization: Accelerating deep network training by reducing internal covariate shift," 2015.

[112] R. Wu, S. Yan, Y. Shan, Q. Dang, and G. J. a. p. a. Sun, "Deep image: Scaling up image recognition," 2015.

[113] Y. Chen, L. Shu, and L. Wang, "Traffic flow prediction with big data: A deep learning based time series model," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, pp. 1010-1011.

[114] G. Hinton, L. Deng, D. Yu, G. Dahl, A.-r. Mohamed, N. Jaitly, *et al.*, "Deep neural networks for acoustic modeling in speech recognition," vol. 29, 2012.

[115] M. Z. Alom, T. M. Taha, C. Yakopcic, S. Westberg, P. Sidike, M. S. Nasrin, *et al.*, "A state-of-the-art survey on deep learning theory and architectures," *Electronics,* vol. 8, p. 292, 2019.

[116] A. Farizawani, M. Puteh, Y. Marina, and A. Rivaie, "A review of artificial neural network learning rule based on multiple variant of conjugate gradient approaches," in *Journal of Physics: Conference Series*, 2020, p. 022040.

[117] I. Aleksander and H. J. T. C. P. Morton, London, "An Introduction to Neural Computing, 1st edn Int," 1995.

[118] J. Zupan and J. Gasteiger, *Neural networks in chemistry and drug design*: John Wiley & Sons, Inc., 1999.

[119] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770-778.

[120] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in neural information processing systems*, 2012, pp. 1097-1105.

[121] K. Simonyan and A. J. a. p. a. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014.

[122] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez*, et al.*, "Attention is all you need," in *Advances in neural information processing systems*, 2017, pp. 5998-6008.

[123] X. He, L. Liao, H. Zhang, L. Nie, X. Hu, and T.-S. Chua, "Neural collaborative filtering," in *Proceedings of the 26th international conference on world wide web*, 2017, pp. 173-182.

[124] Y. J. F. Bengio and t. i. M. Learning, "Learning deep architectures for AI," vol. 2, pp. 1-127, 2009.

[125] D. P. Kingma and J. J. a. p. a. Ba, "Adam: A method for stochastic optimization," 2014.

[126] C. Szegedy, A. Toshev, and D. Erhan, "Deep neural networks for object detection," in *Advances in neural information processing systems*, 2013, pp. 2553-2561.

[127] J. J. N. n. Schmidhuber, "Deep learning in neural networks: An overview," vol. 61, pp. 85-117, 2015.

[128] G. Montavon, W. Samek, and K.-R. J. D. S. P. Müller, "Methods for interpreting and understanding deep neural networks," vol. 73, pp. 1-15, 2018.

[129] C. Szegedy, D. Erhan, and A. T. Toshev, "Object detection using deep neural networks," ed: Google Patents, 2016.

[130] H. Jo, H. Son, H. J. Hwang, and E. J. a. p. a. Kim, "Deep Neural Network Approach to Forward-Inverse Problems," 2019.

[131] H. Wang, Z. Cao, and B. Hong, "A network intrusion detection system based on convolutional neural network," *Journal of Intelligent & Fuzzy Systems,* pp. 1-15, 2019.

[132] Y. Bengio, A. Courville, P. J. I. t. o. p. a. Vincent, and m. intelligence, "Representation learning: A review and new perspectives," vol. 35, pp. 1798-1828, 2013.

[133] Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle, "Greedy layer-wise training of deep networks," in *Advances in neural information processing systems*, 2007, pp. 153-160.

[134] G. E. Hinton, S. Osindero, and Y.-W. J. N. c. Teh, "A fast learning algorithm for deep belief nets," vol. 18, pp. 1527-1554, 2006.

[135] B. Widrow and M. A. J. P. o. t. I. Lehr, "30 years of adaptive neural networks: perceptron, madaline, and backpropagation," vol. 78, pp. 1415-1442, 1990.

[136] L. Wang, Z.-H. You, X. Chen, S.-X. Xia, F. Liu, X. Yan*, et al.*, "A computational-based method for predicting drug–target interactions by using stacked autoencoder deep neural network," *Journal of Computational Biology,* vol. 25, pp. 361-373, 2018.

[137] H. Zhang, J. Hao, and X. Li, "A Method for Deploying Distributed Denial of Service Attack Defense Strategies on Edge Servers Using Reinforcement Learning," *IEEE Access,* vol. 8, pp. 78482-78491, 2020.

[138] K. Amarasinghe, K. Kenney, and M. Manic, "Toward explainable deep neural network based anomaly detection," in *2018 11th International Conference on Human System Interaction (HSI)*, 2018, pp. 311-317.

[139] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in *2018 international joint conference on neural networks (IJCNN)*, 2018, pp. 1-8.

[140] Z. Liu, Y. He, W. Wang, and B. Zhang, "DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN," *China Communications,* vol. 16, pp. 144-155, 2019.

[141] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in iot networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0452-0457.

[142] J. Spaulding and A. Mohaisen, "Defending internet of things against malicious domain names using D-FENS," in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, 2018, pp. 387-392.

[143] D. Chamou, P. Toupas, E. Ketzaki, S. Papadopoulos, K. M. Giannoutakis, A. Drosou*, et al.*, "Intrusion Detection System Based on Network Traffic Using

Deep Neural Networks," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1-6.

[144] N. Chockwanich and V. Visoottiviseth, "Intrusion Detection by Deep Learning with TensorFlow," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 2019, pp. 654-659.

[145] P. Khuphiran, P. Leelaprute, P. Uthayopas, K. Ichikawa, and W. Watanakeesuntorn, "Performance Comparison of Machine Learning Models for DDoS Attacks Detection," in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, 2018, pp. 1-4.

[146] O. Amosov, Y. Ivanov, and S. Amosova, "Recognition of Abnormal Traffic Using Deep Neural Networks and Fuzzy Logic," in *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 2019, pp. 01-05.

[147] U.-J. Baek, S.-H. Ji, J. T. Park, M.-S. Lee, J.-S. Park, and M.-S. Kim, "DDoS Attack Detection on Bitcoin Ecosystem using Deep-Learning," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2019, pp. 1-4.

[148] S. Haider, A. Akhunzada, G. Ahmed, and M. Raza, "Deep Learning based Ensemble Convolutional Neural Network Solution for Distributed Denial of Service Detection in SDNs," in *2019 UK/China Emerging Technologies (UCET)*, 2019, pp. 1-4.

[149] R. Paffenroth and C. Zhou, "Modern Machine Learning for Cyber-defense and Distributed Denial of Service Attacks," *IEEE Engineering Management Review*, 2019.

[150] A. Elsaeidy, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "A Machine Learning Approach for Intrusion Detection in Smart Cities," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019, pp. 1-5.

[151] T. U. Sheikh, H. Rahman, H. S. Al-Qahtani, T. K. Hazra, and N. U. Sheikh, "Countermeasure of Attack Vectors using Signature-Based IDS in IoT Environments," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2019, pp. 1130-1136.

[152] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting iots from mirai botnet attacks using blockchains," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1-6.

[153] A. Abusnaina, A. Khormali, D. Nyang, M. Yuksel, and A. Mohaisen, "Examining the robustness of learning-based ddos detection in software defined networks," in *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, 2019, pp. 1-8.

[154] Q. Niyaz, W. Sun, and A. Y. Javaid, "A deep learning based DDoS detection system in software-defined networking (SDN)," *arXiv preprint arXiv:1611.07400,* 2016.

[155] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," *IEEE Access,* vol. 8, pp. 83765-83781, 2020.

[156] M. H. Haghighat, Z. A. Foroushani, and J. Li, "SAWANT: Smart Window Based Anomaly Detection Using Netflow Traffic," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 2019, pp. 1396-1402.

[157] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K.-K. R. Choo, *et al.*, "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," *Ieee Access,* vol. 8, pp. 53972-53983, 2020.

[158] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," *IEEE Transactions on Network and Service Management,* 2020.

[159] R. A. Shaikh and S. Shashikala, "An Autoencoder and LSTM based Intrusion Detection approach against Denial of service attacks," in *2019 1st International Conference on Advances in Information Technology (ICAIT)*, 2019, pp. 406-410.

[160] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," *IEEE Access,* vol. 8, pp. 77396-77404, 2020.

[161] U. Sabeel, S. S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar, and K. El-Khatib, "Evaluation of Deep Learning in Detecting Unknown Network Attacks," in *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 2019, pp. 1-6.

[162] M. Essaid, D. Kim, S. H. Maeng, S. Park, and H. T. Ju, "A Collaborative DDoS Mitigation Solution Based on Ethereum Smart Contract and RNN-LSTM," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2019, pp. 1-6.

[163] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and V.-L. Nguyen, "An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection," *IEEE Access,* vol. 8, pp. 30387-30399, 2020.

[164] T. V. Phan, S. Sultana, T. G. Nguyen, and T. Bauschert, "$ Q $-TRANSFER: A Novel Framework for Efficient Deep Transfer Learning in Networking," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2020, pp. 146-151.

[165] S. Tariq, S. Lee, H. K. Kim, and S. S. Woo, "CAN-ADF: The Controller Area Network Attack Detection Framework," *Computers & Security,* p. 101857, 2020.

[166] Y. Yu and N. Bian, "An Intrusion Detection Method Using Few-Shot Learning," *IEEE Access,* vol. 8, pp. 49730-49740, 2020.

[167] L. Wang and Y. Liu, "A DDoS Attack Detection Method Based on Information Entropy and Deep Learning in SDN," in *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2020, pp. 1084-1088.

[168] R.-H. Hwang, M.-C. Peng, and C.-W. Huang, "Detecting IoT Malicious Traffic based on Autoencoder and Convolutional Neural Network," in *2019 IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1-6.

[169] M. Roopak, G. Y. Tian, and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 0562-0567.

[170] M. S. Yadav and R. Kalpana, "Data Preprocessing for Intrusion Detection System Using Encoding and Normalization Approaches," in *2019 11th International Conference on Advanced Computing (ICoAC)*, 2019, pp. 265-269.

[171] A. Telikani and A. H. Gandomi, "Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of Things," *Internet of Things*, p. 100122, 2019.

[172] X. Liang and T. Znati, "A Long Short-Term Memory Enabled Framework for DDoS Detection," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1-6.

[173] Z. Shi, J. Li, and C. Wu, "DeepDDoS: Online DDoS Attack Detection," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1-6.

[174] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," *IEEE Access,* vol. 7, pp. 154560-154571, 2019.

[175] K. Yang, J. Zhang, Y. Xu, and J. Chao, "DDoS Attacks Detection with AutoEncoder," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, 2020, pp. 1-9.

[176] O. Amosov, S. Amosova, Y. Ivanov, and S. Zhiganov, "The Use of Deep Neural Networks to Recognize Network Traffic Abnormalities in Enterprise Information and Telecommunication Systems," in *2019 Twelfth International Conference" Management of large-scale system development"(MLSD)*, 2019, pp. 1-5.

[177] A. Thantharate, R. Paropkari, V. Walunj, C. Beard, and P. Kankariya, "Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 0852-0857.

[178] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network," *IEEE Access,* vol. 8, pp. 89337-89350, 2020.

[179] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," in *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, pp. 1-6.

[180] F. Liu, W. Huo, Y. Han, S. Yang, and X. Li, "Study on Network Security Based on PCA and BP Neural Network Under Green Communication," *IEEE Access,* vol. 8, pp. 53733-53749, 2020.

[181] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems,* 2020.

[182] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications,* vol. 21, p. 100198, 2020.

[183] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Computers & Security,* vol. 92, p. 101752, 2020.

[184] S. M. Kasongo and Y. Sun, "A Deep Long Short-Term Memory based classifier for Wireless Intrusion Detection System," *ICT Express,* 2019.

[185] N. Chouhan and A. Khan, "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network," *Applied Soft Computing,* vol. 83, p. 105612, 2019.

[186] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks,* vol. 90, p. 101842, 2019.

[187] D. Sovilj, P. Budnarain, S. Sanner, G. Salmon, and M. Rao, "A Comparative Evaluation of Unsupervised Deep Architectures for Intrusion Detection in Sequential Data Streams," *Expert Systems with Applications,* p. 113577, 2020.

[188] S. M. Kasongo and Y. Sun, "A Deep Gated Recurrent Unit based model for wireless intrusion detection system," *ICT Express,* 2020.

[189] A. Abusitta, M. Bellaiche, M. Dagenais, and T. Halabi, "A deep learning approach for proactive multi-cloud cooperative intrusion detection system," *Future Generation Computer Systems,* vol. 98, pp. 308-318, 2019.

[190] Z. Wu, J. Wang, L. Hu, Z. Zhang, and H. Wu, "A network intrusion detection method based on semantic Re-encoding and deep learning," *Journal of Network and Computer Applications,* p. 102688, 2020.

[191] A. Ayodeji, Y.-k. Liu, N. Chao, and L.-q. Yang, "A new perspective towards the development of robust data-driven intrusion detection for industrial control systems," *Nuclear Engineering and Technology,* 2020.

[192] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," *Journal of King Saud University-Computer and Information Sciences,* 2019.

[193] F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, "Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device," *Ad Hoc Networks,* vol. 84, pp. 82-89, 2019.

[194] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT," *Procedia Computer Science,* vol. 167, pp. 1561-1573, 2020.

[195] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, "An Effective Convolutional Neural Network Based on SMOTE and Gaussian Mixture Model for Intrusion Detection in Imbalanced Dataset," *Computer Networks,* p. 107315, 2020.

[196] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing,* vol. 387, pp. 51-62, 2020.

[197] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *Journal of Network and Computer Applications,* vol. 143, pp. 167-177, 2019.

[198] M. Z. Hasan, K. Z. Hasan, and A. Sattar, "Burst header packet flood detection in optical burst switching network using deep learning model," *Procedia computer science,* vol. 143, pp. 970-977, 2018.

[199] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: Towards secure IoT architecture," *Internet of Things,* vol. 3, pp. 82-89, 2018.

[200] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory,* p. 102031, 2019.

[201] P. Wang, L. T. Yang, X. Nie, Z. Ren, J. Li, and L. Kuang, "Data-driven software defined network attack detection: State-of-the-art and perspectives," *Information Sciences,* vol. 513, pp. 65-83, 2020.

[202] B. Bouyeddou, B. Kadri, F. Harrou, and Y. Sun, "DDOS-attacks detection using an efficient measurement-based statistical mechanism," *Engineering Science and Technology, an International Journal,* 2020.

[203] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of Network and Computer Applications,* p. 102662, 2020.

[204] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. Augusto-Gonzalez, and M. Ramos, "Deep learning with dense random neural networks for detecting attacks against iot-connected home environments," in *International ISCIS Security Workshop*, 2018, pp. 79-89.

[205] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things," *Internet of Things,* p. 100112, 2019.

[206] B. A. NG and S. Selvakumar, "Deep radial intelligence with cumulative incarnation approach for detecting denial of service attacks," *Neurocomputing,* vol. 340, pp. 294-308, 2019.

[207] N. Sameera and M. Shashi, "Deep transductive transfer learning framework for zero-day attack detection," *ICT Express,* 2020.

[208] Y. Li, Y. Xu, Z. Liu, H. Hou, Y. Zheng, Y. Xin, *et al.*, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement,* vol. 154, p. 107450, 2020.

[209] Y. Li, P. Zhang, and L. Ma, "Denial of service attack and defense method on load frequency control system," *Journal of the Franklin Institute,* vol. 356, pp. 8625-8645, 2019.

[210] M. Asadi, M. A. J. Jamali, S. Parsa, and V. Majidnezhad, "Detecting botnet by using particle swarm optimization algorithm based on voting system," *Future Generation Computer Systems,* vol. 107, pp. 95-111, 2020.

[211] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. Narayan, "Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud," *Procedia Computer Science,* vol. 167, pp. 2297-2307, 2020.

[212] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," *Computer Networks,* vol. 168, p. 107042, 2020.

[213] P. Bedi, N. Gupta, and V. Jindal, "Siam-IDS: Handling class imbalance problem in Intrusion Detection Systems using Siamese Neural Network," *Procedia Computer Science,* vol. 171, pp. 780-789, 2020.

[214] S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms," *Future Generation Computer Systems,* 2020.

[215] Y. Zhong, W. Chen, Z. Wang, Y. Chen, K. Wang, Y. Li, *et al.*, "HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning," *Computer Networks,* vol. 169, p. 107049, 2020.

[216] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," *Journal of Network and Computer Applications,* vol. 136, pp. 71-85, 2019.

[217] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation," *Computer Networks,* vol. 160, pp. 165-191, 2019.

[218] A.-H. Muna, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of Information Security and Applications,* vol. 41, pp. 1-11, 2018.

[219] T. A. S. Srinivas and S. Manivannan, "Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm," *Computer Communications,* 2020.

[220] A. S. Almogren, "Intrusion detection in Edge-of-Things computing," *Journal of Parallel and Distributed Computing,* vol. 137, pp. 259-265, 2020.

[221] V. Bartos, M. Zadnik, S. M. Habib, and E. Vasilomanolakis, "Network entity characterization and attack prediction," *Future Generation Computer Systems,* vol. 97, pp. 674-686, 2019.

[222] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems,* 2019.

[223] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems,* vol. 100, pp. 779-796, 2019.

[224] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge," *IEEE Transactions on Network and Service Management,* vol. 17, pp. 45-59, 2020.

[225] Y. Xu, Z. Liu, Y. Li, H. Hou, Y. Cao, Y. Zhao, *et al.*, "Feature data processing: Making medical data fit deep neural networks," *Future Generation Computer Systems,* 2020.

[226] S. Revathi and A. Malathi, "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection," *International Journal of Engineering Research & Technology (IJERT),* vol. 2, pp. 1848-1853, 2013.

[227] M. Gharaibeh and C. Papadopoulos, "Darpa-2009 intrusion detection dataset report," *Tech. Rep.,* 2014.

[228] W. M. WorkingGroup, "Mawi working group traffic archive," ed, 2013.

[229] J. CAIDA and A. U. Agreement, "The cooperative association for internet data analysis," *measurement,* 2003.

[230] M. Zulkiflee, M. Azmi, S. Ahmad, S. Sahib, and M. Ghani, "A framework of features selection for ipv6 network attacks detection," *WSEAS Trans Commun,* vol. 14, pp. 399-408, 2015.

[231] R. Saad, S. Manickam, E. ALOMARI, M. ANBAR, and P. SINGH, "DESIGN & DEPLOYMENT OF TESTBED BASED ON ICMPv6 FLOODING ATTACK," *Journal of Theoretical & Applied Information Technology,* vol. 64, 2014.

[232] O. E. Elejla, M. Anbar, B. Belaton, and S. Hamouda, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," *Neural Computing and Applications,* vol. 31, pp. 3629-3646, 2019.

[233] T. Van Hauser, "Attacking the IPv6 protocol suite," ed, 2006.

[234] B. R. Patil, M. Moharir, P. K. Mohanty, G. Shobha, and S. Sajeev, "Ostinato-A Powerful Traffic Generator," in *2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, 2017, pp. 1-5.

[235] A. Singh, *Instant Wireshark Starter*: Packt Publishing Ltd, 2013.

[236] A. Orebaugh, G. Ramirez, and J. Beale, *Wireshark & Ethereal network protocol analyzer toolkit*: Elsevier, 2006.

[237] S. Kumarasamy and A. Gowrishankar, "An active defense mechanism for TCP SYN flooding attacks," *arXiv preprint arXiv:1201.2103,* 2012.

[238] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," ed: RFC 2461, December, 1998.

[239] A. H. NasserElDeen, "ICMPv6 Router Advertisement Flooding."

[240] J. N. Goel and B. Mehtre, "Dynamic IPv6 activation based defense for IPv6 router advertisement flooding (DoS) attack," in *2014 IEEE International Conference on Computational Intelligence and Computing Research*, 2014, pp. 1-5.

[241] J. Yang and G. Yang, "Modified convolutional neural network based on dropout and the stochastic gradient descent optimizer," *Algorithms,* vol. 11, p. 28, 2018.

[242] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, "Inception-v4, inception-resnet and the impact of residual connections on learning," in *Thirty-first AAAI conference on artificial intelligence*, 2017.

[243] C. Nwankpa, W. Ijomah, A. Gachagan, and S. Marshall, "Activation functions: Comparison of trends in practice and research for deep learning," *arXiv preprint arXiv:1811.03378,* 2018.

[244] J. Duchi, E. Hazan, and Y. J. J. o. m. l. r. Singer, "Adaptive subgradient methods for online learning and stochastic optimization," vol. 12, pp. 2121-2159, 2011.

[245] T. Tieleman and G. J. C. N. n. f. m. l. Hinton, "Lecture 6.5-rmsprop: Divide the gradient by a running average of its recent magnitude," vol. 4, pp. 26-31, 2012.

[246] P. Ramachandran, B. Zoph, and Q. Le, "Searching for activation functions. arXiv 2017," *arXiv preprint arXiv:1710.05941*.

[247] S. I. Collaboration, "Machine Learning and Health Care Disparities in Dermatology," 2018.

[248] M. D. Zeiler, M. Ranzato, R. Monga, M. Mao, K. Yang, Q. V. Le*, et al.*, "On rectified linear units for speech processing," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 3517-3521.

[249] G. E. Dahl, T. N. Sainath, and G. E. Hinton, "Improving deep neural networks for LVCSR using rectified linear units and dropout," in *2013 IEEE international conference on acoustics, speech and signal processing*, 2013, pp. 8609-8613.

[250] G. Perin and S. Picek, "On the Influence of Optimizers in Deep Learning-based Side-channel Analysis," Cryptology ePrint Archive, Report 2020/977, 2020. https://eprint. iacr. org ….

[251] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Communications of the ACM,* vol. 60, pp. 84-90, 2017.

[252] V. Badrinarayanan, A. Kendall, and R. Cipolla, "Segnet: A deep convolutional encoder-decoder architecture for image segmentation," *IEEE transactions on pattern analysis and machine intelligence,* vol. 39, pp. 2481-2495, 2017.

[253] M. Lin, Q. Chen, and S. Yan, "Network in network," *arXiv preprint arXiv:1312.4400,* 2013.

[254] Y. Wang, Y. Li, Y. Song, and X. Rong, "The influence of the activation function in a convolution neural network model of facial expression recognition," *Applied Sciences,* vol. 10, p. 1897, 2020.

[255] B. Yu, L. Xie, and F. Wang, "An Improved Deep Convolutional Neural Network to Predict Airfoil Lift Coefficient," in *Proceedings of the International Conference on Aerospace System Science and Engineering 2019*, 2020, pp. 275-286.

[256] W. McKinney, "Data structures for statistical computing in python," in *Proceedings of the 9th Python in Science Conference*, 2010, pp. 51-56.

[257] S. Van Der Walt, S. C. Colbert, G. J. C. i. S. Varoquaux, and Engineering, "The NumPy array: a structure for efficient numerical computation," vol. 13, p. 22, 2011.