

Intrusion Detection System for Wireless Sensor Networks using Computational Intelligence Techniques

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Computer Science and Engineering

By

Vaishnavi Sivagaminathan

Registration Number: 41900547

Supervised By

Dr. Manmohan Sharma

Professor, Networks Domain

School of Computer Application

Lovely Professional University

Co-Supervised by

Dr. Santosh Kumar Henge

Associate Professor

Department of Computer Applications

Manipal University

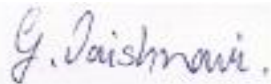


Transforming Education Transforming India

LOVELY PROFESSIONAL UNIVERSITY, PUNJAB
2024

DECLARATION

I, hereby declare that the presented work in the thesis entitled “Intrusion Detection System For Wireless Sensor Networks using Computational Intelligence Techniques” in fulfillment of degree of **Doctor of Philosophy (Ph.D.)** is outcome of research work carried out by me under the supervision **Dr. Manmohan Sharma** working as **Professor**, Networks Domain, School of Computer Application, Lovely Professional University, Punjab, India. In keeping with general practice of reporting scientific observations, due acknowledgments have been made whenever work described here has been based on findings of other investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.



(Signature of Research Scholar)

Name of the scholar: **Vaishnavi Sivagaminathan**

Registration No.: **41900547**

Department/school: **Department of Computer Science and Engineering**

Lovely Professional University,

Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled “Intrusion Detection System For Wireless Sensor Networks using Computational Intelligence Techniques” submitted in fulfillment of the requirement for the reward of degree of **Doctor of Philosophy (Ph.D.)** in the **Computer Science & Engineering** is a research work carried out By **Mrs. Vaishnavi Sivagaminathan, 41900547** is bonafide record of her original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.



(Signature of Supervisor)

Name of supervisor: **Dr. Manmohan Sharma**

Designation: **Professor**

Department/school: **Networks Domain, School of Computer Application**

University: **Lovely Professional University, Punjab, India**



(Signature of Co-supervisor)

Name of Co-supervisor: **Dr. Santosh Kumar Henge**

Designation: **Associate Professor**

Department/school: **Department of Computer Application**

University: **Manipal University, Rajasthan, India**

Acknowledgments

First and foremost, on the successful completion of the research work and this thesis, I would like to pay all praise to the almighty God. In this thesis the work presented would not have been possible without my close association with many people. With utmost humbleness, I would like to take this opportunity to extend my deep sense of gratitude to all those who made this research thesis possible. First and foremost, I am indebted to my supervisor Dr. Manmohan Sharma working as Professor in the Department of Computer Science and Application of Lovely Professional University, Punjab, India, for his dedicated support, timely advice, inspiration, encouragement, and continuous support throughout my Ph.D. I am grateful to my family who always inspired me to do this work. Their affection and love can't be expressed in words. As always it is not possible to mention everybody who had a constructive impact on this work, directly and indirectly, however, there are those whose support is even more important, and I extend my thanks to all those peoples.

Vaishnavi Sivagaminathan

Abstract:

Systems for detecting network intrusions are being used to spot malicious activity on networks. A lot of effort is required to do this by examining traffic network activities using Network Intrusion Detection Systems (NIDS). To discover abnormalities, the NIDS largely relies on machine learning (ML) and data mining techniques. The efficiency of NIDS is greatly improved in terms of feature selection. This is true since a variety of time-consuming attributes are used in anomaly identification. As a result, the feature selection approach affects how long it takes to examine movement patterns and increase the level of clarity. The goal of the study is to offer NIDS with an attribute selection approach. The underlying principles of this notion include Grey wolf improvement, firefly enhancement, particle swarm enhancement, and evolutionary methods. The suggested paradigm seeks to make NIDS more user-friendly. The proposed model manages the mutual knowledge, which was built using 13 sets of rules using the GA, PSO, GWO, and FFA algorithms and employing wrapper-based spam detection techniques. The performance parameters of the proposed model were evaluated using Anaconda software. In light of the UNSW-NB15 datasets, support vector machines, J48 ML classifiers, as well as features produced from the proposed model, are assessed. Rule13 reduces the characteristics, using the experiment as a guide, to 30 components. Under Rule 12, the attributes are reduced to 13 aspects a guide, to 30 components. Under Rule 12, the attributes are reduced to 13 aspects. The best findings are obtained when examining effectiveness, clarity, and F-measure using Rules 13 and 12. The genetic algorithm (GA) produced a favourable failed negative rate (FNR), as well as true positive rate. Despite PSO's superior accuracy and True Negative Rate, Rules 11, 9, and 8 perform well with relation to False Positive Rate and True Negative Rate. A technique for finding intrusions was shown to be more accurate with fewer characteristics. The Symmetry magazine addresses the attribute selection approach for NIDS to discover computer and network assault patterns that follow rules. Any harmful behaviour or illegal activities would be recognized by the intrusion detection system in the network to protect the customers' huge confidential data from being hacked, and thus the system will prove to be beneficial to society. In Cisco Packet Tracer, the simulations was conducted using three computers, one DNS server, one DHCP server, two mobiles, two routers, and two switches. The simulation were put to the test using a dynamic IP setup, with Cisco training datasets used to produce the source and destination IP addresses.

Wireshark's data environment was used to replicate this IOT network architecture in order to get real-time packet, protocol, time, and IP datasets during a 10-minute interval. For the particle time data, a set of seven protocols were tried on a framework of reasoning for the training method was devised. A training method is provided in this study, that takes the form of an algorithm to replicate or initialize the first iteration of model construction. The study on network datasets demonstrates the originality of the method used to generate the first model for the creation of fuzzy logic or neural network logic. As part of the acquiring knowledge for simple simulation of an intelligent computer strategy. Rest of the study is based on the simulation of various infiltration tactics. This project will use a group of communication methods in relation to system architecture as the core paradigm for all machine learning. The extensive usage of computer system interconnection and interoperability has become an unavoidable requirement for enhancing the daily operations. Simultaneously, it opens the door for automation where human control will not play any important role, and to avoid the security threats, there is a necessity of high end security protocols. Deep learning architectures have been proven as a method to categorize the network threats and to identify intrusions with greater accuracy.

Consequently main aim among the suggested deep learning network will be understand the daily network intrusion, adapts to automation learning from daily data, reduce the risk of intrusion with eradication of any intruder anomaly. Using the UNSW-NB15 datasets, show a figure's performance, which reflects the working network communication behavior along with artificially produced attack operations. Given the task of ensuring computer hackers has grown increasingly challenging due to the concerning increase in technology connectivity and the availability of desktop apps. A highly secured system is also necessary to protect it from various threats. Finding irregularities and risks in such system security protocols helps with data security. Artificial intelligence in particular is a subset represented by ML techniques (AI). A useful solution was developed utilizing pro technologies powered by information. This study investigated two distinct intrusion detection (ID) categorization reaches, every having its own particular range of useful situations. Prior to using the two techniques for categorization, multiplicity was decreased using the particle swarm optimization approach. In this study, categorization criteria used to describe network anomalies were examined. Three classifiers are used: PSO plus ANN, PSO + K - nearest neighbors and PSO plus Selection

Tree. Using 99 datasets, the foundation's information retrieval techniques identified and verified its findings. The following measures, such as recall, support provided, correctness, reliability, and consistency were utilised to check computer hacker's records for cybercrime. To determine which performs better, the precision, comparisons of the two involved response times (DR) and totally fabricated rates were also made (FPR).The existing IDS was then compared to the proposed solution. The findings show that PSO+ANN works better at networks currently abnormalities than PSO+KNN and PSO+DT classification approaches.

List of Figures

Content	Page No.
Figure 1.1: Types of wireless attacks	20
Figure 1.2: Recognition of anomalies according to class	25
Figure 3.1: Showing the test network architecture in cisco packet tracer	43
Figure 3.2: Shows the whole work flow for collection of data for any network simulation model	43
Figure 4.1: Multiclass classification model learning curve accuracy	52
Figure 4.2: Types of attacks vs Detection rate	52
Figure 4.3: Multiclass classification model learning curve accuracy	53
Figure 4.4: Types of attack vs detection rate	53
Figure 5.1: Conceptual System Block Flow	57
Figure 5.2: Working of Improved IDS SYSTEM	58
Figure 5.3: Proposed PSO integration with ML models	62
Figure 6.1: Phases involved in a Machine Learning Application	64
Figure 6.2: IoT environment threat dimensions	68
Figure 6.3: The architectural of the suggested paradigm.	70
Figure 6.4: Wolves' hierarchy	72
Figure 6.5: UNSW-NB15 testbed	78
Figure 8.1: - Shows protocols vs (192.168.239.1) Source IP	89
Figure 8.2: Shows protocols vs (192.168.239.254) Source IP	89
Figure 8.3: Shows protocols vs (fe80: f9fc:ad11:1e14: b75) source IP	90
Figure 8.4: Shows protocols vs (VMware_c0:00:08) source IP	90
Figure 8.5: Shows protocols vs (VMware_fc:23: ae) source Ip	91
Figure 8.6: Shows protocols vs (192.168.239.255) destination IP	91
Figure 8.7: Shows protocols vs (224.0.0.22) destination IP	92
Figure 8.8: Shows protocols vs (224.0.0.251) destination IP	92
Figure 8.9: Shows protocols vs (224.0.0.252) destination IP	93
Figure 8.10: Shows protocols vs (239.255.255.250) destination IP	93
Figure 8.11: Shows protocols vs (Broadcast) destination IP	94
Figure 8.12: Shows protocols vs (ff02: 1:3) destination IP	94

Figure 8.13: Shows protocols vs (ff02::16) destination IP	95
Figure 8.14: Shows protocols vs (ff02::fb) destination IP	95
Figure 8.15: True Positive Rate (TPR).	102
Figure 8.16: False Negative Rate (FNR).	103
Figure 8.17: False Positive Rate (FPR).	103
Figure 8.18: True Negative Rate (TNR).	104
Figure 8.19: Accuracy.	104
Figure 8.20: The accuracy rate.	105
Figure 8.21: The sensitivity rates.	106
Figure 8.22: The F-measure rate.	106
Figure 8.23: showing the test network architecture in Cisco packet tracer	107
Figure 8.24: Shows protocols vs (ff02: 1:3) destination IP	108
Figure 8.25: Shows protocols vs (192.168.239.1) Source IP	109
Figure 8.26: Creation of Wireless Sensor Networks consisting of nodes in NS2	110
Figure 8.27: A Physical Network Created consisting of Laptop, Mobile and 5 Node MCUs	111
Figure 8.28: Block Diagram of the Proposed System	112

List of Tables

Content	Page No.
Table 1.1: (a) Using Decision Trees Algorithm	21
Table 1.2: (b) Using Decision Trees Algorithm	22
Table 1.3: (c) Using Decision Trees Algorithm	23
Table 5.1: Testing and training instances	56
Table 5.2: Showing the proposed algorithm	62
Table 6.1: The proposed model's guidelines.	75
Table 6.2: Characteristics Listed in the UNSW-NB15 Dataset.	80
Table 6.3: Confusion matrix.	81
Table 8.1: Shows the Source, Destination and Protocol dataset with respect to our test environment of network topology as shown in fig 1.1	89
Table 8.2: The Cast of Confusion for oddity with Regular intensity.	96
Table 8.3: Types of Network Traffic	97
Table 8.4: Matrix of confusion for PSO+DT classifier	97
Table 8.5: PSO+KNN uncertainty cast	97
Table 8.6: Measures of Efficiency of Suggested Classifications	98
Table 8.7: Evaluation of proposed classifiers	98
Table 8.8: Comparative evaluation of the current system	99
Table 8.9: Important selected features.	100
Table 8.10: The conclusions drawn from J48.	101
Table 8.11: The conclusions drawn using SVM.	101
Table 8.12: showing Source, Destination and Protocol Dataset with respect to our test environment of network topology as shown in fig 9.23	109
Table 8.13: Proposed classifiers evaluation	112
Table 8.14: Comparative analysis with existing system	113

List of Research Publications

1. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2020) "Intrusion Detection and Prevention Systems: A Review", Inventive Communication and Computational Technologies, 2020 **Scopus.**

(Published)

2. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2021) "Dynamic Communication Protocol modelling for Intrusion traces using Cisco Packet Tracer integration with Wireshark", IJRDO -International Journal of Research & Development Organisation Design Engineering, Toronto, 2021

Scopus. (Published)

3. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2023) "Intrusion Detection System for Wireless Sensor Networks using Computational Intelligence Techniques", Cybersecurity, 2023 **Scopus.**

(Published)

4. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2023) "Integration of Deep Neural Network Architecture for Network Intrusion Detection System", International Conference on Recent Advances in Computing Sciences, 2023

Scopus. (Published)

5. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2023) "Intrusion Detection System for Wireless Sensor Networks using Particle Swarm Optimization Integrated with Machine Learning Algorithms", International Conference on Materials Science and Sustainable Manufacturing Technology (ICMSSMT), 2023

(Presented)

6. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2023) "Intrusion Detection System for Wireless Networks Using PSO with ML Algorithms (Copyright)", Copyright Office, Govt. of India, 2023

(Published)

7. Vaishnavi Sivagaminathan, Dr. Manmohan Sharma (2023) "Integration of Secure Blades through Particle Swarm Optimization and Decision Trees for Analyzing External Attacks in Intrusion Detection Systems", Journal of Discrete Mathematical Sciences and Cryptography, 2023

(Communicated)

Table of Contents

Content	Page No.
Abstract	
Chapter-1: Introduction.....	13
1.1 Types of Intrusion Detection Systems.....	18
1.2 Types of Attacks in a network.....	19
1.3 Types of Networks.....	20
1.4 Machine Learning Techniques useful for Intrusion Detection and Prevention System are.....	20
1.5 Objectives of the proposed work.....	27
1.6 Thesis Organization.....	27
Chapter-2: Literature Review.....	29
2.1 Previous work done.....	35
Chapter-3: Methodology.....	38
3.1 IDPS Based Network system.....	39
3.1.1 Wireless IDPS.....	40
3.2 Proposed Methodology.....	42
3.3 Proposed Algorithm.....	43
Chapter-4: Implementing a Network Intrusion Detection System using a Deep Neural Network Architecture.....	46
4.1 DoS attack.....	47
4.2 Control Area Network (CAN).....	47
4.3 IDPS.....	48
4.4 Intrusion Prevention System (IPS).....	48
4.5 NIDS.....	46
4.6 SSIDS.....	49
4.7 Technology Limitations.....	50
4.8 Security Capabilities.....	51
4.9 Data-set.....	51
A. UNSW-NB15 datasets used for model testing for pre-partitioned.....	51

B. UNSW-NB15 datasets used for Model testing for user define.....	52
 Chapter-5: PSO Integration with ML Models.....	54
5.1 Resources and Techniques.....	55
5.1.1 Dataset Description.....	55
5.1.2 Classification Methodologies.....	55
5.1.3 Proposed System.....	56
5.1.4 Proposed Algorithm.....	58
Chapter-6: Systems for Detecting Network Intrusions (NIDS).....	63
6.1 Companion Works.....	64
6.2 The Proposed Model.....	69
6.2.1 The Pre-Processing Stage.....	69
6.3 The Choice of Characteristics Applying Metaheuristic techniques influenced by biology.....	71
6.3.1 Selection of GA Features.....	71
6.3.2 Selection of PSO Features.....	71
6.3.3 Choosing GWO Features.....	72
6.3.4 Selection of FFA Features.....	73
6.4 The Model for Feature Selection using ML.....	73
6.5 Classifiers Using ML.....	74
6.5.1 Classifier SVM.....	74
6.5.2 Classifier (C4.5 Logic Tree) J48, 3.4.2.....	75
6.6 System Model: Pre-Processing.....	75
6.6.1 Data Cleaning and Normalization.....	76
6.7 Dataset Overview.....	77
6.8 Measures for Present Assessment.....	80
 Chapter-7: Proposed System for Wireless Network Intrusion Detection and Prevention.....	82
7.1 Proposed Methodology.....	83
 Chapter 8: Comparison of Results with Discussions.....	86
8.1 Intrusion Protocols Results.....	87

8.1.1 Initialization Step.....	87
8.1.2 Result.....	88
8.2 Performance Evaluation (PSO).....	96
8.3 Selection Keyword Research Results.....	99
8.3.1 Findings of the Practical Assessment.....	100
8.4 Cisco packet tracer Results and Discussions.....	107
 Chapter 9: Conclusion.....	 114
References.....	118

Chapter-1

Introduction

Chapter 1

Introduction

Now a days intrusion is in every field wherever networking is involved. For improving computer security and for detecting dangers and anomalies, machine learning techniques, more especially artificial intelligence (AI) technology, were used to develop a meaningful data system for preventing intrusions. Cyberspace has altered the world in the areas of contract, social contact, information sources, and economics, to mention a very few. It had a big impact on how quickly the economies of different countries developed as well as how many people used network services [1]. Nevertheless, the complexity of data protection, which is developing daily [2, 3], is inexorably tied to the rise of internet accessible. Data centers are becoming more proficient every day as an outcome of their great success. Although efforts at penetration may be detected and protections may be present, it is still possible to lessen the effect of an attack on the network. However, security management vulnerability avoidance now seems to be unattainable [4, 5]. When it becomes evident that invasion preventative measures like antivirus programs, entrance controls, and cryptography, to mention a few, are inadequate to combat the danger presented by web applications and high security, IDS is crucial. It is crucial to emphasize the significance of Intrusion detection system core design terms for efficacy and evaluation. Employing pattern identification methods like Bayesian Network (NB) and ANN requires a thorough understanding of ML as a sub field of AI. [6].

A sophisticated IDS technique, like centralized component protection, is something that AI strives to deliver, with a bonus layer, such as defence, using machine learning techniques. Researchers can monitor network connections and hunt for indicators of penetration using this infiltration (ID) approach. It has used a number of vulnerability scanning datasets over the past three decades, the Information retrieval from records, Kdd data set collections, in particular, to analyse overall system progress for identifying intrusions. The progression via Machine learning approaches include k-means, groups, K - nearest neighbors [2, 3], Bayesian network, neural networks , and neural network. Which are now being used on these collections. Without being explicitly programmed, a robot can use ML to learn from

experience and enhance its automated abilities [8]. IDS employs ML algorithms because they are capable of accurately and quickly identifying attacks in massive volumes of data.

Assault by Man in the Middle (MITM), Attacks including services interruption, sinkhole assault, floods attacks, wormhole attacks and selectively redirection are only a few examples.

DoS attacks include flooding a network's server with phoney messages in order to generate bottleneck in the network, preventing genuine traffic from reaching the server. This is especially true in the realm of big shopping website or aggregator website. A site's servers can be purposefully overburdened by false packets from a rival site. Is it also important to identify and prevent intrusions [9].

Wireless sensor networks are a growing field, intrusion detection is also required. Agriculture, industry, roadway construction, transportation networks, military, communication, and medical and health professions all use WSNs. Watching patients' movement, monitoring their whereabouts, and monitoring elderly patients are all examples of medical applications [10]. This research aims to provide an overview of IDPS technology. It describes the primary roles of IDPS technology as well as the detection methods they employ. It then goes through the most critical features of each of the primary IDPS technology classes. The study also goes over several types of IDPS security capabilities, as well as technological constraints and obstacles.

Cyber crime has risen significantly on account of fast technical progress also the global expansion the web networks. In 2015, Crypto-ransomware was one of 362 new malware types discovered by the Internet Security Threat Report (ISTR). In 2018, cyber crime is projected to have generated 1.5 trillion dollars in revenue. If there is one obvious conclusion in 2019, it is that no business, big or little, is immune to a cyber attack. Cyber attacks have never been more sophisticated, evasive, or targeted. [11]. As a result, new security methods must be created on a regular basis.

An important component of privacy is a host - based intrusion detection device, as It can recognize invasions and alerts would be the proper authorities. We may divide IDS into two categories depending on detection methods: [12]:

- Anomaly Based IDS: When an anomaly is detected, the user is alerted to the possibility of a network intrusion because it develops a database of typical activities.
- Misuse Based Detection: This describes the database's assault activity and when many possibilities exist in a network, they are referred to as assaults.

When the number of cyber-crime kinds grows, a mechanism for detecting anomalies outperforms the method for detecting abuse in terms of constructing a breach in the network detection method. A program which detects anomalies was more suited to detecting unknown assaults.

Several Algorithms for artificial intelligence (AI) created as the abuse detecting anomalies and detecting them systems. Principle approaches, Data mining and machine learning are examples of initiate methods besides implementing such IDSs. The first foundation is data mining that has been presented for the construction of IDS. Information may be extracted from a big database by using data mining techniques. A knowledge base may be mined to find patterns that can be used to anticipate future incursions in connected dataset. [13]

Although most rule-based IDS have their advantages, they can have their drawbacks as well. Due to the fact that these signatures are not in their knowledge base, they cannot recognize fresh assaults that use updated comments. To address these constraints, deep learning methods had proposed. Within deep learning, DNN is one of the most commonly used algorithms.

DNNs possess a appealing fundamental detecting of intrusions feature known as instruction by experience, that enables them to infer fresh knowledge and make decisions. This differentiates DNNs from all other programming methods and turns it into an expert system. [13]

ML is employed to create an IDS for this investigation. As a consequence, the usual and abnormal behaviors of a network system are classified using a tractor trailer supervised learning [14]. Machine learning techniques were evaluated using the Knowledge discovery 99 collection, and the results show exceptional performance in recognizing anomalies, particularly Neptune and the Smurf aberrations. Using co-

variance sensor data, the overall effectiveness of the anticipated with IDS was evaluated in a similar way.

The remainder of the essay is separated into the following sections: The evaluation of the existing empirical approach is the main goal of this section. The material, along with the databases and procedures utilized to carry out this study, was addressed in Section 3 [15, 16]. The observations obtained during the technology installation as well as the conclusions reached were covered in Section 4. For the study, Section 5 came to a conclusion. Here, more research is suggested.

Everywhere communication is engaged in the globe, infiltration is a concern. Examples are in home area networks, in E-Commerce, Internet of Things, wireless sensor networks, wifi networks of big organizations etc. Secure storage of sensitive data across several databases is essential. That is to protect data like pan numbers, date of birth, Aadhar card numbers etc. related to customers seems to be of prime significance. Thus the Devices for vulnerability scanning are required. Not only Intrusion detection but also Intrusion preventive techniques are required.

Assault can take many different forms, including Man in the Middle attacks, or attack of services (MITM), Hole in the ground, Selected Filtering, Flooding, Wormhole, etc. DoS attacks include flooding a server with fictitious messages to clog the network and prevent real traffic from getting to the host. This specifically occurs in the sphere of e-commerce. The opposite site may deliberately overload a site's server with fake traffic. So is identification of intrusions and Prevention required [17].

In the same vein, intrusion detection is essential in wireless sensing networking as a sector. WSNs are found in all fields such industrial, agriculture, roadways development, traffic networks, defense, telecoms, healthcare, and medicinal areas. In the medical fields, such as monitoring and tracing the whereabouts of patients, keeping tabs on older patients [18].

A few IPDS systems the following have emerged in a variety of fields:-

- a. A network intrusion detection system (IDPS) that contrasts its efficiency with Snort, a widely used NIDS tool, was previously published. All Snort regulations in the conceptual model use prefixed and random addressing

approaches, and primary patterns are developed to decrease packet sniffer time and detection rate even during periods of intense network activity. [19].

- b. The Synchrophasor Specific A tool called Network Security Systems is used to spot malicious attacks in synchrophasor devices. This programme utilises a behaviour-based approach and heterogeneity whitelist to detect both reported and unreported assaults [20].
- c. HANIDPS is a ZigBee-based anomaly - based intrusion detection system for home region networking. Has been created to guard against infiltration [21].
- d. Planning an IDPS has been installed to safeguard linked cars' Inter - integrated Network (CAN) buses. The Area Network Connections bridge, which links electromechanically components and senses in a systems for system control, makes it possible to give real-time vehicle information. [22].

1.1 Types of Intrusion Detection Systems

There's many three primary categories of IDSs: hybrid, misuse-based and anomaly-based (often referred to as bio metrics)

Misallocation strategies use the signatures of known attacks to locate them. They efficiently identify assaults of a recognized type while producing a manageable quantity of near misses. Novel (zero-day) assaults are not detected by misallocation approaches.

Exceptional case approaches simulate the typical behavior of networks and systems and discover anomalies as departures from this pattern. They are desirable since they can identify zero-day assaults. Since formerly unknown (but valid) system behaviors may be classified as anomalies, the fundamental drawback of exceptional case approaches is the possibility for large false alarm rate (FARs).

Hybrid methods integrate anomalous and abuse identification. These are utilized to increase the identification of known intrusions and lower the likelihood of false positives (FP) for unidentified assaults.

IDSs are also divided into internet and host-based categories according to where they search for invasive activity. An IDS that operates across a system tracks remote access activity for breaches. An IDS that is host-based keeps track of the processes and files used by the software configuration connected to a particular host.

1.2 Types of Networks

Types of Networks are wired networks, wireless networks [25], Internet of Things networks, wireless sensor networks, Cloud environment, Home Area Networks(HAN), connected cars network etc.

The wired networks basically include the LAN in any premises or buildings where computers are connected through wired connections.

Wireless networks includes WAN, MAN,PAN etc, where the various buildings in a city are interconnected to one another or the networks exist among cities through MAN etc. These are all examples of wireless networks.

The Internet of things network which exist in smart homes is a kind of network where the home appliances are all interconnected and automated to the devices of the members of the house.

The Cloud networks exist when multiple cloud environments of various similar type of organizations communicate with one another.

Home area networks include appliances in smart homes like smart door with a locking system, smart devices like fan, washing machine, air conditioner, television,microwave oven etc.

Also networking exist among cars which are running on roads.They are interconnected to one another through networks.So intrusion can come into picture in any of the above networks.

1.3 Types of Attacks in a network

There are various types of attacks in a wireless network.

The figure below illustrates several wireless assaults [27].

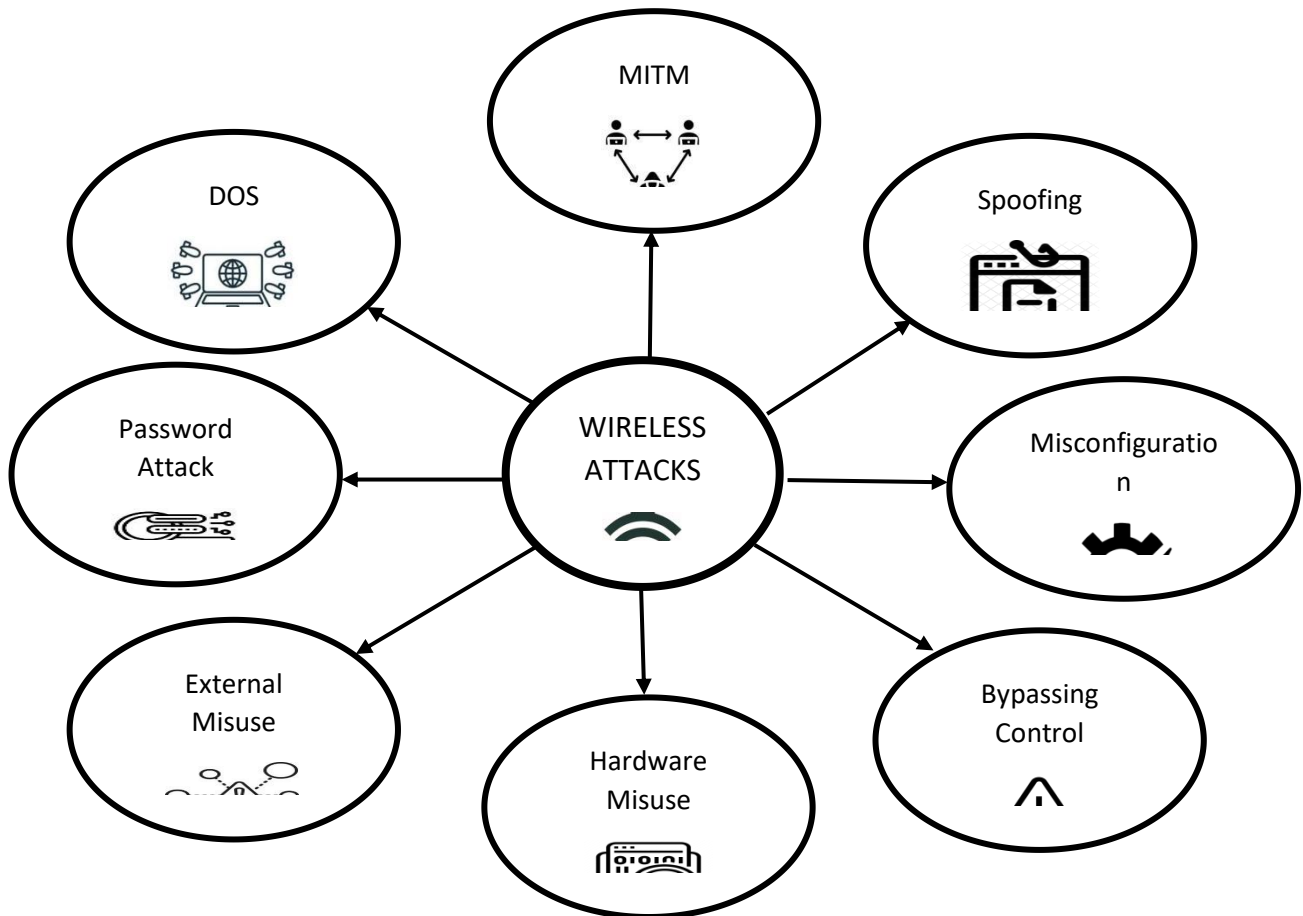


Figure 1.1: Various wireless assaults

Figure 1.1 shows the types of Wireless attacks i.e Denial of service attacks, Man in the Middle Attacks, sinkhole attacks, cautious forwarding, Blackhole and Grayhole assaults, and floods.

- i. The DoS Attack involves jamming the server, in a network with bogus information in order to block real traffic from reaching the server. This specifically occurs in the sphere of e-commerce. The opposite site may deliberately overload a site's server with fake traffic.
- ii. A hostile network called as the aggressor engages in Selective Forwarding attack drops packets in any order, i.e randomly. Its entire original content is disassembled, and it is difficult to tell if the data packet has been changed because it arbitrarily transmits some messages and rejects any messages at arbitrary. Basically that assault causes the entire routing path to degrade. [26].

- iii. In a sinkhole assault, the perpetrator wants to maximum crowd at the reception point, thus deteriorating its collection capacity. A rogue datatype main objective is to undermine the program's dependability and authenticity [26].
- iv. Assault by a blackhole means throughout this assault, the malware delivers erroneous route-related responses without previously examining the routing database, to the sender node. Additionally, it rejects the recipient's request to forward the message. The path that mandatorily redirects packets will be chosen even if it accepts to transmit one[23].
- v. A deliberate packet-dropping attack is v. Grayhole. Here, attacker node blocks received communication packet with a predefined frequency and in a professional manner.
- vi. A flooded assault entails overloading transmitting unnecessary data to the server node in order to use up network resources and take up genuine nodes' time [24]. Scheduling attack exploits networking resources like energy, space, time, and WSNs at a predefined period, similar to flooding attack [17] [24].

1.3 Machine Learning Techniques useful for Intrusion Detection and Prevention System

A. Decision Trees

An instrument for making choices is a tree structure. It is a pictorial depiction that is employed to investigate many possibilities starting at a root node and ending at the branches of the tree in order to discover a variety of solutions to specific challenges. The ending terminals are really the branches. As a result, there are several pathways one may take first from root of the tree to achieve various ends. [18].

B. Support Vector Machines

The method for machine learning supervised The Support Vector Machine is a tool that may be applied to regression and classification issues. SVM is based on

the idea of judgment surfaces, which specify the limits of assessment. A judgement plane is used to arrange a collection of objects into clearly defined categories. [18].

C. Ensemble Learning

To address a specific computational intelligence issue, many models, such as classifiers or experts, are deliberately developed and merged in an ensembles educational process. The main purposes of ensemble methods are to enhance classification, prediction, function approximation, etc.

Table 1.2 (a) Using Decision Tree Algorithm

Assets	Router			
Communication Network	Wired	Wireless	IoT	Cloud Environment
Judging parameters for the proposed system				
Quality Parameters	Moderate	Less	Less	Moderate
Failure Rate	Regulate	Regulate	Moderate	Strong
Durability	Average	Nice	Nice	Average
Defect rate	Moderate	Less	Less	Moderate
False positives	Strong	Strong	Less	Regulate
False negatives	Strong	Strong	Regulate	Moderate
Performance	Good	Greatest	Greater	Greater
Features	Moderate	Less	Less	Moderate
Reliability	Less	High	High	High
Conformance	Average	Nice	Nice	Nice
Durability	Less	Strong	Strong	Strong
Servicability	Less	Strong	Strong	High
Perceived Quality	Less	High	High	Very High

Table 1.2: (b) Using Decision Trees Algorithm

Assets	Firewall			
Communication Network	Wired	Wireless	IoT	Cloud Environment
Judging parameters for the proposed system				
Quality Parameters	Less	Less	Regulate	Regulate
Failure Rate	Regulate	Less	Regulate	Regulate
Durability	Nice	Nice	Nice	Average
Defect rate	Moderate	Less	Moderate	Moderate
False positives	Regulate	Regulate	Less	Regulate
False negatives	Regulate	Regulate	less	Less
Performance	Nice	Nice	Better	Nice
Features	Less	Less	Moderate	Moderate
Reliability	Less	High	High	Less
Conformance	Average	Nice	Nice	Nice
Durability	Less	Strong	Strong	Less
Servicability	Less	High	High	Less
Perceived Quality	Less	Very High	High	Less

The above table shows that how firewall works for wired, wireless, IoT and Cloud environments. The performance of firewall for these environments is judged on the basis of above mentioned parameters. The main fact regarding firewall is that it works on the basis of certain rules applied over it.i.e it will block only those traffic in the network, which falls under malicious category according to the set of rules applied over it or fed to it.

Table 1.3: (c) Using Decision Trees Algorithm

Assets	IDS			
Communication Network	Wired	Wireless	IoT	Cloud Environment
Judging parameters for the proposed system				
Quality Parameters	Less	Less	Moderate	Less
Failure Rate	Moderate	Less	Less	Less
Durability	Good	Best	Good	Good
Defect rate	Less	Less	Moderate	Less
False positives	Less	Less	Less	Moderate
False negatives	Less	Less	Less	Moderate
Performance	Better	Best	Better	Best
Features	Less	Less	Moderate	Less
Reliability	Really high	Really high	Strong	Strong
Conformance	Good	Best	Best	Best
Durability	Very high	Really high	Strong	Really high
Serviceability	Very high	High	High	Really high
Perceived Quality	High	Really high	Strong	Strong

The above table shows that how IDS works for wired, wireless, IoT and Cloud environments. The performance of IDS for these environments is judged on the basis of above mentioned parameters. The main fact regarding IDS is that it works based on the training given to it and its performance depends on the kind of datasets taken for training and also the machine learning models used as classifiers.

Table 1.4: (d) Using Decision Trees Algorithm

Assets	IPS			
Communication Network	Wired	Wireless	IoT	Cloud Environment
Judging parameters for the proposed system				
Quality Parameters	Less	Less	Less	Less
Failure Rate	Less	Less	Moderate	Less
Durability	Good	Best	Good	Good
Defect rate	Less	Less	Less	Less
False positives	Less	Less	Moderate	Less
False negatives	Less	Less	Less	Less
Performance	Good	Better	Better	Best
Features	Less	Less	Less	Less
Reliability	Strong	Really high	Really high	Strong
Conformance	Good	Best	Best	Good
Durability	Strong	Really high	Very high	Strong
Serviceability	Strong	Really high	Strong	Strong
Perceived Quality	Strong	Very high	Very high	High

The above table shows that how IPS works for wired, wireless, IoT and Cloud environments. The performance of IPS for these environments is judged on the basis of above mentioned parameters. The main fact regarding IPS is that it works based on the training given to it and its performance depends on the kind of datasets taken for training and also the machine learning models used as classifiers.

Table 1.5: (e) Using Decision Trees Algorithm

Assets	Honeypot			
Communication Network	Wired	Wireless	IoT	Cloud Environment
Judging parameters for the proposed system				
Quality Parameters	Less	Less	Less	Less
Failure Rate	Less	Less	Less	Less
Durability	Good	Good	Good	Best
Defect rate	Less	Less	Less	Less
False positives	Moderate	Less	Less	Less
False negatives	Less	Less	Less	Less
Performance	Better	Best	Best	Best
Features	Less	Less	Less	Less
Reliability	Strong	Really high	Strong	Really high
Conformance	Best	Best	Best	Best
Durability	Strong	Really high	Strong	Really high
Servicability	Strong	Really high	Strong	Really high
Perceived Quality	Strong	Really high	Strong	Really high

False positives & False Negatives- 30-40%-High
20-30-Moderate
10-20%- less

Failure Rate - 10-20%-less
20-30%-Moderate
40% & Above-High

Conformance-Less than 50%-Average
50-80%-Good
Above 80%- Best

Performance- 50-70%-Good
70-80%-Better
Above 80%- Best

After analyzing the various performance parameters, it can be concluded from above tables 1.1,.1.2,.1.3, that the shortcomings of router was later replaced by firewall whose shortcomings were overcome by Intrusion Detection systems, then Intrusion Prevention systems and then Honeypots finally.

According to Vinchurkar and Reshamwala [28] IDSs are "active processes or devices that review device and connection activities for unapproved and disagreeable behavior." IDS are available in three flavors. These categories include HIDS, NIDS, and hybrid-based IDS [29]. The HIDS seeks to keep track of internal computer system activity. The NIDS's objective is to dynamically monitor this system traffic in the present. In order to ascertain any potential connections intrusions, the NIDS tries to accomplish that. It tries to do that by using the right detection techniques.

There are three distinct categories: hybrid IDS built on an IDS, exploitation identification, and anomaly detection [30]. A collection of specified characteristics or criteria is used in the detection system to identify recognized hazards. The anomaly detection mechanism detects unidentified attacks on a regular basis. This is achieved by evaluating if the device's state is normal. The IDS classification for anomaly detection is shown in Figure 1.1 A hybrid IDS may be able to spot both known and unidentified attacks. The focus of this essay is the NIDS. NIDS uses the entire network's traffic characteristics to detect threats. The NIDS is the subject of this article. NIDS uses the whole network's traffic characteristics to find hazards. The utilization of all capabilities is not necessary for attack detection. A smaller number of characteristics may shorten the time required for detection and accelerate it. Additionally, feature selection provides a number of advantages for learning algorithms. For instance, it minimizes noise sensitivity, eliminates over-fitting, and enhances prediction performance.

Choosing a subsection of basic techniques to use in the construction of a model is referred to as feature choice. It seeks to increase the accuracy of the data. In equation (1) below, the subset of characteristics is indicated by the letter S.

$$S = \{s_1, s_2, s_3, s_4, s_{2n-1}\}. \quad (1)$$

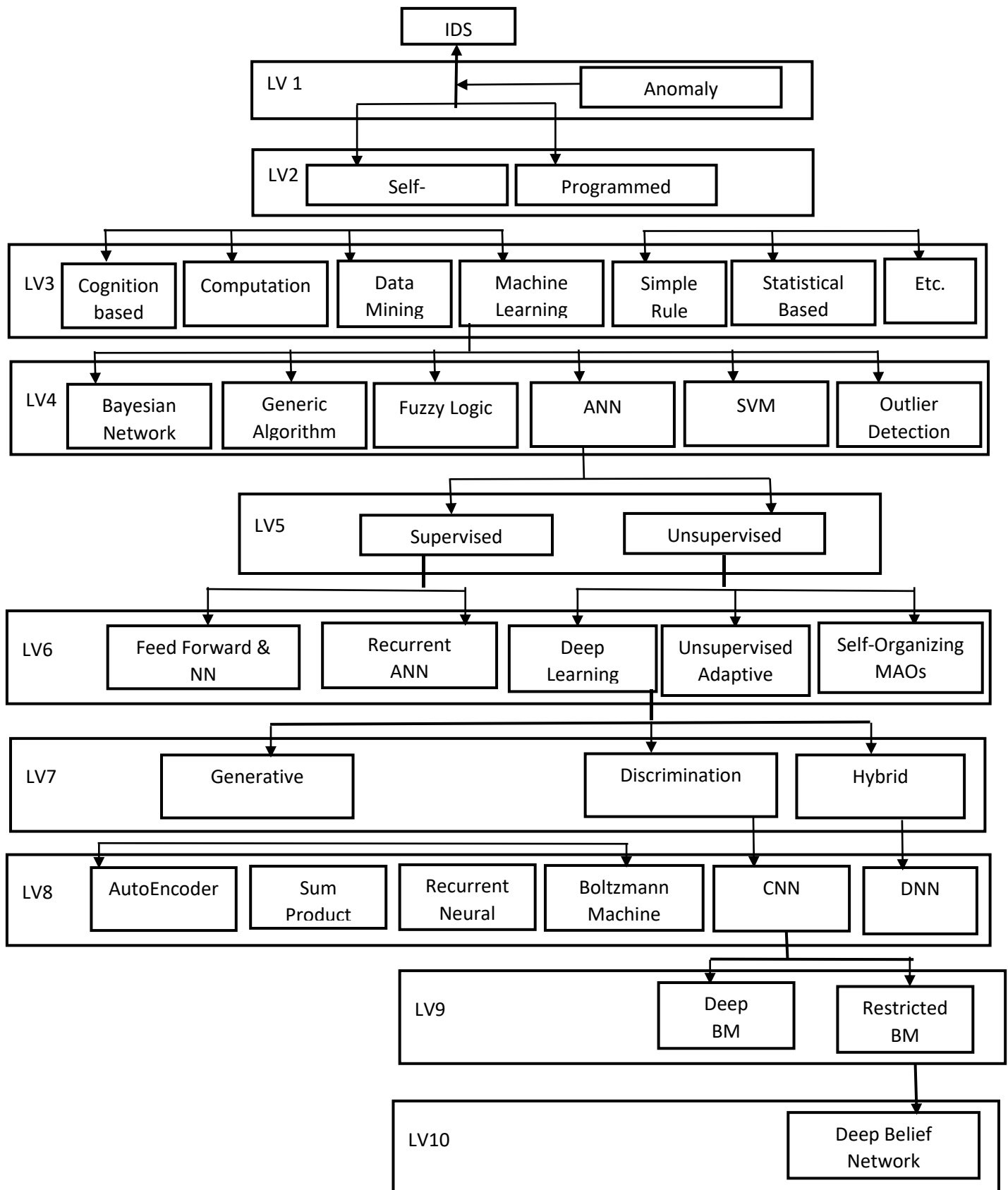


Figure 1.2: Recognition of anomalies according to class [31].

It is common practise to choose features. It is used, for example, in IDSs. Three options exist for selecting features: filter [34–35], embedded methods [36], and wrapper [32–33]. The embedded approach is used to include the characteristic extraction for a certain learning algorithm within the training phase. Using a variety of learning approaches, the wrapper method would be used to choose the traits that can be predicted with a great level of precision. Using the use of a selection of characteristics from the initial set, this filtering system approach attempts to classify a subset. These features are chosen based on the evaluation criteria. It was designed to lessen the amount of attributes such as boost NIDS activity consequently increase the precision rate. Although there have been several alternative NIDS models developed by academics, the current work attempts to create a model based on four popular metaheuristics that are affected by biological systems: the Firefly optimization algorithm (FFA) [43, 44], the genetic algorithm (GA) [27–38], the PSO [39–40], and the GWO [41–42]. ML classifier, J48 (C4.5) [46–47], and SVM [45–46] were used to evaluate the latter model.

A technique for choosing NIDS characteristics was proposed by the study's researcher; the algorithms PSO, GWO, FFA, and GA are used as the paradigm's cornerstone. By limiting how many functions are there that are chosen, it seeks to enhance the functioning of NIDS. SVM and the J48 ML classifier were used to evaluate it.

It was significant because the present investigation's goal was to:

Select the ideal feature set from the dataset UNSW-NB15. The FFA, GA, GWO and PSO methods were used in the current situation work to achieve this.

Make a technique for NIDS feature extraction that is filter-based. In the current attempt, this was accomplished using the algorithms FFA, PSO, GA and GWO. It was intended to decrease the quantity of the chosen attributes.

The PSO, GWO, FFA, and GA algorithms should be employed effectively in conjunction. The purpose of this inquiry was to determine if the detection technique would be more successful if the selected characteristics were filtered.

1.4 Objectives of the proposed work

- 1.To study various existing Intrusion Detection Systems and analyse them based on a variety of evaluation criteria.
- 2.To design a framework for detecting breaches in wireless sensor systems using Computational Approaches for Intelligence.
- 3.To analyse overall effectiveness of a suggested Intrusion Detection prototype and then in comparison to existing Intrusion Detection Systems.

1.5 Thesis Organization

The thesis is categorized into ten chapters, each covering a separate module of Machine learning algorithm models for various environments in Networks for intrusion detection system. Each chapter is described in detail below:

Chapter 1: This chapter gives us idea regarding the type of algorithms used like Deep Learning Algorithm will be used as we have huge amount of data to get the idea behind the types of network attack and their analysis for Network Intrusion Detection System.

Chapter 2: Prior work on Intrusion Detection Systems is discussed in this Chapter. This chapter analyses the outcomes of several techniques. Several methodologies are used to compare the presented findings, including accuracy, sensitivity, specificity, precision, and recall.

Chapter 3: The proposed technique is thoroughly explained in this chapter using terminology similar to that of the utilized software, Cisco Packet Tracer. A simulation network is created using the said simulation software and an actual network is also created. Intrusions are induced in these networks.

Chapter 4: In this chapter, kinds of machine learning algorithms and their detection rates are compared which illustrates the type of attack, and also the features selected by PSO algorithm are discussed here. The dataset with the reduced number of features is shown and the logic applied for detecting the types of attacks i.e DoS, probe, U2R, R2L is discussed in this chapter.

Chapter 5: This chapter describes an enhanced intrusion detection system, including a proposed system and flow chart, as well as a dataset description. PSO integration with the ML models has been described here. PSO with Decision Trees, knn and ANN was evaluated. And also the proposed IDS is being compared with existing IDS.

Chapter 6: This chapter demonstrates all Machine Learning and Deep Learning methods step by step, including data preparation, data reduction, and data training and data testing, classification based on training and testing datasets, and all numerical computations.

Chapter 7: This chapter provides detailed explanations of the proposed methodology for each of the research phases that were conducted. Also the proposed methodology is evaluated in terms of F1 score, precision, Recall, accuracy and the proposed IDS is also compared other existing IDS.

Chapter 8: In this Chapter, the final results of all stated objectives are provided, such as Model Accuracy, True Measure Rate (TMR), F-measure, Precision and Accuracy Rates, False Positive Rate, and Software Implementation of Cisco Packet Tracer.

Chapter 9: This study included critical components as well as major cyber security flaws and vulnerabilities related with exposure. To draw conclusions, transfer learning is employed, which takes use of relevant datasets. That are now accessible, will be used in the future to enhance model segmentation using the dataset UNSW-NB15 and to improve the proposed models' ability to deal with zero-day attacks. The research proposed a new IDS built using PSO+DT, PSO+ANN, and PSO+KNN techniques.

Chapter-2

Literature Review

Chapter 2

Literature Review

This Chapter discusses the prior work on Intrusion Detection Systems. It analyses the outcomes of several techniques. Several methodologies are used to compare the presented findings, including accuracy, sensitivity, specificity, precision, and recall.

2.1 Previous work done

Almomani. I *et al* [48] presented a technique which worked on a Collecting information for WSNs nets' IDS. These concepts showed the mechanism of vulnerability scanning and prevention methods in wireless networks which partially failed in order to identify intrusion attempts.

Abdulaziz I *et al* [49] presented a technique wherein Gradient Boosting Computers as well as Decisions Forests MI Algorithms were utilized to generate the datasets for predicting DOS assaults within Wireless sensor nodes. It was discovered that Decision Trees were more effective than SVMs.

M.Firoz Kabir *et al* [50] proposed an IDPS its effectiveness is assessed in comparison to that of Snort, a commercial NIDS programme. Initial as well as stochastic structuring methods have been applied to each Snort criteria inside this proposed model, as well as main concepts were established to cut down upon low error rates including during periods of significant internet activity.

Y.Yang,K.McLaughlin *et al* [51] created a Synchronization Relevant IDSs programme for identifying harmful computer hackers among a synchronization network, that includes a diversity baseline as well as behavior-based method for recognizing established models assaults.

Paria Jokar *et al* [52] designed an HANIDPS, a method enabling detecting and preventing intrusions into Wireless LAN embedded systems that was developed for protecting home area networks from intrusion.

Priyanka Sharma *et al* [53] described an IDPS in order to safeguard linked automobiles' CAN-bus, or Regulate Internet Connection. The Control Area Network

bus links signal conditioning units, detectors, and other devices in a framework for embedded devices capable of providing accurate data concerning automobile.

M. Archana *et al* [54] proposed a paper which compares Blackhole attack and Grayhole an embedded systems assault. The detection of these attacks becomes very essential regarding ids.

B. Al-Kasasbeh *et al* [55] displayed an evaluation study of the LEACH algorithm during DoS assaults. Various WSN algorithms are employed for structured, plain, as well as site applications. This study employs the organizationally scheduling algorithm known as LEACH to gain information on WSN characteristics in various traffic situations.

D. S. De Couto *et al* [56] regarding multi-hop wifi networking within wifi communication, a high bandwidth route statistic was proposed. In this paper various types of wireless networks are considered and the performance of the path metric in these types of wireless networks are compared to one another.

Sarika Choudhary *et al* [57] described a paper in which Throughout the IoT technology, filtering threats including quicksand as well as specific transferring were recognized, as well as 2 various security techniques, KMA and CBA, were utilized. It was found that Cluster Based Algorithm gave better results than Key Match Algorithm.

Jafar Abo Nada *et al* [58] presented a program known as WIDPAS that assaults the offender as well as notifies the operator of the encroachment. Since the exact comprehensive security technology established for cellular broadband is being employed for wifi communication, such approach has been presented.

Ghassan kbar *et al* [59] designed a system in which a thorough strategy is suggested for safeguarding a cellular servers. The study findings were employed about it. HID and FF, ADC, as well as PF. Whenever a data moves via aforementioned phases with in aforementioned ratio, the functional behavior an encroachment. The access control system includes analog to digital converter as well as HID.

Sajaan Ravji *et al* [60] explained a system which uses Throughout offering a positive space mostly in virtual machine, phishing scam is incorporated into the concept of ids. The advantage of using Honeypots over firewall is that firewalls block the entire

traffic whereas honeypots block only abnormal traffic, so they have no problem of exhaustion of resources like firewalls and IDS.

Vinit Kumar Gunjan *et al* [61] proposed a paper which provides a quick introduction of every aspects of cybercrime, including its origins, kinds, research papers, methods of prevention, and the departments attempting to battle it.

Mohiuddin Ahmed *et al* [62] created a methodology that provides a thorough study of the four main types of aberration prediction models, including categorization, analytical, computational modeling, as well as segmentation. The study further emphasizes the difficulties in conducting investigation through using databases towards detecting anomalies.

M. Uma and G. Padmavathi *et al* [63] conducted an investigation that involved a thorough analysis of different botnet to raise knowledge of different sorts of assaults including how they operate even though suitable defence methods may have been started towards such assaults.

Ozlem Yavanoglu *et al* [64] wrote a review paper by doing a comparative study of foremost widely utilized statistics. The key approaches to assessing web activity as well as spotting anomalies were ai as well as ml approaches. This research concentrated mostly on statistics employed within those approaches.

Waleed Bul'ajoul *et al* [65] created and tested a system that organized networks as well as throughput utilizing unique QoS architecture inside a multi-layer router as well as increased data forwarding performance utilizing parallelism approaches. Various traffic kinds, tactic, as well as bandwidths were used to evaluate the design concept. The trial outcomes demonstrated design enhances system security efficiency, covering up to 8 GB/s with no missed particles. It is possible to increase this quantity (8 GB/s), but it relies upon that resource utilization, that is always constrained.

Evgeny A. Basinya *et al* [66] developed a novel strategy in their study that involves floating mimicry, providing credentials, as well as detecting a covert diversion of such suspect's various links in order to shield computer networks via defensive and offensive network monitoring tools.

Pankaj Ramchandra Chandre *et al* [67] discovered that formally validating procedures in WSNs is a crucial study topic. This study uses the AVISPA software and the

HLPSL dialect to design and officially validate certain breach identification techniques. The outcomes of the verification as well as DoS attacks which been discovered are provided throughout this study article, however it is important to avoid assaults of this nature. We propose a computers continuing to learn approach to prevent wsns infiltration. As a result, a WSNs might use the provided strategy to prevent invasions.

Adwitiya Mukhopadhyaya *et al* [68] proposed a system based on Wi-Fi 802.11b that detects invasions and disasters in a situation involving smart homes by taking into account different forms of data flow. Here, residents receive notifications through a cloud server. The effectiveness of the alarm method is intended to be increased by a multi-tiered detection and data transmission method.

Goyal, Abhilash *et al* [69] discussed an a strategy to increase the security of software defined connectivity by enabling it to recognize and stop different harmful assaults.

Christos Constantinides *et al* [70] suggested a state-of-the-art SVM system with a self-organizing progressive neural net for intrusion detection in networks. The suggested system's structure enables it to offer a warning system that can precisely and instantly defend against known and unknown attacks without depending on fingerprints or regulations. The proposed system has the capability of online iterative learning updates, which, depending on its test findings that use the NSL KDD collection, enables it for efficient and robust practical production.

Reza Parsamehr *et al* [71] a cutting-edge network intrusion detection device (IDPS) for mobile small cells with NC capabilities was exhibited. The suggested technique employs a cryptography message verification code technique. that detects intrusive incidents by looking for null spaces, and then applies the relevant risk mitigation techniques. The suggested system has been implemented in Kodo, and the computation overhead efficiency has been assessed.

Rifki Indra Perwira *et al* [72] developed a DoS assault detection and prevention method that uses anomaly-based dynamic enhancing. The experimental test results shown its dynamic enhancing approach is 93.3% successful at identifying threats and may restrict in real-time. This outcome was that the adaptive augmenting approach may be used to build the detection and prevention of intrusions systems. Simon D. Duque Anton *et al* [73] worked on, a study undertaking Insect IUNO that strives to

offer and improve security mechanisms that don't require specialized security expertise in order to enable small and medium enterprises to respond to the increasing threat in cyberspace. In this publication, the IUNO Insec project is briefly introduced. Additionally, the authors' contributions to the field of intrusion detection are described and contextualized, focusing in particular on machine learning-based solutions for industrial contexts.

Sui Xin *et al* [74] introduced significant progress of intrusion detection technology. The second section of this study introduces novel intrusion prevention systems technology. The report also looks forward to the development of intrusion detection systems.

Md Zahangir Alom *et al.* [75] showed using neuromorphic cognitive computing's Deep Learning in IDS for network intrusion detection and prevention. The velocity of computer security and incredibly low power consumption of xeromorphic computers have been combined with the computational power of DL. This approach uses numerical encoding to prepare the data for training with Auto Encoder (AE), an unsupervised deep learning technique. For the supervised neural network The computed values of AE are utilized as initial weights throughout the testing period. The discrete vector factorization (DVF) of the ultimate weights yields stanchion elements, synapses loads, and sensitivities for cells. Finally, the synapses and stanchions are assigned the produced handlebar loads, synapses loads, target value, and leakage values.

Chie-Hong Lee *et al* [76] applied an Extreme learning machine for network intrusion detection with equality constraints. To calculate the ideal number of buried neurons, a training technique that is adaptively incremental is suggested. The optimization criteria and a method for binary search-based adaptively growing hidden neurons are established. In order to evaluate the suggested method's potential, network intrusion detection is used. Experiments demonstrate that our suggested strategy is successful in developing models with high attack detection rates and quick learning rates.

Cyber security was shown by Md. Zahangir Alom *et al.* [77] by using uncontrolled Technology for DL) and a unique Intrusion Prevention Program (IDS).The SNORT fetch problem, a rules-based method, and supervised learning are frequently used to detect new types of assaults. In this approach, the incoming examples are numerically

encoded and feature extraction and dimension reductions are accomplished using the unsupervised the deep learning algorithms Auto Encoding (AE) and Limited (RBM). Then, using only three characteristics, iterative k-means clusters is utilized to group items in a lower multidimensional space. This method further makes use of the unmonitored extreme learning system for supervised learning.

Hassan Azwar *et al* [78] did a thorough investigation of a number of machine learning approaches to determine the underlying causes of problems with how well they detect intrusive activity additionally, each of their drawbacks is discussed. The article also includes a number of machine learning data mining equipment's.

2.2 Methodology Used ,Observations and Limitations of above research work

1. “Using Machine Learning to Scan Wireless sensors networks for DoS Attacks [49]”

The Methodology used is the dataset is being trained using both Vector Support Networks and Decisions Trees Deep Learning Techniques in order to detect DOS attacks in WSN are identified, and it is determined that Decision Tree algorithms outperform SVM. [49].

This was discovered that Decision trees outperformed supported vector machines inside the shortened data, which only included the three attacks (Grey holes and flood assaults) that made up the complete range of data. Less factors were included in training. [49].

The limitation was the time consumption required for testing both machine learning algorithms here was more, as here first Decision trees was tested with full dataset and then with reduced dataset. Similar was the case with SVM also [49].

2. “Prevention and detection of Routing Attacks in the Internet of Things [57]”

The Algorithms used here are both detection and preventative techniques, Mmrda (Key game Algorithm) and Cbf (Cluster Based Heuristic), used in the Iot devices to recognize routing threats like hole and selected relaying. [57].

It was observed that CBA gave more true positive results for detecting intrusions in Internet of Things, than KMA. There were multiple small algorithms designed systematically in CBA and KMA [57].

The disadvantage was the time complexity involved in the sub algorithms in KMA and CBA was more [57].

3. “An envisioned system for wireless intrusion prevention, prevention, and attack [58]”

Unlicensed spectrum cannot employ the very same intrusion prevention and detection solution that was built for landline networks. In order to tackle this, a device called as Cordless Vulnerability Scanning Prevention and Attack Method (or "WIDPAS") is suggested. This system assaults the offender and informs the administrator. [58].

It was observed that the WIDPAS system alerts the admin about any abnormal behaviour by sending warnings to it [58].

The limitations were combining the methods for machine learning for comparison purposes between normal and abnormal behaviour, but using which machine learning algorithm, it is not specified here [58].

4. "A Complete Protection Method for Protecting the Network of the Organization Against Cyberattacks [59].”

The net of an enterprise is protected using a technique that makes use of filter firewalls, honeypot security devices, intelligent video surveillance systems, & preventive firewalls. [59].

The observations include all HID and AID molecules can be synchronized using the suggested system. This synchronizing corrects the owner's incorrect positives and negatives. Because of this outcome, effectively blocked entities that were subsequently flagged as problematic is admitted with in system, and back. [59].

The limitation is that the system design is complicated as it involves the synchronization mechanism to be involved for synchronizing both agents, HID and AID [59].

5. “Cyber Security Challenges: Designing an Effective Intrusion Detection System” [50]

A detection of intrusions strategy (IDPS) has also been presented, and its effectiveness has been compared to that of Snort, a commercially available gaunt tool. [50].

It was observed that Prefix or randomized indexing methods are applied to all Snort criteria in the current plan, while core themes are constructed to decrease spam filtering time and false negative rate even during periods of high network traffic. [50].

The disadvantage is sensitive threat detection rate needs to be improved and the estimated signatures that need to be examined is high for each incoming packet and the computational cost is also high [50].

6. “Synchrophasor Systems Intrusion Detection System for Network Security” [51]

In order to detect hostile botnet in a synchronized phasor system, a tool called Power system Specialist Anti - malware System (Solutions containing) has been designed. Such technique utilizes a uniform whitelist and a behavior-based approach to detecting both known and unknown assaults. [51].

It was observed that the suggested system offers a more complete and all-encompassing method for dealing with both known and unforeseen assaults. [51].

The limitations are several behaviour-based detectors are involved in this proposed system owing to which its overall cost and design complexity is increased [51].

7. “In Smart Grids, intrusion prevention and detection for ZigBee-based Home Area Networks”[52]

HANIDPS is a Security and Intrusion Prevention system for local area systems using ZigBee, has been developed for protecting home area networks from intrusion [52].

The observations were no prior knowledge about attacks is needed for HANIDPS, as Dynamic training is employed for threat detection, while a model-based method is utilized for intrusion detection. [52].

The limitations are the algorithm involved in HANIDPS is only dependable for protecting static wireless sensors but ineffective for dynamic networks [52].

8. “Protecting ECUs and Vehicles Internal Networks”[53]

An IDPS has really been devised to guard connected automobiles' Precursor For an integrated Network (CAN) bus. The Control LAN bus incorporates microcontrollers, sensing, and a control software application to give actual vehicle data. It is an automobile serial bus network. [53].

It was observed that the suggested system effectively identifies intrusion and any strange behaviour in connected vehicles since it uses auto encoder rather than fins networks, which can handle any input using their local storage as well. [53].

The disadvantages were recommended IDPS should be improved to be capable of detecting invasion in real time, have low power, and have a lower percentage of false negative errors. [53].

Chapter-3

Methodology

Chapter 3

Methodology

Intrusion detection and Prevention system(IDPS) monitors and evaluates traffic for specific sections of systems or machines, in order to look for unusual activities. At intersection of two networks, an IDPS built on topologies is most frequently utilized. The IDPS network cards are connected in full duplex mode, which causes them to accept every packet they come across, no matter where they are meant to travel. A large portion of the analysis by network-based IDPSs is performed on applications, such as three protocols are used for sending and receiving email: HTTP, SMTP, and DNS, where the majority of the assaults come from. To identify and mitigate attacks at these layers, they also analyse activities at the transport (for example, TCP, UDP) and network (like IPv4) levels, for instance. They also allow for investigation of the application layer. Using network-based IDPSs, they can indeed conduct a limited amount of research at the device layer (e.g., Address Resolution Protocol [ARP]).The proposed technique is thoroughly explained in this chapter using terminology similar to that of the network simulator, Cisco Packet Tracer.

3.1 IDPS Based Network system

There are two approaches to deploy network-based IDPS sensors, either inline or passive. As the traffic it monitors runs straight past it, an inline sensor is deployed in this case. The following paragraphs go into depth about several integrated detectors that are combination of network security gadgets. Sensors inline are intended to detect assaults by preventing vehicles from passing past them. A passive sensor must be installed; no actual traffic passes through the sensor; this allows for the monitoring of a duplicate of the urban scenarios. Passive sensors can make use of an intrusion detection system (IDS) capacity proportioning valve, which gathers and directs traffic to a desired site. In addition to a transfer extending connection, it has traffic visibility attempting to pass along with into the change. A connectivity tap assigns a detector directly into the physical wireless medium, such as a fiber optics. In order to avoid invasions, the majority of solutions require the detector to be placed inline mode. The ability of a detector to passively stop traffic, however, is frequently ineffective. A sensor array may occasionally inject packets into a network to try to break a

connections, although such methods become less efficient than integrated ones.

With the exception of interfaces used mostly for Intrusion detection and prevention management, network devices are rarely assigned to sense access points which was used to direct traffic. Network devices are allocated to watch endpoints of the detector. Given that it conceals them and blocks connections from other hosts, it improves the security of the sensors, therefore increasing their overall security. However, attackers may be able to establish which product is in use by looking at the preventative measures taken by the sensor, as opposed to detecting its existence. If you want to monitor secured networks and find out which scan patterns trigger particular responses, you may need to perform such an inquiry.

3.1.1 Wireless IDPS

An IDPS for wireless networks, on the other hand, utilizes the Wi-Fi protocols analyzed by the IDPS to track and evaluate wireless communication data in order to spot inappropriate activity. So much prevalent are wifi intrusion detection and prevention systems (IDPSs) (WLAN). WLANs are frequently used mostly by gadgets in commercial properties or on corporate campuses as extensions to current wired networked local area networks (WLANs), and they are designed to enable user mobility by extending the range of current connected wireless LANs.

Most wireless networks make use of LAN (WLAN) wireless technology. It is based on the IEEE 802.11 standard family. There are 2 essential parts needed to construct IEEE 802.11 WLANs. On one hand we have a wireless endpoint device, the station, while on the other hand we have the network Access Points i.e special temporary authorities(STAs) which are conceptually connected to other networks or a company's connected communications infrastructure via an internet connectivity station through Access points (AP). In between base stations and the internet connection, wireless switches serve as a conduit which are also used in some WLANs. The infrastructure mode is used for networks with STAs and access points. The ad hoc mode is used for networks without access points, where STAs connect directly to each other. Almost all of the organization's 11 WLANs operate in infrastructure mode. In a WLAN, each access point (AP) is assigned a name called a service set identity (SSID) (SSID). In order for access points to distinguish between various WLANs, SSIDs(Service Set Identifier) are required.

Wireless IDPS components are identical to network-based ones, except for sensors. Wireless sensors operate considerably differently from traditional sensors due to the difficulty of keeping an eye on communication links. A portable IDPS examines the traffic, as opposed to an infrastructure IDPS, which may view all information on the connections it watches and on the networks it monitors. Rather than seeing it all at once, 2.4 And 5 gigahertz [GHz] are the two frequency bands being monitored, and each band is split via channels. A sensor must only watch one station at a time in order to remain track of all the information on a spectrum.

Longer periods of time spent watching one channel increases your chances of failing to identify malicious behaviour occurring on other channels during the same time frame. Sensors that often change channels, a process known as channel scanning, are a typical way to avoid this. In order to reduce the quantity of channel scanning necessary, specialized sensors with several radios and high-powered antennas have been developed. The increased sensitivity of high-power antennas allows them to monitor a wider area than traditional antennas.

It is possible to minimize the number of channels that each sensor has to monitor by coordinating scanning patterns among sensors with overlapping ranges.

There are many different types of wireless sensors, from very simple to quite complicated. Instead of transferring data transfer from one place to another like active sensors, dedicated sensors execute wireless IDPS functions but do not communicate data. Fixed or mobile deployments of specialized sensors are conceivable, influencing the effectiveness, mostly for contingency planning and reporting (e.g., to locate rogue wireless devices). Additionally, wireless switches and APs may get sensor software updates. If the STAs are equipped with these capacities, detector programs could also be capable of imposing security constraints over them, like preventing wireless connection.

If a company employs WLANs, it will frequently instil smart communication to keep an eye on the radio frequency (RF) bandwidth of its Wireless connections, which may include portable elements like Personal computers (PCs) and individual digital assistants. Many businesses utilize sensors to keep an eye on the channels and bands that their WLANs shouldn't be using, in addition to the sections of their buildings in which there shouldn't be any wireless action.

3.2 Proposed Methodology: -

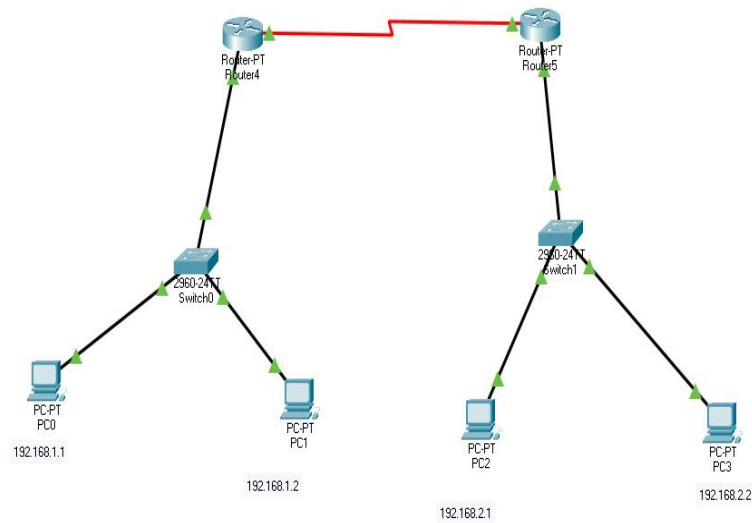


Figure 3.1: Showing the test network architecture in Cisco packet tracer.

Figure 3.1 shows a simulation network created in Cisco packet tracer. Here data packets during communication are captured using Wireshark tool. And the various network communication parameters involved, are studied for finding the regular pattern of communication.

As shown in Flowchart Figure 3.2, the methodology incorporated in our proposed work was to design first the network system with proper node configuration. This node was established based on the different network architecture. For this purpose, we have initialized to model the whole network infrastructure using Cisco Packet Tracer. In this system we have designed the test network environment consisting of 5 source IP, 13 Destination IP and 9 protocols. This network protocols were ARP, BROWSER, DHCP, ICMPV6, IGMPV3, LLMNR, MDNS, NBNS and SSDP. The protocol was initiated using for the period of 10 min using the Cisco packet tracer simulator. The run time was properly initialized and there was no run time error while running the simulation. We have used wire shark system to collect the data packets values with respect to source, destination IP and protocols with respect to time, so that time domain model can be initialized and proper prediction model becomes more efficient and reliable.

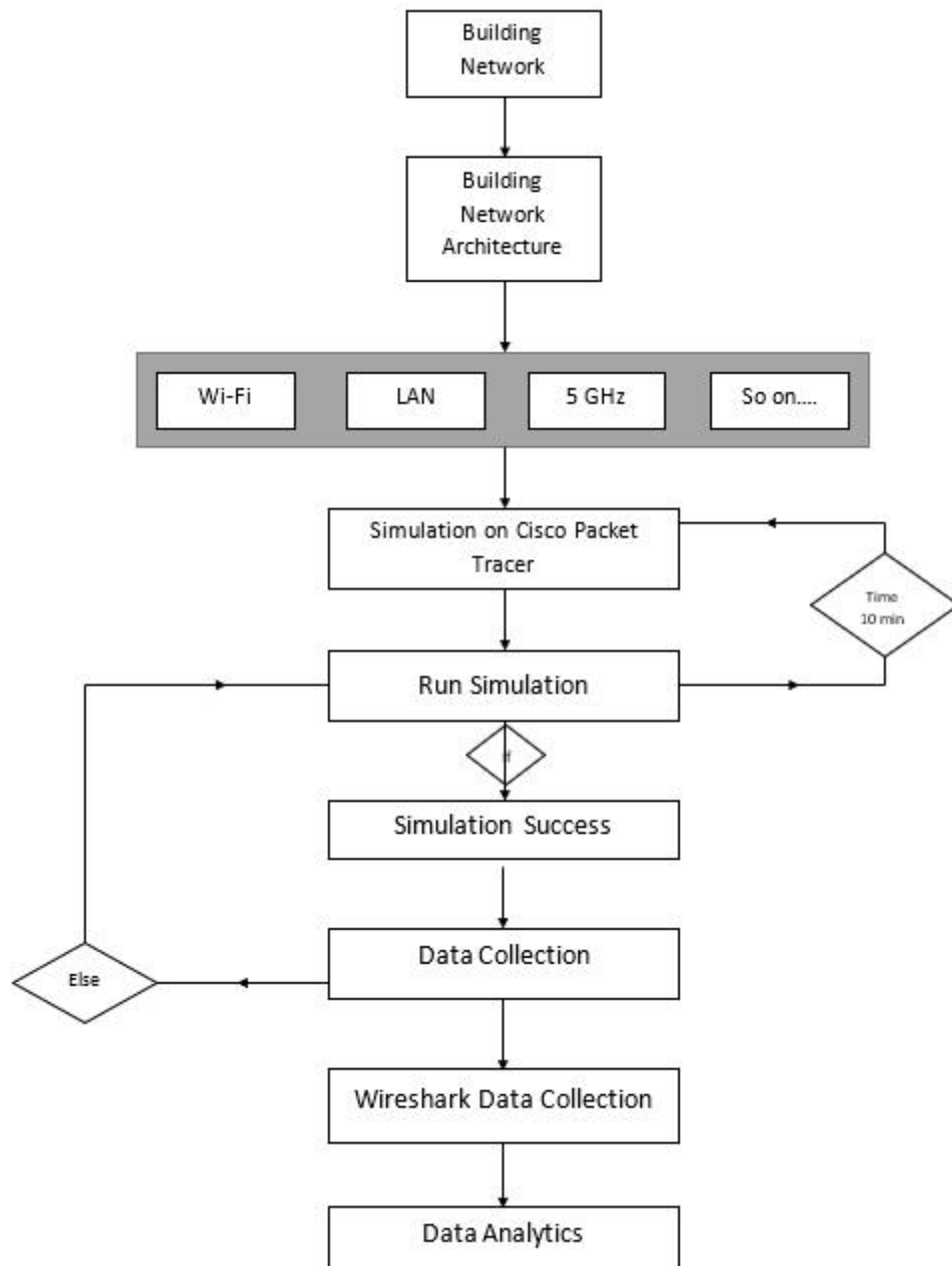


Figure 3.2: Shows the whole work flow for collection of data for any network simulation model

3.2.1 The Suggested Approach

The proposed approach aims to lessen the network impact intrusion characteristics for proper management of source and destination protocols on the given network bandwidth. This algorithm can be implemented on any network like Bluetooth, 3G, 4G, 5G, WIFI 2.4 GHz etc. The characteristics lies in knowledge of the system for

knowing the past characteristics of intrusion flow on the particular network. This analysis is being trained using neural network to understand the future mutation in the intrusion over any network bandwidth. As shown below the algorithm starts with the function $A(x, y, z)$, where x , y , and z are source IP, destination IP and intrusion protocols respectively.

We have i as variable which detects the intrusion characteristics, j as the probability with which the intrusion may be detected; x , y and z are parameters which depends on functions simulation model.

Initially Action

For $i = 1$ to N do

$$A(x, y, z) = N[A(x) * A(y) * A(z)]$$

Iteration Step

$$B[A(i, t)] = \text{Null}$$

For $t = 0$ to T do

For $i = 1$ to N

For $j = \text{Null}$ to Value

$$\text{Network Intrusion}(i, t) = \text{MAX}_{j=1, N} (\text{Network Intrusion}(j, t-1) * P(C_i|C_j)) * P(wt|C_i) * N[A(x) * A(y) * A(z)]$$

Step of Sequence Identification

$$C(T) = i \text{ that enhances Network Intrusion}(x, y, z, i, j) \propto T$$

Back trace to find the sequence of Intrusion

Network Intrusion array (X, Y, Z, i, j) maintains the probability of optimal sequence. for source, destination, protocols, intrusion and values characteristics. $C(T)$ functions will be having probability and weight age for particular network characteristics.

3.2.2 The Types of Network used in the Research

1. Using Cisco Packet Tracer, a network is developed in the simulation environment consisting of PCs, switch and Routers connected in LAN. Fig 3.1 above shows that.
2. Using Wireshark tool, packets transmitted during above communication and other activities carried in the laptop system is captured for 10 minutes. The protocols involved, source IPs, destination IPs, and the time taken for communication between a particular sources with a particular destination is all extracted with the help of Wireshark tool.
3. Now taking each protocol separately, by applying filters, it is studied that which destination is having maximum time, by plotting graphs. The destination showing maximum time in the graph means that is the most affected one. Maximum time is shown in a particular destination means it offered maximum resistance to any abnormal incoming packet from a source. So this abnormal incoming packet may be an Intrusion.
4. After this, trials are made to track the source from which this packet originated to that destination which offered maximum resistance to it, by applying filters to that particular destination. Again by finding out the source which has maximum time in the graph, the suspected intrusion source IP can be found out.

The above points are shown in the following graphs 3.3 and 3.4, plotted in R.

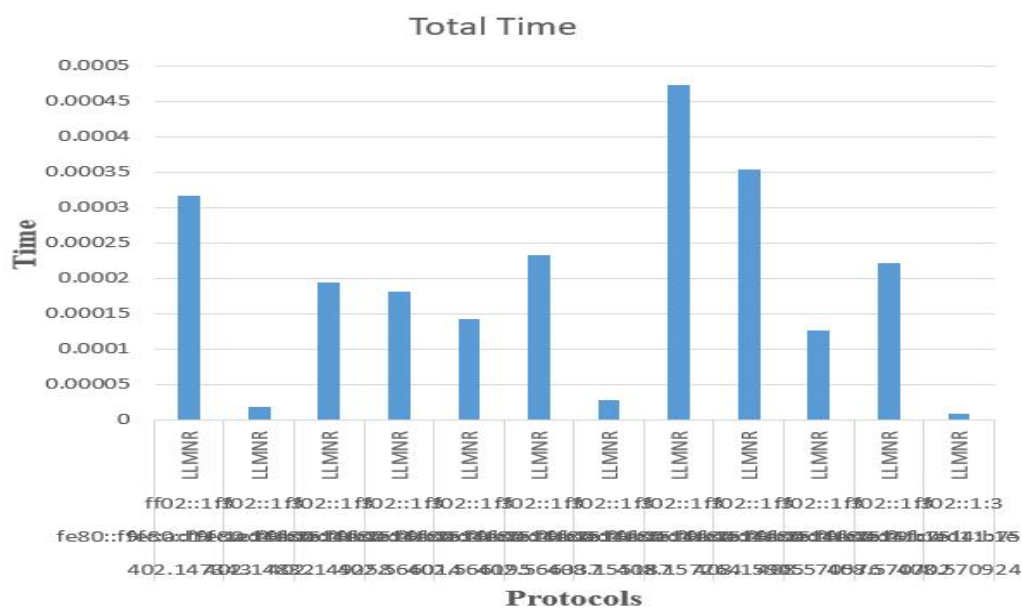


Figure 3.3: Shows protocols vs (ff02: 1:3) destination IP

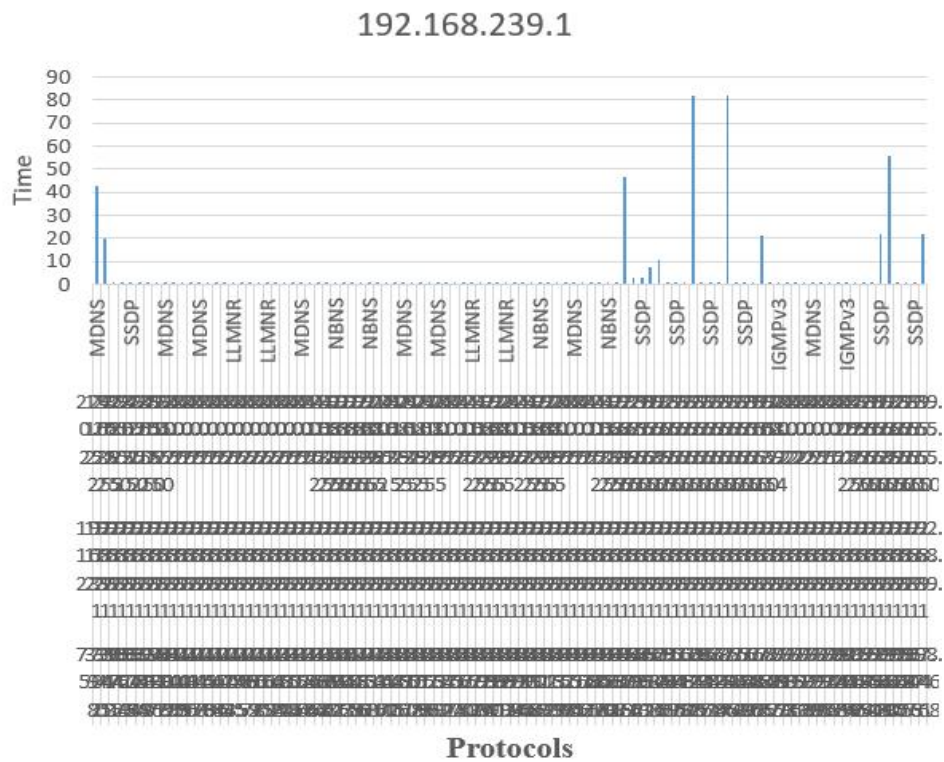


Figure 3.4: Shows protocols vs (192.168.239.1) Source IP

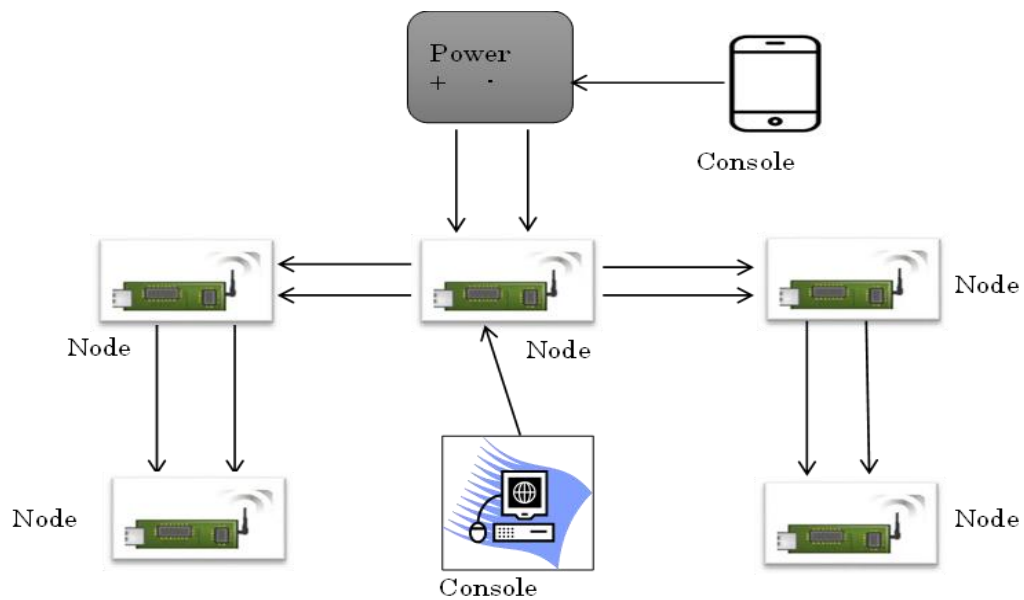


Figure 3.5 Actual physical network created using end users, console devices and 5 node MCUs connected mobile network

A physical network was created consisting of IoT environment such as Laptop, Mobile and 5 node MCUs as depicted in fig 3.5 .And datasets were obtained i.e. without malicious activity and with malicious activity. So following datasets are available now.

1. Normal dataset involving a simulation network in Cisco Packet Tracer, obtained with the help of Wireshark tool.
2. Normal dataset obtained involving IoT environment (consisting of node MCUs) in wireless networks.
3. NSDL dataset from Kaggle which is used to train the neural network (which consists of details about various types of attacks).
4. Perturbed dataset created by inducing some disturbances in the network consisting of IoT shown above in fig 3.5, created in the research .
5. UNSW dataset from Github which consists of many types of virus induced data.
6. Kddcup_99 dataset.

The Particle Swarm Optimization (PSO) has been applied in the research work, which is used for feature selection of the above mentioned datasets and the datasets containing the reduced set of features is used for training various Machine Learning algorithms, such as Artificial Neural Networks (ANN), Decision Trees(DT), k nearest neighbour algorithm (knn) and their accuracy percentages of detecting some malicious activity is found out.

The following is the system's planned block diagram shown in figure 3.6.

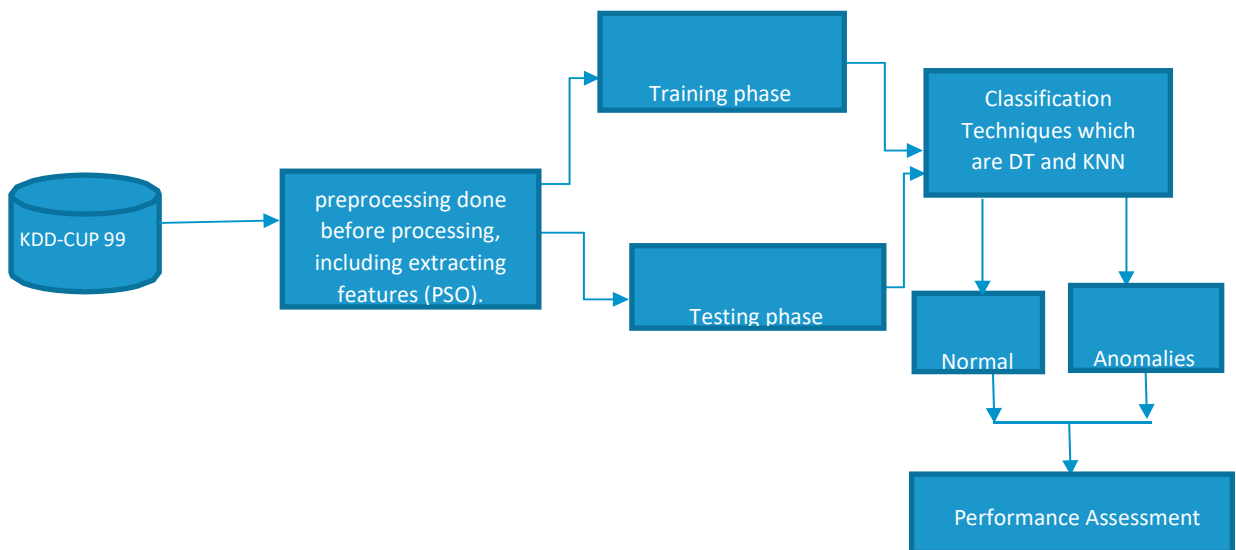


Figure 3.6: Proposed System Block Diagram

The whole of the Methodology can be summarized as follows:-

1. Simulation network created using Cisco Packet Tracer and normal datasets was obtained.
2. An actual physical network created using IoT components, and here also, normal datasets and intrusion induced datasets .i.e perturbed datasets were obtained .
3. PSO was applied on all the datasets, as feature reduction technique and the datasets with reduced set of features were obtained.
4. The novelty of the research lies in the extra sets of datasets created from the above networks used in the research apart from the standard datasets from kaggle, UNSW, kdd etc.
5. The increased number of datasets were used for training various Machine Learning models which act as classifiers in detecting intrusions in any network, which are capable of detecting any malicious entry in any network, other than the normal behaviour.

Chapter-4

Implementing Deep neural networks in a network intrusion detection system Architecture

Chapter-4

Implementing Deep neural networks in a network intrusion detection system Architecture

An IPS should be able to identify low rates of untrue and low recognition alerts that include misleading results. Some IPS devices can also protect against attacks that have not yet been detected, such as those generated by a Vulnerability. In terms of the former, there must be three most common detection and avoidance methodologies: misrepresent detectors, novel or fault diagnosis, and state full packet analysis. In terms of the IPS's residence, we may establish another distinction. In this regard, IPS is often classified into host-based, Network Behaviour Analysis (NBA), and infrastructure tools to enhance, which may be differentiated primarily based on the kind of events they are able to recognize and the methods they use to spot possible issues [95]. This chapter discusses attack kinds as well as their detection rates are employed to illustrate the data, and more detailed network attacks are studied.

4.1 DoS attack

The most hazardous sorts of significant mistakes are DoS attacks, according to Chen et al. and Doshi et al. (2018) [79, 80]. Small network services, like smart houses (Ranga and Verma, 2019) [81], are impacted by such assaults, which target clever gadgets inside such settings (for instance, intelligent door locks, set-top boxes, and smart incandescent bulbs) and prevent the potential recipient from accessing them. In this situation, some recent research (For instance, see Vaccari, Aiello, and Cambiaso, 2020; Syed et al., 2020; and Anthi et al., 2018;) [82, 83, 84] have focused on safeguarding such devices to DoS attacks. DoS attacks have the advantage of being easy to launch by creating bespoke packets.

Because DoS assaults are soul in the environment of AML, an attacker can change numerous DoS packet properties without annulling the attack. DoS/DDoS attacks on SDNs can flood the network control, data plane, or user plane bandwidth, whereas an assault on the control plane of an SDN can cause the network connection to fail [85]. Additional aim of DoS/DDoS attacks in the data plane is the emergence of several

fresh processes that don't correspond to the operator's flow table entries. By instructions, these entries are delayed. The Cyber attack works differently at the operating system than it does at others layers. As the switch before being forwarded to the management through wrap a result, the discovery of a DoS attack is essential to the design of an IDS [86].

4.2 Control Area Network (CAN)

A widely used for communication protocol is the Controller Area Network (CAN), particularly when genuine information is communicated. Message scheduling on the CAN corresponds to giving identifiers (IDs) to messages based on their priorities, with the CAN message ID being divided into two distinct parts: the first is determined by the changing priority of the text, while the other identifies the message itself. The number of bits allotted to the adaptive routing component. Priority-based arbitrate is used on the CAN bus, with CAN frames with lower IDs transmitting first on the bus. Because there are no missing transmission here on bus when collision occurs, that strong approach applied over CAN bus enhances the durability of transmissions and also preserves resources [87].

4.3 IDPS

The process of interpreting network or system intrusions is known as vulnerability scanning. Events for signals of likely incidents, such as breaches or threats to computer security laws, permitted usage guidelines, or basic security processes [88]. A software-based intrusion detection system (IDS) facilitates the attack identification process [89]. The process of doing intrusions and seeking to avoid discovered probable occurrences is known as antivirus software. IDPS detects potential security breaches, logs information about them, tries to prevent them, and notifies security professionals [90].

The identification of potentially occurring events is the major objective of IDPSs. An illustration of what an IDPS may spot is after a hacker's total penetration of a system by means of a vulnerability [91]. This could be the case whenever an IDPS is used. After that, the IDPS might tell administrators about the incidence, which would enable the administrators to promptly begin incident response operations in an effort to lessen the harm brought on by an accident. Additionally, a large number of IDPs

may be set up to look for security policy infractions [92]. It Identifies network activity that breaks security or usage limits set by the company. Some IDPSs, for instance, may be intended to seem like rule sets for a firewall. Furthermore, some Intrusion detection systems are able to trace large files and identify suspect those that involve moving a sizable database to a user's notebook [93]. There are several host - based intrusion detection technologies (Internally displaced persons), and these systems range greatly among themselves in terms of the sorts of incidents they can detect and the methods they employ to classify occurrences.

The main duties of a system for preventing intrusions (IPS) are to recognize harmful behaviour, record knowledge about that, keep on preventing or stop it, and expose it. By deploying detection devices in-line, IPS were created to overcome ambiguity in passive network scanning. IPS may now make user access choices based upon the type content instead than IP addresses or ports, as classic firewalls could. IPS systems and intrusion detection systems are still connected [94], since IPS systems were initially a literal development of intrusion detection systems. Web filtering systems can also be used to halt potentially harmful behaviour at the host level.

4.4 NIDS

A protection tool called a Network Intrusion Prevention System (NIDS) mechanism made up of application and/or hardware that detects cyber attacks on networks and servers [96, 97]. Apart from a data gram sorting firewall, which would only access and filter connections packets based on partial information contained in the data grams, an NIDS can use Deep Packet Inspection (DPI) to describe details of cyber-attacks from the packet of data grams, revealing their hidden agenda of affecting the PC to which they would be addressed. To identify intrusions and irregularities, an NIDS channels all network traffic via its sensors. Hardware upgrades include specialized packet sniffer cards and additional utility of the CPU and memory of the machine and changing the NIDS software to accommodate greater traffic and spread both connectivity and identification rules among NIDS node to use a cluster of NIDS [98].

NIDS monitors malicious activity such as denial-of-service attacks, including activities, scanning, and cognitive dissonance attempts. Every data frames are scanned by NIDS for any anomalous activity. Once risks have been identified and their

seriousness determined, the system will take action, such as contacting directors [99]. NIDS are also used to monitor and examine networks where a machine must be secured from infrastructure attacks. With the dramatic growth in internet usage, cyber security has been one of the most serious challenges for internet consumers and service providers [100]. A secure system is one that is protected against different breaches by its hardware or software. Implementing robust monitoring, analysis, and defence systems can help protect a network.

NIDS refers to a group of systems that use these methods to defend a connection against intrusions through both insiders and outsiders. Sophisticated monitor and analyse a network's data flow, perform time-based analysis, and alert users when an intrusion is identified [101]. Misuse detection (MD) and anomaly detection (AD) are two main categories of NIDS (AD). To identify intrusions, MD-based NIDS employ signatures or patterns from previous assaults [115, 116]. While AD-based NIDS look for tight deviations from typical network traffic characteristics and flag them as an attack [102].

4.5 SSIDS

Synchrophasor assessments, also known as synchronized phasor measurements, measures that use GPS eternal time to provide a time stamp for system properties including voltage, current, and frequency [105]. These measurements of system parameters are precise time-synchronized measurements. Synchronization technology ought to play an important part in the upcoming Smart Grid monitoring, security, and control, which will likely take place in the future. On the other side, these technologies present a plethora of potential flaws and cyber hazards that might originate from malicious attackers or dissatisfied employees. If exploited, these vulnerabilities and risks could result in inaccurate spatial awareness or significant harm [106].

To identify known and novel threats, The SSIDS employs a behavior-based strategy and a diverse whitelist [103], which discusses defensive measures to shield synchrophasor data from passive traffic attacks. They protect against attacks that combine random data concatenation with arbitrary packet cropping, since they are unable to manage the data amount and time involved [104].

4.6 Technology Limitations

Despite being effective at detection and analysis [117, 118], wireless IDPSs have a few significant disadvantages that need to be addressed. The utilization of evasion strategies, in particular those directed against gauge channel scanning methods, is a problem that exists with a number of wireless IDPS sensors [107]. One instance is launching attacks in brief bursts on channels that aren't being watched right now [110]. An attacker might potentially conduct simultaneous strikes on those systems [108]. If the sensor will detect the first assault, it will be unable to detect any second until it scans off from the very first attack's channel [116].

4.7 Security Capabilities

Typically, networking systems can identify a variety of harmful behavior [111]. The majority of systems rely on outlier detection, while some technology lack detection capabilities, enabling management to manually install customized filters that serve as signatures to recognize or stop specific threats [109].

4.8 Data-set

For user-defined datasets and the pre-partitioned UNSW-NB15 train and test datasets, the architecture is combined with a semi-dynamic hyper-parameter tuning strategy.

A. UNSW-NB15 datasets used for model testing for pre-partitioned

Deep learning benchmarks using the fully-featured UNSW-NB15 collection that has been from the range 74.3 percent [79] to 98.54 percent when using a wrapper-based strategy like the one described in [84]. [79] and [84] respectively. Model efficiency is greatly improved as a result of the suggested structure and optimizer approach, with the testing dataset obtaining an accuracy of 95.3 percent [112]. The method suggested integrating categorical cross entropy via momentum-based Adam optimization [113]. This was done to prevent the problem of over fitting. The learning rate of the approach is 0.001, and its initial two double-stacked layers have a reduced dropout rate [114], whereas the dropout rate for the last layer is significantly higher. The multi class classification model's accuracy of the learning curve is shown in Figure 4.1. The rate of detection for each form of assault is shown in Figure 4.2, which can be seen

here. As was established, the identification rate for underrepresented groups was substantially lower than the overall rate.

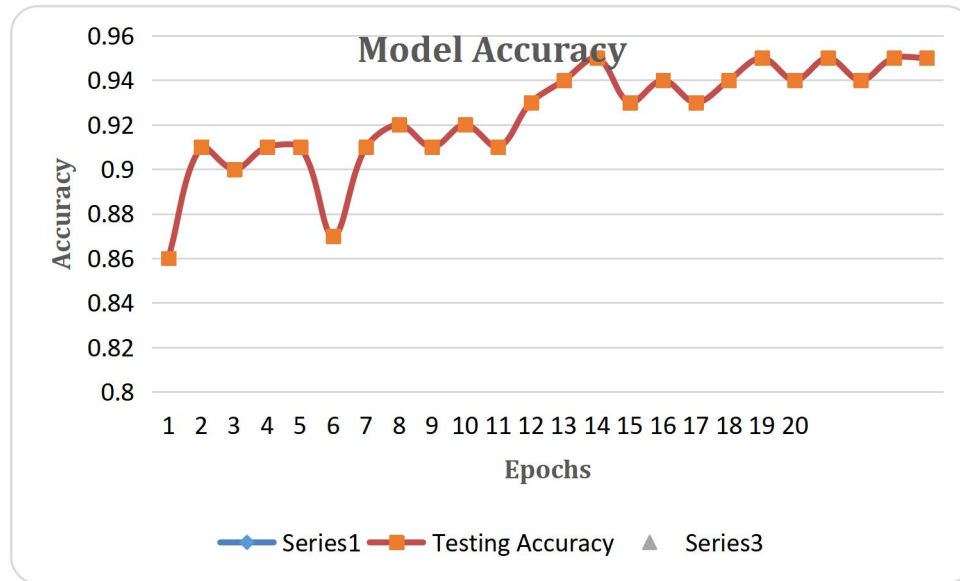


Figure 4.1: Multiclass classification model learning curve accuracy

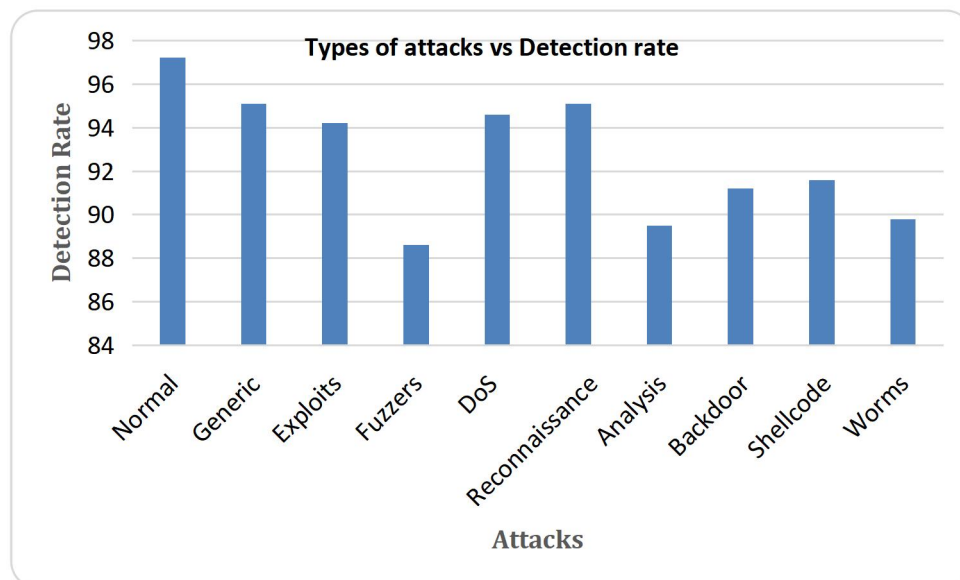


Figure 4.2: Types of attacks vs. Detection rate

B. UNSW-NB15 datasets used for Model testing for user define

When compared to the pre-partitioned data, the benchmarks obtained by applying deep learning models to a user-defined UNSW-NB15 dataset partition that contains a complete set of features achieve significantly better results. Applying the suggested architecture and hyper parameter technique to the testing dataset, which made up 25%

of the total, resulted in a model that performed well, with 95.6 percent accuracy. The technique suggests using momentum-based Nadam optimization and "categorical cross entropy," much like it did with the prior. To prevent this, over fitting, was done. The method yields a slightly higher information gain of 0.005% despite the same loss frequency structure.

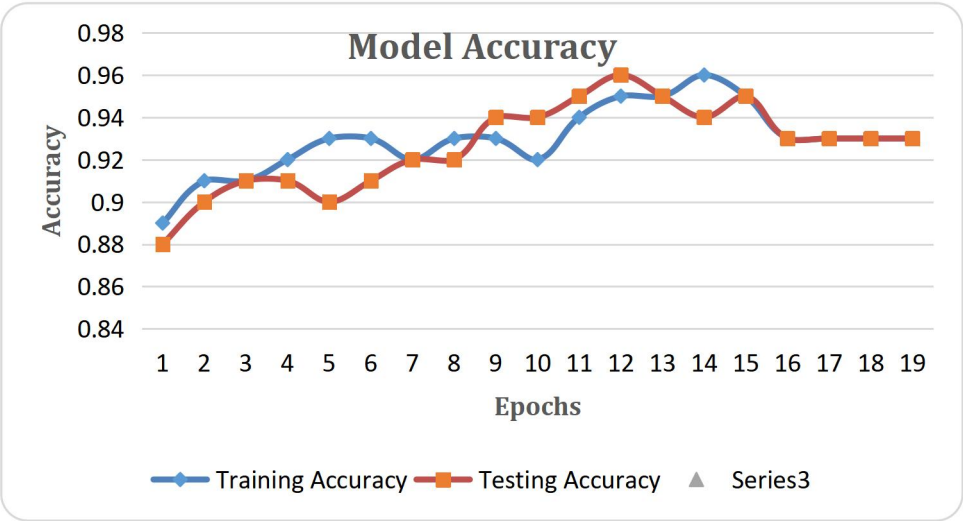


Figure 4.3: Multiclass classification model learning curve accuracy

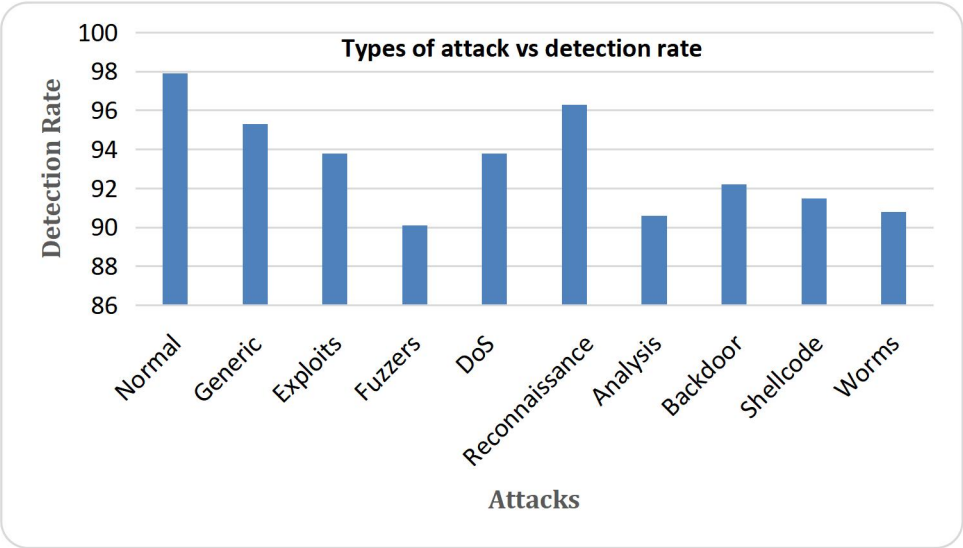


Figure 4.4: Types of attack vs detection rate

Figure 4.3 depicts the multiclass classification model's precision learning curve. Amount of detection for each form of assault is shown in Figure 4.4, which can be seen here. The from before the information strategy was comparable in that the responded for the underserved groups was substantially lower.

Some standard datasets like the NSDL dataset, UNSW dataset were used for training the Machine Learning models as shown below in figure 4.5 and fig 4.6.

[illegible]

Figure 4.5 NSDL Datasets used for training various ML models.

	swin	stcpb	dtcpb	dwin	tcprtt	synack	ackdat	smean	dmean	trans_depre	response_ct	srv_src	ct_state	t_ct_dst	ltnr	ct_src_dpi	ct_dst_sp	ct_dst_src	is_flow	log_ct	ftp_cm	ct_fiw	htct	src_ltnr	ct_srv_dst	is_sm	ips	label
J	0	0	0	0	0	0	0	248	0	0	0	2	2	1	1	1	2	0	0	0	1	2	0	0				
J	0	0	0	0	0	0	0	881	0	0	0	2	2	1	1	1	2	0	0	0	1	2	0	0				
J	0	0	0	0	0	0	0	534	0	0	0	3	2	1	1	1	3	0	0	0	1	3	0	0				
J	0	0	0	0	0	0	0	450	0	0	0	3	2	2	2	1	3	0	0	0	2	3	0	0				
J	0	0	0	0	0	0	0	1063	0	0	0	3	2	2	2	1	3	0	0	0	2	3	0	0				
J	0	0	0	0	0	0	0	392	0	0	0	2	2	2	2	1	2	0	0	0	2	2	0	0				
J	0	0	0	0	0	0	0	980	0	0	0	2	2	2	2	1	2	0	0	0	2	2	0	0				
J	0	0	0	0	0	0	0	692	0	0	0	3	2	1	1	1	3	0	0	0	1	3	0	0				
J	0	0	0	0	0	0	0	46	0	0	0	2	2	2	2	2	2	0	0	0	2	2	1	0				
J	0	0	0	0	0	0	0	46	0	0	0	2	2	2	2	2	2	0	0	0	2	2	1	0				
J	0	0	0	0	0	0	0	46	0	0	0	2	2	2	2	2	2	0	0	0	2	2	1	0				
J	0	0	0	0	0	0	0	46	0	0	0	2	2	2	2	2	2	0	0	0	2	2	1	0				
J	0	0	0	0	0	0	0	727	0	0	0	3	2	1	1	1	3	0	0	0	1	3	0	0				
J	0	0	0	0	0	0	0	1031	0	0	0	3	2	1	1	1	3	0	0	0	1	3	0	0				
J	0	0	0	0	0	0	0	1020	0	0	0	1	2	1	1	1	1	0	0	0	1	1	0	0				
J	0	0	0	0	0	0	0	526	0	0	0	3	2	1	1	1	3	0	0	0	2	3	0	0				
J	0	0	0	0	0	0	0	157	0	0	0	2	2	1	1	1	2	0	0	0	1	2	0	0				
J	0	0	0	0	0	0	0	887	0	0	0	2	2	1	1	1	2	0	0	0	1	2	0	0				
J	0	0	0	0	0	0	0	784	0	0	0	3	2	1	1	1	2	0	0	0	1	2	0	0				
n	n	n	n	n	n	n	n	1077	n	n	n	2	2	1	1	1	2	n	n	n	2	2	n	n				

Figure 4.6 UNSW Datasets used for training various ML models

Prior to that, Particle Swarm Optimization (PSO) was used as an optimization method for feature selection on the datasets. The total number of features involved in the datasets is 48. Out of these features the PSO selected the 25 features which were most relevant for training. Following feature selection, a variety of machine learning models for detecting network attacks have been trained using the datasets as shown in figure 4.5 and 4.6. These models include Adaboost, Support Vector Machines (SVM), Naive Bayes, K Nearest Neighbour(knn), Decision Trees (DT), and Artificial Neural Networks(ANN).

The accompanying illustration demonstrates that a regular situation will be labelled as a 0, whereas an attack of the types such as Neptune, Smurf, Pod, etc., which can be categorized as Denial of Service (DOS) will be labelled as 1, Probe attack as 2, R2L attack as 3 and U2R attack as 4. The Fig.4.7 is representing the correlations among the data values which it's in training mode.

In attack_class normal means 0, DOS means 1, PROBE means 2, R2L means 3 and U2R means 4.

```
In [14]: train.loc[train.attack=='normal', 'attack_class']=0

train.loc[(train.attack=='back') | (train.attack=='land') | (train.attack=='pod') | (train.attack=='neptune') |
(train.attack=='smurf') | (train.attack=='teardrop') | (train.attack=='apache2') | (train.attack=='udpstorm') |
(train.attack=='processtable') | (train.attack=='worm') | (train.attack=='mailbomb'), 'attack_class']=1

train.loc[(train.attack=='satan') | (train.attack=='ipsweep') | (train.attack=='nmap') | (train.attack=='portsweep') |
(train.attack=='mscan') | (train.attack=='saint'), 'attack_class']=2

train.loc[(train.attack=='guess_passwd') | (train.attack=='ftp_write') | (train.attack=='imap') | (train.attack=='phf') |
(train.attack=='multihop') | (train.attack=='warezmaster') | (train.attack=='warezclient') | (train.attack=='spy') |
(train.attack=='xlock') | (train.attack=='xsnoop') | (train.attack=='snmpguess') | (train.attack=='snmpgetattack') |
(train.attack=='httptunnel') | (train.attack=='sendmail') | (train.attack=='named'), 'attack_class']=3

train.loc[(train.attack=='buffer_overflow') | (train.attack=='loadmodule') | (train.attack=='rootkit') | (train.attack=='perl') |
(train.attack=='sqlattack') | (train.attack=='xterm') | (train.attack=='ps'), 'attack_class']=4

In [15]: test.loc[test.attack=='normal', 'attack_class']=0

test.loc[(test.attack=='back') | (test.attack=='land') | (test.attack=='pod') | (test.attack=='neptune') |
(test.attack=='smurf') | (test.attack=='teardrop') | (test.attack=='apache2') | (test.attack=='udpstorm') |
(test.attack=='processtable') | (test.attack=='worm') | (test.attack=='mailbomb'), 'attack_class']=1

test.loc[(test.attack=='satan') | (test.attack=='ipsweep') | (test.attack=='nmap') | (test.attack=='portsweep') |
(test.attack=='mscan') | (test.attack=='saint'), 'attack_class']=2

test.loc[(test.attack=='guess_passwd') | (test.attack=='ftp_write') | (test.attack=='imap') | (test.attack=='phf') |
(test.attack=='multihop') | (test.attack=='warezmaster') | (test.attack=='warezclient') | (test.attack=='spy') |
(test.attack=='xlock') | (test.attack=='xsnoop') | (test.attack=='snmpguess') | (test.attack=='snmpgetattack') |
(test.attack=='httptunnel') | (test.attack=='sendmail') | (test.attack=='named'), 'attack_class']=3

test.loc[(test.attack=='buffer_overflow') | (test.attack=='loadmodule') | (test.attack=='rootkit') | (test.attack=='perl') |
```

Figure 4.7 Training given to various Machine Learning Models

The figure 4.8 showing the integration of Adaboost-ML sequences with their obtained results based on the seeds.

Training was given to a variety of Machine Learning models like Adaboost, logistic regression, etc. using the datasets from the research study as discussed in previous chapter as well as some of the standard datasets like UNSW, kdd cup, and NSDL as shown in figures 4.5 and 4.6 and their accuracy percentage of detecting attacks is shown below in figure 4.8.

```
1. AdaBoost

AdaBoost was perhaps the first successful boosting ensemble algorithm. It generally works by weighting instances in the dataset by how easy or difficult they are to classify, allowing the algorithm to pay or less attention to them in the construction of subsequent models.

In [142]: from sklearn.ensemble import AdaBoostClassifier

In [143]: seed = 7
num_trees = 30
kfold = model_selection.KFold(n_splits=10, random_state=seed)
model = AdaBoostClassifier(n_estimators=num_trees, random_state=seed)
results = model_selection.cross_val_score(model, X_train, y_train, cv=kfold)
print(results.mean())

c:\users\rahul\appdata\local\programs\python\python36\lib\site-packages\sklearn\model_selection\_split.py:296: FutureWarning: Setting a random_state has no effect since shuffle is False. This will raise an error in 0.24. You should leave random_state to its default (None), or set shuffle=True.
FutureWarning

0.9982297655949475

In [144]: model.fit(X_train, y_train)

Out[144]: AdaBoostClassifier(algorithm='SAMME.R', base_estimator=None, learning_rate=1.0,
```

Figure 4.8 Integration of Adaboost ML sequences with their obtained results based on the seeds

So it is well evident that some Deep Learning models like Adaboost, Artificial Neural Networks, Convolutional neural networks, Recurrent neural networks were used in the research work as training models for which above shown datasets were used.

Chapter-5

PSO Integration with ML Models

Chapter-5

PSO Integration with ML Models

This chapter describes an enhanced intrusion detection system, including a proposed system and flow chart, as well as a dataset description. The proposed system involves creation of simulation network and an actual network and inducing intrusions in the network. Basically the idea is that the proposed system should get trained to various types of attacks in the network so that it can create an alert to the admin whenever the need arises. Actually datasets are obtained by inducing intrusions in a network. These datasets contain the data regarding various types of attacks specified in the previous section. These datasets are subjected to particle swarm optimization technique, where feature selection is done and relevant features are extracted. This reduced dataset is the used for training various machine learning models, which in turn detect intrusions in any network.

5.1 Techniques and Materials

This section covers models for the database, the proposed system, and the suggested classification method for the system. The proposed system includes creation of network, inducing intrusions into them, capturing of the data packets during communication and creation of datasets. Then PSO has been applied on these datasets for getting reduced dataset. These reduced datasets are used for training various ML models.

5.1.1 Description of Dataset

KDD99 was the first order DARPA placed for IDS. The label "abnormalities" was used to model and categorize attacks of various types. Two different forms of both normal and unusual network traffic have been used for this investigation which are widely tested network. According to [119], this dataset has issues, despite being often employed. Visit the following URL to get the Kdd repository dataset: <https://datahub.io/machine-learning/kddcup99>. There are characteristic sets and just a label indicating if the data is an attack or a common property (and type of attack). The learning phase employs 41 features and 345818 examples, whereas evaluation stage employs 41 features and 148205 cases [120]. The training and testing cases

that were used in this investigation are shown in Table 5.1.

Table 5.1: Example of training and testing

Stages	Occurrences
Learning	345818
Checking	148205
Sum	494024

5.1.2 Classification Techniques

PSO algorithm as an Optimization technique

By maximizing the threshold, the suggested method is applied in this study to increase class variance in both normal and disordered networks. PSO is a powerful algorithm with comprehensive, reliable characteristics of searching which could be employed for multipurpose reductions. The movement of particles from within the cluster is influenced by a level of proficiency or skill. Due to this socialization, a searching is capable of reversing an earlier continuous provincial underneath the targeted area [121].

K-Nearest Neighbors (KNN)

Non-parametric KNN is a type of statistical reinforcement methods that frequently use the distance metric. The KNN methodology is the fundamental method used in density-built anomalous recognition. The methodology is a straightforward, non-lazy learning strategy to categorize data using distance metrics such as Euclidean, Flatiron's approach, or squared euclidean [122].

Choice Plant (CP)

Due to its various benefits over other classification methods, CP is especially well suited to locating exceptions. To be further exact, those who have such a framework that is simple to understand and are less susceptible to the craziness of multitude [123]. A proper air conditioning technique called a choice trees imitates the roots and branches of a tree. The simplicity, scalability, and transparency of CP make it

preferable to traditional machine-learning approaches [124, 125]. In military applications like vulnerability detection and DDoS, CPs is widely used as classifications technique [126].

Suggested approach

In this study, the KDD-CUP 99 data individuals were used to run the suggested technique ML classifier [129, 130]. Data points are first imported through into platform, after which procedures like cleaning up, normalizing, etc. are performed on them. The rounds of training and testing come next [131]. This study employed a 70:30 proportion for training and assessment [132]. This 30% validation data is then sent to the suggested classifiers, DT and KNN, who subsequently classify the data as normal or anomalous [133, 134]. This cross statistics are used for assessing the performance of the classifiers to recalculate the numbers for performance measures such as correctness, improvement in accuracy, and other performance evaluations such as FPR, among other things, and dependability.

Figure 5.1 shows the suggested system flow.

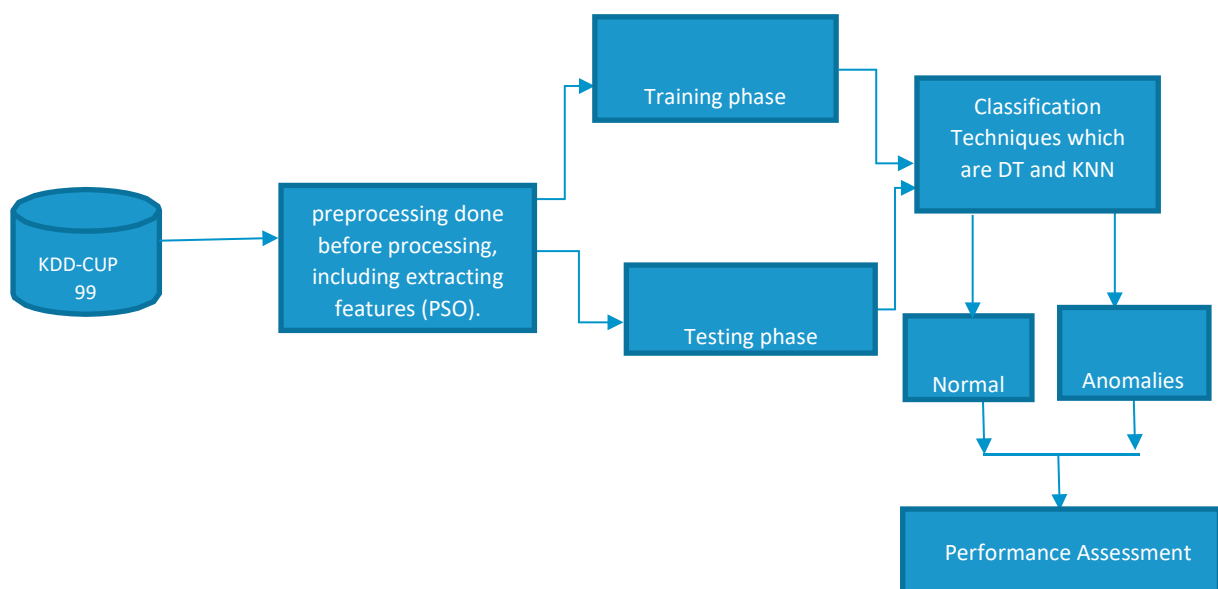


Figure 5.1: Blocks stream of a hypothetical system

Import data gathering: In a supervised learning technique, a training technique with particular samples is necessary, and the model can recognize the comparable observed

data that the algorithm learns with the help of this training. [135, 136]. Not every piece of information is accurate because the database comprises 41 characteristics and 1 class label [137]. As a reason, it offers a significant amount of data about incident trends. It is an issue that affects resource utilization significantly, [138]. Additionally, these input might include a range of loud elements and far less important characteristics that aren't necessary for identifying an assault strategy [139]. In order to achieve maximum data quality and dimension reduction, accuracy must be reached, as well as effectiveness in terms of memory and time utilization has to be achieved. The whole idea is depicted in the figure 5.2.

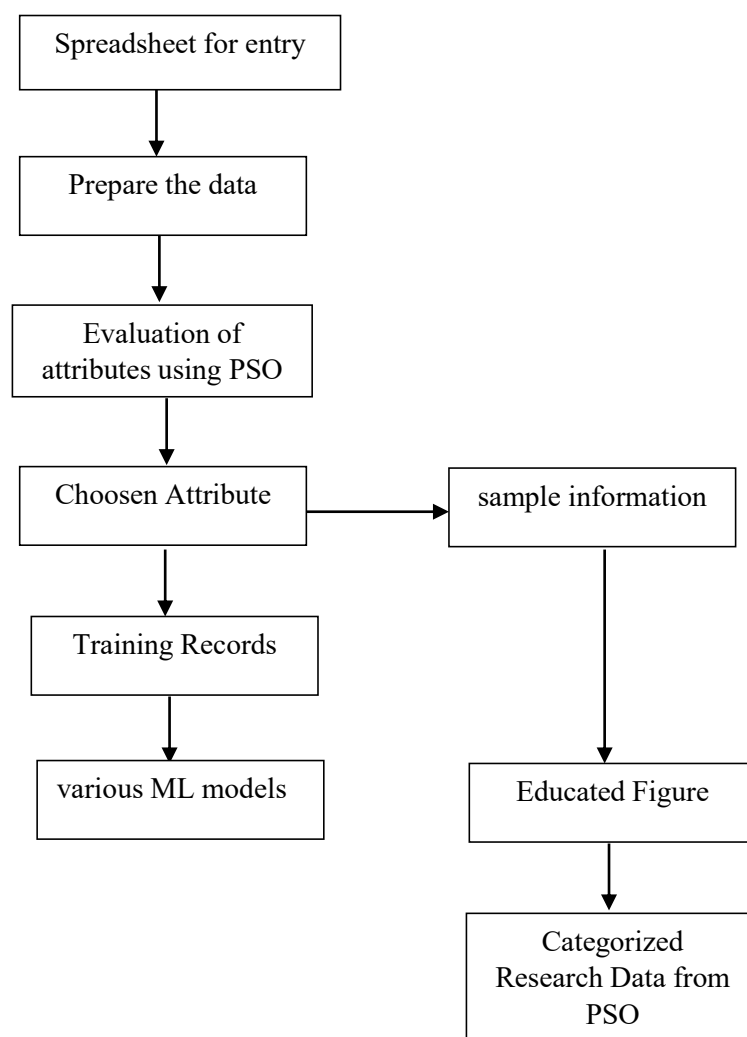


Figure 5.2: Operating a Better IDS System

Processing of information: This strategy is mostly used to make the data understandable. This strategy simply uses several technique combos to eliminate

extraneous information from the collection. No one answer, works for everyone. Planning for gathering data is needed. As a consequence, many techniques were used to reduce the loud noises in this situation. The absent qualities or outlier are the subject of this chapter. For every data point, the input pattern examples is scrutinized in this situation. Each pattern's feature is evaluated throughout this scanning. If a threshold data or null property is discovered, the norms are erased, as a result of the possibility that it may change the deep learning individual's capacity for choice.

Evaluation of attributes using PSO: Get new information that has the incomplete data instances or which got deleted from the dataset or has some incomplete information. This method may result in a reduction in the amount of data instances, enabling the dataset's size to be altered. The PSO method is then used in combination with the updated data to identify important features. Thus, the fundamental PSO algorithms are taught first.

1995 saw the creation of PSO (Particle Swarm Optimization) by Kennedy and Bernhard. This method is inspired by the behaviour and dynamics of bee, bird, and shark movement. This is a global diffusion stochastic search approach for getting continuous data. PSO intended to apply effectively to a variety of problems, showing structural planning, neural nets, and optimized structure [127, 128].

Benefits

- Ignoring the scale of model parameters
- The installation process is simple.
- It is simple to replicate computing.
- It is Derivative-free
- These methods' settings are not that many.
- Excellent all-purpose search service

Drawbacks

- Inside the intensive research stage, agreement is sluggish (weak local capacity to seek)

The conventional algorithm looks like this:

$x_k^i = \text{Particle position}$

$v_k^i = \text{Particle velocity}$

$p_k^i = \text{Best "remembered" individual particle position}$

$p_k^g = \text{Best "remembered" swarm position}$

$c_1, c_2 = \text{Cognitive and social indicators}$

$r_1, r_2 = \text{arbitrary figures from 0 and 1}$

The following changes have been made to particles roles:

$$x_{k+1}^i = x_k^i + v_{k+1}^i$$

Used this mobility calculated below:

$$v_{k+1}^i = v_k^i + c_1 r_1 (p_k^i - x_k^i) + c_2 r_2 (p_k^g - x_k^i)$$

Algorithm Steps

1. Initialize

- a. Set constant k_{max}, c_1, c_2
- b. place the particle's starting location as arbitrary $x_0^i \in D$ in IR^n for $i = 0, 1, 2, \dots, p$
- c. erratic that molecule's speed $0 \leq v_0^i \leq v_0^{max}$ for $i = 0, 1, 2, \dots, p$
- d. Set $k = 1$

2. Enhancement

- a. Functionality evaluation f_k^i with the use of designing space coordinates x_k^i
- b. If $f_k^i \leq f_{best}^i$ then $f_{best}^i = f_k^i, p_k^i = x_k^i$
- c. If $f_k^i \leq f_{best}^g$ then $f_{best}^g = f_k^i, p_k^g = x_k^i$
- d. If the situation stops then move to step 3
- e. Whole particles must be of updated velocity v_k^i for $i = 1, \dots, p$
- f. Whole particles must be of updated positions x_k^i for $i = 1, \dots, p$
- g. Increment k
- h. Went to 2(a)

3. End

Few functions: An optimization tool is the PSO algorithm (Figure 5.3). This method is used here with the attribute foundation to compare all goal results with every feature and rate each feature properly in order to find the features that are most important. The greatest 21 qualities have been picked to be examined in this article.

Dataset remodeling: The guided trained model will then be tested and trained using the selected features. As a result, testing and teaching are divided into separate groups to represent these features. 70% of the examples that fit the criteria are randomly selected to be used for training.

Test setup: To evaluate the proposed model-the remaining 30% of sample data are separated and their membership functions are used. The algorithm makes the use of these classifiers to measure progress during confirmation.

5.1.3 Novel Method

This article describes the potential technique phases for the finding of invasions. The steps to follow are shown in the following algorithm.

Algorithm displaying the suggested method

Input: Input mixed dataset D1

Output: Classified Samples C1

Parameter:-

While M is a certain machine learning model as well as I is the numbers of ML models for a certain intrusion detection system

Pi is the probability model for utilizing the ML method to find the specific anomaly.

For a specific dataset, there are several anomalies.

Process:

1. $R_n = readDataset(D1)$
2. $P_m = PreprocessData (R_n)$
3. $P_i = PreprocessData (P_i)$

4. $A_j = \text{PreprocessData}(A_j)$
5. $F_o = \text{PSO.SelectFeatures}(P_m, 21)$
6. $[Train, Test] = F_o \cdot \text{Split}(70, 30)$
7. For $i=0 \parallel j=0$ where P_i, A_j
8. $T_{model} = ML \cdot \text{Train}(Train)$
9. *for* ($i = 1; i < Test.Length; i++$)
10. *for* ($j = 1; j < Test.Length; i = j++$)
11.
 - a. $C = T_{model} \cdot \text{Classify}(T_i)$
 - b. $C = T_{model} \cdot \text{Classify}(T_j)$
12. *end for*
13. Return C1

After acquiring the datasets from the simulation network and the actual created network, these datasets along with some of the standard datasets like UNSW, NSDL, KDD were subjected to PSO, which acts as an optimization algorithm. It is used for feature selection, and the reduced datasets obtained were used for training the various machine learning algorithms. For training of the ML 70% of the datasets was used and for testing remaining 30% of the datasets was used. The kind of attacks that the proposed system could detect includes DoS, probe attacks, U2R and R2L. The efficiency of the various ML algorithms was compared in terms of the parameters such as accuracy, detection rates, false positive rates, precision etc.

Also the proposed IDS is compared with the existing IDS in order to find the efficiency of the proposed system and it was found that the proposed system proved to be more efficient than other existing IDS.

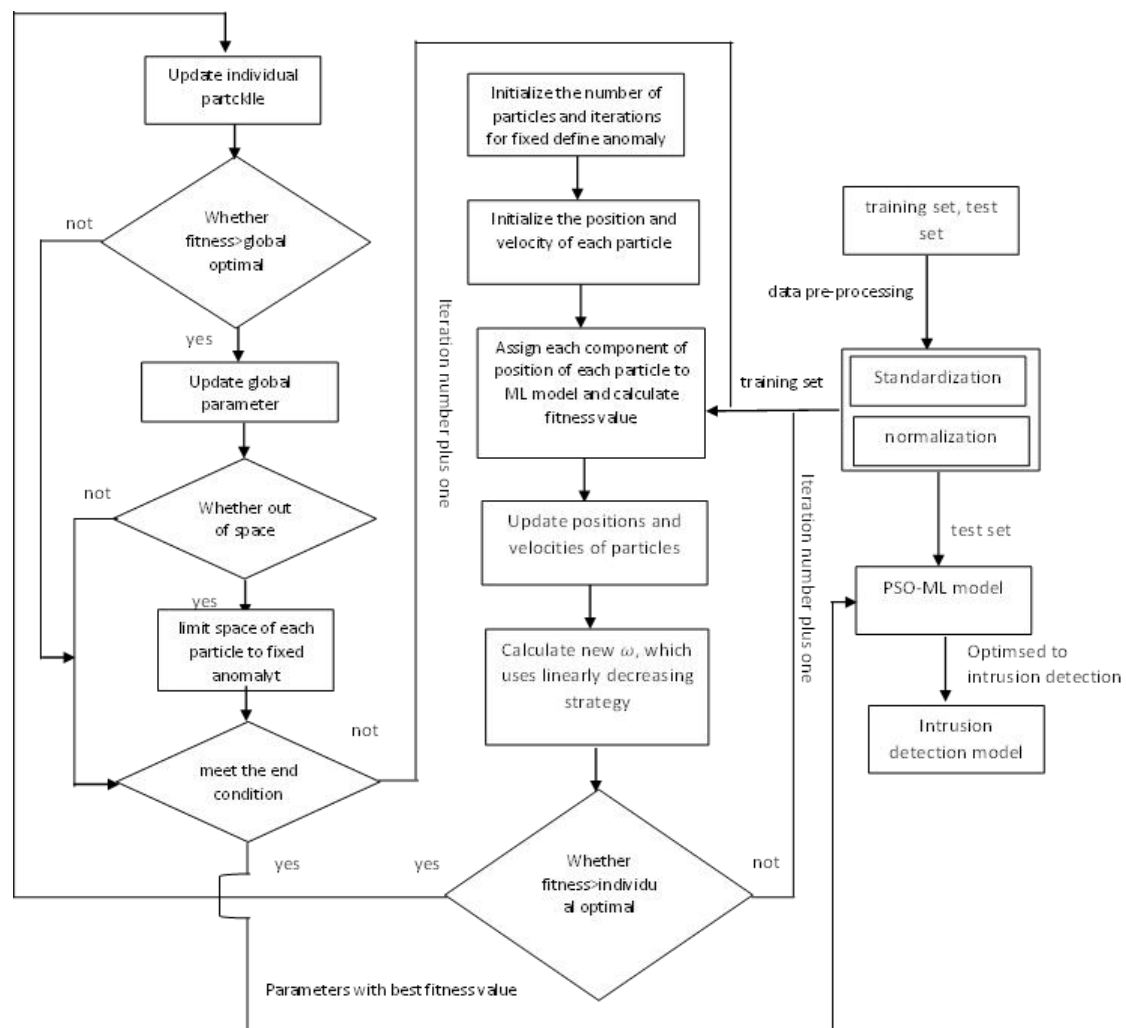


Figure 5.3: Proposed PSO integration with ML models

The proposed system as shown in figure 5.3, involves creation of simulation network and an actual network and inducing intrusions in the network. Basically the idea is that the proposed system should get trained to various types of attacks in the network so that it can create an alert to the admin whenever the need arises. Actually datasets are obtained by inducing intrusions in a network. These datasets contain the data regarding various types of attacks specified in the previous section. These datasets are subjected to particle swarm optimization technique, where feature selection is done and relevant features are extracted. This reduced dataset is the used for training various machine learning models, which in turn detect intrusions in any network.

5.1.4 Results of Classification

Training was given to a variety of Machine Learning models like Adaboost, logistic regression, etc. using the datasets from the research study as discussed in Chapter 3, as well as some of the standard datasets like UNSW, kdd cup, and NSDL as discussed in Chapter 4, and their accuracy percentage of detecting attacks is shown below in figures 5.4 and 5.5.

The figure 5.4 showing the integration of Adaboost-ML sequences with their obtained results based on the seeds. The figure 5.5 showing the integration of Logistic Regression sequences with their obtained results based on the communication data seeds.

```
1. AdaBoost

AdaBoost was perhaps the first successful boosting ensemble algorithm. It generally works by weighting instances in the dataset by how easy or difficult they are to classify, allowing the algorithm to pay or less attention to them in the construction of subsequent models.

In [142]: from sklearn.ensemble import AdaBoostClassifier

In [143]: seed = 7
num_trees = 30
kfold = model_selection.KFold(n_splits=10, random_state=seed)
model = AdaBoostClassifier(n_estimators=num_trees, random_state=seed)
results = model_selection.cross_val_score(model, X_train, y_train, cv=kfold)
print(results.mean())

c:\users\rahul\appdata\local\programs\python\python36\lib\site-packages\sklearn\model_selection\_split.py:296: FutureWarning: Setting a random_state has no effect since shuffle is False. This will raise an error in 0.24. You should leave random_state to its default (None), or set shuffle=True.
FutureWarning

0.9982297655949475

In [144]: model.fit(X_train, y_train)

Out[144]: AdaBoostClassifier(algorithm='SAMME.R', base_estimator=None, learning_rate=1.0,
```

Figure 5.4: Integration of Adaboost ML sequences with their obtained results based on the seeds

Building logistic Regression

1) LogisticRegression

```
47]: lr_clf = LogisticRegression(random_state=0, solver='lbfgs', multi_class='multinomial').fit(X_train, y_train)

c:\users\rahul\appdata\local\programs\python\python36\lib\site-packages\sklearn\linear_model\_logistic.py:940: ConvergenceWarning: lbfgs failed to converge (status=1):
STOP: TOTAL NO. of ITERATIONS REACHED LIMIT.

Increase the number of iterations (max_iter) or scale the data as shown in:
https://scikit-learn.org/stable/modules/preprocessing.html
Please also refer to the documentation for alternative solver options:
https://scikit-learn.org/stable/modules/linear\_model.html#logistic-regression
extra_warning_msg=_LOGISTIC_SOLVER_CONVERGENCE_MSG)

48]: y_pred=lr_clf.predict(X_test)
y_pred

Out[48]: array([1., 0., 2., ..., 1., 0., 2.])

49]: from sklearn.metrics import accuracy_score
accuracy_score(y_test, y_pred)

Out[49]: 0.8376879740939538
```

Figure 5.5: Integration of Logistic Regression sequences with their obtained results based on the seeds

Here is a comparison of PSO with each of the three classifiers: K Nearest Neighbour (KNN), ANN, and Decision trees (DT). The following table 5.2 shows the measurements of performance for proposed classifiers in combination with PSO and the table 5.3 shows the assessment of the suggested classifications.

Table 5.2. Measurements of performance for proposed classifier.

Measure	PSO+DT (%)	PSO+K NN (%)	PSO+ANN (%)
Predictability	98.7	99.6	99.7
Accuracy	75.2	88.4	90.2
Low Statistical Value (NPV)	99.5	99.8	99.8
F1 Rank	81.7	92.1	94.1

Table 5.3. Assessment of suggested classifications

Measures	PSO+DT (%)	PSO+K NN (%)	PSO+ANN (%)
Precision	98.5	99.5	99.77
Detection Rate (DR)	89.5	96.1	97.2
False Positive Rate (FPR)	1.2	0.3	0.02

The results of classification of various classifiers has been shown above by comparing various parameters.

Chapter-6

Systems for

Detecting Network

Intrusions (NIDS)

Chapter-6

Systems for Detecting Network Intrusions (NIDS)

This chapter discusses all ML and DL procedures, involving data pre-processing, feature extraction, data and testing, categorization based on train and test set, and all quantitative procedures.

An IDS feature selection model based on multi layer perception was created by Ahmad et al (MLP). Principal component analysis (PCA) and generalized additive modelling are both used in this model (GA). Using PCA, later researchers organized the subspace into a primary feature vector. Amongst qualities, the best eigenvectors were chosen [148]. The classifier may not recognize the PCA selected features well enough. GA was used to search the primary feature space for the most sensitive group. The MLP classifiers were built using PCA and GA attribute sets. The proposed results have been validated and are based on the KDDCup'99 dataset. There were 41 qualities listed, but only 12 were chosen. Perfect characteristics increased detecting efficiency. In the latter situation, 95 percent accuracy was obtained.

6.1 Companion Works

To categorize IDS anomalies, ML is frequently utilized. Machine learning is defined as a set of computing paradigms that learn from training data in order to become more proficient, produce precise estimations, and understand data. The procedures required to construct an ML application are shown in Fig 6.1 [142].

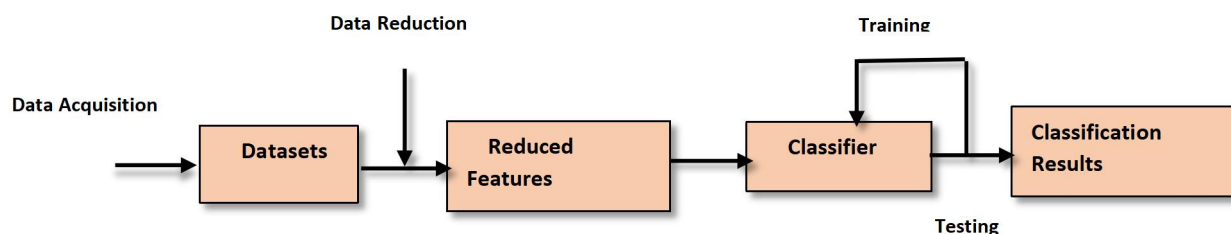


Figure 6.1: Phases involved in a Machine Learning Application

In computer vision, the selection of features is an essential pre-processing step. It improves the efficiency of the classification component while reducing the dimension

of the information [143, 144]. Develops a number of feature selection strategies for IDS. These strategies are recommended for categorizing significant characteristics based on various criteria [140, 141]. This section [145] briefly discusses the most recent methodologies for image processing techniques, which are based on ML classifications and microbe meta heuristic processes. The latter strategies aim to improve the functioning of IDS.

Oblique reference [150] researchers developed an SVM and GA hybrid model for intrusion detection systems. This strategy allows the 41 chosen criteria to be reduced to ten characteristics. The classes were built using GA and the weighted significant attributes of the provided components. The most important traits are prioritized [146]. The traits with the second lowest are prioritized third. This was done in order to spread the features. For example, four characteristics are prioritized over the rest, followed by four more. Two other features come in third place. The investigation relied on the KDD'99 data sets [147]. The combination module has a positive detection performance of 0.973. The false detection rate was determined to be 0.017.

The artificial bee colony (ABC) method for choosing IDS features was created by Ghanem and Jantan [152]. The latter method consists of two steps:

In step 2, an ABC, a PSO, and a classification technique that feeds forward (FFNN) were employed to evaluate the feature subsets formed in the first stage of the technique. In the first step of the technique, optimum non-dominated solutions were used to produce the subgroups.

As a result, the proposed technique employs a different paradigm for feature selection. It is known as the "ABC approach with many aims", unique features extraction methodology. It is known as the "ABC approach with many aims." There are aspects of internet traffic that can be lowered in aggregate. The latter method makes use of a novel categorization mechanism [149]. The method is known as the "hybrid ABC-PSO strategy." The updated FFNN is used in the following strategy to categorize the data obtained in the initial stage.

In Reference [153], researchers developed a system for selecting attributes for IDSs. The GA, PSO, and different evolution optimization algorithms were used to choose these traits (DE). Researchers tested numerous strategies to see how well they

performed. They were validated using a computational model, an SVM, and data from the 99th KDD Cup. In that order, GA, PSO, and DE considered the following attributes were the best: 16, 15, and 13. They were chosen to represent the dataset's 41 properties. They discovered that DE training takes 1.62 seconds. They discovered that DE is considered as the best categorization approach. The categorization efficiency of DE, in instance, is 99.75%.

Research on a new IDS model may be found in reference [154]. The latter idea makes use of a simple set to create a dynamic, intelligent swarm. "Simple swarm optimization" is the abbreviation for (IDS-RS) (SSO). It is recognized as a revolutionary weighted local search (WLS) strategy that offers a fresh perspective on PSO. The most important aspects of the dataset are chosen for reduction using IDS-RS and a weighted sum fitness function. Only six of the characteristics that were chosen and are available in the KDD99 dataset were collected. In the last step, finding cases and reaching 93.3% allocation accuracy are needed for the SSO classifier.

The research described in References [155] sought to determine how effectively the NIDS feature selection model performed. They planned to look into it with the feature selection techniques GA and PSO. With the aid of GA and PSO, the full count of features gathered was decreased. Numerous studies have shown showing GA is capable of effectively reducing selection criterion decreased from 41 to 15. They discovered that PSO was capable of effectively reducing the number of variables selected from 41 to 9. When using knn as a classification, the accuracy of the reduced GA dataset—which retains 37% of the fully recognized features, climbed from 99.28% to 99.70%. When applying the classifier k-nearest neighbour, the condensed datasets of the GA implementation time are implemented 4.8 times faster than the first dataset (k-NN). PSO completes the job in the quickest period of time, using the same classifier and only using 22% of the initial input (7.2 times quicker than the original dataset's execution time). Additionally, from 99.28 to 99.26%, its reliability has somewhat declined.

The GWO for grey wolf optimization method was used by researchers in Reference [156] to explore the ideal feature subset in the feature space that increases classification accuracy. The latter strategy made use of ideas based on common understanding and filters. Second, the classifiers' performance was enhanced using the

wrapper technique. The effectiveness of the recommended tactic was assessed. Numerous NSL-KDD meta heuristic algorithms were compared to the suggested technique's accuracy.

Citation [44]: Researchers selected the features using the Firefly algorithm, which is founded on wrapper feature selection techniques. They also suggested a method for increasing dimensionality. C4.5, "mutual information," the Bayesian classifier using the wrapper ensemble approach, and "MI" (41 characteristics) were originally included in the KDDCUP 99 dataset. That method, however, condensed those attributes into eleven features. As a consequence, the classifier's computation cost decreased.

Al-Yaseen [157] used the SVM and Firefly algorithms to create a novel feature selection methodology. The recommended strategy improves the intrusion detection system's efficacy. By removing the extraneous components, this is improved. This is improved because the categorization process takes less time. By reducing the amount of data, it cuts down on this time. Later studies coupled NSL-KDD with conventional intrusion detection system defenses. These indicators include, to mention a few, absolute reliability, higher accuracy, and number of false alarms. The proposed approach's total accuracy rate is 78.89 percent. It has been shown that the recommended feature selection strategy enhances NIDS's performance.

The purpose of this study was to determine how the MI (Machine Intelligence) of PSO, FFA, GWO, and GA functioned in selecting the best set of NIDS characteristics. This was the desired result. In none of the NIDS-focused investigations, ML was taken into account in the algorithms for PSO, GA, GWO, and FFA. The section that follows gives more information about the suggested model.

Threats to IoT settings come in many forms, both physical and virtual. Figure 6.2 demonstrates the many forms of cyber security included in the IoT process, including user interface, cloud services with multiple-system creation, and attack level. All of the above-mentioned categories have a high degree of assault, hence these procedures demand high-security characteristics on several dimensions. Despite the fact that several IoT systems provide poor attack characteristics, protocol-level feature implementations significantly superior than that used by all people. As a result, to

prevent any sort of hazard from accessing the defined system, a greater feature is necessary.

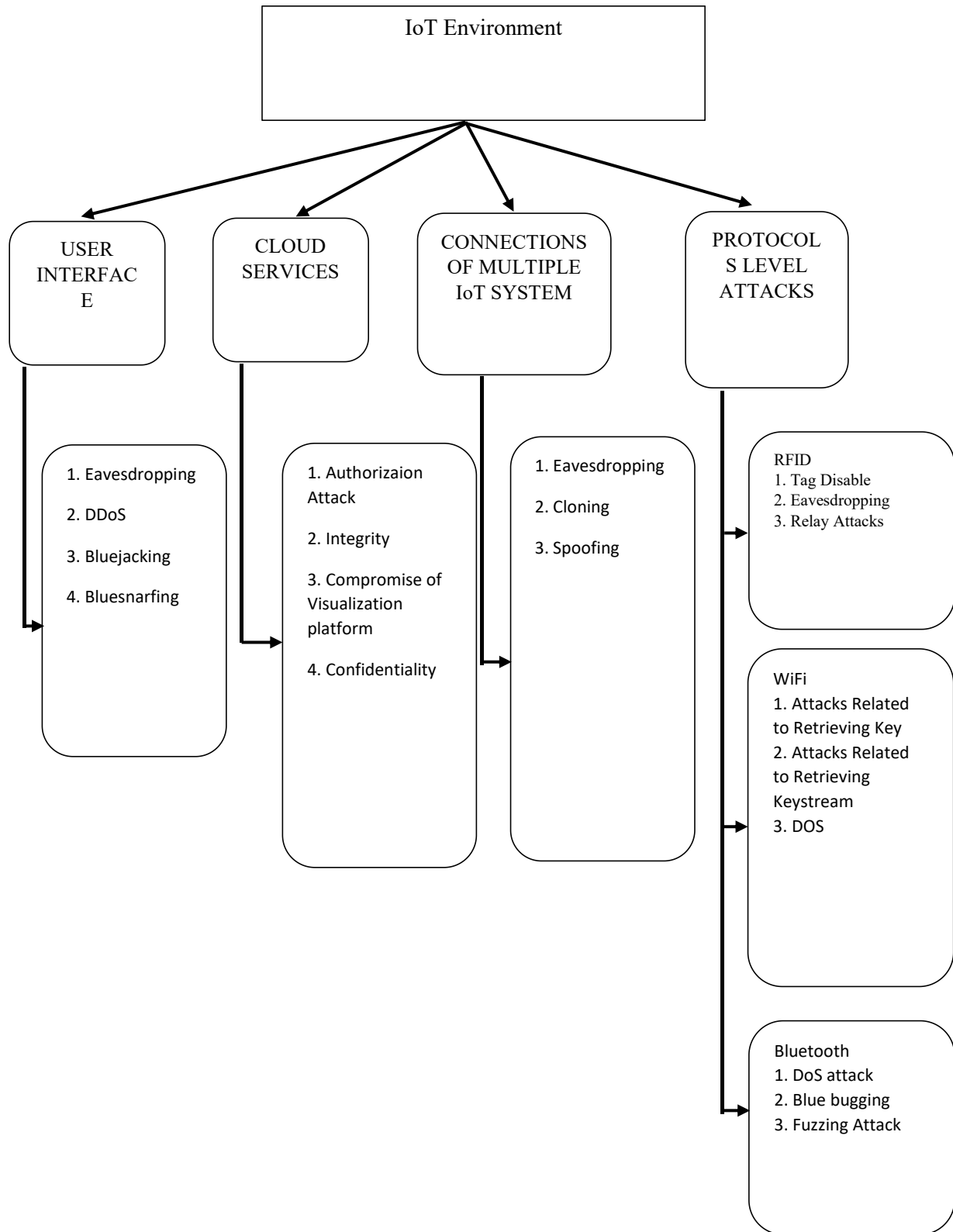


Figure 6.2: IoT environment threat dimensions

6.1.1 The Proposed Model

The attribute selection strategy tries to make NIDS more beneficial. Several academics have used in recent years, data mining and machine learning (ML) techniques have been created to address problems and boost system performance. The last approach and fewer characteristics were utilized in this study to enhance NIDS efficiency. Figure 6.3 depicts the recommended model's organizational structure. The following sections precisely list the phases of the proposed model.

6.1.2 The Pre-Processing Stage

The UNSW-NB15 datasets was pre-processed in order to provide more useful information for the EvoloPy-FS optimization approach [158, 159]. Here is a list of these actions:

A. Label removal: Each attribute has a label in the original NB15-UNSW datasets. For the purpose of updating the datasets for the EvoloPy-FS environment, several labels must be removed:

B. 45 features made up the initial UNSW-NB15 dataset. Classifiers are one of two types of characteristics (the other being labels). It is impossible to classify the attack as a feature. It is crucial to remove it as a result. This work's main objective is indicated by reducing the features, removing them is crucial.

C. Several of the labels in the dataset have been assigned string values, including protocol, status, and service type. Therefore, having these concepts encoded into numerical numbers is highly important.

D. Data binarization: The dataset contains numerical data in a variety of ranges. These data offer the classifier a number of problems throughout the training phase in order to account for such differences. As a result, each feature's values need to be standardized. Therefore, the lowest value for each feature needs to be 0. The highest amount should, however, be 1. It increases the homogeneity of the classifier. The distinction between both numbers of each aspect is preserved.

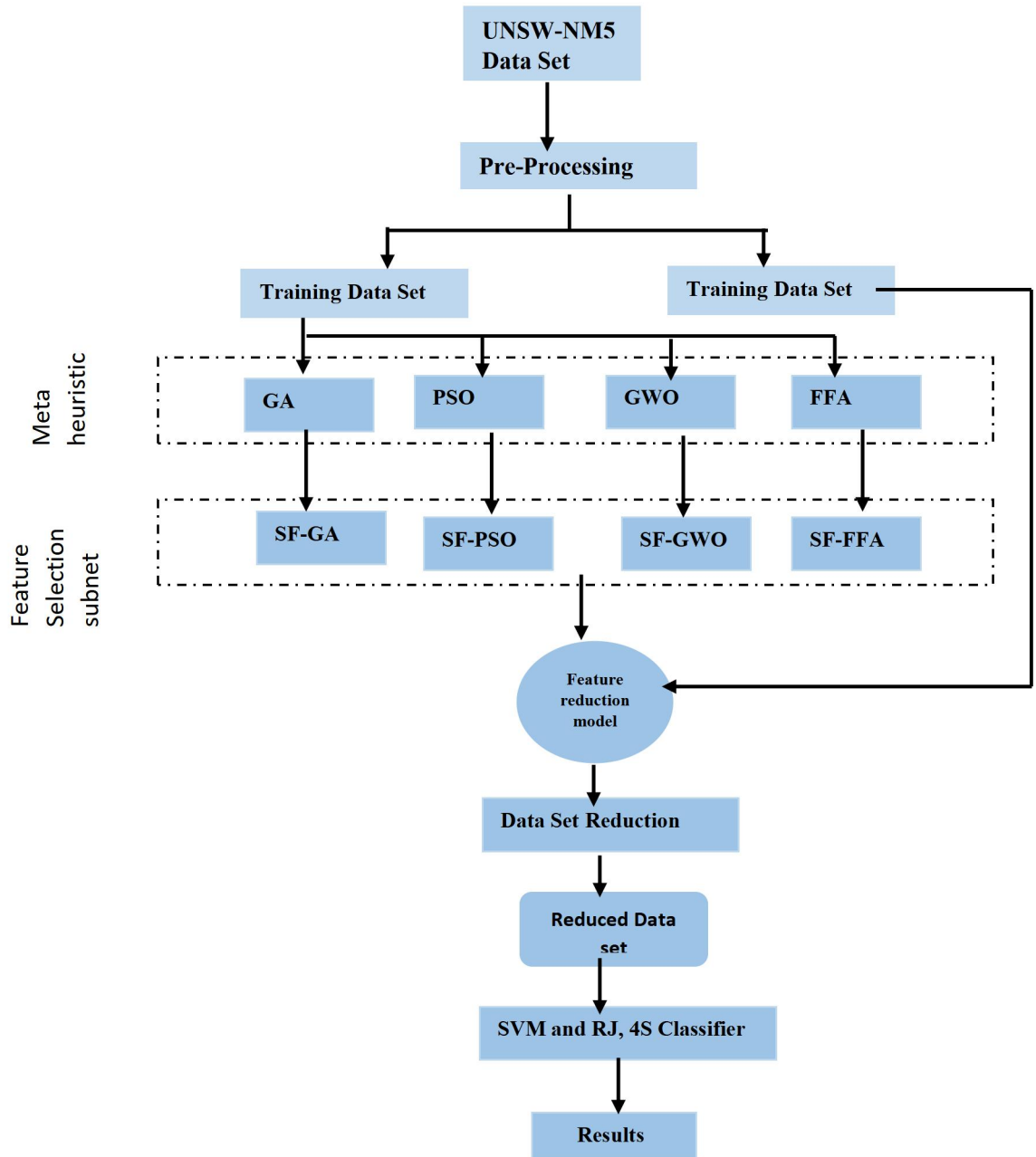


Figure 6.3: The architecture of the suggested paradigm.

6.2 The Choice of Characteristics Applying Metaheuristic techniques influenced by biology

The choice of subgroup characteristics presents a challenging problem. When the feature is highly dimensional, it cannot be managed effectively. Meta heuristic algorithms with a bio-inspired design are appropriate for handling this problem. They can provide excellent solutions within a fair length of time and with a reasonable

amount of effort [160, 161].

6.2.1 Selection of GA Features

The use of GA [37–38] is an adaptive search technique for solving objective functions depending on the idea of unbiased choice. GA encodes a number of optimization issues and their solutions. Construct a population, those responses are selected randomly. After that, GA assesses this population using a fitness function. The problem that needs to be solved determines which approach is better. Reliability, or F-measure, the space beneath the curvature, may be evaluated using the root mean square deviation, or AUC. The more physically fit individuals are chosen for crossover and mutation, two types of reproduction operations. Until it satisfies the termination requirement, this operation is repeated. A group of generations will be created as a result of this.

6.2.2 Selection of PSO Features

Optimizing using the Particle Swarms Algorithm was created by James Kennedy and Russell Eberhart [162]. It was made utilizing a simple concept motivated by the motion of fish groups and bird flocks. The creation of it was based on several computational simulation-based analyses. PSO makes use of several agents (particles) that aggregate into swarms. To locate the answer regarded as the best, this swarm moves about in the search area. It modifies each particle's "flying" inside the target region to mimic both the motion of many other particles and its own.

Particles that are generated at random and whose velocities correspond to the search's speed release PSO. The elements are then put through a fitness evaluation process, much like the GA technique. Following this assessment, two significant exams are administered. The first test, known as personal best, compares a particle's experience with itself (pbest). The second test contrasts a particle's fitness with the overall swarm experience. Using the term "global best" (gbest), the winning particles are saved once these two tests are completed. The termination requirement is therefore satisfied.

6.2.3 Choosing GWO Features

Mirjalili et al. [41] proposed a GWO. It evolved as a result of hunting techniques. It was created using the grey wolf's leadership abilities. Figure 6.4 depicts the wolf social structure. It describes the beta, alpha, omega, and delta wolves.

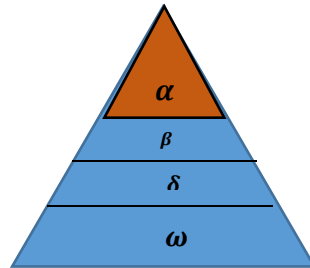


Figure 6.4: Wolves' hierarchy [41].

Wolf pack leaders make decisions. Although they might not be the toughest wolves in the group, they are unquestionably the best at leading the group. This is because coordinating and leading the group is far more crucial than simply being physically powerful. In the pack, Beta is a lesser wolf. It serves as the alpha's advisor. In the event of the alpha's passing or under any other conditions, it should be able to step in. Additionally, it helps the other pack members accept the alpha's judgments. It gives the alpha information about how the pack members feel about the alpha's choice. The pack's lowest-level wolf is known as Omega. It serves as a scapegoat for the other wolves in the pack. The presence of omega is crucial. Omega maintains the prevailing structure and pleases everyone in the pack, which explains why. The remaining members of the squad, known as "delta," submit to alpha and beta. This level's members are sentinels, scouts, elders, caregivers, and hunters.

The three primary steps of the group hunting procedure are carried out based on this hierarchy. These are the steps to take:

- (1) Pursuing, approaching, and tracking the prey;
- (2) Following, enclosing, and disturbing the victim to halt its movement;
- (3) Going after the prey that is being pursued. The algorithm replicates the entire hierarchy and group hunting processes that were explained. It imitates those processes to address challenging engineering issues.

6.2.4 Selection of FFA Features

A meta heuristic approach considering feature extraction and the Firefly optimization algorithm(FFA). Xin-She Yang [163] came up with the concept. Its foundation is how tropical fireflies exchange messages. Additionally, the idealized behaviour of flashing patterns serves as its foundation. FFA builds the statistical method of the algorithm using the following idealized rules:

- a. Fireflies are gender-neutral.
- b. Their brightness is related to how attractive they are, and the surroundings of the optimal solutions determines and influences the light of the firefly.
- c. In the maximum problem, the intensity can be inversely linked to the worth of the optimization problem.

The default Firefly algorithm involves two crucial parts. Estimating the quantity of light is the primary consideration. The second observation is that the appeal has been changed. It is safe to infer that the recorded target feature landscape will have an impact on the firefly's brightness. The adjustment of attraction and the fluctuation in light intensity must be described.

6.3 The Model for Feature Selection using MI

The set of bio-inspired meta heuristic selection methods for properties is stated as follows:

- PSO (S1)-based feature set selection;
- GWO (S2) was used to select the feature set.
- FFA (S3)-based attribute set selection;
- based upon GA, particular feature set (S4).

Using MI and several rules, a combination of those extracted features is produced, as shown in Table 6.1.

Table 6.1: The guidelines for the proposed model.

Rule Number	Rules	Output
R1	$S \{f: f \in (S1 \cap S2)\}$	S5

R2	$S \{f: f \in ((S1 \cap S3))\}$	S6
R3	$S \{f: f \in ((S1 \cap S4))\}$	S7
R4	$S \{f: f \in ((S2 \cap S3))\}$	S8
R5	$S \{f: f \in ((S2 \cap S4))\}$	S9
R6	$S \{f: f \in ((S3 \cap S4))\}$	S10
R7	$S \{f: f \in ((S1 \cap S2 \cap S3))\}$	S11
R8	$S \{f: f \in ((S1 \cap S2 \cap S4))\}$	S12
R9	$S \{f: f \in ((S1 \cap S3 \cap S4))\}$	S13
R10	$S \{f: f \in ((S2 \cap S3 \cap S4))\}$	S14
R11	$S \{f: f \in ((S1 \cap S2 \cap S3 \cap S4))\}$	S15
R12	$S \{f: f \in ((S11 \cap S12 \cap S13 \cap S14))\}$	S16
R13	$S \{f: f \in ((S5 \cap S6 \cap S7 \cap S8 \cap S9 \cap S10))\}$	S17

6.4 Classifiers Using ML

Machine learning classifies data by using MLCs. As a consequence, the output of the recommended model rules, which yields a feature set, acts as the ML classifier's input. By identifying the incoming information as normal or abnormal, the classifier fulfills its function. SVM and the J48 classification are both used in the current investigation.

6.4.1 Classifier SVM

A binary classifier is the SVM. It is a typical method for classifying things into two groups. Based on the structural risk reduction principle, a super plan is developed in SVM to separate the material that can be applied to the class from the unfavourable sample class [164, 165]. Alternately, SVM can address the issues with linear classification by selecting the best kernel function. SVM may be expanded to handle scenarios of nonlinear classification. Due to the fact that it makes use of statistical theory of learning, it is a crucial method for machine learning (ML) identification [166]. The structural risk reduction approach, which SVM is used in, also has high generalization capabilities. Therefore, SVM is a strategy that is superior to any prospective classifier and more effective. It has been established via analysis of the pertinent publications that illuminate IDSs that SVM is a powerful classifier with a bigger capability than some other classifiers [150, 167].

6.4.2 Classifier (C4.5 Logic Tree) J48, 3.4.2

The most widely used tree classifier is the J48 method. In fact, Quinlan [168] created it. It is a predictive ML model-based extension of the ID3 method. To cut down on classification errors, the J48 algorithm employs an improved tree pruning strategy. The greedy dividing-and-conquering technique is another method the J48 usesorithm uses to repeatedly create the tree structure that contains the characteristics from the dataset for a second classifier. With the J48 classifier approach, datasets are divided according to attribute values in order to identify the likely forecast. Using the conceptual attribute values of the availability method, the decision tree for the J48 classification approach consists of the ID3 method. To cut down on classification errors, the J48 algorithm employs an improved tree pruning strategy. The greedy dividing-and-conquering technique is another method the J48 algorithm use to repeatedly create the tree structure that contains the characteristics from the dataset for a second classifier. With the J48 classifier approach, datasets are divided according to attribute values in order to identify the likely forecast. Using the conceptual attribute values of the available learning method the decision tree for the J48 classification approach... The J48 method also estimates the value separately for each feature. The estimation procedure continues until the prediction phase is finished. A characteristic is valuable if it offers a wealth of details about the data instances. The J48 method's potential to improve IDS accuracy has been the subject of several studies [169].

6.5 Pre-Processing of System Model

Both datasets serve as the experimental analysis's starting data sources. The following evaluation data is then analyzed to remove noise and incomplete data [170]. Because of the severe features, the categorizers generated a large number of false warnings. As a result, pre processing is required. Classification methods cannot be avoided since some common characteristics increase computation time and memory requirements. The following approximate variables are classified in the NSL-KDD dataset [171]:

$$r_s = \{f_{s1} + f_{s2} + \dots + f_{sn}\} \quad (2)$$

Where n denotes the different properties of the dataset

Rougher capabilities lack conventional performance due to the added expense and redundancies. The following are the corrected rough characteristics [171]:

$$r_s = \{f_{s1}, f_{s2}, f_{s3} \dots \dots \dots f_{sp}\} \quad (3)$$

Where p indicates the most distinguishing features

Certain unpleasant characteristics remain after eradication. Following the gathering and evaluation of data to determine its relative importance, pre processing is undertaken to maximize feature collection. The study employs a variety of data preparation strategies to achieve this goal, such as information extraction, normalization, integrating, and stage characterization.

6.5.1 Data Cleaning and Normalization

Data cleansing is the procedure of changing information that is false, out of place, redundant, insufficient, or poorly presented. Data analysis does not require information because it would be redundant. Errors in the outcomes are more challenging to make. In addition to purging, evidence is eliminated during data cleansing [172, 173]. Data cleansing includes improper data updates, data removals, and the elimination of superfluous information. The primary objective was to remove data in order to standardize data evaluation and make it simpler to find pertinent data for the study. It was critical to update the missing information in order to improve quality by deleting harmful data because some of the data was already partial or confusing. For integrating and normalizing data, the Min max normalization strategy is essential. While the smallest value is set to 0, the highest feature worth is assigned to 1. Each value between 0 and 1 is converted to its binary counterpart. The normalization method is described in Equation (4). [174].

$$R_{norm} = \frac{R_i - R_{min}}{R_{max} - R_{min}} \quad (4)$$

If R_i denotes data points, R_{min} defines the smallest data point's value, and R_{max} represents the greatest data point's value

In the presence of structured data, all three factors decide the normalized value at two designated data points [176, 175]. Because of polluted traffic data, the data will remain suspect even following the entire the normalization of unstructured data has been completed. The collection of these attributes from a range of complex systems allows for the evaluation of assault prediction [175].

6.6 Dataset Overview

The dataset is crucial for performance testing and evaluating an IDS. Many IDS datasets have been made available during the past few decades [177]. Among these datasets are the UNSW-NB15, KDDCup99, NSL-KDD, and DARPA Dataset. Usually, a dataset contains a number of characteristics [178]. These properties have names like class and feature. KDDCup99 and NSL-KDD were employed in the bulk of investigations that looked into IDSs [179]. The KDDCup99 and NSL-KDD databases were unable to meet the requirements of this research. Thus, it turned to the UNSW-NB15 dataset. The need to fulfil operational needs and the quick evolution of network security are to blame for this [180]. A dataset typically has numerous properties. These properties have names like class and feature. KDDCup99 and NSL-KDD were employed in the bulk of investigations that looked into IDSs [181]. The KDDCup99 and NSL-KDD databases were unable to meet the demands of this investigation, so it turned to the UNSW-NB15 dataset. The need to fulfil operational needs and the quick evolution of network security are to blame for this [182].

The researchers recently finished producing the dataset UNSW-NB15. The UNSW-NB15 testbed is shown in Figure 6.5 [183]. A hybrid dataset called the UNSW-NB15 database combines simulations with real-world attacks to track real-time network activity. The authors of the research used a dataset called UNSW-NB15. The attack creation programme IXIA Perfect Storm was used to construct the database UNSW-NB15. It includes nine groups of real and modified assaults. Numerous servers are the targets of these assaults. The authors acquired tcp dump traces of network activity covering 31 hours at the start of 2015. Using these network records, a dataset with 49 attributes for each data transmission was created [183].

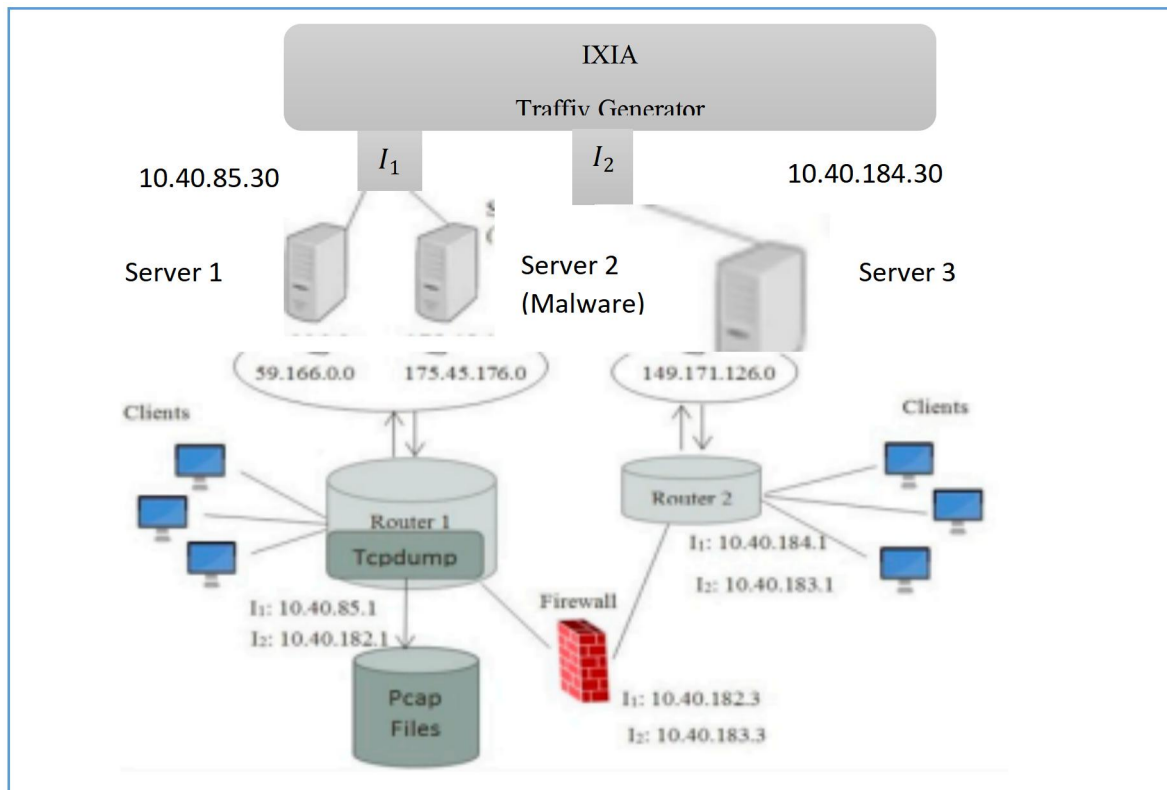


Figure 6.5: UNSW-NB15 testbed

There is assistance provided using specialized tools like Argus and Bro-IDS. With the help of this tool, it is possible to extract the traits when creating the UNSW-NB15 database. The pcap files are supplied to Argus and Bro-IDS. Argus is capable of controlling the network's unfiltered traffic. The server Argus in a client-server setup converts raw pcaps files to an Argus-compliant format. After that, the functions will be read and extracted from the Argus scripts by the Argus client. There are 49 connection features accessible for each data instance. Others are numerical, while some traits are statistical. Other features include time stamp values. Training datasets were created using the dataset for UNSW-NB15. There are 175,341 total elements throughout the practise set. 82,332 recordings totaling both regular, detailed traffic statistics and recordings of various assaults are included in the testing collection. There are 45 features total in both the training and testing datasets. More information about these traits is provided in Table 6.2. The test and training datasets for UNSW-NB15 lack several attributes. Among these traits are sports, scrip, s-time, l-time, and d-stip.

Table 6.2: The following characteristics are listed in the UNSW-NB15 Dataset.

Feature No	Feature Name	Feature No	Feature Name	Feature No	Feature Name
1	Id	16	Dloss	31	response_body_len
2	Dur	17	Sinpkt	32	ct_srv_src
3	Proto	18	Dinpkt	33	ct_state_ttl
4	Service	19	Sjit	34	ct_dst_ltm
5	State	20	Djit	35	ct_src_dport_ltm
6	Spkts	21	Swin	36	ct_dst_sport_ltm
7	Dpkts	22	Stcpb	37	ct_dst_src_ltm
8	sbytes	23	Dtcpb	38	is_ftp_login
9	Dbytes	24	Dwin	39	ct_ftp_cmd
10	Rate	25	Tcprtt	40	ct_flw_http_mthd
11	Sttl	26	Synack	41	ct_src_ltm
12	Dttl	27	Ackdat	42	ct_srv_dst
13	Sload	28	Smean	43	is_sm_ips_ports
14	Dload	29	Dmean	44	attack_cat
15	sloss	30	Trans_depth	45	Label

6.7 Measures for Present Assessment

All subsequent statistics, which take into account a wide range of variables, decide how well these suggested models work. The initials (FP, FN, TP, TN) designate these measures, which comprise false positive, false negative, true positive, and true negative [184]. The True negative and True positive rate were determined using the matrix of misinterpretation (Table 6.3) (FP rate). Other parameters could be derived from these numbers. Perception, accuracy, consistency, and the F-measure are examples of these components.

Table 6.3: Confusion matrix.3

		Predicted	
		Normal	Attack
Actual	Normal	a (TP)	b (FN)
	Attack	c (FP)	d (TN)

The amount of normal data recognized as such is determined using TPR.

This is how the equation appears:

$$TPR = \frac{a}{a+b} \quad (5)$$

The amount of attack knowledge classified as a result of assault data as determined by TNR.

The procedure is as follows:

$$TNR = \frac{d}{d+c} \quad (6)$$

The fraction of assault data which is categorized when regular data are determined using FPR. The equation looks like this:

$$FPR = \frac{c}{c+d} \quad (7)$$

The fraction of information that's also typically labelled due to assault data determined using FNR. The equation reads Following is:

$$FNR = \frac{a}{a+b} \quad (8)$$

A percentage is used to indicate accuracy. It describes how well the cases are predicted in general. The equation reads as follows:

$$Accuracy = TPR + TNR \quad (9)$$

$$TPR + TNR + FPR + FNR$$

The proportion of decisions that are deemed correct serves as a measure of precision. The TP, which is the result of the FP and TP, reflects this. The following is the

formula:

$$\text{Precision} = \frac{TP}{TP + FP} \quad (10)$$

Vulnerability is measured by the ratio of the overall quantity of positive evaluations to the overall number of TP evaluations. The method is as follows:

$$\text{Sensitivity} = \frac{TP}{TP + FN} \quad (11)$$

The degree of precision is evaluated using the F-measure. It alludes to the harmony that exists between sensitivity and precision on the one hand. The formula is as follows:

$$F \text{ Measure} = 2 * \text{Accuracy} * \text{Sensitivity} \quad (12)$$

$$\text{Precision} + \text{Sensitivity}$$

6.8 Performance Analysis of the Proposed Model

Few parameters considered for the experimental scenario which are collected from the existing IDS environment are shown in the table1. The various existing IDS are compared in terms of the following parameters.

Table 6.4. The Parameters studied for the existing IDS.

Existing IDS Tools	Accuracy	Detection rate	False Positive Rate	Precision	F1 score	Specificity	Negative Predictive Value
Snort	98.6	89.6	1.1	75.3	81.8	98.8	99.6
Suricata	98.4	87.9	0.5	88.5	92.2	97.8	99.9
Wireless Intrusion Detection Prevention and Attack System	99.7	96.2	0.7	90.1	94.2	99.2	92.2
Synchrophasor Specific Intrusion Detection system (SSIDS) tool	99.6	97.1	0.8	92.2	97.5	98.6	90.1

The proposed IDS research results are compared with the existing IDS, and the following observations are made according to table 6.5.

Table 6.5: Analysis of the existing IDS in comparison to the proposed system

Authors	Algorithm	Accuracy (%)	FPR (%)
Vu Viet Thang, F. F. Pashchenko (189)	DT	98.2	0.016
Preeti, Kusum Deep (190)	GA(Genetic Algorithm)	96.4	0.05
Guo Jun Li (191)	KNN	98.45	0.048
	TCM + KNN	99.4	0.1
Proposed Classifier	PSO+DT	98.5	0.011
	PSO+KNN	99.6	0.004
	PSO+ANN	99.78	0.003

The following graphs,figure 6.6 and figure 6.7 shows the comparative analysis of the existing IDS with the proposed IDS in terms of Accuracy and False Positive Rate.

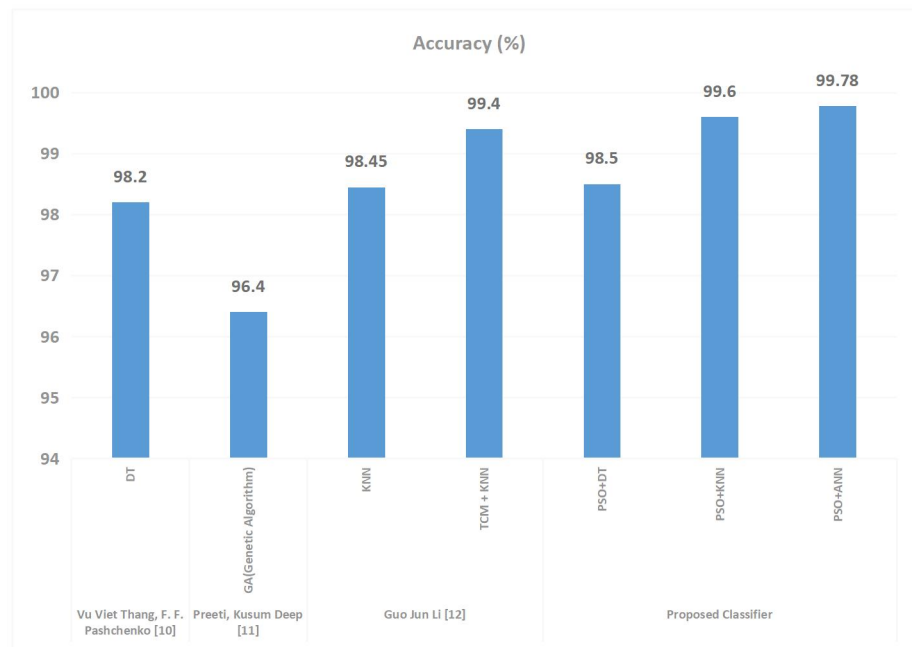


Figure 6.6 : Comparison evaluation of the current system to generate the accuracy assessment

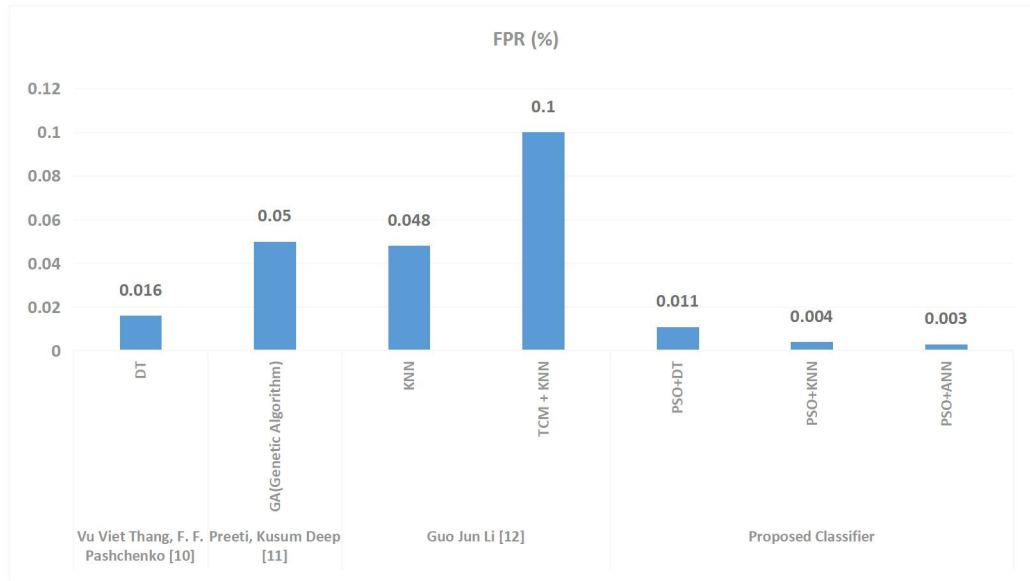


Figure 6.7: Comparison evaluation of the current system to generate the false positive rate assessment

As a result, it can be said that the suggested IDS, PSO+ANN, offers the highest accuracy and the lowest FPR when compared to other systems. In comparison to the other IDS, the Proposed IDS exhibits the best attack detection accuracy, of 99.78%, and the lowest False Positive rate, of 0.003%, as seen in table 6.5.

Chapter-7
Proposed System
for Wireless
Network Intrusion
Detection and
Prevention

Chapter-7

Proposed System for Wireless Network Intrusion Detection and Prevention

This chapter provides detailed explanations of the proposed methodology for each of the research phases that has been conducted.

Finally, a method for detecting and preventing intrusions in wireless devices is provided. The total effectiveness of the proposed system will be enhanced by its capacity to halt the attacker and protect the wireless connection from various assaults by informing the administrator and so protecting the network's genuine nodes.

As a result, an intrusion prevention system would be created for safeguarding any organization's assets, in which the main aim is to protect genuine nodes from repeated attacks by informing the administrator, as well as using algorithms based on clusters to separate the components and ML approaches to trace the DoS attack.

7.1 Proposed Methodology

The proposed methodology of the entire research work has been summarized below. The figure 7.1 representing Experimental setup two distinct networks, one representing an enterprise virtual private network and another representing a secure blade-simulated virtual network.

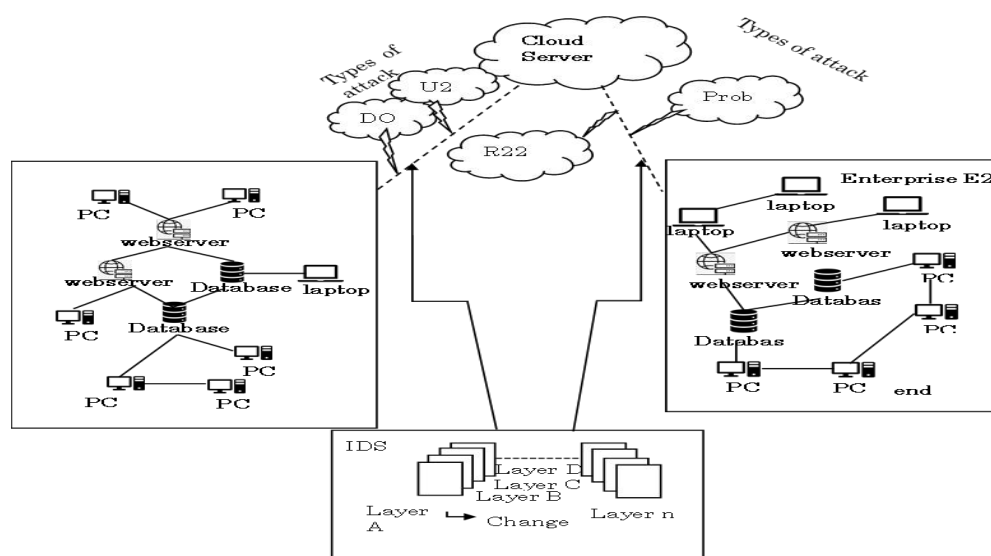


Fig. 7.1: Experimental setup two distinct networks, one representing an enterprise virtual private network and another representing a secure blade-simulated virtual network

Experimental Set up in figure 7.1 has integrated a test case as shown in the figure. Two to four virtual networks were created. Each Virtual network consists of 2 database servers, 2 web servers and 250 PCs i.e., end users. This virtual network was named Enterprise E1. Similarly, there were enterprises E2, E3, E4. These virtual networks were connected to each other through cloud servers. Now different attacks were produced on the web servers or database servers of any enterprise or the Cloud server itself, like Dos attack, probe attack, U2R, R2L etc. The proposed IDS could identify these attacks and it produced an alert to the network admin where the attack was made.

The IDS could figure out the IP address of the attacker, its Operating System used, whether the attacker is in an enterprise or an individual and other details of the attacker. Also, if an unauthorized user tries to see the password 'abc' suppose of any legal user's encrypted file, then the proposed IDS changes from layer A to layer B and thus changes the password from 'abc' to 'def' suppose. And if the hacker sees this changed password also then the IDS changes the layer from B to C and the password. This goes on repeating; Thus, the proposed IDS is tried to be made more powerful by building many numbers of hidden layers in it.

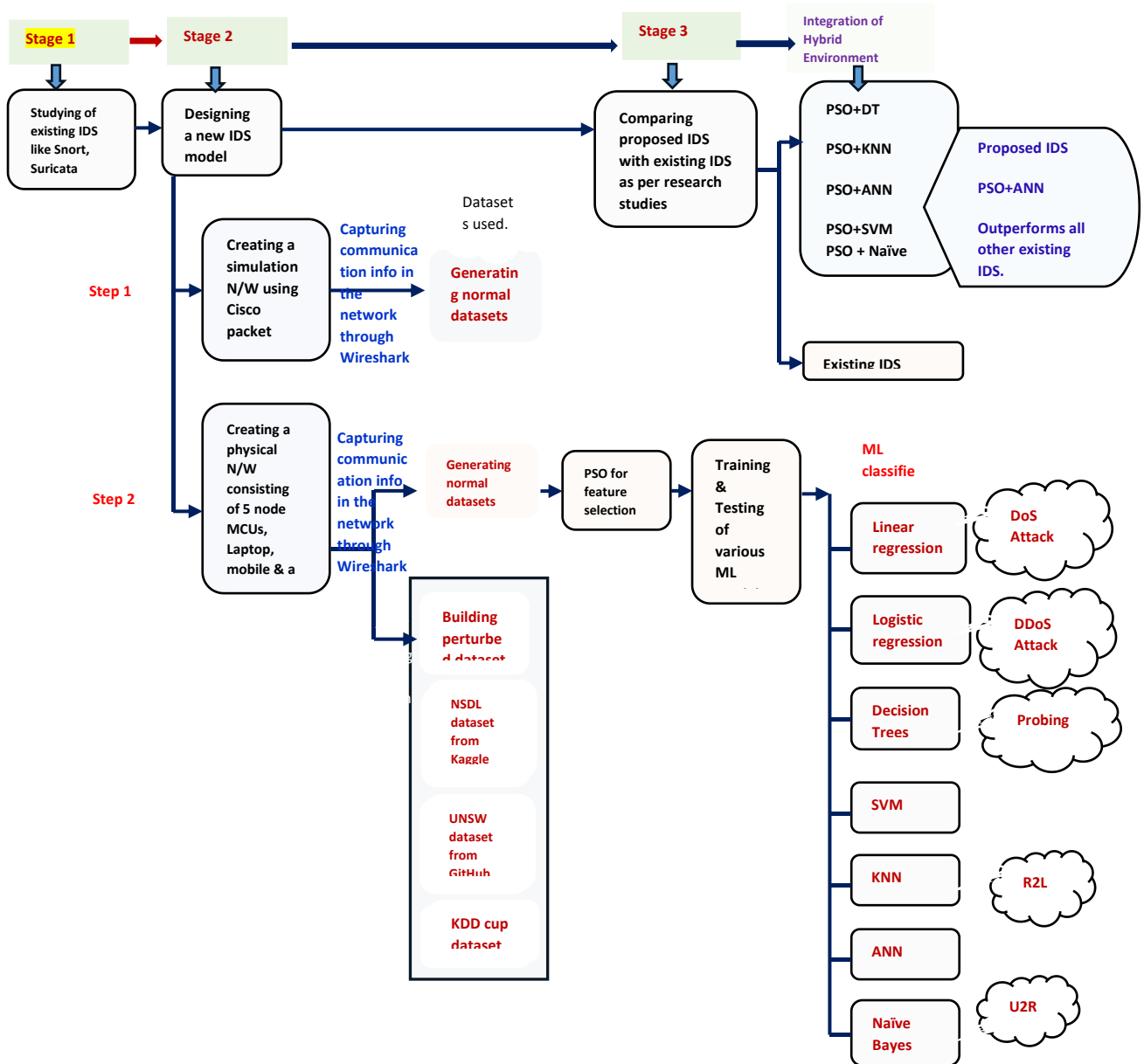


Fig.7.2:Communication channel and simulated network among end user, console devices through routers through Particle Swarm based Optimization

The simulation network has been fulfilled in the following manner: The suggested research work's methodology entails building several wireless networks using Cisco Packet Tracer, which uses PCs, servers, and routers connected through wires and LAN connections, and then using the Wireshark application to record communication that occurs between them. In addition, a mobile hotspot internet connection was used to connect a laptop, a mobile phone, and five node MCUs to a real physical network, and the Wireshark application was used to record the traffic between them. The

communication channel and simulated network among end user, console devices. Figure 7.2 illustrates how routers may be optimized using Particle Swarm Theory.

These datasets, along with some common datasets like UNSW, the KDD Cup dataset, and the NSDL dataset, are used to train the various machine learning models so that they become skilled at spotting attacks in each network after being collected. The datasets main features include source IP addresses, destination IP addresses, travel times between sources and destinations, and protocols that are involved. Prior to that, PSO was used on these datasets as an optimization approach, as well as for feature selection, which decreases the number of features in the datasets and makes it simpler for machine learning algorithms to detect intrusions. Additionally, the suggested method is contrasted with the current IDS in a comparison study.

Chapter 8

Comparison of Results with Discussions

Chapter 8

Comparison of Results with Discussions

The final findings of all specified objectives, including such Predictive Performance, True Measure Rates (TMR), and False Positive Rate for F-Measure (FPR), Precision and Accuracy Rates, and Application Platform of Cisco Packet Tracer, are reported in this Chapter.

Factors like efficiency, responsiveness, retraining length, and other terms of a comparable kind can be used to analyze the efficiency of various classifiers. The clustering approach serves as the basis for evaluating several factors. The cast of uncertainty [185] may be used to calculate the number of times a classifier model has been effectively or incorrectly estimated. The clustering technique is commonly presented as the Actual Positive, Actual Negative, Fake Positive, and True Positive values.

8.1 Analysis of Protocols' influence in the network

Several protocols involved in the communication were used to plot the graphs between the source IPs and the destination IPs. Here the graphs were plotted for different protocols. It was observed that at some point of time, maximum resistance was offered by the destination IPs to some particular source IPs. So it was concluded that the points where maximum resistance was offered could be the points of intrusions.

8.1.1 Initialization Step

For $i = 1$ to N do

$A(x, y, z) = N [A(x) * A(y) * A(z)]$

Iteration Step

$B[A(i, t)] = \text{Null}$

For $t = 0$ to T do

For $i = 1$ to N

For j = Null to Value

NetworkIntrusion (i, t) = MAX_{j=1, N} (NetworkIntrusion (j, t-1) * P (C_i|C_j)) * P (wt|C_i) * N [A(x) * A(y) * A (z)]

Identifying Sequence Step

C (T) = i that maximizes NetworkIntrusion (x, y, z, i, j) \propto T

Backtracking to determine the order of intrusion

The NetworkIntrusion (X, Y, Z, I j) array records the frequency of the best sequence for sources,destination, protocols, intrusion and values characteristics. C (T) functions will be having probability and weight age for particular network characteristics.

8.1.2 Result

Several protocols involved in the communication were used to plot the graphs between the source IPs and the destination IPs. Here the graphs were plotted for different protocols. It was observed that at some point of time, maximum resistance was offered by the destination IPs to some particular source IPs. So it was concluded that the points where maximum resistance was offered could be the points of intrusions.

Table 8.1: Shows the Source, Destination and Protocol dataset with respect to our test environment of network topology as shown in fig 1.1

Source	Destination	Protocol
192.168.239.1	192.168.239.1	ARP
192.168.239.254	192.168.239.254	BROWSER
fe80::f9fc:ad11:1e14:b75	192.168.239.255	DHCP
VMware_c0:00:08	224.0.0.22	ICMPv6
VMware_fc:23:ae	224.0.0.251	IGMPv3

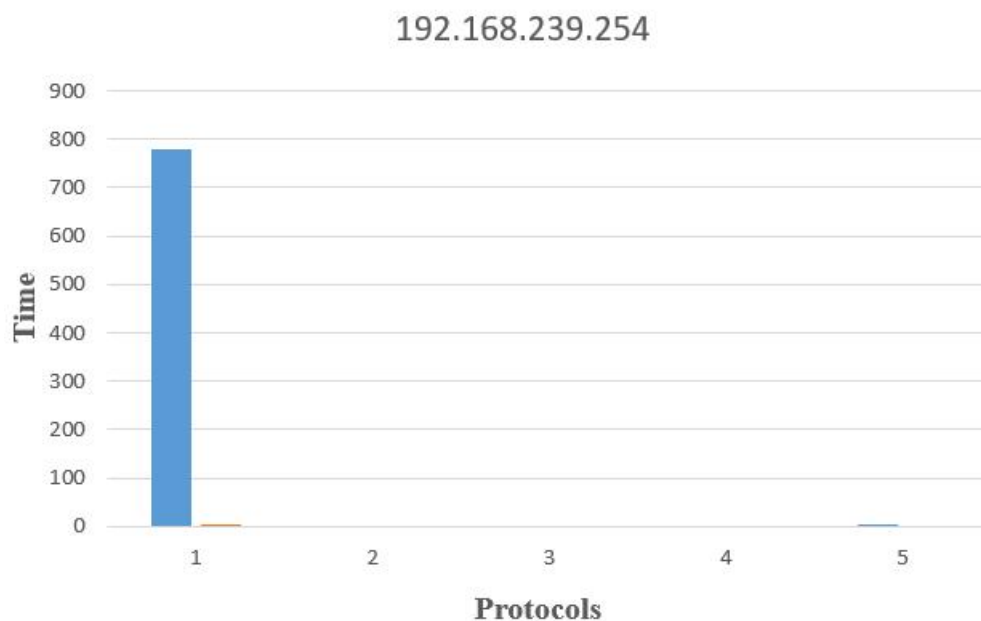


Figure 8.2: Shows protocols vs (192.168.239.254) Source IP

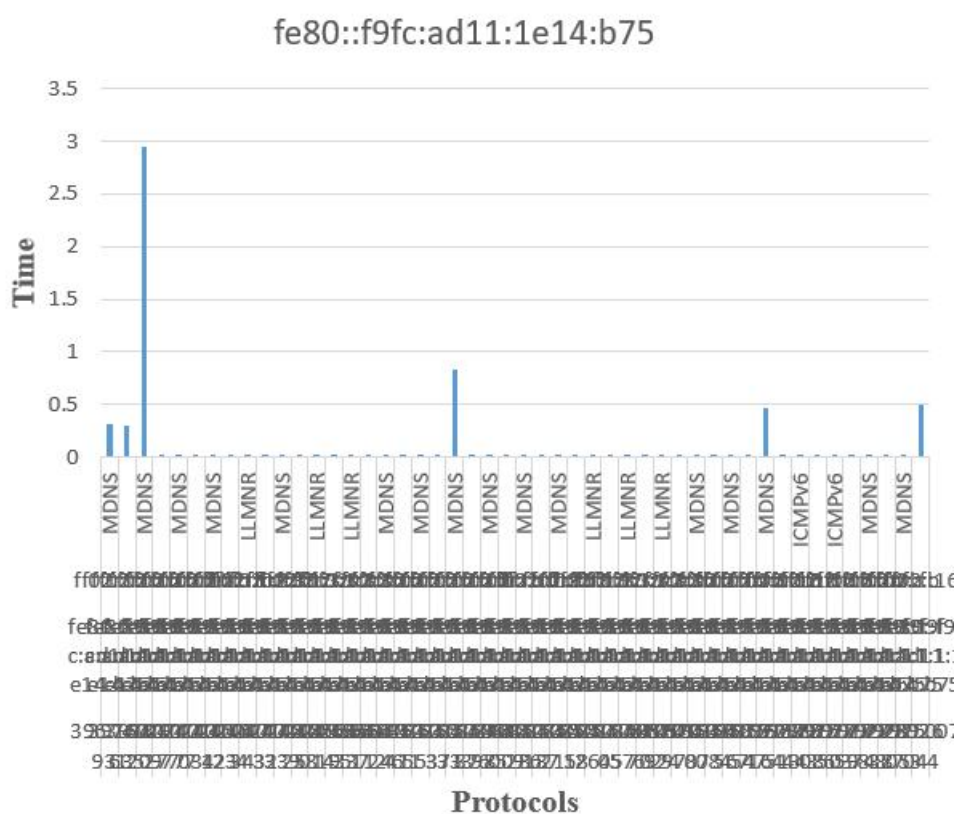


Figure 8.3: Shows protocols vs (fe80: f9fc:ad11:1e14: b75) source IP

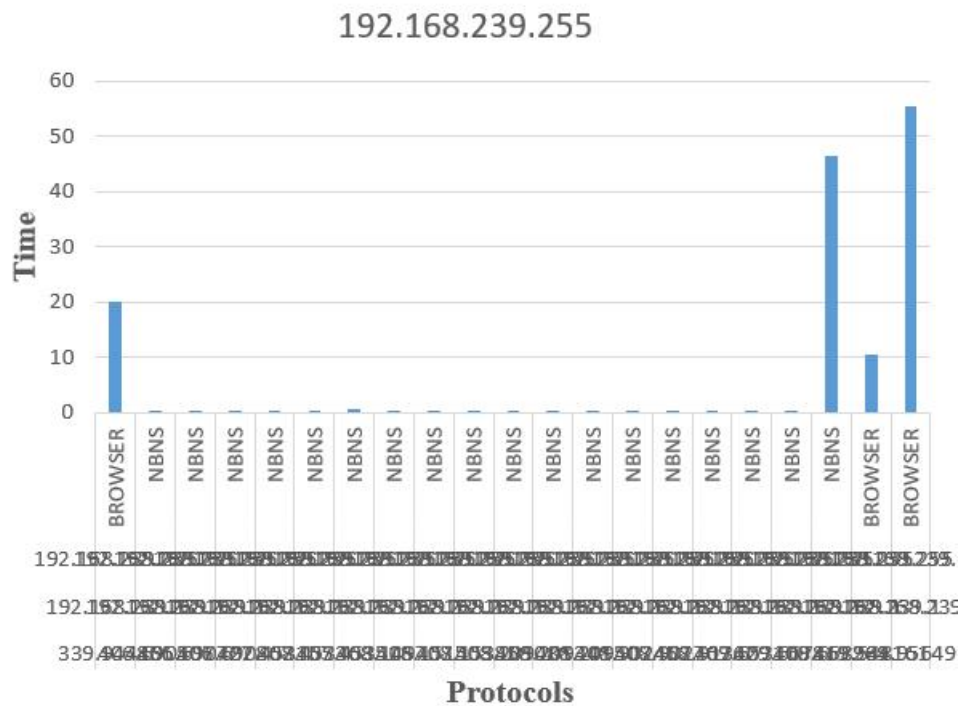


Figure 8.6: Shows protocols vs (192.168.239.255) destination IP

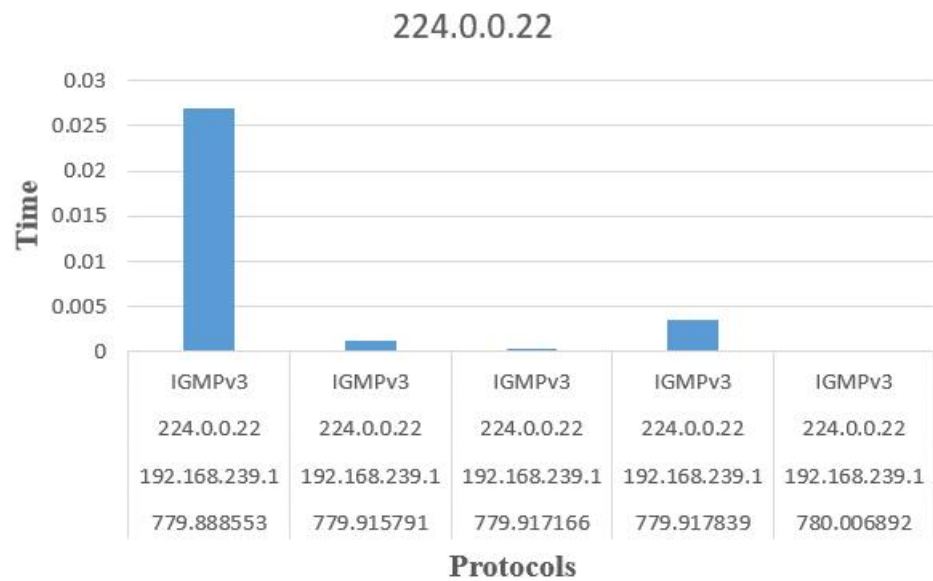


Figure 8.7: Shows protocols vs (224.0.0.22) destination IP

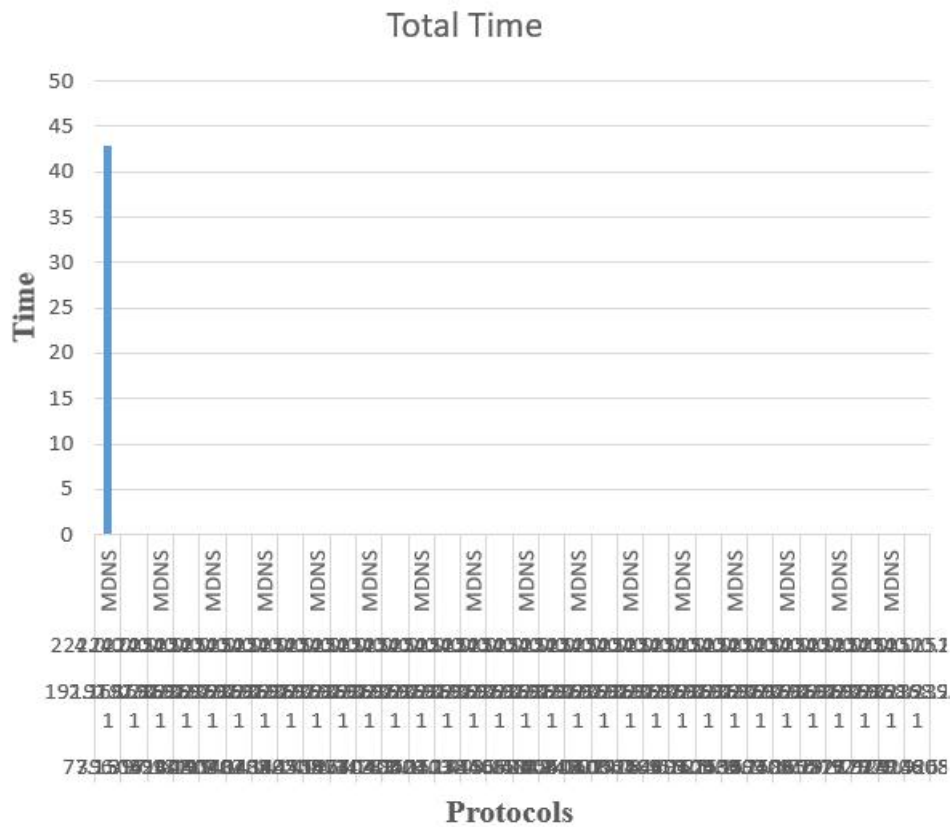


Figure 8.8: Shows protocols vs (224.0.0.251) destination IP

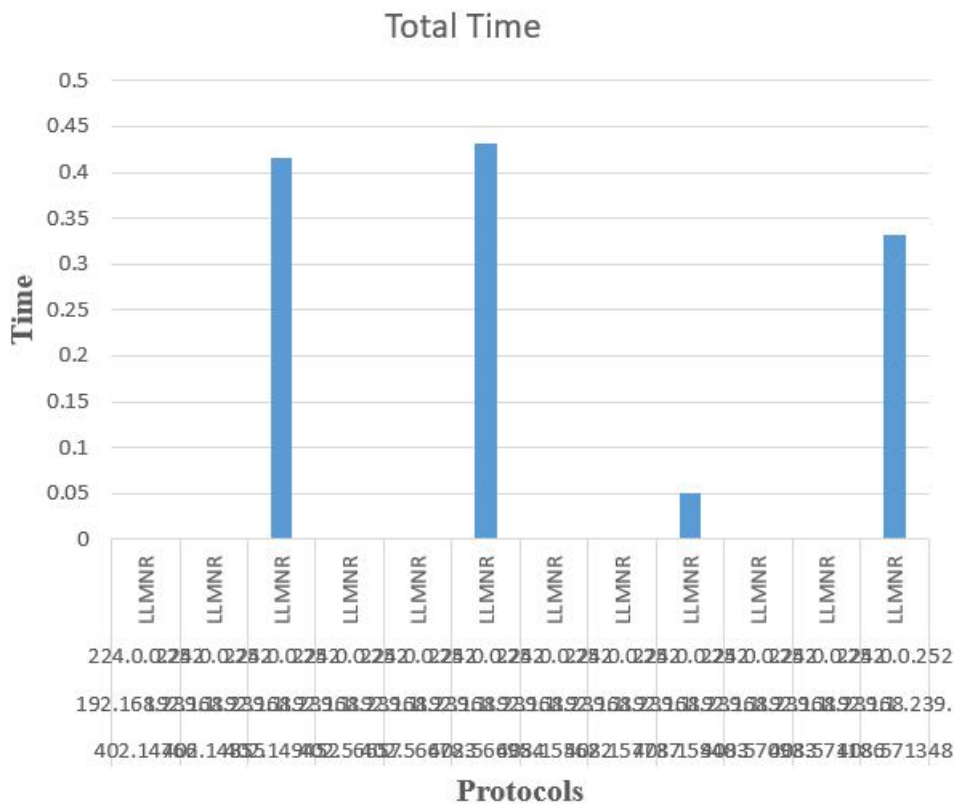


Figure 8.9: Shows protocols vs (224.0.0.252) destination IP

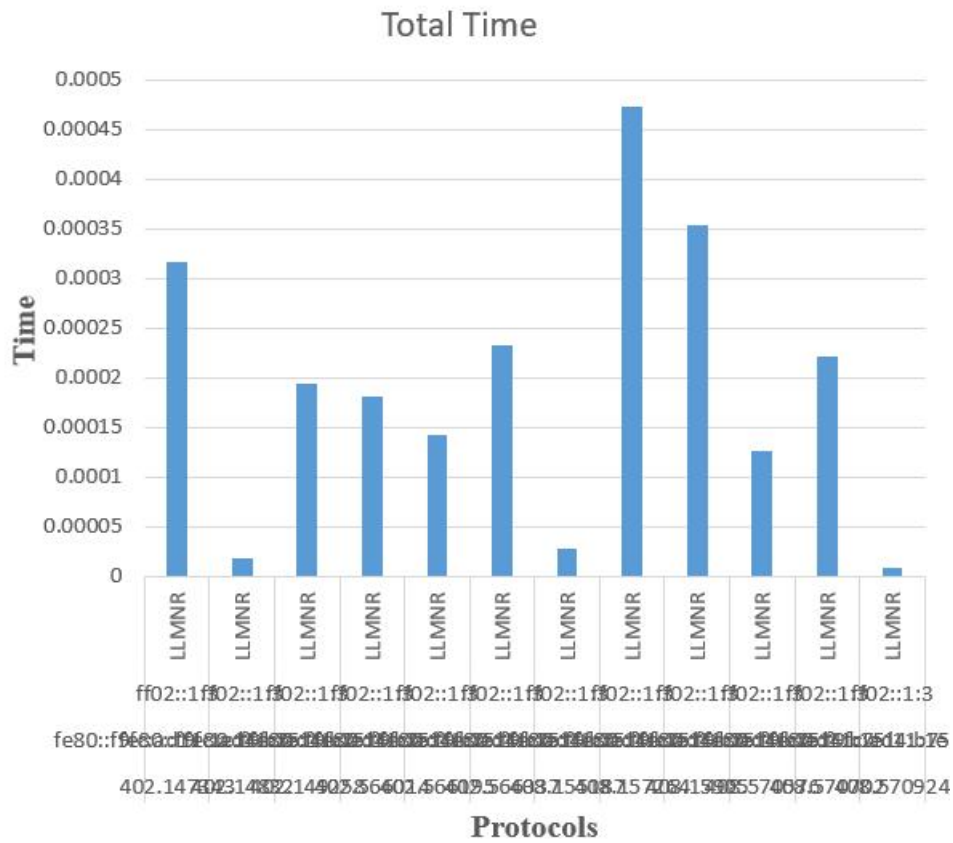


Figure 8.12: Shows protocols vs (ff02: 1:3) destination IP

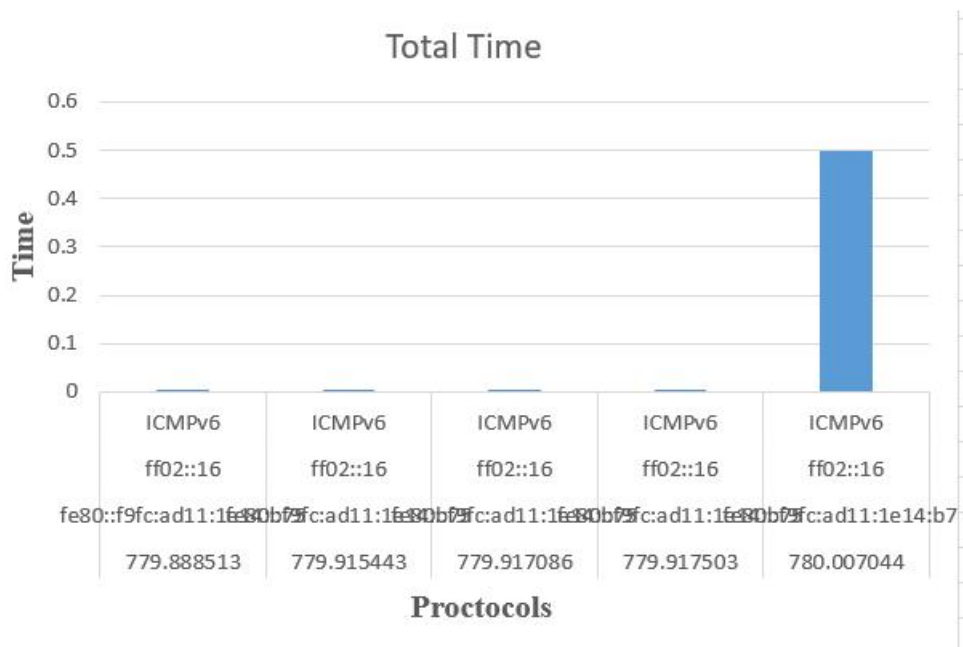


Figure 8.13: Shows protocols vs (ff02::16) destination IP

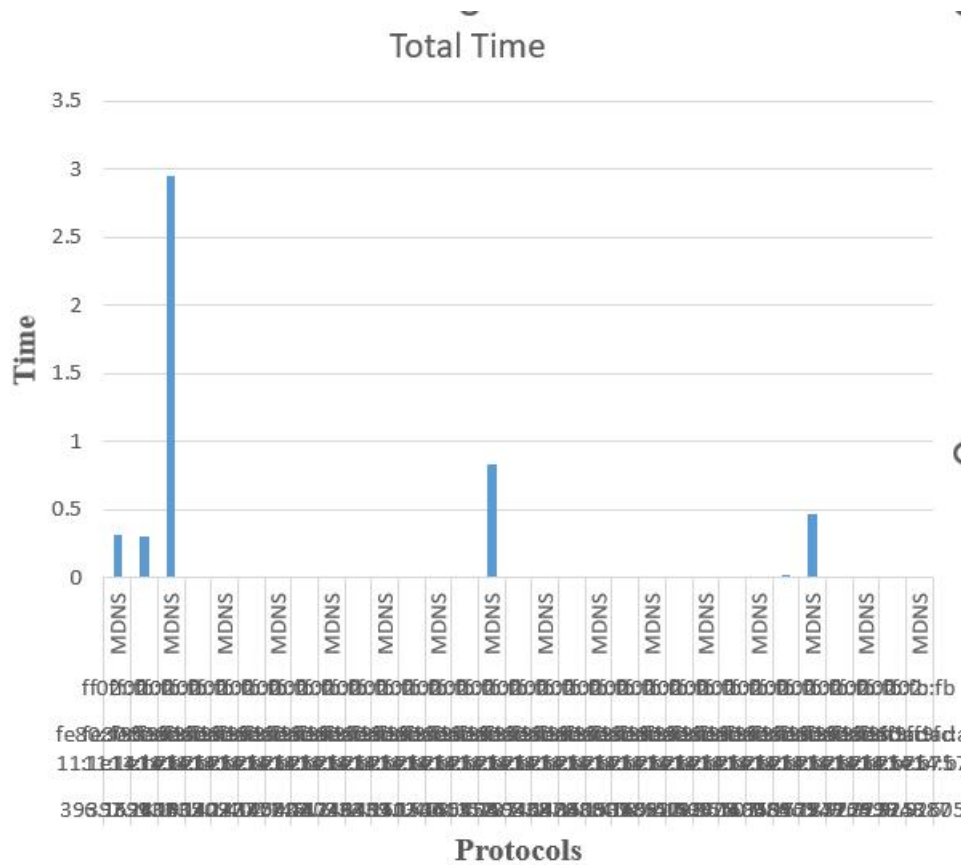


Figure 8.14: Shows protocols vs (ff02::fb) destination IP

As shown in fig 8.1 to fig 8.14, we've done data visualization with regard to the several protocols shown in the table 8.1 above, with respect to various source IPs and destination IPs. The Fig. 8.1 displays data visualization on source IP in relation to the different protocols. The data is verified for source and destination IP with the two VM being common in both the rows of table 8.1 called as VMware_c0:00:08 and VMware_fc:23:ae. This VM machine are the link between the cisco packet tracer network test model and simulation environment of wireshark. Protocols such as LLMNR, MDNS, NBNS are easily been identified just by our simple modelling of network nodes with functions of communication protocols. This protocols if considered independent of source and destination IP, then the proposed way of simulation model is perfect to design any network infrastructure for live monitoring of intrusion through any protocols.

8.2 Performance Evaluation

Factors like efficiency, responsiveness, retraining length, and other terms of a comparable kind can be used to analyze the efficiency of various classifiers. The

clustering approach serves as the basis for evaluating several factors. The cast of uncertainty [185] may be used to calculate the number of times a classifier model has been effectively or incorrectly estimated. The clustering technique is commonly presented as the Actual Positive, Actual Negative, Fake Positive, and True Positive values, as given in Table 8.2 [7, 8]. The following requirements are summarized in Table 8.2:

TP: This denotes circumstances that are accurately predicted as being usual.

FN: This shows that real assaults are classified as typical and that the incidence prediction is incorrect.

FP: This offers an idea of the amount of assaults detected that are consistent of the present situation.

TN: This includes officially classified activities like a strike.

Table 8.2: The Confusion Cast for Extraordinary Intensity.

Absolute	Expected	Common	Oddity
	Common	genuine positive	false negative
	Oddity	False positive	True negative

The method was put to the test utilizing two rule classifiers and two types of anomalous network traffic: back and Neptune. To put the proposed technique into action, training and evaluation datasets for both usual and a typical network traffic patterns are employed.

Table 8.3 lists the Knowledge discovery 99 dataset's network traffic classifications. The test instances were 29154 for normal traffic, the training examples for aberrant network traffic were 425901, and the test instances were 119051. The number of test cases was 29153, whereas the number of typical training examples was 68122 for normal traffic.

Table 8.3: Network Traffic Types

Types of Network Traffic	Learn	Evaluate
Normal	68122	29153

Anomalies	425901	119051
-----------	--------	--------

Table 8.4 the suggested extractor PSO+DT's TN, TP, FP, and FN values are 141204, 4846, 1594, and 560, correspondingly. This image depicts the prediction system for this classifier.

Table 8.4: Matrix of confusion for PSO+DT classifier

Absolute	Predicted	Common	Oddity
	Common	True negative=141205	False =1593
	Oddity	False negative= 561	True P =4845

The PSO+KNN classifier was the next proposed classifier, and its parameters for the contingency table were TN = 143675, TP = 3872, FP = 505, and FN = 154 (Table 8.5). The statistics from the contingency table are used to assess the effect of the implemented system.

Table 8.5: PSO+KNN uncertainty cast

Absolute	Predicted	Common	Oddity
	Common	TN=143675	FP =505
	Oddity	FN= 154	TP =3872

The Accuracy, Exactness, NPV, and F1 score estimation techniques for the classifier are shown in Table 8.6. The graph clearly demonstrates how PSO+ANN integrates other two algorithms in terms of Accuracy (99.7%), Exactness (90.2%), NPV (99.8%), and F1 score (94.3%).

Table 8.6: Performance Metrics for Proposed Categorizations

Evaluates	PSO+DT (%)	PSO+KNN (%)	PSO+ANN
------------------	-------------------	--------------------	----------------

Accuracy	98.8	99.6	99.7
Exactness	75.2	88.6	90.2
Negative Predictive Value	99.7	99.8	99.8
F1 Score	81.9	92.3	94.3

Table 8.7 Intrusion Detection aims for maximum output correctness and precision while minimizing false-positives [186]. This table depicts the detection performance and false alarm rate for the proposed algorithms PSO+DT, PSO+KNN and PSO+ANN. PSO+ANN has a detection results of 97.1%, a lower FPR of 0.03%, and an accurate results of 99.78%, according to the results.

Table 8.7: Assessment of suggested classifiers

Evaluat es	PSO+DT (%)	PSO+KNN (%)	PSO+ANN (%)
Correct ness	98.5	99.6	99.78
DR	89.7	96.2	97.1
FPR	1.2	0.4	0.03

The recommended study exceeded Sindhu, Geetha, and Kannan [186], Mohammad Sazzadul Hoque [187], and Guo [188] in terms of a better accuracy of 99.7% and a reduced FPR of 0.003%, according to Table 8.8's assessment to the current model.

Table 8.8: Analysis of the existing ID system in comparison to the proposed system

Authors	Algorithm	Accuracy (%)	FPR
Sindhu, Geetha & Kannan [186]	DT	98.2	0.016
Mohammad Sazzadul Hoque [187]	GA	96.4	0.05
Guo [188]	KNN	98.45	0.049

	TCM+KNN	99.4	0.2
Proposed Classifier	PSO+DT	98.8	0.11
	PSO+KNN	99.6	0.04
	PSO+ ANN	99.7	0.003

8.3 Selection Keyword Research Results

All testing was done using Windows 7 and an Intel Core i7 processor running at 3.40 GHz with 6.0 GB of memory. For the experiments, Anaconda Python Open Source [128] was utilized. The traits that have been picked and are believed to be significant are shown in Table 8.9 in accordance with the suggested model rules for identifying attacks.

Table 8.9: Important selected features.

Rule	Select Features	Features Number
PSO	f2, f4, f5, f7, f11, f12, f16, f17, f18, f19, f20, f22, f23, f24, f25, f26, f28, f30, f31, f33, f34, f39, f40, f41, f43	25
GWO	f1, f4, f5, f6, f9, f13, f16, f17, f22, f23, f26, f28, f29, f35	20
FFA	f1, f2, f3, f6, f8, f9, f10, f11, f12, f13, f16, f19, f26, f28, f35, f37, f39, f40, f41, f43	21
GA	f1, f2, f3, f4, f6, f8, f9, f11, f13, f16, f21, f24, f25, f27, f28	23
(R1) PSO \cap GWO	f4, f5, f16, f17, f22, f23, f26, f28, f35, f39, f41, f43	12
(R2) PSO \cap FFA	f2, f4, f11, f12, f16, f26, f28, f35, f37, f39, f40	11
(R3) PSO \cap GA	f2, f4, f5, f11, f16, f24, f25, f28, f33, f39, f41	11
(R4) GWO \cap FFA	f1, f9, f16, f26, f28, f35, f37, f41, f43	9
(R5) GWO \cap GA	f1, f4, f6, f9, f16, f22, f23, f35, f41, f43	10

(R6) FFA \cap GA	f1, f2, f3, f8, f9, f11, f13, f16, f28, f35, f37, f41, f43	13
(R7) PSO \cap GWO \cap FFA	f4, f5, f16, f17, f22, f23, f26, f28, f35, f41, f43	11
(R8) PSO \cap GWO \cap GA	f4, f5, f16, f22, f23, f35, f41, f43	8
(R9) PSO \cap FFA \cap GA	f2, f4, f11, f16, f28, f35, f37, f41, f43	9
(R10) GWO \cap FFA \cap GA	f1, f9, f16, f26, f28, f35, f37, f41, f43	9
(R11) PSO \cap GWO \cap FFA \cap GA	f16, f28, f35, f41, f43	5
(R12) (PSO \cap GWO \cap FFA) \cup (PSO \cap GWO \cap GA) \cup (PSO \cap FFA \cap GA) \cup (GWO \cap FFA \cap GA)	f1, f2, f4, f6, f9, f11, f13, f16, f26, f28, f35, f37, f41, f43	13
(R13) (PSO \cap GWO) \cup (PSO \cap FFA) \cup (PSO \cap GA) \cup (GWO \cap FFA) \cup (GWO \cap GA) \cup (FFA \cap GA)	f1, f2, f3, f4, f5, f6, f7, f8, f9, f11, f12, f13, f16, f17, f19, f22, f23, f24, f25, f26, f28, f31, f32, f33, f34, f35, f37, f39, f40, f41, f43	31

8.3.1 Findings of the Practical Assessment

The J48 and SVM-ML classifiers are used to assess the proposed model. The investigation's results are shown in Table 8.10, using the J48 categorization as a starting point. Table 8.11 displays the outcomes of the SVM-based experiment. Using the J48 classifier as a base, the classification accuracy rates of the suggested method range from 79.175 to 90.484 percent. The suggested approach's classification accuracy rates range from 79.077 to 90.119 percent for SVM-based classifiers.

The majority of the reduction rules in the research's suggested models are more accurate than all of the characteristics put together. Accuracy, sensitivity, precision, F1-measure, TPR, FNR, TPR, and FPR of each method and rule were assessed. It was found that the efficiency of the rules in the suggested model varies.

Table 8.10: The conclusions drawn from J48.

Rule	TPR	FNR	FPR	TNR	Accurac y	Precisio n	Sensitivit y	F- Measur e
All	63.99%	36.01%	4.57%	95.42%	81.29%	91.94%	63.98%	75.46%
PSO	80.844 %	19.156 %	2.817%	97.183 %	89.613 %	96.107%	80.844%	87.817 %
GW O	93.797 %	6.203%	20.952 %	79.048 %	85.605 %	78.513%	93.797%	85.732 %
FFA	96.586 %	3.414%	22.592 %	77.408 %	86.073 %	77.674%	96.586%	86.157 %
GA	96.700 %	3.300%	3.382%	96.618 %	96.794 %	96.626%	96.700%	96.798 %
R1	81.097 %	18.903 %	22.331 %	77.669 %	89.210 %	74.477%	81.097%	77.807 %
R2	93.854 %	6.146%	24.307 %	75.693 %	83.854 %	75.912%	93.854%	84.205 %
R3	94.314 %	5.686%	24.307 %	75.693 %	84.017 %	76.011%	94.314%	84.173 %
R4	94.314 %	5.686%	24.307 %	75.693 %	84.061 %	76.061%	94.314%	84.193 %
R5	94.314 %	5.686%	24.265 %	75.735 %	84.063 %	76.868%	94.314%	83.896 %
R6	94.314 %	5.686%	24.265 %	75.735 %	84.063 %	76.868%	94.314%	83.896 %
R7	86.481 %	13.519 %	25.691 %	74.309 %	80.493 %	73.932%	86.481%	79.651 %
R8	86.349 %	13.651 %	26.681 %	73.319 %	79.175 %	72.539%	86.349%	78.844 %
R9	86.349 %	13.651 %	26.681 %	73.319 %	79.175 %	72.539%	86.349%	78.844 %
R10	96.549 %	3.451%	25.451 %	74.549 %	84.215 %	75.592%	96.549%	84.273 %
R11	89.051 %	10.949 %	26.681 %	73.319 %	80.389 %	73.617%	89.051%	80.517 %
R12	96.872	3.128%	16.587	83.413	89.589	85.281%	96.872%	89.055

	%		%	%	%			%
R13	97.141 %	2.859%	14.950 %	85.050 %	90.484 %	84.136%	97.141%	90.172 %

Table 8.11: The conclusions drawn using SVM.

Rule s	TPR	FNR	FPR	TNR	Accurac y	Precisio n	Sensitivit y	F- Measur e
All	63.965 %	36.035 %	4.809%	95.191 %	81.158 %	91.566 %	63.965%	75.316 %
PSO	79.562 %	20.438 %	2.596%	97.404 %	89.152 %	96.345 %	79.562%	87.153 %
GW O	84.156 %	15.844 %	2.931%	97.069 %	90.852 %	96.028 %	84.156%	89.756 %
FFA	95.235 %	4.765%	22.592 %	77.408 %	85.429 %	77.519 %	95.235%	85.469 %
GA	96.970 %	3.030%	3.382%	96.618 %	96.794 %	96.626 %	96.970%	96.798 %
R1	80.827 %	19.173 %	23.265 %	76.735 %	78.576 %	74.477 %	80.827%	77.248 %
R2	93.884 %	6.116%	24.994 %	75.006 %	83.388 %	79.643 %	93.884%	83.385 %
R3	94.154 %	5.846%	24.526 %	75.474 %	83.508 %	75.082 %	94.154%	83.746 %
R4	94.154 %	5.846%	24.526 %	75.474 %	83.748 %	75.377 %	94.154%	83.727 %
R5	94.154 %	5.846%	24.130 %	75.870 %	83.844 %	75.430 %	94.154%	83.204 %
R6	94.154 %	5.846%	24.130 %	75.870 %	83.844 %	75.430 %	94.154%	83.204 %
R7	86.751 %	13.249 %	24.978 %	75.022 %	80.293 %	73.923 %	86.751%	79.825 %
R8	96.872 %	3.128%	18.981 %	81.019 %	88.946 %	82.542 %	96.872%	89.160 %
R9	86.403 %	13.597 %	26.092 %	73.908 %	79.077 %	72.387 %	86.403%	78.776 %

R10	96.872 %	3.128%	25.631 %	74.369 %	84.215 %	75.405 %	96.872%	84.573 %
R11	88.784 %	11.216 %	19.634 %	80.366 %	84.212 %	76.922 %	88.784%	82.414 %
R12	96.586 %	3.414%	16.587 %	83.413 %	89.589 %	85.281 %	96.586%	89.055 %
R13	96.870 %	3.130%	15.391 %	84.609 %	90.119 %	83.706 %	96.870%	89.808 %

The statistics are normal and are recognized as normal based on the TPR. The TPR for J48 and the SVM-based rules are shown in Figure 8.15.

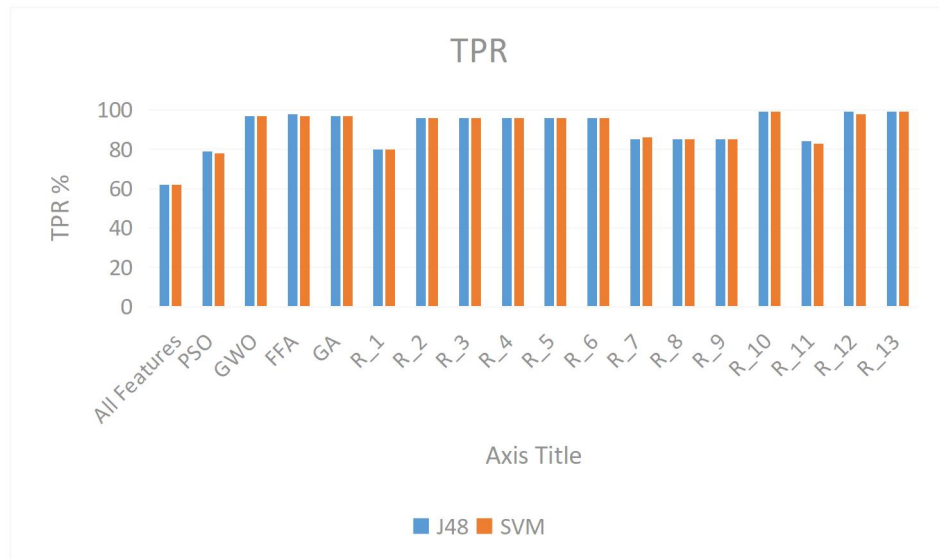


Figure 8.15: True Positive Rate (TPR).

TPRs for J48 and SVM classifier-based characteristics are 63.99 and 63.96 percent, respectively. J48 performs somewhat superior to SVM in terms of performance. According to the SVM classifier, GA has the greatest TPR. The greatest TPR is shown by R13, according to the classification J48.

The FNR proves that the information is true and that it is considered to be an attack. Results for the SVM and J48 FNR are shown in Figure 8.16.

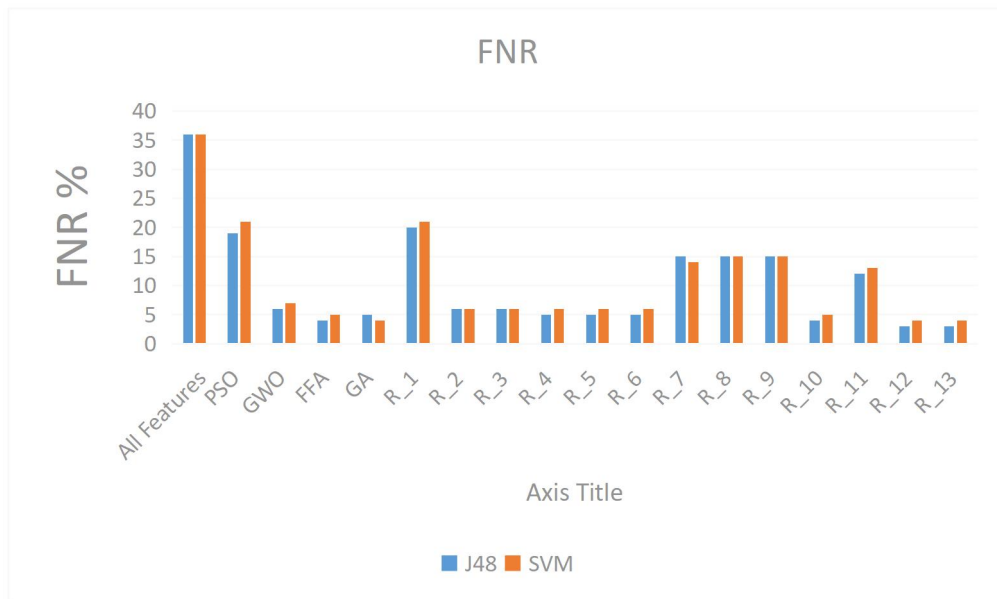


Figure 8.16: False Negative Rate (FNR).

The J48 and SVM-based features generated the highest FNR. GA reportedly boasts the SVM classifier's lowest FNR. According to the J48 classifier, its lowest FNR is R13.

The FPR demonstrates that the numbers are still under assault and assumed to be true. Figure 8.17 depicts the SVM and J48 findings-based on FPR.

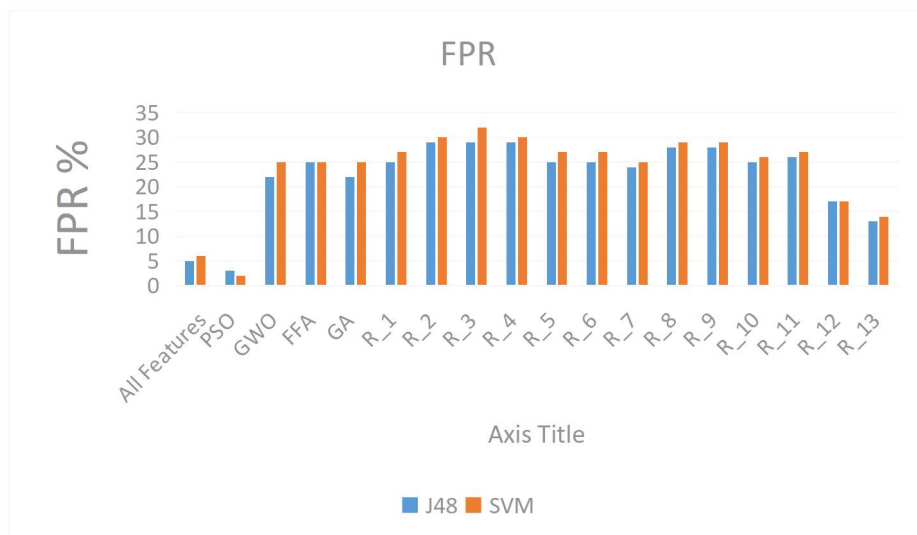


Figure 8.17: False Positive Rate (FPR).

R11, R9, and R8 earned the highest FPR with J48 and SVM. In accordance with the PSO, it has the lowest FPR among SVM with J48 classifier.

The TN has classified the information as threat information. The TNR outcomes of SVM and J48 for the recommended model is depicted in Figure 8.18.

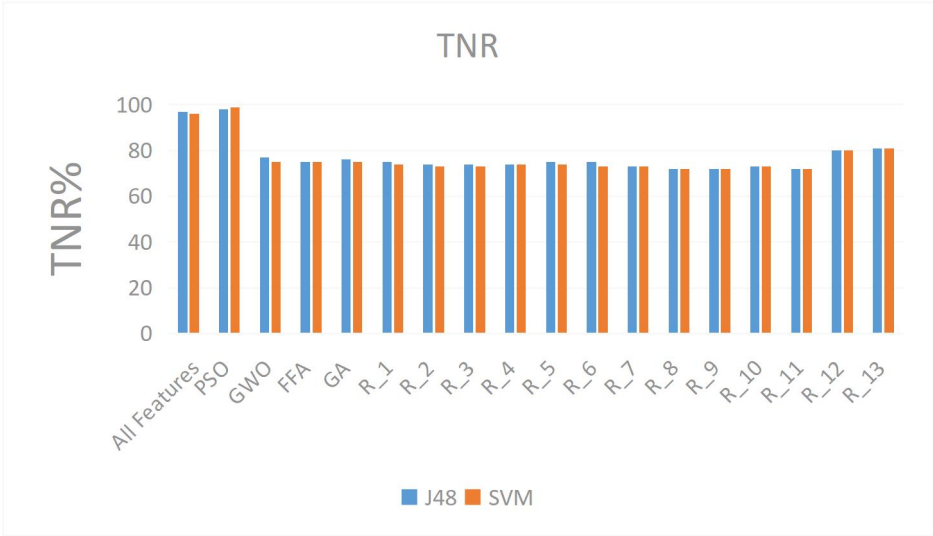


Figure 8.18: True Negative Rate (TNR).

The PSO for J48 and SVM produced the greatest TNR. Lower prices for SVM and J48 were attained by R11, R9, and R8.

The precision represents the categorization of good and bad activities. It is determined using the proportion of data that is accurately categorized across all dataset ranges. Figure 8.19 displays the recommended model's accuracy of SVM and J48.

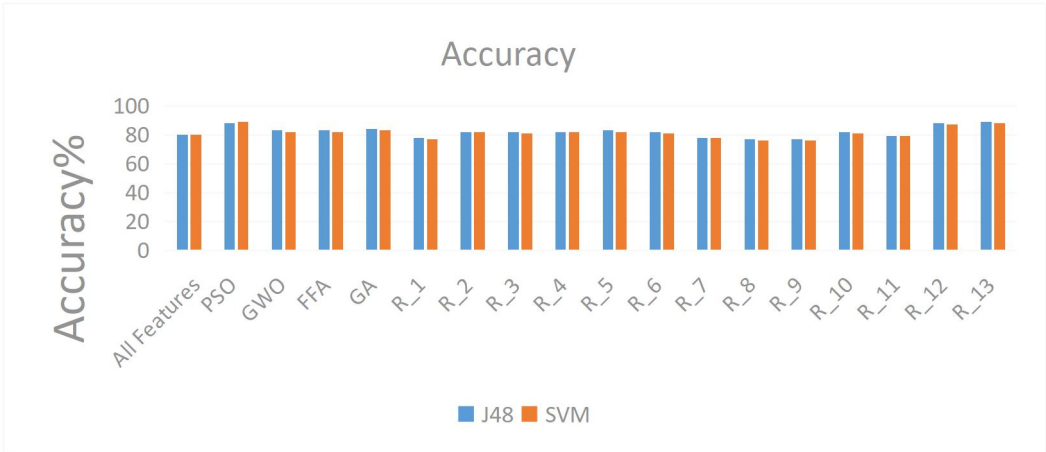


Figure 8.19: Accuracy.

R13 and R12 have the greatest levels of accuracy, according to the findings of Figure 8.19. Based on J48, R13 has a precision of 90.48 percent. It has a 90.12 percent accuracy rate and uses SVM. The number of attributes was decreased to 30

in R13. Based on J48 and SVM, R12 has 89.58 and 89.33 percent consistency, respectively. Following the R12 feature reduction, 13 features remained.

The proportion of genuinely positive outcomes to all positive results is known as precision. The suggested model's precision using SVM and J48 is shown in Figure 8.20. The highest level of precision was found to be PSO.

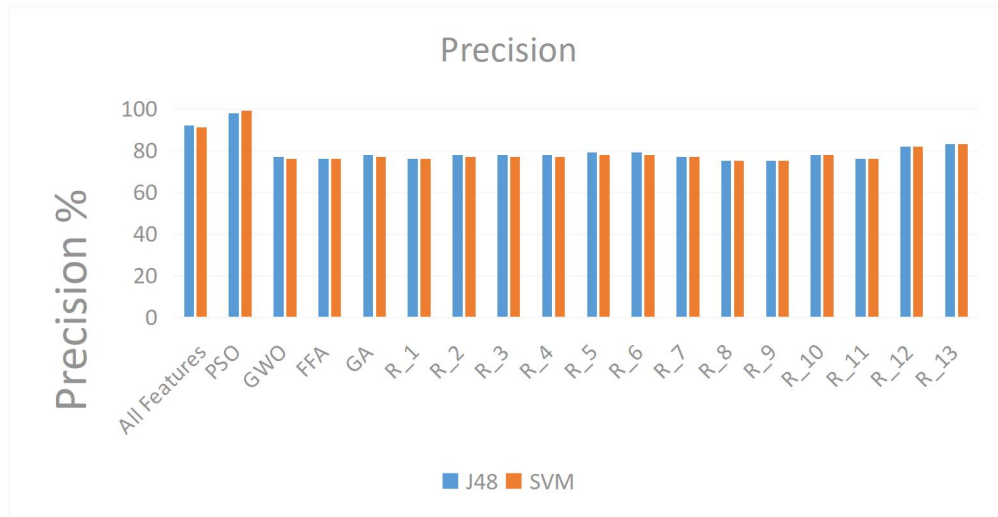


Figure 8.20: The accuracy rate.

The sensitivity level of the suggested model is depicted in Figure 8.21, using J48 and SVM. Sensitivity measures an IDS's ability to recognize an attack in a connection.

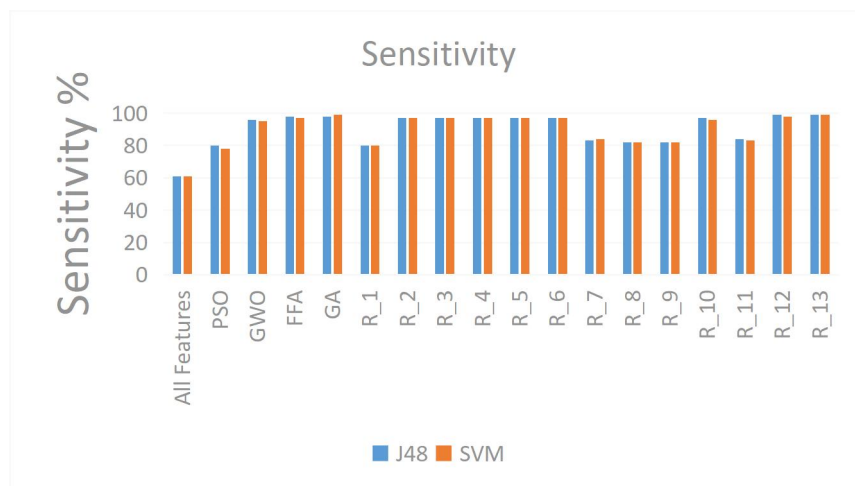


Figure 8.21: The sensitivity rates.

Figure 8.21 shows that R13 and R12 have the greatest degrees of sensitivity. According to both classifiers, the other attributes have the poorest sensitivity rates.

Thus, it may be shown that R13 and R12 more quickly and successfully identify anomalies.

The F-measure takes sensitivity and accuracy into account. The F-measure strikes a balance between sensitivity and precision. It acts as a light sensitivity and accuracy indicator. The suggested model's F-measure values are shown in Figure 8.22 and are based on J48 and SVM.

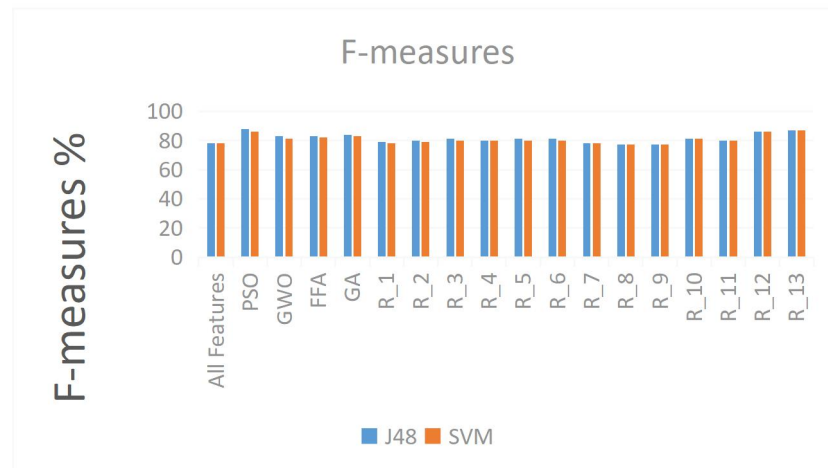


Figure 8.22: The F-measure rate.

According to the results demonstrating that the greatest F-measure rates are for R13 and R12, while the opposite qualities have the poorest F-measure rates, given the aforementioned facts. It is obvious that any evaluation method could impact how effective IDS are. The overall effectiveness of the NIDS may be evaluated using the F-measure rate and accuracy.

According to all experiments, for SVM with J48 classifiers, F-measure, precision, and sensitivity results with R13 and R12 were the best. GA has good FNR and TPR outcomes compared to H11, H9, and H8, which all have strong FPR results. PSO provides excellent accuracy and TNR outcomes.

8.4 Cisco packet tracer Results and Discussions

Some simulation networks were created using Cisco Packet Tracer. The communication of packets was studied using Wireshark tool. Here above graphs were plotted between various destination IPs versus source IPs for different protocols. It was found that wherever maximum time is taken by a destination IP for a source IP,

those could be the points of intrusions, that is the places where maximum resistance was being offered by a destination IP.

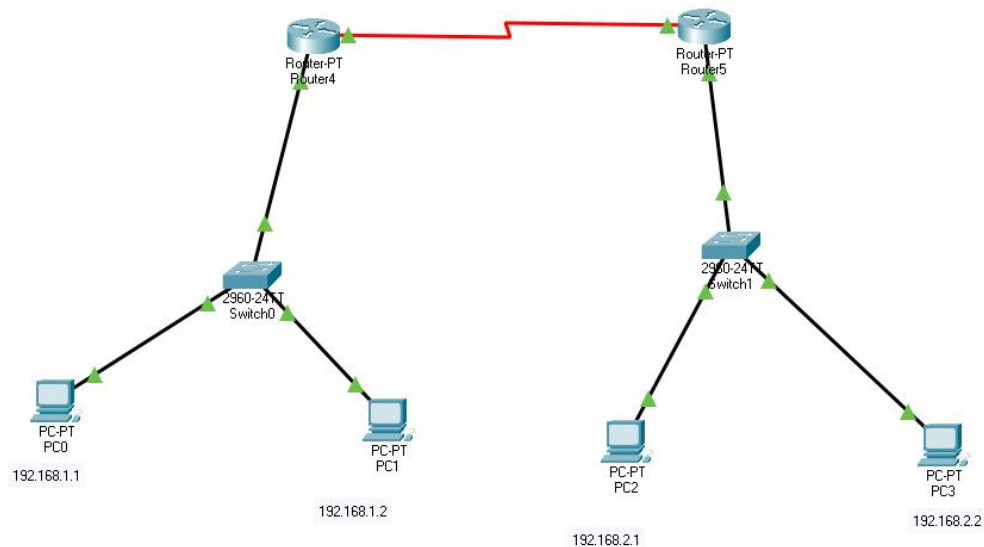


Figure 8.23: showing the test network architecture in Cisco packet tracer

1. Using Cisco Packet Tracer, a network is developed in the simulation environment consisting of PCs, switch and Routers connected in LAN. Fig 8.23 above shows that.
2. Using Wireshark tool, packets transmitted during above communication and other activities carried in the laptop system is captured for 10 minutes. The protocols involved, source IPs, destination IPs, and the time taken for communication between a particular sources with a particular destination is all extracted with the help of Wireshark tool.
3. Now taking each protocol separately, by applying filters, it is studied that which destination is having maximum time, by plotting graphs. The destination showing maximum time in the graph means that is the most affected one. Maximum time is shown in a particular destination means it offered maximum resistance to any abnormal incoming packet from a source. So this abnormal incoming packet may be an Intrusion.
4. After this trials are made to track the source from which this packet originated to that destination which offered maximum resistance to it, by applying filters to that particular destination. Again by finding out the source

which has maximum time in the graph, the suspected intrusion source IP can be found out.

The above points are shown in the following graphs 8.24 and 8.25, plotted in R.

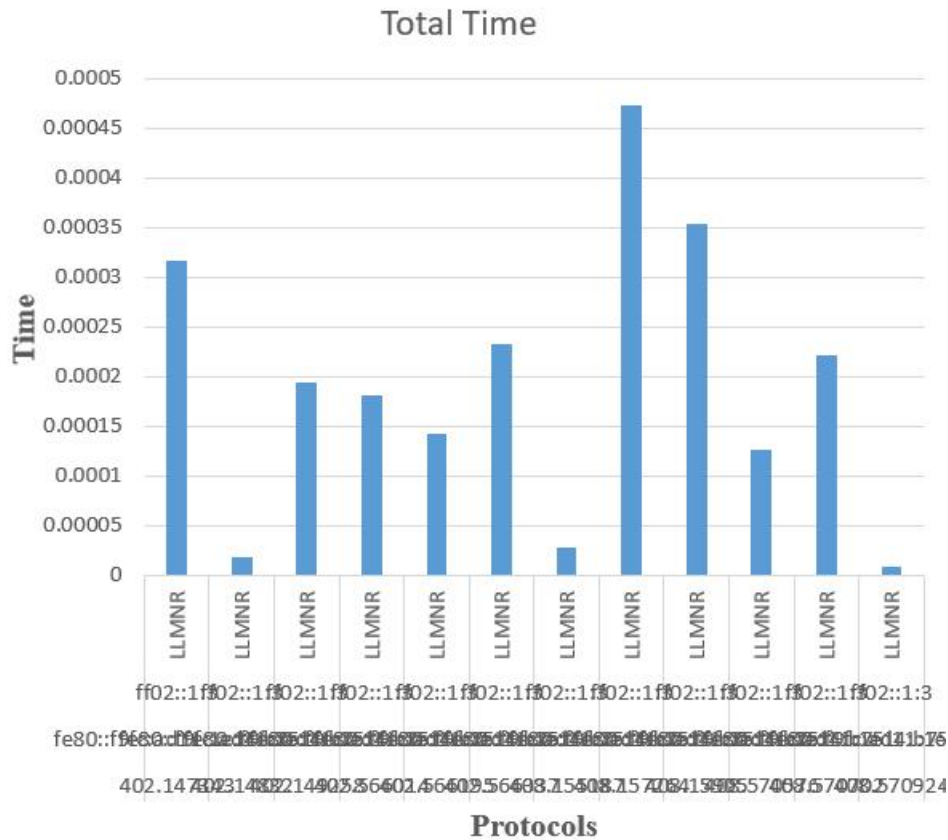


Figure 8.24: Shows protocols vs (ff02: 1:3) destination IP

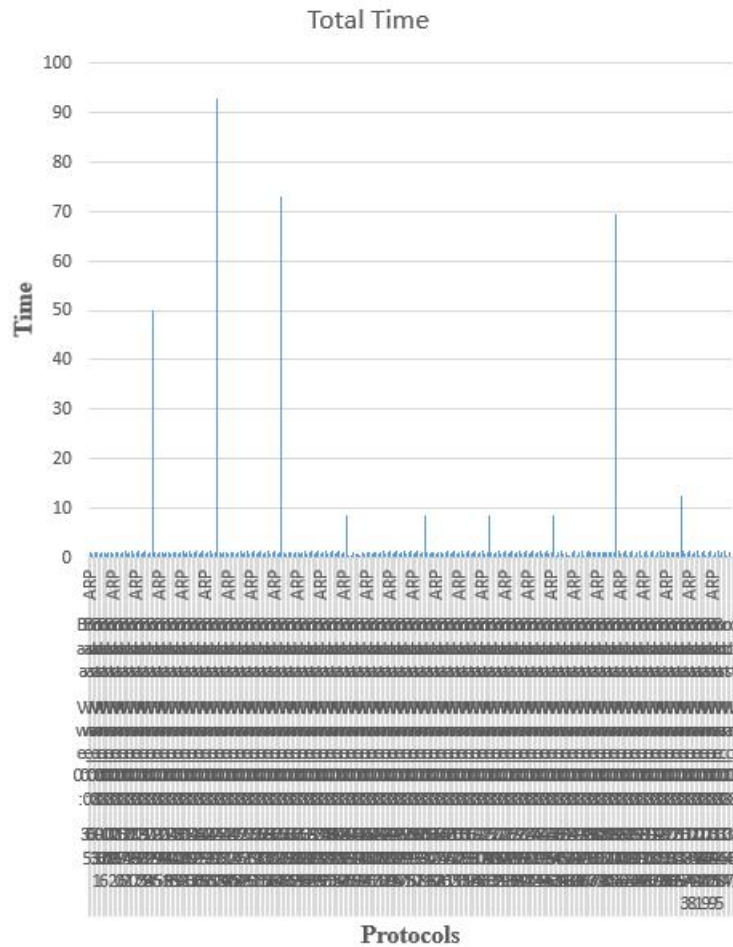


Figure 8.25: Shows protocols vs (192.168.239.1) Source IP

The various parameters by which above graphs are plotted are the different Source IPs, Destination IPs, Protocols involved and the time taken for the protocol to affect a particular destination IP and then a source IP. The parameters are shown below in Table 8.12: -

Table 8.12: showing Source, Destination and Protocol Dataset with respect to the test environment of network topology as shown in fig 8.23

Source	Destination	Protocol
192.168.239.1	192.168.239.1	ARP
192.168.239.254	192.168.239.254	BROWSER
fe80::f9fc:ad11:1e14:b75	192.168.239.255	DHCP

VMware_c0:00:08	224.0.0.22	ICMPv6
VMware_fc:23:ae	224.0.0.251	IGMPv3
	224.0.0.252	LLMNR
	239.255.255.250	MDNS
	Broadcast	NBNS
	ff02::1:3	SSDP
	ff02::16	
	ff02::fb	
	VMware_c0:00:08	
	VMware_fc:23:ae	

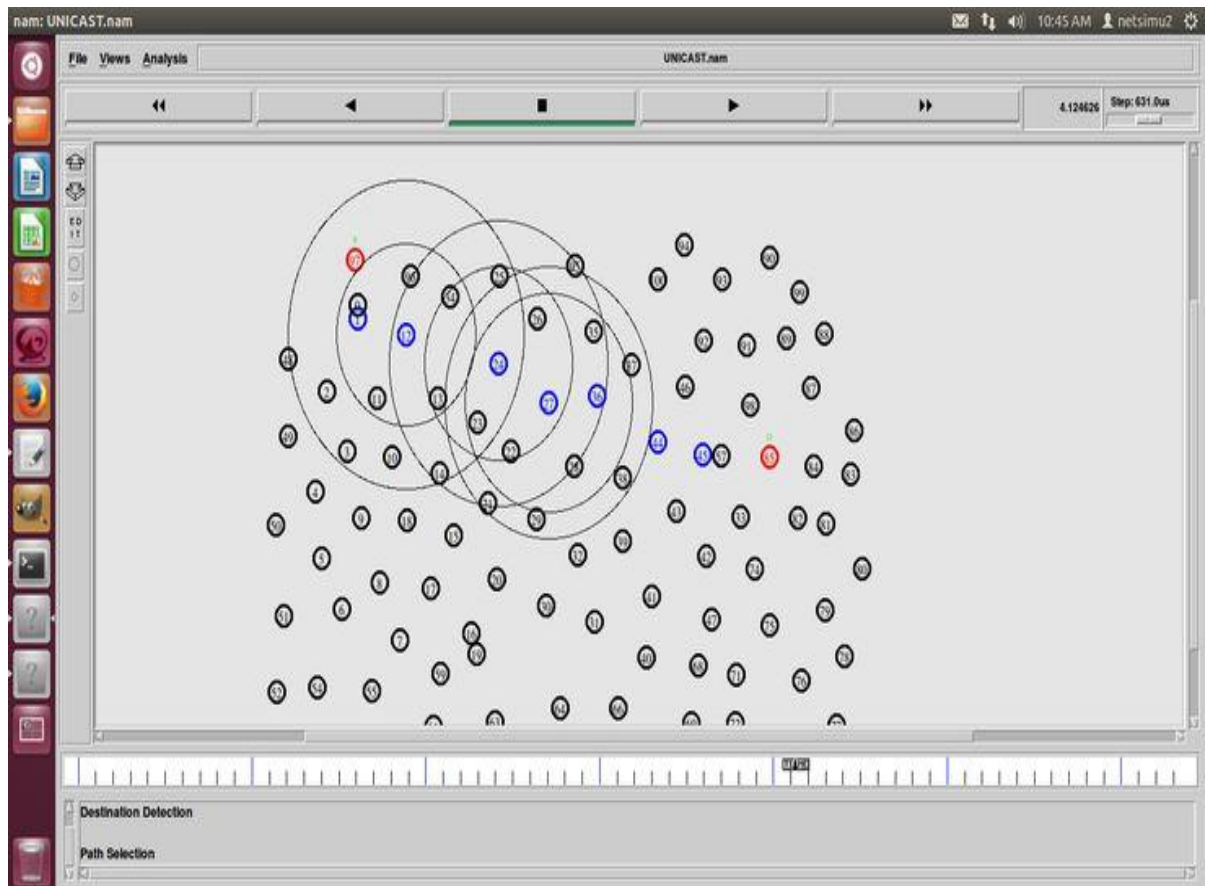


Figure 8.26: Creation of Wireless Sensor Networks consisting of nodes in NS2

A network is shown in NS2 simulation environment above in figure 8.26, where there are multiple nodes which act as destination IPs and source IPs. Communication of packets takes place in between these nodes. The actual motto behind creating this network in the above simulation environment is that some kind of abnormal behaviour in the network from external sources is to be identified which may be useful in the research work of detecting intrusions in any network.

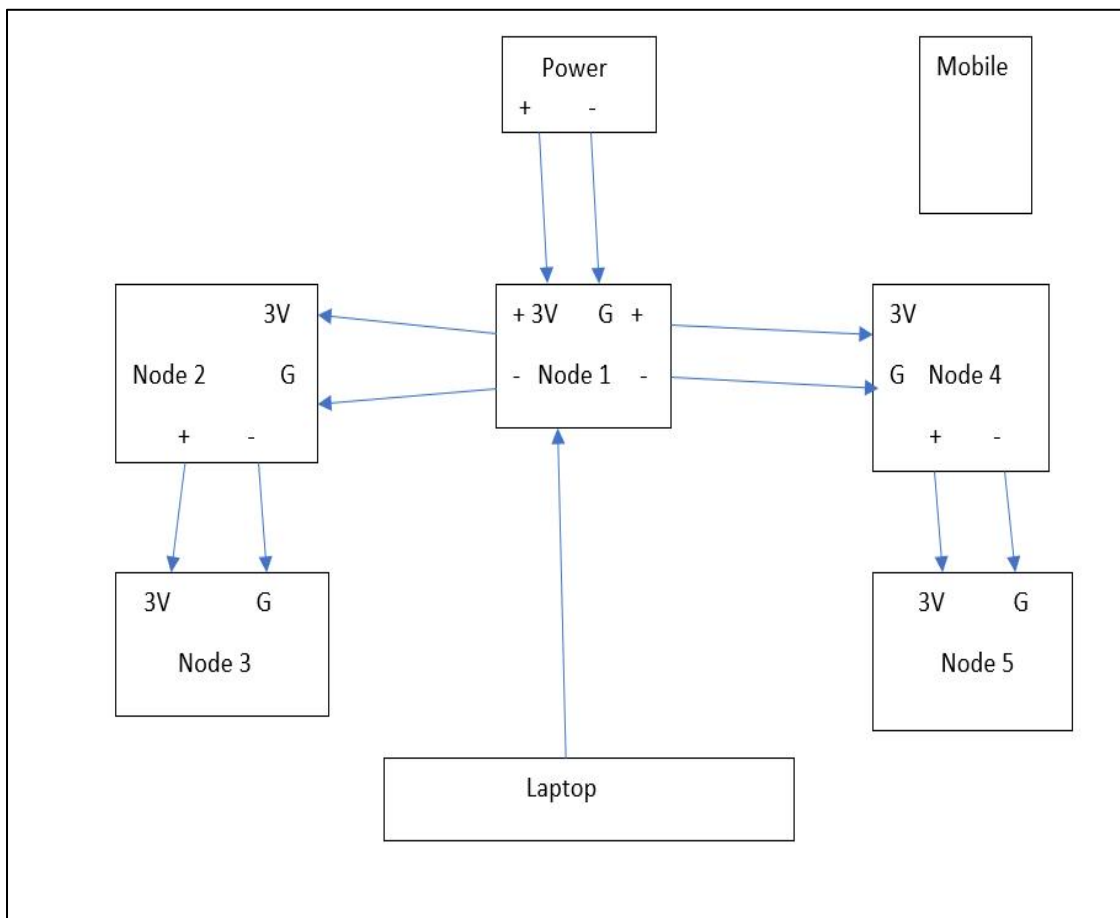


Figure 8.27: A Physical Network Created consisting of Laptop, Mobile and 5 Node MCUs

A physical network was created consisting of Laptop, Mobile and 5 node MCUs as depicted in fig 8.27. And dataset was obtained i.e. without malicious activity and with malicious activity. So following datasets now available now.

1. Normal dataset involving a simulation network in Cisco Packet Tracer, obtained with the help of Wireshark tool.

2. Normal dataset obtained involving IoT environment (consisting of node MCUs) in wireless networks.
3. NSDL dataset from Kaggle which is used to train the neural network (which consists of details about various types of attacks).
4. Perturbed dataset created by inducing some disturbances in the network created by us consisting of IoT.
5. UNSW dataset from Github which consists of many types of virus induced data.
6. Kddcup_99 dataset.

These datasets were used to train the various classifiers, stated in Table 8.10, and their accuracy percentages of detecting some malicious activity is found out.

The following is the system's planned block diagram shown in figure 8.28.

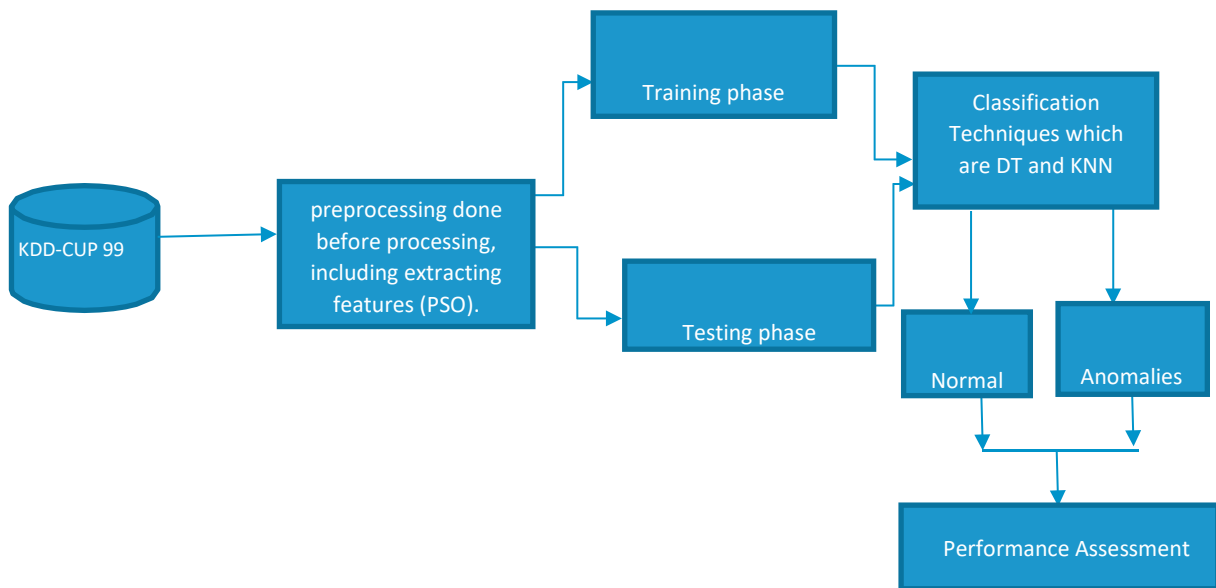


Figure 8.28: Proposed System Block Diagram

Table 8.13: Proposed classifiers evaluation

Measures	PSO+DT (%)	PSO+KNN (%)	PSO+ANN (%)
Accuracy	98.6	99.6	99.78
DR	89.6	96.2	97.1

FPR	1.1	0.4	0.03
-----	-----	-----	------

Table 8.14: Comparative with the current paradigm

Authors	Algorithm	Accuracy (%)	FPR
Sindhu, Geetha & Kannan [186]	DT	98.2	0.016
Mohammad Sazzadul Hoque [187]	GA	96.4	0.05
Guo [188]	KNN	98.45	0.048
	TCM+KNN	99.4	0.1
Proposed Classifier	PSO+DT	98.6	0.011
	PSO+KNN	99.6	0.04
	PSO+ ANN	99.78	0.003

The proposed system's accuracy, detection rate and false positive rate are evaluated in which it was observed that PSO+ANN provided the best results with the most efficient accuracy and detection rate and least false positive rate.

The proposed IDS was also compared with other existing Intrusion detection systems which involved other ML algorithms like Decision Trees, Genetic Algorithm and KNN. It was found that the proposed system PSO+ANN gave better results than other existing IDS.

Chapter 9

Conclusion and Future Scope

Chapter 9

Conclusion and Future Scope

It's been observed that time line undertaken for processing of different communication protocol on the given test environment has various range from 0.002 second to maximum of 40 second based on different data bandwidth communications. This time of data packet transfer which is the function of communication protocols has been observed in the research which directly implies the dependability of intrusion to time and processing ability of the network architecture or network nodes or network cloud. These analytics hence gives the secondary view for looking the communication and network dataset in the format of co-relation matrix which can optimize the dependability criteria for source and destination IP to communicate with maximum bandwidth. The communication time gap is easily predictable for small set of network infrastructure, but once the nodes in communication protocols increase, the problem of network intrusion protocols becomes the problem statement of big data, where machine learning and deep learning can give higher order precision in network intrusion detection. The model which is mostly frequency dependent is considered, so wired or wireless communication can also be modelled with the same infrastructure for test dataset collection.

The most current simulated network traffic dataset was used to illustrate network intrusion detection techniques in this post. Topics covered in this article included key components, as well as prominent cyber security weaknesses and associated with exposure. When compared to the outcomes of comparable methods for detecting need plenty networking incursions, as findings of the suggested a tractor trailer fully convolutional classifications infrastructure hyper-parameter clocking strategy showed a considerable improvement to multiclass models (IDSs). The models showed that the suggested technique had a 95.6% overall accuracy for user-defined multiclass classification and 95.3% for pre-partitioned multiclass classification.

In spite of the fact that the models that were given produced encouraging results, we are aware of the fact that there is room for advancement, notably in the form of the application of tactics that involve feature reduction. Transfer learning, which makes use of relevant datasets that are currently available, will be used to enhance model

classification in the future using the dataset UNSW-NB15 and to boost the capacity of our models to deal with zero-day assaults. Along with transfer learning, we will investigate different bootstrapping procedures that can be used to construct a dataset that is balanced in order to prepare a model for multiclass categorization. Deep learning models for anomaly detection will be used to modify cybersecurity architectures in order to create systems for detecting network intrusions that are flexible and robust. These systems will be able to accurately find common weaknesses and exposures, as well as zero-day behavioural characteristics of networks, which will reduce the likelihood that the network will be compromised.

The most urgent problem Network interference exists in the world of communication networks today. Network infrastructure is seriously endangered by the increasing frequency of internet attacks. Several research were also conducted in order to establish a suitable and efficient method of terminating network contact while protecting networks confidentiality and security. For the purpose of locating any instances of atypical network traffic flow, DL is an essential research technique. This study suggests two artificial intelligence strategies that employ feature extraction methods to classify certain unusual netflow occurrences. PSO+ANN, PSO+DT, and PSO+KNN are used to create a distinctive IDS. Approaches was suggested by the inquiry. The total performance of the suggested approach is enhanced by FN frequency, incorrect price, and detecting efficiency are compared to identify the incursion.

The computation effectiveness in detecting network intrusions is demonstrated by the suggested approach, PSO+ANN, with recognition rates of 97.1%, 0.003 for the FP rate, and 0.102 for the FN price. The proposed technique PSO+KNN illustrates the algorithm's efficacy in detecting assaults, with a classification results of 96.2%, a lowered entirely false rate of 0.004, and a FN rate of 0.104. The PSO+DT based system, on the other hand, had a detection rate of 89.6%, with rejections for FP and FN at 0.011 and 0.038, correspondingly.

With the suggested computer vision, potential intrusion prevention datasets could be used, and IDS could also make use of deep learning techniques.

It's challenging to upgrade an intrusion detection system. The number of characteristics influences how well a NIDS detects threats. Improving detection precision and the main objectives of data mining are to reduce the positive false-

positive rate for NIDS and ML approaches, respectively. Even though the most recent models made use of every attribute from using the UNSW-NB15 dataset, they were unable to locate the network vulnerability. The current study's goal was to provide an NIDS model with 17 attribute eligibility criteria. The UNSW-NB15 dataset is used to create the following model. The bio-inspired techniques PSO, GWO, FFA, GA, and MI form the basis for the suggested feature selection model. When it comes to bio-inspired algorithms, PSO and GWO each lower the number of the chosen characteristics to 25 and 20, respectively. In comparison to FFA, GA reduces the number of chosen qualities to only 23, leaving only 21 traits. R1 permits a maximum of 12 attributes for PSO, GWO, FFA, and GA's MI; R2 limits the number of permitted properties to only 11. R3 limits the greatest quantity of acceptable characteristics to 12; R4 restricts the number of permitted attributes to 11; and R5 restricts the number of permitted attributes to 10. R7 limits the number of features permitted to six, whereas R8 restricts the allowed the number of characteristics to five. Reduces the number of selected qualities to six with R6. In R10, the quantity of qualities is reduced to nine; in R11, the selected traits are reduced to five; in R12, to thirteen; and in R13, to thirty.

The J48 and SVM-ML algorithms indicate that R13 and R12 provide the most favourable outcomes in terms of F-measure, reliability, and sensibility. Recurrent and convolutional neural networks may be used in future studies (RNNs), two varieties of deep learning architectures, to assess how well the proposed model performs (CNN).

The proposed classifier is designed as a single source of entry. Developing this integrated model has resulted in differential models, which have played a major role in detecting the security anomaly. The algorithm can be managed to bring accuracy above 98.5%, but that's not possible due to the amalgamated data we have used to train the model. If data annotations are optimized, there can be a mesh with DL and PSO, that can attain greater precision and accuracy.

Future Scope

1 Hybrid Models with Other Evolutionary Algorithms

- **Genetic Algorithms (GA), Ant Colony Optimization (ACO), and Cuckoo Search:** While **Particle Swarm Optimization (PSO)** is a widely used optimization technique, integrating other evolutionary algorithms, such as **Genetic Algorithms (GA)** or **Ant Colony Optimization (ACO)**, could provide additional optimization strategies that may improve detection accuracy and efficiency. A hybrid approach that combines **PSO** with these algorithms may enhance the model's robustness in feature selection and hyperparameter tuning.
- **Differential Evolution (DE):** Another promising evolutionary optimization method is **Differential Evolution (DE)**, known for its robust global search capabilities. Incorporating **DE** alongside machine learning classifiers like **Support Vector Machines (SVM)** or **Random Forests** could lead to improved classification performance in the IDS framework.

2 Feature Engineering and Selection

- **Advanced Feature Selection:** While **PSO** is effective for feature selection, other methods like **Recursive Feature Elimination (RFE)** or **L1 Regularization** could further refine the feature selection process, leading to better model performance. Additionally, **Autoencoders** can be explored for learning compressed representations of the feature space, which may improve efficiency and detection accuracy.
- **Feature Fusion:** Combining multiple feature sets, or integrating data from various sources (e.g., packet-level features, log data, or system behavior), can improve the detection of more sophisticated attacks. **Feature fusion** techniques, which merge the outputs of different models or features, can provide a richer representation of network activity and enhance intrusion detection accuracy.

3 Cloud and IoT Integration

- **Cloud-Based IDS:** As cloud computing becomes more prevalent, the integration of IDS systems into cloud environments (such as **AWS**, **Azure**, or **Google Cloud**) is increasingly important. **Cloud-native intrusion detection systems** can scale dynamically, taking advantage of the elasticity and distributed architecture of cloud infrastructures.
- **IoT-Specific IDS:** As the Internet of Things (IoT) expands, specialized IDS techniques tailored to monitor IoT networks could be developed. IoT devices often generate unique traffic patterns, and the ability to monitor and detect threats in IoT environments will be crucial for securing **smart homes**, **industrial IoT (IIoT)**, and **connected healthcare devices**.

4 Quantum Computing and Cryptographic Attacks

- **Quantum-Resistant Algorithms:** As quantum computing progresses, traditional cryptographic algorithms may become vulnerable to quantum-based attacks. It will be essential for IDS systems to evolve to handle these potential threats by integrating **quantum-resistant encryption** and **quantum-safe algorithms**.
- **Quantum Machine Learning:** **Quantum machine learning (QML)** is an emerging field that may offer significant improvements in processing power and pattern recognition capabilities for IDS. Investigating the application of quantum algorithms to accelerate model training and enhance data analysis could provide a competitive advantage in IDS performance.

5 Adaptive IDS Using Reinforcement Learning

- **Reinforcement Learning (RL):** Integrating **Reinforcement Learning (RL)** can allow the IDS to **adapt and evolve** over time. RL algorithms, such as **Q-Learning** and **Deep Q Networks (DQNs)**, enable the system to autonomously learn optimal strategies for intrusion detection. The system could continuously improve its detection capabilities by interacting with the network environment, adjusting to new attack strategies without human intervention.

- **Self-Tuning Mechanisms:** By using RL, the IDS could autonomously adjust model hyperparameters, select features, and even choose which classifier to deploy based on the current network conditions and attack patterns. This adaptive capability would significantly enhance the system's effectiveness in real-world environments.

6 Explainable AI (XAI) in IDS

- **Model Interpretability:** One challenge with deep learning models such as ANNs is the lack of interpretability. To improve the trustworthiness and transparency of the IDS, **Explainable AI (XAI)** techniques can be integrated. Methods like **LIME (Local Interpretable Model-agnostic Explanations)** and **SHAP (SHapley Additive exPlanations)** offer ways to explain how models arrive at specific predictions, which is critical for security analysts when validating alerts and making decisions.
- **Decision Tree Transparency:** Since **Decision Trees (DTs)** are inherently interpretable, they can be used alongside visualization techniques, such as **feature importance plots** and **decision path visualizations**, to provide meaningful insights into how the system classifies network traffic and detects intrusions.

Conclusion

The future scope of intrusion detection systems is vast, with many potential avenues for enhancement. Building on existing models that combine **PSO** with classifiers like **KNN**, **DT**, and **ANN**, incorporating advanced techniques such as **deep learning**, **semi-supervised learning**, **ensemble methods**, **real-time response**, and **explainable AI** will substantially improve the performance, scalability, and adaptability of IDS. As new technologies emerge, especially in the fields of **cloud computing**, **IoT**, and **quantum computing**, the development of an intelligent, adaptive IDS capable of addressing complex cybersecurity challenges becomes increasingly critical.

References:

- [1] Mebawondu, J. O., Mebawondu, O. J., Atsanan, A. N., & Suleiman, M. N. (2012). The impact of information technology on poverty alleviation in Nigeria. *Continental Journal of Information Technology*, 6(1), 1-5.
- [2] Adetunmbi, A. O., Alese, B. K., Ogundele, O. S., & Falaki, S. O. (2007). A data mining approach to network intrusion detection. *Journal of Computer Science & Its Applications*, 14(2), 24-37.
- [3] Opeyemi, O. G., Adewale, O. S., Adetunmbi, A. O., Alese, B. K., & Ogunde, A. O. (2010). Deadlock detection in agent-based virtual knowledge communities. *Annals. Computer Science Series*, 8(2).
- [4] Boppana, R. V., & Su, X. (2010). On the effectiveness of monitoring for intrusion detection in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 10(8), 1162-1174.
- [5] Mebawondu, J. (2018). Development of a Network Intrusion Detection System Using Neural Network M. Tech, Federal University of Technology.
- [6] Vinchurkar, D. P., & Reshamwala, A. (2012). A review of an intrusion detection system using neural network and machine learning. *J. Eng. Sci. Innov. Technol*, 1, 54-63.
- [7] Ennert, M., Chovancová, E., & Dudláková, Z. (2015). Testing of IDS model using several intrusion detections tools. *Journal of Applied Mathematics and Computational Mechanics*, 14(1).
- [8] Abdulsalam, S.O., Mohammed, A.A., Ajao, J.F., Babatunde, R.S., Ogundokun, R.O., Nnodim, C.T., Arowolo, M.O. (2020). Performance Evaluation of ANOVA and RFE Algorithms for Classifying Microarray Dataset Using SVM. *Lecture Notes in Business Information Processing*, 402, pp. 480-492.
- [9] Silvio E. Quincozes, Célio Albuquerque, Diego Passos, Daniel Mossé, A survey on intrusion detection and prevention systems in digital substations, *Computer Networks*, Volume 184, 2021, 107679, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2020.107679>.
- [10] Shashank Gavel, Ajay Singh Raghuvanshi, Sudarshan Tiwari, Maximum correlation based mutual information scheme for intrusion detection in the data networks, *Expert Systems with Applications*, Volume 189, 2022, 116089, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2021.116089>.

- [11] S. B. Casey Cane, "33 Alarming Cybercrime Statistics You Should Know in 2019," CYBER SECURITY REPORT 2020, 2019.
- [12] N. D. Malony Alphonso and Louella Colaco, "Intrusion Detection System for Network Data Set using Data Mining Techniques," 2017.
- [13] Kun Xie, Mouna Chellal and Ilyas Benmessahel, "A new evolutionary neural networks based on intrusion detection systems using multiverse optimization," Springer Science, 2017.
- [14] Ravinder Kumar, Amita Malik, Virender Kumar Ranga, An intellectual intrusion detection system using Hybrid Hunger Games Search and Remora Optimization Algorithm for IoT wireless networks, Knowledge-Based Systems, 2022, 109762, ISSN 0950-7051, <https://doi.org/10.1016/j.knosys.2022.109762>
- [15] Geetha T.V., Deepa A.J., A FKPCA-GWO WDBiLSTM classifier for intrusion detection system in cloud environments, Knowledge-Based Systems, Volume 253, 2022, 109557, ISSN 0950-7051, <https://doi.org/10.1016/j.knosys.2022.109557>.
- [16] Ibrahim Hayatu Hassan, Abdullahi Mohammed, Mansur Aliyu Masama, Yusuf Sahabi Ali, Abdulrazaq Abdulrahim, An Improved Binary Manta Ray Foraging Optimization Algorithm based feature selection and Random Forest Classifier for Network Intrusion Detection, Intelligent Systems with Applications, 2022, 200114, ISSN 2667-3053, <https://doi.org/10.1016/j.iswa.2022.200114>.
- [17] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: a Dataset for intrusion detection systems in wireless sensor networks," in Journal of Sensors, 1-16, 2016, <http://dx.doi.org/10.1155/2016/4731953>.
- [18] Abdulaziz I. Al-issa¹, Mousa Al-Akhras¹⁺², Mohammed S. ALSahl¹, Mohammed Alawairdhi¹, "Using Machine Learning to Detect DoS Attacks in Wireless Sensor Networks," in IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, 2019.
- [19] M.Firoz Kabir, Sven Hartmann, "Cyber Security Challenges: An Efficient Intrusion Detection System Design", in IEEE International Young Engineers Forum, 2018.

- [20] Y. Yang, K. McLaughlin, S. sezer, T. Littler, B. Pranggono, P. Brogan, H.F. Wang, "Intrusion Detection System for Network Security in Synchrophasor Systems", 2018.
- [21] Paria Jokar, Victor C.M. Leung, "Intrusion detection and prevention for ZigBee-Based Home Area Networks in Smart Grids", in IEEE Transaction on Smart Grid, 2016.
- [22] Priyanka Sharma,Dietmar P.F. Moller, "Protecting ECUs and Vehicles Internal Networks", in IEEE conference, 2018.
- [23] M. Archana, G. S. Binu, and G. Vinod, "A survey on defense mechanisms against Black hole and Gray hole attacks in Wireless Sensor Networks," in IJEDR, vol. 5, no. 1, pp. 177-182, 2017.
- [24] I. Almomani and B. Al-Kasasbeh, "Performance analysis of LEACH protocol under Denial of Service attacks," 2015 6th International Conference on Information and Communication Systems (ICICS), Amman, 2015, pp. 292-297. doi: 10.1109/IACS.2015.7103191
- [25] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris. A highthroughput path metric for multi-hop wireless routing. *Wireless networks*, 11(4):419–434, 2005
- [26] Sarika Choudhary,Nishta Kesswani ,” Detection and Prevention of Routing Attacks Internet of Things ”, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications
- [27] Jafar Abo Nada, Mohammad Rasmi Al-Mosa, “A Proposed Wireless Intrusion Detection Prevention and Attack System”, IEEE978-1-7281-0385-3/18/\$31.00 ©2018 IEEE.
- [28] U. S. Musa, S. Chakraborty, M. M. Abdullahi and T. Maini, "A Review on Intrusion Detection System using Machine Learning Techniques," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 541-549, doi: 10.1109/ICCCIS51004.2021.9397121.
- [29] Subhash Waskle, Lokesh Parashar and Upendra Singh Intrusion Detection System Using PCA with Random Forest Approach International Conference on Electronics and Sustainable Communication Systems (ICESC),2020
- [30] Bang, Raghav, Manish Patel, Vasu Garg, Vishal Kasa, Jyoti Malhotra, and Sambhaji Sarode. "Redefining smartness in township with Internet of Things

- & Artificial Intelligence: Dholera city." In E3S Web of Conferences, vol. 170, p. 06001. EDP Sciences, 2020.
- [31] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019.
- [32] Rintyarna, B. S., Sarno, R., & Fatichah, C. (2019). Evaluating the performance of sentence level features and domain sensitive features of product reviews on supervised sentiment analysis tasks. *Journal of Big Data*, 6, 1–19
- [33] Jing Wang, Dakun Lin, Yuanzi Zhang, Shiguo Huang, An adaptively balanced grey wolf optimization algorithm for feature selection on high-dimensional classification, *Engineering Applications of Artificial Intelligence*, Volume 114, 2022, 105088, ISSN 0952-1976, <https://doi.org/10.1016/j.engappai.2022.105088>.
- [34] Rajalaxmi Ramasamy Rajammal, Seyedali Mirjalili, Gothai Ekambaram, Natesan Palanisamy, Binary Grey Wolf Optimizer with Mutation and Adaptive K-nearest Neighbour for Feature Selection in Parkinson's Disease Diagnosis, *Knowledge-Based Systems*, Volume 246, 2022, 108701, ISSN 0950-7051, <https://doi.org/10.1016/j.knosys.2022.108701>.
- [35] Hossein Jafari Siahroodi, Hamed Mojallali, Seyed Saeid Mohtavipour, A novel multiobjective framework for harmonic power market including plug-in electric vehicles as harmonic compensators using a new hybrid gray wolf-whale-differential evolution optimization, *Journal of Energy Storage*, Volume 52, Part C, 2022, 105011, ISSN 2352-152X, <https://doi.org/10.1016/j.est.2022.105011>.
- [36] Yefeng Yang, Bo Yang, Shilong Wang, Tianguo Jin, Shi Li, An enhanced multiobjective grey wolf optimizer for service composition in cloud manufacturing, *Applied Soft Computing*, Volume 87, 2020, 106003, ISSN 1568-4946, <https://doi.org/10.1016/j.asoc.2019.106003>.
- [37] Jianlu Zhu, Guocong Wang, Yuxing Li, Zhili Duo, Chongzheng Sun, Optimization of hydrogen liquefaction process based on parallel genetic algorithm, *International Journal of Hydrogen Energy*, 2022, ISSN 0360-3199, <https://doi.org/10.1016/j.ijhydene.2022.06.062>.

- [38] Ranjita Joon, Parul Tomar, Energy Aware Q-learning AODV (EAQ-AODV) routing for cognitive radio sensor networks, Journal of King Saud University - Computer and Information Sciences, 2022, ISSN 1319-1578, <https://doi.org/10.1016/j.jksuci.2022.03.021>.
- [39] Mohineet Kaur, Manoj Kumar Dutta, Restoration and quality improvement of distorted tribal artworks using Particle Swarm Optimization (PSO) technique along with nonlinear filtering, Optik, Volume 245, 2021, 167709, ISSN 0030-4026, <https://doi.org/10.1016/j.ijleo.2021.167709>.
- [40] Abbaszadeh, Maliheh & Soltani Mohammadi, Saeed & Najah, Al-Mahfoodh. (2022). Optimization of support vector machine parameters in modeling of Iju deposit mineralization and alteration zones using particle swarm optimization algorithm and grid search method. Computers & Geosciences. 165. 105140. 10.1016/j.cageo.2022.105140.
- [41] Preeti, Kusum Deep, A random walk Grey wolf optimizer based on dispersion factor for feature selection on chronic disease prediction, Expert Systems with Applications, Volume 206, 2022, 117864, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117864>.
- [42] Qusay M Alzubi, Mohammed Anbar, Yousef Sanjalawe, Mohammed Azmi Al-Betar, Rosni Abdullah, Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization, Expert Systems with Applications, Volume 204, 2022, 117597, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117597>.
- [43] Huai-xi Xing, Hua Wu, You Chen, Kun Wang, A cooperative interference resource allocation method based on improved firefly algorithm, Defence Technology, Volume 17, Issue 4, 2021, Pages 1352-1360, ISSN 2214-9147, <https://doi.org/10.1016/j.dt.2020.07.006>.
- [44] Hadeel Alazzam, Ahmad Sharieh, Khair Eddin Sabri, A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer, Expert Systems with Applications, Volume 148, 2020, 113249, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2020.113249>.
- [45] Neha Gupta, Vinita Jindal, Punam Bedi, and LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system, Computer Networks, Volume 192, 2021, 108076, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2021.108076>.

- [46] Yanda Lu, Su Zhou, Ding Yin, Lei Fan, Gang Zhang, Jianhua Gao, Simultaneous fault diagnosis of proton exchange membrane fuel cell systems based on an Incremental Multi-label Classification Network, *International Journal of Hydrogen Energy*, 2022, ISSN 0360-3199, <https://doi.org/10.1016/j.ijhydene.2022.05.231>.
- [47] Rajalaxmi Ramasamy Rajammal, Seyedali Mirjalili, Gothai Ekambaram, Natesan Palanisamy, Binary Grey Wolf Optimizer with Mutation and Adaptive K-nearest Neighbour for Feature Selection in Parkinson's Disease Diagnosis, *Knowledge-Based Systems*, Volume 246, 2022, 108701, ISSN 0950-7051, <https://doi.org/10.1016/j.knosys.2022.108701>.
- [48] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: a Dataset for intrusion detection systems in wireless sensor networks," in *Journal of Sensors*, 1-16, 2016, <http://dx.doi.org/10.1155/2016/4731953>.
- [49] Abdulaziz I. Al-issal, Mousa Al-Akhras¹⁺², Mohammed S. ALSahlil, Mohammed Alawairdhi¹, "Using Machine Learning to Detect DoS Attacks in Wireless Sensor Networks," in *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology*, 2019.
- [50] M.Firoz Kabir, Sven Hartmann, "Cyber Security Challenges: An Efficient Intrusion Detection System Design", in *IEEE International Young Engineers Forum*, 2018.
- [51] Y.Yang, K. McLaughlin, S. sezer, T. Littler, B. Pranggono, P. Brogan, H.F. Wang, "Intrusion Detection System For Network Security In Synchrophasor Systems", 2018.
- [52] Paria Jokar, Victor C.M. Leung, "Intrusion detection and prevention for ZigBee-Based Home Area Networks in Smart Grids", in *IEEE Transaction on Smart Grid*, 2016.
- [53] Priyanka Sharma, Dietmar P.F. Moller, "Protecting ECUs and Vehicles Internal Networks", in *IEEE conference*, 2018.
- [54] M. Archana, G. S. Binu, and G. Vinod, "A survey on defense mechanisms against Black hole and Gray hole attacks in Wireless Sensor Networks," in *IJEDR*, vol. 5, no. 1, pp. 177-182, 2017.
- [55] I. Almomani and B. Al-Kasasbeh, "Performance analysis of LEACH protocol under Denial of Service attacks," 2015 6th International Conference on

- Information and Communication Systems (ICICS), Amman, 2015, pp. 292-297. doi: 10.1109/IACS.2015.7103191
- [56] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris. A highthroughput path metric for multi-hop wireless routing. *Wireless networks*, 11(4):419–434, 2005
- [57] Sarika Choudhary, Nishta Kesswani, "Detection and Prevention of Routing Attacks Internet of Things ", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications
- [58] Jafar Abo Nada, Mohammad Rasmi Al-Mosa, "A Proposed Wireless Intrusion Detection Prevention and Attack System", IEEE 978-1-7281-0385-3/18/\$31.00 ©2018 IEEE.
- [59] Ghassan kbar, Ammar Alazab, "A Comprehensive Protection Method for Securing the organization's network against Cyberattacks", 978-1-7281-2600-5/19/\$31.00 ©2019 IEEE DOI 10.1109/CCC.2019.00005.
- [60] Sajaan Ravji, Maaruf Ali, "Integrated Intrusion Detection and Prevention System with Honeypot in Cloud Computing", 978-1-5386-4904-6/18/\$31.00 ©2018 IEEE.
- [61] Vinit Kumar Gunjan 1, Amit Kumar 2, Sharda Avdhanam3, "A Survey of Cyber Crime in India", 978-1-4673-2818-0/13/\$31.00 ©2013 IEEE.
- [62] Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu, "A survey of network anomaly detection techniques", 1084-8045/& 2016 Elsevier Ltd.
- [63] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification", *International Journal of Network Security*, Vol.15, No.5, PP.390-396, Sept. 2013.
- [64] Ozlem Yavanoglu, Murat Aydos, "A Review on Cyber Security Datasets for Machine Learning Algorithms".
- [65] WALEED BUL'AJOUL 1,2, ANNE JAMES1 , AND SIRAJ SHAIKH3 , "A New Architecture for Network Intrusion Detection and Prevention", 2169-3536 2019 IEEE
- [66] Evgeny A. Basinya1,2, Yuliya K. Ravtovich1,2, "Implementation of an Intrusion Detection and Prevention System Module for Corporate Network Traffic Management", 978-1-5386-7054-5/18/\$31.00 ©2018 IEEE
- [67] Pankaj Ramchandra Chandre , Parikshit Narendra Mahalle, Gitanjali Rahul Shinde, "Machine Learning Based Novel Approach for Intrusion Detection

- and Prevention System: A Tool Based Verification”, 978-1-5386-5201-5/18/\$31.00 ©2018 IEEE
- [68] Adwitiya Mukhopadhyay, Y Vinayaka R, “A Multi-Tiered Alert Mechanism for Intrusion and Disaster Prevention in a Smart Home Scenario”, 978-1-5386-8158-9/19/\$31.00©2019IEEE.
- [69] Goyal, Abhilash, Gupta, Divyansh, “Intrusion Detection and Prevention in Software Defined Networking”, 978-1-5386- 81343/18//\$31.00©2019IEEE.
- [70] Christos Constantinides, Stavros Shiaeles, Bogdan Ghita, Nicholas Kolokotronis, “A Novel Online Incremental Learning Intrusion Prevention System”, 978-1-7281-1542-9/19/\$31.00 ©2019 IEEE.
- [71] Reza Parsamehr, Alireza Esfahani, Georgios Mantas, “A Novel Intrusion Detection and Prevention Scheme for Network Coding-Enabled Mobile Small Cells”, 2329-924X © 2019 IEEE.
- [72] Rifki Indra Perwira, Yuli Fauziah, Putu Retya Mahendra, “Anomaly-based Intrusion Detection and Prevention Using Adaptive Boosting in Software-defined Network” 978-1-7281-2380-6/19/\$31.00 ©2019 IEEE.
- [73] Simon D. Duque Anton, Mathias Strufe, d Hans Dieter Schotten, “Modern Problems Require Modern Solutions: Hybrid Concepts for Industrial Intrusion Detection”, 978-1-7281-2380-6/19/\$31.00 ©2019 IEEE.
- [74] Sui Xin,” Research of Intrusion Detection System”, 978-0-7695-5004-6/13 \$26.00 © 2019 IEEE.
- [75] Md Zahangir Alom and Tarek M. Taha, “Network Intrusion Detection for Cyber Security on Neuromorphic Computing System”, 978-1-5090-6182-2/17/\$31.00 ©2020 IEEE.
- [76] Chie-Hong Lee, Yann-Yean Su, Yu-Chun Lin and Shie-Jue Lee, “ Machine Learning Based Network Intrusion Detection”, 978-1-5386-2030-4/17/\$31.00 ©2020 IEEE
- [77] Md Zahangir Alom and Tarek M. Taha, “Network Intrusion Detection for Cyber Security using Unsupervised Deep Learning Approaches” 978-1-5386-3200-0/17/\$31.00 ©2020 IEEE
- [78] Hassan Azwar, Muhammad Murtaz, “Intrusion Detection in secure network for Cybersecurity systems using Machine Learning and Data Mining”, 978-1-5386-7966-1/18/\$31.00 ©2018 IEEE.

- [79] Chen Q, Chen H, Cai Y, Zhang Y, Huang X. Denial of service attack on IoT system. In: 2018 9th International Conference on Information Technology in Medicine and Education (ITME). IEEE; 2018. p. 755–8.
- [80] Doshi, R., Apthorpe, N., Feamster, N., 2018. Machine learning DDoS detection for consumer internet of things devices. arXiv preprint arXiv:1804.04159
- [81] Verma A, Ranga V. Machine learning based intrusion detection systems for IoT applications. *Wirel. Pers. Commun.* 2019;1–24.
- [82] Anthi E, Williams L, Malgortzata G, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT. *IEEE Internet Things J.* 2018; 78:477–90.
- [83] Syed NF, Baig Z, Ibrahim A, Valli C. Denial of service attack detection through machine learning for the IoT. *J. Inf. Telecommun.* 2020;4(4):482–503
- [84] Vaccari I, Aiello M, Cambiaso E. SlowTT: a slow denial of service against IoT networks. *Information* 2020; 11(9):452.
- [85] I. Ahmad, S. Namal, M. Ylianttila, A. Gurtov, Security in software defined networks: A survey, *IEEE Commun. Surv. Tutor.* 17 (4) (2015) 2317–2346.
- [86] Deepak Kshirsagar, Sandeep Kumar, An efficient feature reduction method for the detection of DoS attack, *ICT Express*, Volume 7, Issue 3, 2021, Pages 371-375, ISSN 2405-9595, <https://doi.org/10.1016/j.ict.2020.12.006>.
- [87] Tao Liu, Ming Cao, Claudio De Persis and Julien. M. Hendrickx, Distributed Event-Triggered Control for Synchronization of Dynamical Networks with Estimators, *IFAC Proceedings Volumes • 2013*
- [88] Abdullah A. Mohamed, “Design Intrusion Detection System Based On Image Block Matching”, *International Journal of Computer and Communication Engineering*, IACSIT Press, Vol. 2, No. 5, September 2013.
- [89] Eirini Anthi, Lowri Williams, Matilda Rhode, Pete Burnap, Adam Wedgbury, Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems, *Journal of Information Security and Applications*, Volume 58, 2021, 102717, ISSN 2214-2126, <https://doi.org/10.1016/j.jisa.2020.102717>.
- [90] Thomas Girdler, Vassilios G. Vassilakis, Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending

- against ARP spoofing attacks and Blacklisted MAC Addresses, *Computers & Electrical Engineering*, Volume 90, 2021, 106990, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2021.106990>.
- [91] M. Thirunavukkarasan, P. Muthusamy, S.P. Ramesh, Mukesh Kumar Jha, K. Ramesh, Detection and rectification of cloned node intruder in wireless sensor network, *Materials Today: Proceedings*, 2021, ISSN 2214-7853, <https://doi.org/10.1016/j.matpr.2020.12.1057>.
- [92] Sergio Iglesias Pérez, Santiago Moral-Rubio, Regino Criado, A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity, *Chaos, Solitons & Fractals*, Volume 150, 2021, 111143, ISSN 0960-0779, <https://doi.org/10.1016/j.chaos.2021.111143>.
- [93] J. Jabez, B. Muthukumar, Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach, *Procedia Computer Science*, Volume 48, 2015, Pages 338-346, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2015.04.191>.
- [94] Celyn Birkinshaw, Elpida Rouka, Vassilios 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*, Volume 136, 2019, Pages 71-85, ISSN 1084-8045, <https://doi.org/10.1016/j.jnca.2019.03.005>.
- [95] Christopher Day, Chapter 72 - Intrusion Prevention and Detection Systems, Editor(s): John R. Vacca, *Computer and Information Security Handbook (Third Edition)*, Morgan Kaufmann, 2013, Pages 1011-1025, ISBN 9780128038437, <https://doi.org/10.1016/B978-0-12-803843-7.00072-7>.
- [96] L.N. Tidjon, M. Frappier, A. Mammar, Intrusion detection systems: A cross-domain overview, *IEEE Commun. Surv. Tutor.* 21 (4) (2019) 3639–3681.
- [97] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecurity* 2 (1) (2019) 20.
- [98] Hårek Haugerud, Huy Nhut Tran, Nadjib Aitsaadi, Anis Yazidi, A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization, *Future Generation*

- Computer Systems, Volume 124, 2021, Pages 254-267, ISSN 0167 739X, <https://doi.org/10.1016/j.future.2021.05.037>.
- [99] B.G. Atli, Y. Miche, A. Jung, Network intrusion detection using flow statistics, in: 2018 IEEE Statistical Signal Processing Workshop (SSP), IEEE, 2018, pp. 70–74.
- [100] Pooja TS, Purohit Shrinivasacharya, Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security, Global Transitions Proceedings, Volume 2, Issue 2, 2021, Pages 448-454, ISSN 2666-285X, <https://doi.org/10.1016/j.gltp.2021.08.017>.
- [101] Soroush M. Sohi, Jean-Pierre Seifert, Fatemeh Ganji, and RNNIDS: Enhancing network intrusion detection systems through deep learning, Computers & Security, Volume 102, 2021, 102151, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2020.102151>.
- [102] Jingmei Liu, Yuanbo Gao, Fengjie Hu, A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM, Computers & Security, Volume 106, 2021, 102289, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2021.102289>.
- [103] Yang, Yi & Mclaughlin, Kieran & Sezer, Sakir & Littler, Tim & Pranggono, Bernardi & Brogan, P. & Wang, H. (2013). Intrusion Detection System for Network Security in Synchrophasor Systems. IET Conference Publications. 2013. 10.1049/cp.2013.0059.
- [104] B. Sikdar and J. H. Chow, "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks," IEEETrans.
- [105] E Balamurugan, Abolfazl Mehbodniya, Elham Kariri, Kusum Yadav, Anil Kumar, Mohd Anul Haq, Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN), Pattern Recognition Letters, Volume 156, 2022, Pages 142-151, ISSN 0167-8655, <https://doi.org/10.1016/j.patrec.2022.02.013>.
- [106] Emad-ul-Haq Qazi, Muhammad Imran, Noman Haider, Muhammad Shoaib, Imran Razzak, An intelligent and efficient network intrusion detection system using deep learning, Computers and Electrical Engineering, Volume 99, 2022, 107764, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2022.107764>.

- [107] Jawad Ahmad, Syed Aziz Shah, Shahid Latif, Fawad Ahmed, Zhuo Zou, Nikolaos Pitropakis, DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things, *Journal of King Saud University - Computer and Information Sciences*, 2022, ISSN 1319-1578, <https://doi.org/10.1016/j.jksuci.2022.07.023>.
- [108] Amir Basati, Mohammad Mehdi Faghih, PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders, *Information Sciences*, Volume 598, 2022, Pages 57-74, ISSN 0020-0255, <https://doi.org/10.1016/j.ins.2022.03.065>.
- [109] Jing Yu, Xiaojun Ye, Hongbo Li, A high precision intrusion detection system for network security communication based on multi-scale convolution neural network, *Future Generation Computer Systems*, Volume 129, 2022, Pages 399-406, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2021.10.018>.
- [110] Ganesh, V., Sharma, M. (2021). Intrusion Detection and Prevention Systems: A Review. In: Ranganathan, G., Chen, J., Rocha, Á. (eds) *Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3_71
- [111] Vaishnavi Sivagaminathan, Dr. Manmohan Sharma. “Dynamic Communication Protocol Modelling for Intrusion Traces Using Cisco Packet Tracer Integration with Wireshark”. *Design Engineering*, Aug. 2021, pp. 4583-99, and <http://thedesigengineering.com/index.php/DE/article/view/3853>.
- [112] Zhao Zhang, Yong Zhang, Da Guo, Lei Yao, Zhao Li, SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system, *Future Generation Computer Systems*, Volume 134, 2022, Pages 154-169, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2022.04.010>.
- [113] Xu Zhao, Guangqiu Huang, Jin Jiang, Lin Gao, Maozhen Li, Task offloading of cooperative intrusion detection system based on Deep Q Network in mobile edge computing, *Expert Systems with Applications*,

- Volume 206, 2022, 117860, ISSN 0957-4174,
<https://doi.org/10.1016/j.eswa.2022.117860>.
- [114] Judy Simon, N. Kapileswar, Phani Kumar Polasi, M. Aarthi Elaveini, Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm, *Computers and Electrical Engineering*, Volume 102, 2022, 108190, ISSN 0045-7906,
<https://doi.org/10.1016/j.compeleceng.2022.108190>.
- [115] Marc Chale, Nathaniel D. Bastian, Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems, *Expert Systems with Applications*, Volume 207, 2022, 117936, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117936>.
- [116] Fawaz S. Al-Anzi, Design and analysis of intrusion detection systems for wireless mesh networks, *Digital Communications and Networks*, 2022,, ISSN 2352-8648, <https://doi.org/10.1016/j.dcan.2022.05.013>.
- [117] Wei Wang, Songlei Jian, Yusong Tan, Qingbo Wu, Chenlin Huang, Representation learning-based network intrusion detection system by capturing explicit and implicit feature interactions, *Computers & Security*, Volume 112, 2022, 102537, ISSN 0167-4048,
<https://doi.org/10.1016/j.cose.2021.102537>.
- [118] Tanzila Saba, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, Saeed Ali Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, *Computers and Electrical Engineering*, Volume 99, 2022, 107810, ISSN 0045-7906,
<https://doi.org/10.1016/j.compeleceng.2022.107810>.
- [119] Shirvai, A., Shirvai, H., Tavallae, M., Ghorbani, A.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Comput. Secur.* 31(3), 357–374 (2012)
- [120] Budilaksono, S., Riyadi, A. A., Azhari, L., Saputra, D. D., Suwarno, M. A., Suwartane, I. G. A., ... & Fauzi, A. (2020, February). Comparison of Data Mining Algorithm: PSO-KNN, PSO-RF, and PSO-DT to Measure Attack Detection Accuracy Levels on Intrusion Detection System. In *Journal of Physics: Conference Series* (Vol. 1471, No. 1, p. 012019). IOP Publishing.

- [121] Kennedy J, Eberhart R (1995) Particle swarm optimization. In: Proceedings of the IEEE international conference on neural networks, IEEE Press, Piscataway, 1942–1948
- [122] KDnuggets, (2017). Introduction to Anomaly Detection. Retrieved on June 3rd, 2021 from <https://www.kdnuggets.com/2017/04/datascience-introduction-anomaly-detection.html>.
- [123] Kotsiantis, S. B. (2013). Decision trees: a recent overview. *Artificial Intelligence Review*, 39(4), 261-283.
- [124] Kotsiantis, S., Kostoulas, A., Lykoudis, S., Argiriou, A., & Menagias, K. (2007). A hybrid data mining technique for estimating mean daily temperature values. *IJICT Journal*, 1(5), 54-59.
- [125] Ogundokun, R.O., Sadiku, P.O., Misra, S., Awotunde, J.B., Jaglan, V. (2021). Diagnosis of Long Sightedness Using Neural Network and Decision Tree Algorithms. *Journal of Physics: Conference Series*, 1767(1), 012021.
- [126] Kim, S. Y., & Upneja, A. (2014). Predicting restaurant financial distress using decision tree and AdaBoosted decision tree models. *Economic Modelling*, 36, 354-362.
- [127] J. F. Schutte, “The Particle Swarm Optimization Algorithm”, EGM 6365 - Structural Optimization Fall 2005.
- [128] Aniss Chohra, Paria Shirani, ElMouatez Billah Karbab, Mourad Debbabi, Chameleon: Optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection, *Computers & Security*, Volume 117, 2022, 102684, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2022.102684>. Ganesh, V., Sharma, M. (2021). Intrusion Detection and Prevention Systems: A Review. In: Ranganathan, G., Chen, J., Rocha, Á. (eds) *Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3_71
- [129] Vaishnavi Sivagaminathan, Dr. Manmohan Sharma. “Dynamic Communication Protocol Modelling for Intrusion Traces Using Cisco Packet Tracer Integration with Wireshark”. *Design Engineering*, Aug. 2021, pp.458399, <http://thedesigengineering.com/index.php/DE/article/view/3853>.
- [130] Subham Kumar Gupta, Meenakshi Tripathi, Jyoti Grover, Hybrid optimization and deep learning based intrusion detection system, *Computers*

- and Electrical Engineering, Volume 100, 2022, 107876, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2022.107876>.
- [131] Muhammad Shabbir Abbasi, Harith Al-Sahaf, Masood Mansoori, Ian Welch, Behavior-based ransomware classification: A particle swarm optimization wrapper-based approach for feature selection, *Applied Soft Computing*, Volume 121, 2022, 108744, ISSN 1568-4946, <https://doi.org/10.1016/j.asoc.2022.108744>.
- [132] Moutaz Alazab, Ruba Abu Khurma, Albara Awajan, David Camacho, A new intrusion detection system based on Moth–Flame Optimizer algorithm, *Expert Systems with Applications*, Volume 210, 2022, 118439, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.118439>.
- [133] Muhammad Hassan Nasir, Salman A. Khan, Muhammad Mubashir Khan, Mahawish Fatima, Swarm Intelligence inspired Intrusion Detection Systems — A systematic literature review, *Computer Networks*, Volume 205, 2022, 108708, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2021.108708>.
- [134] Mohammed Nasser Al-Andoli, Shing Chiang Tan, Wooi Ping Cheah, Distributed parallel deep learning with a hybrid backpropagation-particle swarm optimization for community detection in large complex networks, *Information Sciences*, Volume 600, 2022, Pages 94-117, ISSN 0020-0255, <https://doi.org/10.1016/j.ins.2022.03.053>.
- [135] Ramkumar M .P . , P.V. Bhaskar Reddy, J.T. Thirukrishna, Ch. Vidyadhari, Intrusion detection in big data using hybrid feature fusion and optimization enabled deep learning based on spark architecture, *Computers & Security*, Volume 116, 2022, 102668, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2022.102668>.
- [136] P. Rajesh Kanna, P. Santhi, Hybrid Intrusion Detection using MapReduce based Black Widow Optimized Convolutional Long Short-Term Memory Neural Networks, *Expert Systems with Applications*, Volume 194, 2022, 116545, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.116545>.
- [137] Reham R. Mostafa, Ahmed A. Ewees, Rania M. Ghoniem, Laith Abualigah, Fatma A. Hashim, and Boosting chameleon swarm algorithm with consumption AEO operator for global optimization and feature selection, *Knowledge-Based Systems*, Volume 246, 2022, 108743, ISSN 0950-7051, <https://doi.org/10.1016/j.knosys.2022.108743>.

- [138] Li Zhang, Chee Peng Lim, Yonghong Yu, Ming Jiang, Sound classification using evolving ensemble models and Particle Swarm Optimization, *Applied Soft Computing*, Volume 116, 2022, 108322, ISSN 1568-4946, <https://doi.org/10.1016/j.asoc.2021.108322>.
- [139] Earum Mushtaq, Aneela Zameer, Asifullah Khan, A two-stage stacked ensemble intrusion detection system using five base classifiers and MLP with optimal feature selection, *Microprocessors and Microsystems*, 2022, 104660, ISSN 0141-9331, <https://doi.org/10.1016/j.micpro.2022.104660>.
- [140] Islam Debicha, Richard Bauwens, Thibault Debatty, Jean-Michel Dricot, Tayeb Kenaza, Wim Mees, and TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems, *Future Generation Computer Systems*, 2022, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2022.08.011>.
- [141] Jing Yu, Xiaojun Ye, Hongbo Li, A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network, *Future Generation Computer Systems*, Volume 129, 2022, Pages 399-406, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2021.10.018>.
- [142] Xu Zhao, Guangqiu Huang, Jin Jiang, Lin Gao, Maozhen Li, Task offloading of cooperative intrusion detection system based on Deep Q Network in mobile edge computing, *Expert Systems with Applications*, Volume 206, 2022, 117860, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117860>.
- [143] Zhao Zhang, Yong Zhang, Da Guo, Lei Yao, Zhao Li, SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system, *Future Generation Computer Systems*, Volume 134, 2022, Pages 154-169, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2022.04.010>.
- [144] Vinayakumar Ravi, Rajasekhar Chaganti, Mamoun Alazab, Recurrent deep learningbased feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system, *Computers and Electrical Engineering*, Volume 102, 2022, 108156, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2022.108156>.

- [145] Wei Lo, Hamed Alqahtani, Kutub Thakur, Ahmad Almadhor, Subhash Chander, Gulshan Kumar, A hybrid deep learning based intrusion detection system using spatial temporal representation of in-vehicle network traffic, *Vehicular Communications*, Volume 35, 2022, 100471, ISSN 2214-2096, <https://doi.org/10.1016/j.vehcom.2022.100471>.
- [146] Zhendong Wang, Zeyu Li, Daojing He, Sammy Chan, A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning, *Expert Systems with Applications*, Volume 206, 2022, 117671, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117671>.
- [147] Tanzila Saba, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, Saeed Ali Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, *Computers and Electrical Engineering*, Volume 99, 2022, 107810, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2022.107810>.
- [148] Wei Wang, Songlei Jian, Yusong Tan, Qingbo Wu, Chenlin Huang, Representation learning-based network intrusion detection system by capturing explicit and implicit feature interactions, *Computers & Security*, Volume 112, 2022, 102537, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2021.102537>.
- [149] Mokhtar Mohammadi, Tarik A. Rashid, Sarkhel H.Taher Karim, Adil Hussain Mohammed Aldalwie, Quan Thanh Tho, Moazam Bidaki, Amir Masoud Rahmani, Mehdi Hosseinzadeh, A comprehensive survey and taxonomy of the SVM-based intrusion detection systems, *Journal of Network and Computer Applications*, Volume 178, 2021, 102983, ISSN 1084-8045, <https://doi.org/10.1016/j.jnca.2021.102983>.
- [150] Meng Wang, Yiqin Lu, Jiancheng Qin, A dynamic MLP-based DDoS attack detection method using feature selection and feedback, *Computers & Security*, Volume 88, 2020, 101645, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2019.101645>.
- [151] Javier Maldonado, María Cristina Riff, Bertrand Neveu, A review of recent approaches on wrapper feature selection for intrusion detection, *Expert Systems with Applications*, Volume 198, 2022, 116822, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.116822>.

- [152] Faezah Hamad Almasoudy, Wathiq Laftah Al-Yaseen, Ali Kadhum Idrees, Differential Evolution Wrapper Feature Selection for Intrusion Detection System, *Procedia Computer Science*, Volume 167, 2020, Pages 1230-1239, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2020.03.438>.
- [153] Mehdi Asadi, Mohammad Ali Jabraeil Jamali, Saeed Parsa, Vahid Majidnezhad, Detecting botnet by using particle swarm optimization algorithm based on voting system, *Future Generation Computer Systems*, Volume 107, 2020, Pages 95-111, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2020.01.055>.
- [154] Chohra, Aniss & Shirani, Paria & Karbab, Elmouatez & Debbabi, Mourad. (2022). Chameleon: Optimized Feature Selection using Particle Swarm Optimization and Ensemble Methods for Network Anomaly Detection. *Computers & Security*. 117. 102684. 10.1016/j.cose.2022.102684.
- [155] İlker Gölcük, Fehmi Burcin Ozsoydan, Evolutionary and adaptive inheritance enhanced Grey Wolf Optimization algorithm for binary domains, *Knowledge-Based Systems*, Volume 194, 2020, 105586, ISSN 0950-7051, <https://doi.org/10.1016/j.knosys.2020.105586>.
- [156] Angela E. Kitali, Seyedmirsajad Mokhtarimousavi, Cecilia Kadeha, Priyanka Alluri, Severity analysis of crashes on express lane facilities using support vector machine model trained by firefly algorithm, *Traffic Injury Prevention*, Volume 22, Issue 1, 2021, Pages 79-84, ISSN 1538-9588, <https://doi.org/10.1080/15389588.2020.1840563>.
- [157] Felipe Souza Lima, Victor Manuel Cunha Alves, Antonio Carlos Brandao Araujo, Metacontrol: A Python based application for self-optimizing control using metamodels, *Computers & Chemical Engineering*, Volume 140, 2020, 106979, ISSN 00981354, <https://doi.org/10.1016/j.compchemeng.2020.106979>.
- [158] AmirPouya Hemmasian, Kazem Meidani, Seyedali Mirjalili, Amir Barati Farimani, VecMetaPy: A vectorized framework for metaheuristic optimization in Python, *Advances in Engineering Software*, Volume 166, 2022, 103092, ISSN 0965-9978, <https://doi.org/10.1016/j.advengsoft.2022.103092>.
- [159] E Balamurugan, Abolfazl Mehbodniya, Elham Kariri, Kusum Yadav, Anil Kumar, Mohd Anul Haq, Network optimization using defender system in

- cloud computing security based intrusion detection system with game theory deep neural network (IDSGT-DNN), *Pattern Recognition Letters*, Volume 156, 2022, Pages 142-151, ISSN 0167-8655, <https://doi.org/10.1016/j.patrec.2022.02.013>.
- [160] Emad-ul-Haq Qazi, Muhammad Imran, Noman Haider, Muhammad Shoaib, Imran Razzak, An intelligent and efficient network intrusion detection system using deep learning, *Computers and Electrical Engineering*, Volume 99, 2022, 107764, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2022.107764>.
- [161] Gaochen Cui, Bo Liu, Wenpeng Luan, Neural Network with Extended Input for Estimating Electricity Consumption Using Background-based Data Generation, *Energy Procedia*, Volume 158, 2019, Pages 2683-2688, ISSN 1876-6102, <https://doi.org/10.1016/j.egypro.2019.02.022>.
- [162] Jun Li, Xiaoyu Wei, Bo Li, Zhigao Zeng, A survey on firefly algorithms, *Neurocomputing*, Volume 500, 2022, Pages 662-678, ISSN 0925-2312, <https://doi.org/10.1016/j.neucom.2022.05.100>.
- [163] Judy Simon, N. Kapileswar, Phani Kumar Polasi, M. Aarthi Elaveini, Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm, *Computers and Electrical Engineering*, Volume 102, 2022, 108190, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2022.108190>.
- [164] Ganesh, V., Sharma, M. (2021). Intrusion Detection and Prevention Systems: A Review. In: Ranganathan, G., Chen, J., Rocha, Á. (eds) *Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3_71.
- [165] Guilherme Ramos, A. Pedro Aguiar, Sérgio Pequito, An overview of structural systems theory, *Automatica*, Volume 140, 2022, 110229, ISSN 0005-1098, <https://doi.org/10.1016/j.automatica.2022.110229>.
- [166] Shenhao Wang, Qingyi Wang, Nate Bailey, Jinhua Zhao, Deep neural networks for choice analysis: A statistical learning theory perspective, *Transportation Research Part B: Methodological*, Volume 148, 2021, Pages 60-81, ISSN 0191-2615, <https://doi.org/10.1016/j.trb.2021.03.011>.

- [167] Meysam Valueian, Mojtaba Vahidi-Asl, Alireza Khalilian, SituRepair: Incorporating machine-learning fault class prediction to inform situational multiple fault automatic program repair, *International Journal of Critical Infrastructure Protection*, Volume 37, 2022, 100527, ISSN 1874-5482, <https://doi.org/10.1016/j.ijcip.2022.100527>.
- [168] Emad E. Abdallah, Wafa' Eleisah, Ahmed Fawzi Otoom, Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey, *Procedia Computer Science*, Volume 201, 2022, Pages 205-212, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2022.03.029>.
- [169] Qi, B.W. Analysis on the Application of artificial Intelligence in classroom. *J. Phys. Conf. Ser.* 2019, 1345, 402–420.
- [170] Mehrnaz Mazini, Babak Shirazi, Iraj Mahdavi, Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms, *Journal of King Saud University - Computer and Information Sciences*, Volume 31, Issue 4, 2019, Pages 541-553, ISSN 1319-1578, <https://doi.org/10.1016/j.jksuci.2018.03.011>.
- [171] Islam Debicha, Richard Bauwens, Thibault Debatty, Jean-Michel Dricot, Tayeb Kenaza, Wim Mees, and TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems, *Future Generation Computer Systems*, 2022, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2022.08.011>
- [172] Ying-Dar Lin, Ze-Yu Wang, Po-Ching Lin, Van-Linh Nguyen, Ren-Hung Hwang, and Yuan-Cheng Lai, Multi-datasource machine learning in intrusion detection: Packet flows, system logs and host statistics, *Journal of Information Security and Applications*, Volume 68, 2022, 103248, ISSN 2214-2126, <https://doi.org/10.1016/j.jisa.2022.103248>.
- [173] Said Salloum, Tarek Gaber, Sunil Vadera, Khaled Shaalan, and Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey, *Procedia Computer Science*, Volume 189, 2021, Pages 19-28, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2021.05.077>.
- [174] Galeano-Brajones, J.; Carmona-Murillo, J.; Valenzuela-Valdés, J.F.; Luna-Valero, F. Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. *Sensors* 2020, 20, 816. <https://doi.org/10.3390/s20030816>

- [175] Bao, H.; He, H.; Liu, Z.; Liu, Z. Research on information security situation awareness system based on big data and artificial intelligence technology. In Proceedings of the 2019 international conference on robots intelligent system (ICRIS), Haikou, China, 15–16 June 2019; pp. 318–322.
- [176] Vaishnavi Sivagaminathan, Dr. Manmohan Sharma. “Dynamic Communication Protocol Modelling for Intrusion Traces Using Cisco Packet Tracer Integration with Wireshark”. Design Engineering, Aug. 2021, pp.458399, <http://thedesigengineering.com/index.php/DE/article/view/3853>.
- [177] Pampapathi B M, Nageswara Gupta M, M S Hema, Towards an effective deep learning-based intrusion detection system in the internet of things, Telematics and Informatics Reports, Volume 7, 2022, 100009, ISSN 2772-5030, <https://doi.org/10.1016/j.teler.2022.100009>.
- [178] Chunying Zhang, Donghao Jia, Liya Wang, Wenjie Wang, Fengchun Liu, Aimin Yang, Comparative research on network intrusion detection methods based on machine learning, Computers & Security, Volume 121, 2022, 102861, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2022.102861>.
- [179] Fawaz S. Al-Anzi, Design and analysis of intrusion detection systems for wireless mesh networks, Digital Communications and Networks, 2022, ISSN 2352-8648, <https://doi.org/10.1016/j.dcan.2022.05.013>.
- [180] Ibrahim Hayatu Hassan, Abdullahi Mohammed, Mansur Aliyu Masama, Yusuf Sahabi Ali, Abdulrazaq Abdulrahim, An Improved Binary Manta Ray Foraging Optimization Algorithm based feature selection and Random Forest Classifier for Network Intrusion Detection, Intelligent Systems with Applications, 2022, 200114, ISSN 2667-3053, <https://doi.org/10.1016/j.iswa.2022.200114>.
- [181] Subhash V. Pingale, Sanjay R. Sutar, Remora whale optimization-based hybrid deep learning for network intrusion detection using CNN features, Expert Systems with Applications, Volume 210, 2022, 118476, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.118476>.
- [182] Sarika Choudhary, Nishtha Kesswani, Analysis of KDD-Cup’99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT, Procedia Computer Science, Volume 167, 2020, Pages 1561-17, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2020.03.367>.

- [183] Said Salloum, Tarek Gaber, Sunil Vadera, Khaled Shaalan, and Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey, *Procedia Computer Science*, Volume 189, 2021, Pages 19-28, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2021.05.077>.
- [184] Oladele, T.O., Ogundokun, R.O., Kayode, A.A., Adegun, A.A., Adebiyi, M.O. (2019). Application of Data Mining Algorithms for Feature Selection and Prediction of Diabetic Retinopathy. *Lecture Notes in Computer Science* (including subseries *Lecture Notes in Artificial Intelligence* and *Lecture Notes in Bioinformatics*), 11623 LNCS, pp. 716-730
- [185] Ganesh, V., Sharma, M. (2021). Intrusion Detection and Prevention Systems: A Review. In: Ranganathan, G., Chen, J., Rocha, Á. (eds) *Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems*, vol 145. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3_71
- [186] Sindhu, S. S. S., Geetha, S., & Kannan, A. (2012). Decision tree-based lightweight intrusion detection using a wrapper approach. *Expert Systems with Applications*, 39(1), 129-141.
- [187] Hoque, M. S., Mukit, M., Bikas, M., & Naser, A. (2012). An implementation of an intrusion detection system using a genetic algorithm. *arXiv preprint arXiv:1204.1336*.
- [188] Guo Y. L., 2007. An active learning-based TCM-KNN algorithm for supervised network intrusion detection. *Computers and Security*, 26, 459-467
- [189] Vu Viet Thang, F. F. Pashchenko, "Multistage System-Based Machine Learning Techniques for Intrusion Detection in WiFi Network", *Journal of Computer Networks and Communications*, vol. 2019, Article ID 4708201, 13 pages, 2019. <https://doi.org/10.1155/2019/4708201>
- [190] Preeti, Kusum Deep, A random walk Grey wolf optimizer based on dispersion factor for feature selection on chronic disease prediction, *Expert Systems with Applications*, Volume 206, 2022, 117864, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117864>.
- [191] Jun Li, Xiaoyu Wei, Bo Li, Zhigao Zeng, A survey on firefly algorithms, *Neurocomputing*, Volume 500, 2022, Pages 662-678, ISSN 0925-2312, <https://doi.org/10.1016/j.neucom.2022.05.100>