Heriot-Watt University

Masters Thesis

Thesis Title

Author:
Joshik Roshan

Supervisor:
Letychevskyi Oleksandr

A thesis submitted in fulfilment of the requirements for the degree of Msc Data Science

in the

School of Mathematical and Computer Sciences

April 2024

Declaration of Authorship

Student Declaration of Authorship

HERIOT WATT UNIVERSITY
UK | DUBAI | MALAYSIA

Course code and name:	F21RP Research Methods And Project Planning
Type of assessment:	**Individual**
Coursework Title:	Research Methods And Project Planning Report
Student Name:	Narayana Joshik Roshan
Student ID Number:	H00449457

Declaration of authorship. By signing this form:

- **I declare** that the work I have submitted for individual assessment OR the work I have contributed to a group assessment, is entirely my own. I have NOT taken the ideas, writings or inventions of another person and used these as if they were my own. My submission or my contribution to a group submission is expressed in my own words. Any uses made within this work of the ideas, writings or inventions of others, or of any existing sources of information (books, journals, websites, etc.) are properly acknowledged and listed in the references and/or acknowledgements section.

- I confirm that I have read, understood and followed the University's Regulations on plagiarism as published on the University's website, and that I am aware of the penalties that I will face should I not adhere to the University Regulations.

- I confirm that I have read, understood and avoided the different types of plagiarism explained in the University guidance on Academic Integrity and Plagiarism

Student Signature: Narayana Joshik Roshan

Date: *16th April, 2024*.

"Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism."

Dave Barry

Abstract

The vulnerability of satellite systems to cyberattacks necessitates robust security measures. An Intrusion Detection System is an application which captures malicious or suspicious activity in the network traffic. This research delves into the application of artificial intelligence (AI) for the development of advanced intrusion detection systems (IDS) within satellite networks. Unlike traditional IDS that rely heavily on known signatures, AI-powered solutions offer a more proactive and adaptable defence strategy. The absence of real-time data significantly complicates this analysis. Machine learning algorithms empower these systems to learn from data patterns, detect subtle anomalies, and flag potential threats even in zero-day attack scenarios. Although there have been many successful researches in the past with excellent accuracies, there is no structured comparison among all the models with different datasets. A detailed comparison among the available datasets with the proposed methodologies is needed to understand satellite attacks in-depth. This project aims to assess the efficiency of various Machine Learning techniques in the context of satellite security. Furthermore, the author evaluates the ML model with various metrics and discusses the limitations which can be taken under consideration in future studies.

Acknowledgements

The acknowledgements and the people to thank go here, don't forget to include your project advisor :)

Contents

Declaration of Authorship i

Abstract iii

Acknowledgements iv

Contents v

List of Figures vii

Abbreviations viii

1 Introduction 1
- 1.1 Current Knowledge Gap . . . 2
- 1.2 Motivation . . . 2
- 1.3 Aim . . . 2

2 Literature Review 4
- 2.1 Background . . . 4
- 2.2 Satellite System Architecture . . . 4
  - 2.2.1 Space segment . . . 5
  - 2.2.2 Ground segment . . . 5
  - 2.2.3 User Segment . . . 6
  - 2.2.4 Link Segment . . . 6
- 2.3 Satellite Communication Layers And Protocols . . . 6
  - 2.3.1 Network Layer: . . . 6
  - 2.3.2 Transport Layer: . . . 7
- 2.4 Satellite System Security Threats . . . 7
- 2.5 Intrusion Detection System . . . 7
- 2.6 ML Techniques used for Intrusion Detection in the Satellite Systems . . . 8
  - 2.6.1 Logistic Regression And IDS . . . 9
  - 2.6.2 Support Vector Machine And IDS . . . 9
  - 2.6.3 Naive Bayes And IDS . . . 10
  - 2.6.4 Random Forest And IDS . . . 10
  - 2.6.5 Neural Networks And IDS . . . 11
- 2.7 ML Models . . . 12
  - 2.7.1 Linear Regression . . . 13

2.7.2 Support Vector Machine . . . 13
2.7.3 Random Forest . . . 13
2.7.4 Neural Networks . . . 14
2.8 Applications of Machine Learning . . . 19
2.9 Conclusion . . . 20

3 *Methodology* 21
3.1 Data Collection . . . 22
3.2 Data pre-processing . . . 23
3.3 Feature Selection . . . 23
3.4 Model Development . . . 23
3.5 Model Optimisation . . . 23
3.6 Model Validation . . . 24

4 *Requirements* 25
4.1 *MoSCoW* . . . 25
4.2 *Functional Requirements* . . . 26
4.3 *Non Functional Requirements* . . . 27

5 *Evaluation* 28

6 *PROFESSIONAL, LEGAL, ETHICAL AND SOCIAL ISSUES* 31

7 *Project Planning* 33
7.1 Gantt Chart . . . 33
7.2 Risk Management . . . 34

A Appendix Title Here 35

Bibliography 36

List of Figures

2.1 High Level Architecture (*Satellite Communication - Quick Guide* [n.d.]) . 5
2.2 IDS Architecture (Zhu and Wang [2019]) 8
2.3 Comparison various deep learning models 11
2.4 Machine learning types Sarker [2021] 12
2.5 Linear Regression 13
2.6 *Support Vector Machine Algorithm* [n.d.] 14
2.7 Random Forest (*Understanding Random Forest* [n.d.]) 14
2.8 Structure of an artificial neuron 15
2.9 Classification of activation functions Dubey et al. [2022] 16
2.10 Perceptron 16
2.11 Single Layer Perceptron Ahamed and Akthar [2016] 17
2.12 Multilayer Perceptron Ahamed and Akthar [2016] 17
2.13 Multilayer Feeback Network Ahamed and Akthar [2016] 18
2.14 CNN 5 Layer Architecture Kriegeskorte and Golan [2019] 18

3.1 WorkFlow 21
3.2 NSL-KDD/ KDD-CUPP99 Description (Ashraf et al. [2022]) 22
3.3 Stin Dataset features (Li et al. [2020]) 22
3.4 Model Development Phases 23

4.1 Comparison of different techniques (Khan et al. [2015]) 25
4.2 Functional Requirements 26
4.3 Non Functional Requirements 27

7.1 Research 34
7.2 Project Planning 34

Abbreviations

ANN	**A**rtificial **N**eural **N**etwork
ML	**M**achine **L**earning
IDS	**I**ntrusion **D**etection **S**ystem
SVM	**S**upport **V**ector **M**achine
DNN	**D**eep **N**eural **N**etwork
CNN	**C**onvolutional **N**eural **N**etwork
DoS	**D**enial **O**f **S**ervice
IP	**I**nternet **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
U2R	**U**ser **T**o **R**oot
R2L	**R**oot **T**o **L**ocal

Chapter 1

Introduction

A Cyber Attack is a deliberate and often malicious attempt to breach the information security of an individual, organization, or government entity. The primary goals of cyber attacks include financial gain, political moves, information theft etc.
Here's the list of some common cyber attacks:

- **Eavesdropping**: interception of information intended for someone else during transmission over a communication channel.
- **Alteration**: unauthorised modification of information.
- **Denial-of-service:** the interruption or degradation of data service or information access.
- **Masquerading:** the fabrication of information that is purported to be from someone who is not the author.
- **Repudiation:** the denial of commitment or data receipt. Example: back out of an online deal.
- **Correlation and traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.

Cyber Attacks in satellite systems have become a major concern in the modern era as the technology emerged like never before. Due to the large attack surface, the probability of attacking satellite systems has also significantly risen. Due to a large number of

interconnected components in satellite systems, the entry of points for cyber attacks increased. Satellite Systems have segments like space segment, user segment, link segment, ground segment etc. Each segment has a threat of being attacked in many ways. Hence it is important to prevent these and identify the underlying patterns of such attacks.

1.1 Current Knowledge Gap

The biggest challenge in developing a solution to this problem is the lack of real datasets. Although there are many proposed solutions to this problem using machine learning techniques, they all have certain limitations such which can be improved. All the existing research has shown excellent accuracies but is limited to a few machine learning techniques. In this report, the author performs various relevant machine learning techniques to analyse the comparison of various machine learning algorithms with different available datasets to provide an evidence-based conclusion.

1.2 Motivation

To remedy this shortfall, several ML techniques can be performed including deep learning to make comprehensive comparisons among the available datasets. This could potentially create an impact on the satellite organisation's cyber security department to understand the intrusions in-depth and make conclusions.

1.3 Aim

The aim of this paper is to :

- Analyse the existing dataset thoroughly to understand the limitations.
- Explore the existing machine learning-based solutions.
- Identify the gaps in the literature.
- Perform various machine learning methods to identify the best one.

- Compare performances of each algorithm by confusion matrix, ROC curve etc.

Through conducting this investigation, the author aims to communicate both the capabilities and constraints of machine-learning methods.

Chapter 2

Literature Review

2.1 Background

Satellites are objects in orbits about the Earth. An orbit is a trajectory able to maintain gravitational equilibrium to circle the Earth without power assist. Satellites are classified by the distance between the orbit they are in and the Earth. There are three different kinds of satellites i.e. LEO, GEO, MEO. Low Earth Orbiting Satellites are at altitudes of 100 to 1200 miles. Medium Earth Orbiting Satellites are at altitudes of 4,000 to 12,000 miles. GEO Stationary Orbiting Satellites are at exactly 23.4 miles altitude from the earth's surface. Roddy [2006]

Satellite communication has three phases. Sending out the signal to the target satellite (Uplink phase), amplifying the received signal by the target satellite (transponder phase), and transferring it back to Earth's ground segment (downlink phase).

2.2 Satellite System Architecture

The Satellite systems have two broad segments namely a space segment and a ground segment.

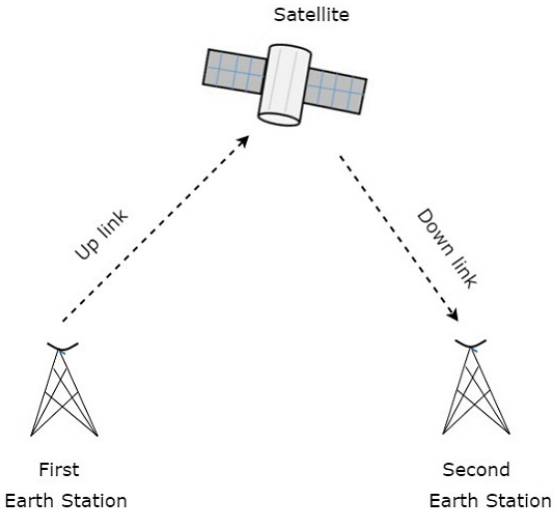


FIGURE 2.1: High Level Architecture (*Satellite Communication - Quick Guide* [n.d.])

2.2.1 Space segment

This is the segment where satellites themselves reside. The most common subsystems of the space segment are the payload, the bus and the transponder.

- **Payload:** The payload refers to the equipment used to provide the service for which the satellite has been launched (Roddy [2006]).
- **Bus:** The bus refers not only to the vehicle which carries the payload but also to the various subsystems which provide the power, attitude control, orbital control, thermal control, and command and telemetry functions required to service the payload (Roddy [2006]).
- **Transponder:** the equipment which provides the connecting link between the satellites' transmit and receive antennas (Roddy [2006]).

2.2.2 Ground segment

This segment is responsible for maintaining communication with satellites by tracking their trajectories. Ground stations, satellite control centres, antenna systems and data processing centres come under this segment. This segment deals with the uplink and downlink phases of satellite communication.

2.2.3 User Segment

The User segment comprises end users who utilise the services provided by the satellite systems.

2.2.4 Link Segment

The Link segment is responsible for communication between different segments in satellite architecture i.e. ground to space, space to ground, ground to ground, and space to space.

2.3 Satellite Communication Layers And Protocols

The most crucial communication layers in the satellite systems communication system are the network layer, transport layer, and application layer.

2.3.1 Network Layer:

This layer is responsible for routing the packets across the network nodes efficiently. Packetizing, Routing, and Forwarding are the key responsibilities of the network layer. The process of encapsulating the data received from the upper layers of the network (also called payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination. Routing is the process of directing the data packets from one device to another device. Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces (*Network Layer Services- Packetizing, Routing and Forwarding* [n.d.]). The most common protocol of this layer is IP

- **Internet Protocol (IP)** This is responsible for uniquely identifying devices across the internet to transmit the data. IPV4(32 bits) and IPV6(128 bits) are its variants.

2.3.2 Transport Layer:

This layer ensures that data flows from end to end properly by controlling network traffic. The most common transport layer protocols are TCP, UDP

- **Transmission Control Protocol:** First, a connection between both ends is established and data is transmitted. It is a reliable protocol
- **User Datagram Protocol:** This is a connectionless protocol unlike TCP protocol, hence unreliable. This is helpful when data transfer speed is prioritized over security and dependability.

2.4 Satellite System Security Threats

The few most common attacks in the satellite system are

- **Denial Of Service Attack (DoS):** Preventing legitimate users from accessing the system. This is considered to be the most dangerous attack.
- **Distributed Denial Of Service Attack (DDOS):** A malicious attack with multiple compromised computers as the network traffic. Distributed Denial Of Service attack is more effective in comparison with Denial Of Service attack.
- **Prob Attacks:** Unauthorised users accessing confidential information from a system.
- **User To Root (U2R) Attacks:** These types of attacks involve gaining the administrator's access by unauthorised users
- **Remote To Local (R2L) Attacks:** This class begins by gaining access to a normal user while sniffing around for passwords to gain access as a root user to a computer resource. (paper reference)

2.5 Intrusion Detection System

An intrusion is any form of unauthorised access to a network or a system. The need for intrusion detection has significantly risen due to a large number of cyber-attacks across

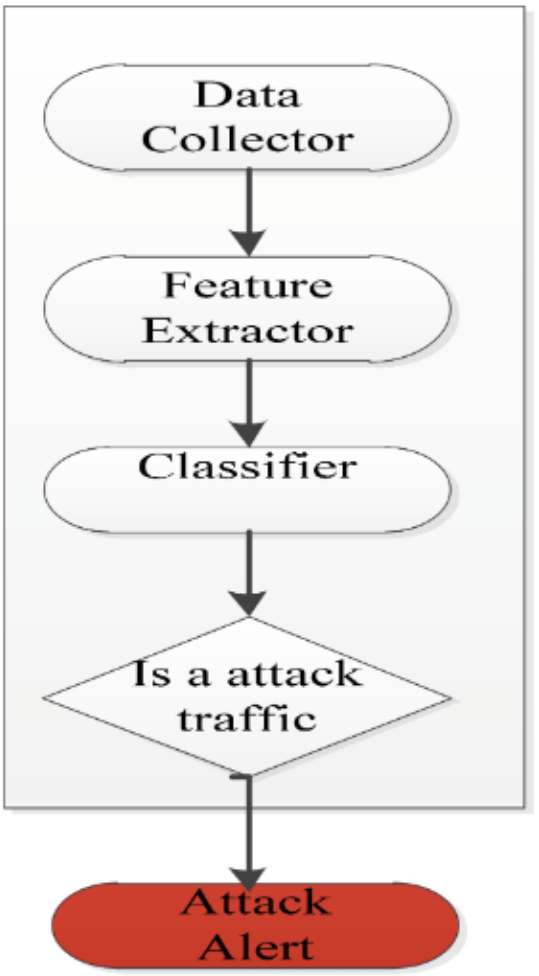


FIGURE 2.2: IDS Architecture (Zhu and Wang [2019])

various networks. Especially in satellite systems, this has become a serious threat. Due to the alarming increase in intrusion attacks in satellite systems, a strong intrusion system is needed.

2.6 ML Techniques used for Intrusion Detection in the Satellite Systems

Since the number of intrusions in satellite systems has been increasing rapidly, many researchers proposed ML-based intrusion detectors. Although there are very few related data sets. Here's the list of some ML techniques used to build a model that classifies if there is an intrusion occurred :

- Logistic Regression

- Naive Bayes
- Support Vector Machine
- Random Forest
- Neural Networks

2.6.1 Logistic Regression And IDS

This finds the best fitting line which predicts the class when we provide features. Logistic Regression is used in binary classification.

Ghosh and Mitra [2015] considers the NSL-KDD dataset for their proposed algorithm. Once the dataset is pre-processed and normalised, Correlation Coefficients are calculated between all pairs of features and the class variable.

In this proposed method authors have built an effective feature selection method for decreasing the storage space as well as processing time without compromising the classification accuracy. Also, they have exploited a way to exploit Logistic Regression for multiclass classification problems.

RESULTS This classifier achieved the accuracy of **74.95%.**

2.6.2 Support Vector Machine And IDS

Support Vector Machine is one of the best machine learning algorithms for binary classification.
Jha and Ragha [2013] used NSL-KDD Dataset for their SVM-based classifier which detects the intrusions in satellite systems. After preprocessing the dataset, the authors performed IGR (Information Gain Ranking) based feature ranking. Further, the authors have used the K Means classifier to compute the detection rate for each subset of features.
The authors further state that although there are many existing SVM-based classifiers, they are computationally very expensive. Hence they tried to extract the most import features which give the best accuracy and better computation at the same time. The proposed approach is based on a hybrid approach which combines filter and wrapper

models for selecting relevant features. This reduced dataset will increase the performance and detection accuracy of SVM based detection model.
RESULTS: This classifier achieved the accuracy of **99.37%.**

2.6.3 Naive Bayes And IDS

Naïve Bayes is a probabilistic machine learning algorithm based on the Bayes Theorem, used in a wide variety of classification tasks (Nagesh Singh Chauhan [n.d.]). Once a hypothesis is defined, we find the probability if the assumed hypothesis is true.
Panda and Patra [2007] performed their experimental analysis with the KDD-CUPP dataset. The authors state that the KDD CUPP is extracted from the DARPA dataset which is famous for IDS, they can get rid of the most time-consuming data pre-processing step. The authors experimented with 10% of the KDD CUPP dataset that contains 65,525 connections. 10 Fold cross-validation is applied on the dataset. One among them is used as a testing dataset and the remaining are used for building the model.
For evaluation authors used false positive rates and detection rates as metrics. This proposal resulted in higher detection rates in comparison with neural networks, cost-efficient and less time-consuming.
RESULTS: This classifier achieved the accuracy of **95.00%.**

2.6.4 Random Forest And IDS

Random Forest is a popular machine learning algorithm for both classification and regression tasks which builds on multiple decision trees to make robust and accurate predictions.
Farnaaz and Jabbar [2016] preprocessed NSL-KDD dataset by discretization technique. The authors proposed to cluster the dataset into four sub-parts and partition them into training, and testing datasets. Further authors select the best-set features using feature subset selection measure Symmetrical uncertainty (SU). For their experimental analysis, while preprocessing the dataset they have replaced all the null values to mean and mode. For discretizing the numeric features, the authors used 10-bin discretization.

The authors compared the proposed random forest modelling with the j48 classier in terms of accuracy, DR, FAR and MCC. The experimental results proved that accuracy,

DR and MCC for four types of attacks are increased by their proposed method.

RESULTS : This classifier achieved an accuracy of **99.73%**

2.6.5 Neural Networks And IDS

Neural Networks are inspired by human brain functionality. Various deep learning-based techniques with different architectures were chosen to detect the intrusion. Gurung et al. [2019] developed a model using the NSL-KDD dataset based on Auto-encoders to detect intrusions which gives a higher accuracy rate in comparison to Signature-Based Intrusion Detection approaches and also reduces the chances of False Positives and Negatives. A recurrent Neural Network based model was proposed by Yin et al. [2017] using the NSL-KDD dataset, compared with traditional classification methods, such as J48, naive Bayesian, and random forest, the performance obtains a higher accuracy rate and detection rate with a low false positive rate, especially under the task of multiclass classification on the NSL-KDD dataset. In 2020, Devan and Khare [2020] proposed a Deep Neural Network model with better accuracy and faster prediction using the same dataset.

RESULTS

Paper Title	Author(S) Name	Dataset	Deep Learning Architecture(S)	Accuracy
A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks.	Yin et al.	NSL-KDD	Recurrent Neural Networks	97.09
Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset.	Gurung et al.	NSL-KDD	Auto-encoders	87.20
AN efficient XGBoost–DNN based classification model for network intrusion detection system	Devan and Khare	NSL-KDD	deep neural networks (DNNs)	97
Deep Learning Approach for Intelligent Intrusion Detection System.	Vinaya kumar et al	KDD CUP-99 NSL-KDD WSN-DS UNSW-NB15 CICIDS 2017	deep neural networks (DNNs)	KDD CUP-99: 92.63 NSL-KDD: 78.63 UNSW-NB15: 62.10 WSN-DS: 96.60 CICIDS 2017: 95.78

FIGURE 2.3: Comparison various deep learning models

2.7 ML Models

A Machine learning model is a program trained by various algorithms that predicts a given input's output. Machines are trained themselves as per the algorithm. Machine learning algorithms are classified into two types i.e. Supervised Learning and Unsupervised Learning.

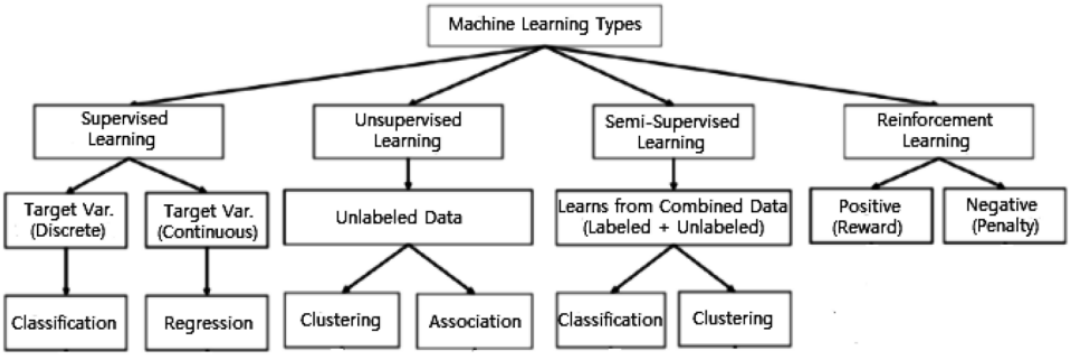


FIGURE 2.4: Machine learning types Sarker [2021]

- **Supervised Learning:** This involves training the dataset which has labelled data. A function maps an input to an output based on the existing input, and output training data. Some of the most common techniques are regression, decision trees, support vector machines etc

- **Unsupervised Learning:** This involves training the dataset which does not have any labels. Unsupervised learning helps discover the patterns. This is widely used for extracting generative features, identifying meaningful trends and structures, groupings in results, and exploratory purposes. Sarker [2021]

- **Semisupervised Learning:** Semi-supervised learning can be defined as a hybridization of the above-mentioned supervised and unsupervised methods, as it operates on both labelled and unlabeled data Sarker [2021]

- **Reinforcement Learning:** Reinforcement learning is a type of machine learning algorithm that enables software agents and machines to automatically evaluate the optimal behaviour in a particular context or environment to improve its efficiency Kaelbling et al. [1996], i.e., an environment-driven approach.

2.7.1 Linear Regression

A statistical technique that fits a linear function to set input-output pairs. A few practical implementations of linear regression include evaluating trends, sales analysis, sports analysis, stock price prediction and weather forecasting. According to Kumari and Yadav [2018] linear regression is important for two reasons

- **Descriptive:** It helps in analyzing the strength of the association between the outcome (dependent variable) and predictor variables
- **Adjustment:** It adjusts for the effect of covariates or the confounders

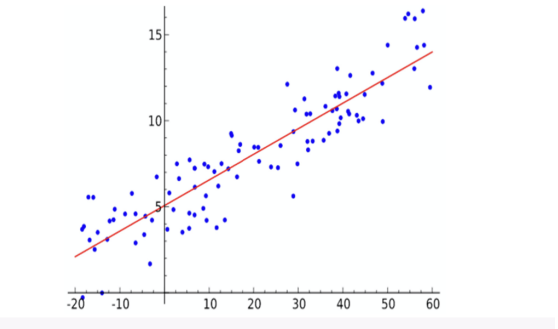


FIGURE 2.5: Linear Regression

2.7.2 Support Vector Machine

A powerful supervised machine learning technique used for classification and regression problems. It provides an added advantage of detecting outliers. It finds the most optimal hyperplane in N-dimensional space which separates the data points. This hyperplane maintains the margin between the closest points of different classes as much as possible. SVM is helpful in medical decision support Veropoulos et al. [1999], time series prediction Fernandez Jr et al. [2017] etc.

2.7.3 Random Forest

A popular supervised machine learning algorithm used in both classification and regression problems. As the name suggests, "Random Forest is a classifier that contains many decision trees on various subsets of the given dataset and takes the average to improve the

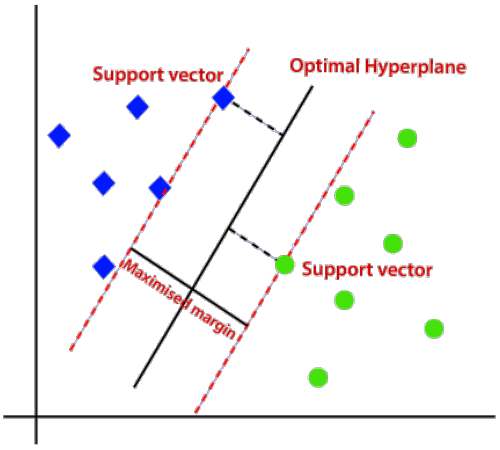


FIGURE 2.6: *Support Vector Machine Algorithm* [n.d.]

predictive accuracy of that dataset." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, it predicts the final output *Support Vector Machine Algorithm* [n.d.]. Random features are selected in the induction process. Prediction is made by aggregating (majority vote for classification or averaging for regression) the predictions of the ensemble. Ali et al. [2012]

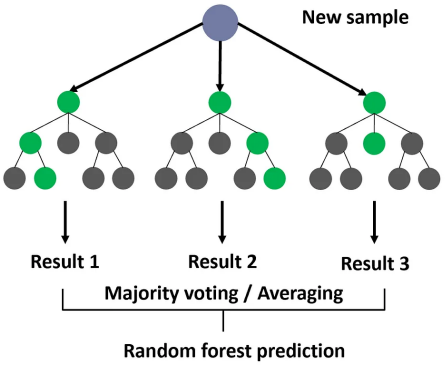


FIGURE 2.7: Random Forest (*Understanding Random Forest* [n.d.])

2.7.4 Neural Networks

Neural networks mimic the complex functions of the human brain. According to Kriegeskorte and Golan [2019], a biological neuron receives multiple signals through the synapses contacting its dendrites and sends a single stream of action potentials out through its axon. The conversion of a complex pattern of inputs into a simple decision (to spike or not to spike) suggested to early theorists that each neuron performs an elementary

cognitive function: it reduces complexity by categorizing its input patterns. Inspired by this intuition, artificial neural network models are composed of units that combine multiple inputs and produce a single output.

A neural network has an input layer, an output layer and several hidden layers in itself. Neural networks involve two major processes i.e. forward propagation and backward propagation. Artificial Neural Networks (ANNs) are computational processing systems of which are heavily inspired by way biological nervous systems (such as the human brain) operate. Kriegeskorte and Golan [2019]

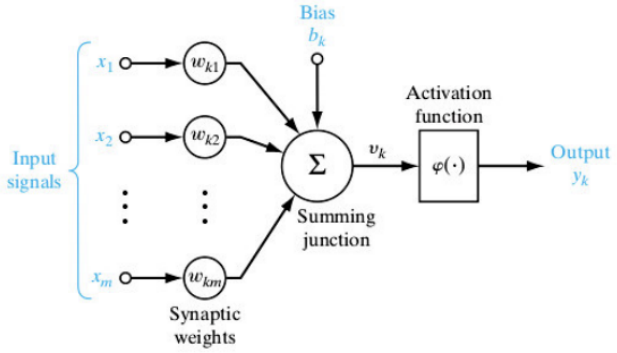


FIGURE 2.8: Structure of an artificial neuron

Architecture of a neural network

- **Input Layer:** This layer receives the input from the raw dataset.
- **Hidden Layer:** There are few advanced neural networks comprising this layer in their architecture.
- **Output Layer:** This layer produces the end result of a trained model processed through various layers.

Activation Function: An Activation Function is the most critical component of a neural network. It is responsible for bringing non-linearity into the model. In the absence of activation functions, the output would be a linear function of the input (linear regression model). Dubey et al. [2022]

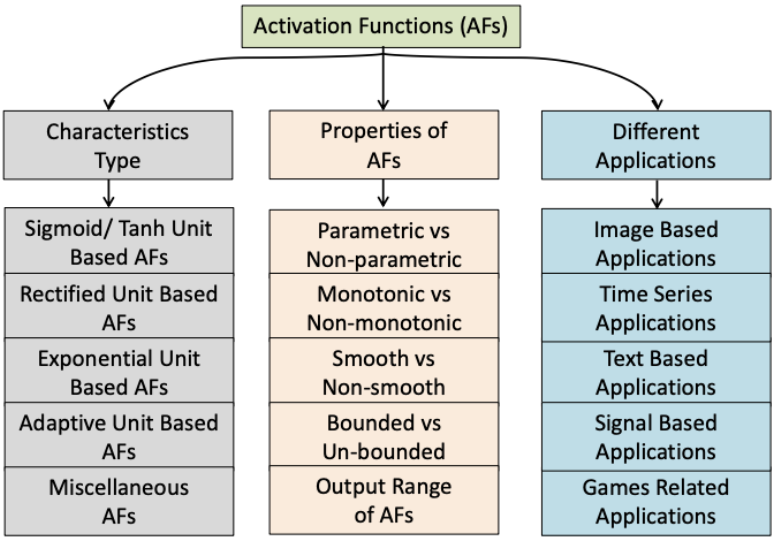


FIGURE 2.9: Classification of activation functions Dubey et al. [2022]

Perceptron: An artificial neuron is also known as perception. It takes several binary inputs and produces a single binary output.

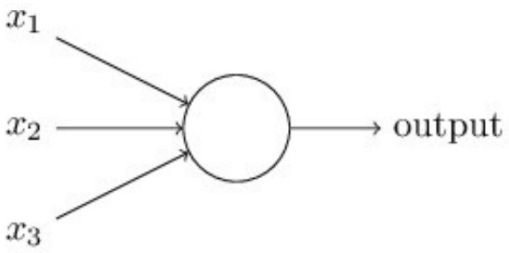


FIGURE 2.10: Perceptron

Types of neural networks

- **Single Layer Perceptron** It is one of the simplest neural networks which comes under supervised learning of binary classifiers. Single-layer Perceptrons can learn only linearly separable patterns. Ahamed and Akthar [2016]
- **Multilayer Perceptron:** Multilayer perceptron solves the limitation of single-layer perceptron. It is capable of learning from non-linear/ complex data. This is the most popular architecture as of today. Ahamed and Akthar [2016]

  Learning Phases:

  - **Forward Propagation** In this type of propagation, input data is passed in the forward direction through several layers till it reaches the output layer.

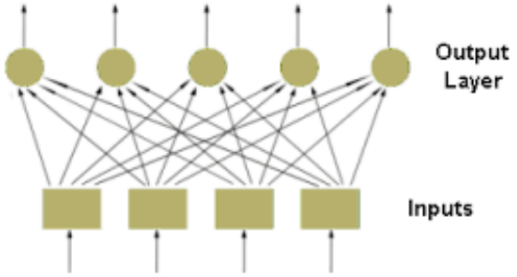


FIGURE 2.11: Single Layer Perceptron Ahamed and Akthar [2016]

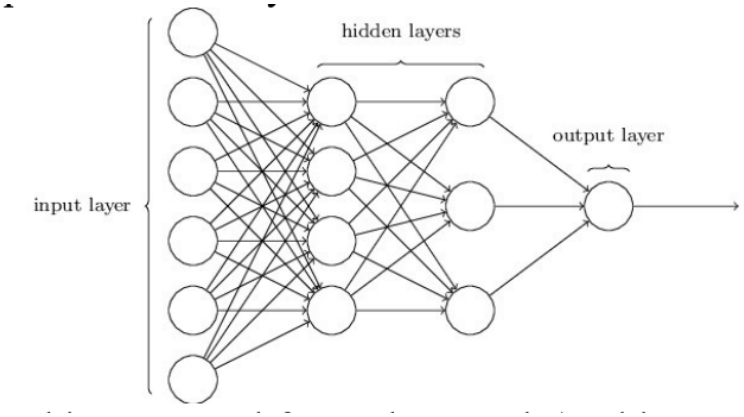


FIGURE 2.12: Multilayer Perceptron Ahamed and Akthar [2016]

Each neuron is associated with some weight. The weight of each neuron describes the strength of the connection. This keeps on varying throughout the training process.

- **Backward Propagation** In this type of propagation, the network learns from the errors. The loss calculation finds the difference between the actual value and the desired value.

- **Feed Forward Neural Network:** A simple artificial neural network which propagates in a single direction. There is no feedback loop present in this type of neural network.

- **Multilayer Feedback Network** These types of neural networks have feedback loops in themselves. According to Ahamed and Akthar [2016], The idea in these models is to have neurons which fire for some limited duration of time, before becoming quiescent. That firing can stimulate other neurons, which may fire a little while later, also for a limited duration

- **Convolutional Neural Networks:** CNNs are analogous to traditional ANNs in that they are comprised of neurons that self-optimise through learning. From the

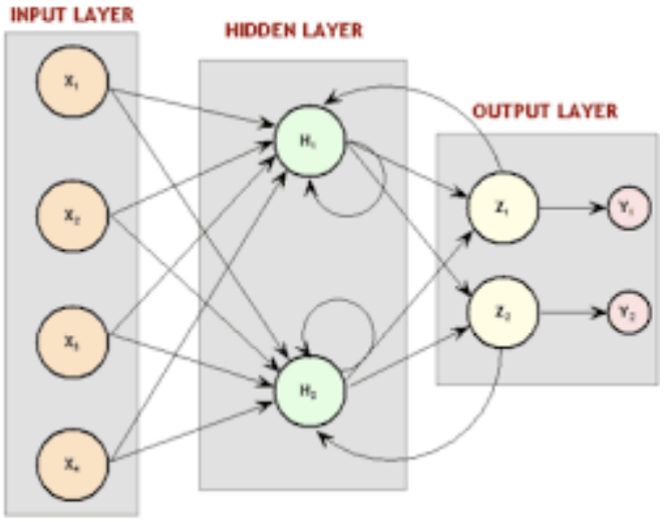


FIGURE 2.13: Multilayer Feeback Network Ahamed and Akthar [2016]

input raw image vectors to the final output of the class score, the entire of the network will still express a single perceptive score function (the weight). Kriegeskorte and Golan [2019]

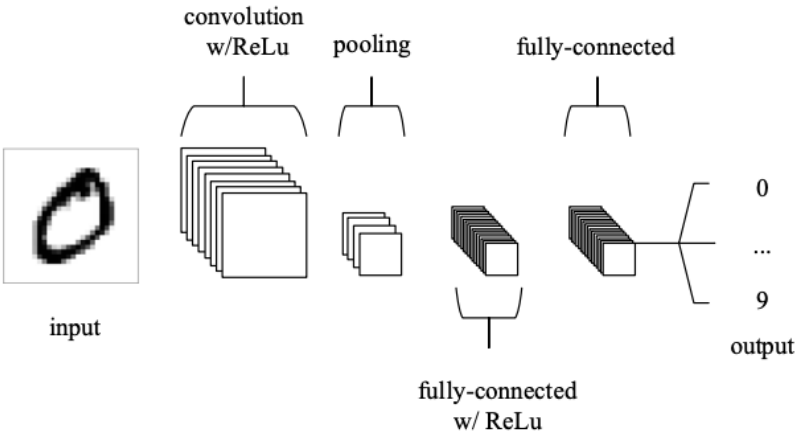


FIGURE 2.14: CNN 5 Layer Architecture Kriegeskorte and Golan [2019]

- **Deconvolutional Neural Networks:** DNN is known as a stacked neural network. It usually contains more than 2 layers i.e. one input layer, one output layer and more than one hidden layer.

2.8 Applications of Machine Learning

- **Predictive analytics and intelligent decision-making**: A major application field of machine learning is intelligent decision-making by data-driven predictive analytics. There are various industries which rely on machine learning-based predictions eg: e-commerce, telecommunications, banking and financial services, healthcare, sales and marketing, transportation, social networking etc. (Sarker [2021])

- **Cybersecurity and threat intelligence:** Cybersecurity is one of the most essential areas of Industry 4.0, which is typically the practice of protecting networks, systems, hardware, and data from digital attacks. (Sarker [2021])

- **Traffic prediction and transportation:** Transportation systems have become a crucial component of every country's economic development. Thus, an intelligent transportation system through predicting future traffic is important, which is an indispensable part of a smart city. (Sarker [2021])

- **Healthcare and COVID-19 pandemic:** Machine learning techniques played a crucial role during the pandemic in predicting diseases/ new variants. Especially ML algorithms have been exceptional in finding patterns like mortality rates, patient risk, etc., which helped doctors give better treatment. (Sarker [2021])

- **E-commerce and product recommendations:** Machine Learning techniques play a vital role in filtering and customizing the recommendations based on the customer's feed and interests. Using predictive modelling based on machine learning techniques, many online retailers, such as Amazon, can better manage inventory, prevent out-of-stock situations, and optimize logistics and warehousing. (Sarker [2021])

- **Image, speech and pattern recognition:** This is one of the most common practical use cases of machine learning. For example, to classify the X-ray as cancerous or not, face detection etc. Speech recognition is also very popular and typically uses sound and linguistic models, e.g., Google Assistant, Cortana, Siri, Alexa, etc. (Sarker [2021])

2.9 Conclusion

The author concludes that many machine-learning techniques have been implemented for detecting intrusions i.e. SVM, linear regression, random forest, and deep learning. Among all of them, models which are developed based on deep learning techniques have performed better in comparison with others. The lack of availability of real-time data was the biggest challenge. However, all the models discussed by the author were accurate, and limited datasets are a problem to be addressed. To generalise the models more data is needed which should be focussed on further study.

Chapter 3

Methodology

High Level Design

The author follows a sequence of techniques during the development of the Machine learning model.

- Data Collection
- Data Pre-processing
- Feature Selection
- Model Development
- Model Evaluation
- Model Optimization

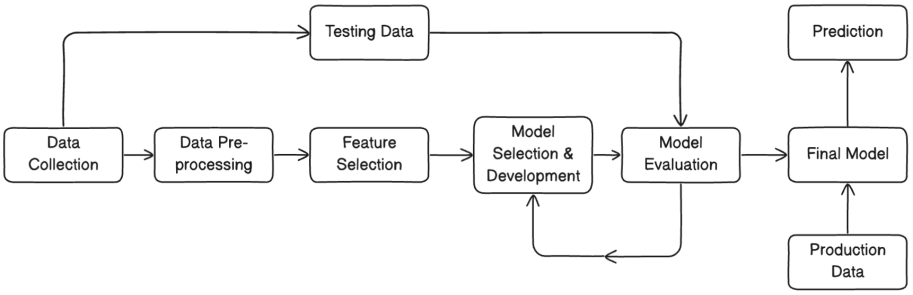


FIGURE 3.1: WorkFlow

3.1 Data Collection

This study mainly considers two datasets KDD-CUP 99 and NSL-KDD datasets. The author optionally considers the STIN dataset. KDD-CUP 99 data is simulated and prepared for 9 weeks in a competition by KDD during 1999. It has 39 attributes, 4898 samples belong to the training set and 311 to the test data set. The other data set is NSL-KDD, which comprises 125,973 samples. It contains the following labels: DoS, Prob, U2R, and R2L types of attacks. STIN dataset contains two types of satellite and nine terrestrial-type attacks.Ashraf et al. [2022]

Classes:	DoS	Prob	U2R	R2L
Sub Classes:	• Apache2 • Back • Land • Neptune • Mailbomb • Pod • Processtable • Smurf • Teardrop • Udpstorm • Worm	• Ipsweep • Mscan • Nmap • Portsweep • Saint • Satan	• Buffer_overflow • Loadmodule • Perl • Ps • Rootkit • Sqlattack • Xterm	• Ftp_write • Guess_password • Httptunnel • Imap • Multihop • Named • Phf • Sendmail • Snmpgetattack • Spy • Snmpguess • Warezclient • Warezmaster • Xlock • xsnoop
Total	11	6	7	15

FIGURE 3.2: NSL-KDD/ KDD-CUPP99 Description (Ashraf et al. [2022])

#	Name	Description
1	fl_dur	Flow duration
2	fw_pk	Total packets in the forward direction
3	l_fw_pkt	Total length of forward packets
4	l_bw_pkt	Total length of backward packets
5	pkt_len_min	Minimum length of a flow
6	pkt_len_max	Maximum length of a flow
7	pkt_len_std	Standard deviation length of a flow
8	fl_byt_s	Packet bytes transmitted per second
9	bw_iat_tot	Total time between of two backward packets
10	bw_iat_min	Minimum time between of two backward packets
11	fw_hdr_len	Number of bytes used in forward packet header
12	bw_pkt_s	Number of backward packets per second
13	syn_cnt	Number of packets with SYN
14	urg_cnt	Number of packets with URG
15	bw_win_byt	Number of backward bytes in the initial window

FIGURE 3.3: Stin Dataset features (Li et al. [2020])

3.2 Data pre-processing

Once the data is collected, the author performs this next step. Data preprocessing is considered to be the core stage in machine learning and data mining. Normalization, discretization and dimensionality reduction are well-known techniques in data preprocessing (Obaid et al. [2019]).

3.3 Feature Selection

Finding the subset of the right features is considered to be one of the crucial steps in building the machine learning model. Feature selection is a technique that effectively reduces the dimensionality of the feature space by eliminating irrelevant and redundant features without significantly affecting the quality of decision-making of the trained model (Theng and Bhoyar [2024]).

3.4 Model Development

Finding the right model in machine learning is essential to make accurate predictions. Once the right set of features is extracted, the author trains the model using several machine learning algorithms which include both supervised and unsupervised techniques.

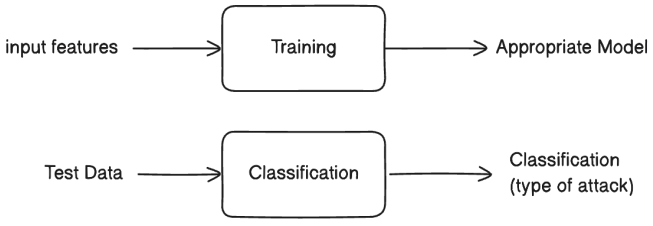


FIGURE 3.4: Model Development Phases

3.5 Model Optimisation

Hyperparameters tuning is a key step to find the optimal machine learning parameters. Determining the best hyper-parameters takes a good deal of time, especially when the

objective functions are costly to determine, or a large number of parameters are required to be tuned

Therefore, the author optimises the developed model by choosing optimal hyperparameters.

3.6 Model Validation

The obtained optimised is validated using the K-fold cross-validation technique to learn its generalizability where the model is trained and tested k times by splitting the data into k folds (equal size) (Maleki et al. [2020]).

Chapter 4

Requirements

Khan et al. [2015] states that, due to limited resources in terms of time, budget and other resources which are considered during development of software and to get customer satisfaction we need to prioritize software requirements. As all the requirements can't be programmed in a single increment, also we don't know which requirements are of higher priority regarding customer satisfaction and which are not.

Evaluation Criteria	Simple Ranking	MoScoW	100 dollar	AHP
Ratio Scale Information			Yes	Yes
High Confidence from User	Yes	Yes	Yes	
Consistent	Yes	Yes	Yes	Yes
Low difficulty	Yes	Yes	Yes	
Low effort	Yes	Yes	Yes	
Able to handle large number of alternatives		Yes		

FIGURE 4.1: Comparison of different techniques (Khan et al. [2015])

4.1 *MoSCoW*

The MoSCoW acronym was coined by D. Clegg and R. Baker, who in 1994 proposed the classification of requirements into Must Have, Should Have, Could Have and Won't

Have (Miranda [n.d.]). Moscow offers a clear distinction between critical and non-critical requirements and prevents scope creep by prioritizing essential features (reference).

MUST-*have* - These provide the Minimum Usable Subset (MUST) of requirements which the project guarantees to deliver (Kralik et al. [2019]).
SHOULD-*have* - Important but not vital (Kralik et al. [2019])
COULD-*have* - Wanted or desirable but less important (Kralik et al. [2019])
WON'T-*have* - These are requirements which the project team has agreed will not be delivered (Kralik et al. [2019])

4.2 *Functional Requirements*

ID	Details	Type	Priority
R1	The data set shall be pre-processed correspondingly to **procedure 3.2 in Chapter 3**	Functional	***Must Have***
R2	Advanced Feature selection techniques shall be performed correspondingly to **procedure 3.3** in **chapter 3**	Functional	***Should Have***
R3	The input shall contain a subset of carefully chosen features via feature selection techniques	Functional	***Must Have***
R4	The output shall be one of the DoS, Probe, U2R, R2L types (type of attack) as explained in **section 3.1 in chapter 3**	Functional	***Must Have***
R5	DNN, SVM, Random Forest, Linear Regression, Naïve Bayes algorithms shall be used to perform experiment correspondingly to **section 2.7 in chapter 2**	Functional	***Must Have***
R6	Machine Learning technique's which were not previously applied shall be used to analyse and compare with existing one's as mentioned in **section 2.6, chapter 2**	Functional	***Should Have***
R7	Performance shall be compared with existing models as specified in **section 2.6, chapter 2**	Functional	***Must Have***
R8	Model shall be optimised correspondingly to **procedure 3.5 in Chapter 3**	Functional	***Must Have***
R9	Maintainable and consistent code shall be written	Functional	***Could Have***
R10	Basic data visualisation shall be performed	Functional	***Could Have***
R11	The experiment shall not be performed with private/ confidential datasets	Functional	***Won't Have***

FIGURE 4.2: Functional Requirements

4.3 *Non Functional Requirements*

ID	Details	Type	Priority
R1	Python, Pandas, Matplotlib, Seaborn, Tensor Flow, Numpy, Jupiter Notebook, GIT shall be used to perform the experiment	Non Functional	***Must Have***
R2	Mac M1 8GB memory OS 14.4 shall be used to perform the experiment	Non Functional	***Could Have***
R3	Well organised documentation shall be written	Non Functional	***Should Have***
R4	Code shall be pushed to Gitlab/ Github on daily basis	Non Functional	***Could have***

FIGURE 4.3: Non Functional Requirements

Chapter 5

Evaluation

Evaluation of the Machine Learning Model is one of the most crucial aspects of the workflow. Evaluation is done once the training is done (using training data) using test data.

To estimate the performance of the Machine Learning Model, performance metrics are used. The most common performance metrics for analysis performance are accuracy, precision, recall, F1 score and mean squared error (MSE) etc. The confusion matrix is a 2 X 2 matrix with True Positive, True Negative, False Positive and False Negative values.

$$\mathbf{M} = \begin{pmatrix} \text{TP} & \text{FN} \\ \text{FP} & \text{TN} \end{pmatrix}$$

- **True positive (TP):** The true positive denotes the number of correctly classified positive samples. (Hicks et al. [2022])
- **True negative (TN):** The true negative denotes the number of correctly classified negative samples. (Hicks et al. [2022])
- **False positive (FP):** The false positive denotes the number of samples incorrectly classified as positive. (Hicks et al. [2022])
- **False negative (FN):** The false negative denotes the number of samples incorrectly classified as negative. (Hicks et al. [2022])

- **Accuracy:** The accuracy is the ratio between the correctly classified samples and the total number of samples in the evaluation dataset. This metric is among the most commonly used in applications of ML in medicine, but is also known for being misleading in the case of different class proportions since simply assigning all samples to the prevalent class is an easy way of achieving high accuracy (Hicks et al. [2022])

$$\text{ACC} = \frac{\#\text{ correctly classified samples}}{\#\text{ all samples}} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

- **Recall:** Te recall, also known as the sensitivity or True Positive Rate (TPR), denotes the rate of positive samples correctly classified and is calculated as the ratio between correctly classified positive samples and all samples assigned to the positive class. (Hicks et al. [2022])

$$\text{REC} = \frac{\#\text{ true positive samples}}{\#\text{ samples classified positive}} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

- **Specificty:** The specificity is the negative class version of the recall (sensitivity) and denotes the rate of negative samples correctly classified. (Hicks et al. [2022])

$$\text{SPEC} = \frac{\#\text{ true negative samples}}{\#\text{ samples classified negative}} = \frac{\text{TN}}{\text{TN} + \text{FP}}$$

- **Precision:** The precision denotes the proportion of the retrieved samples which are relevant and is calculated as the ratio between correctly classified samples and all samples assigned to that class. (Hicks et al. [2022])

$$\text{PREC} = \frac{\#\text{ samples correctly classified}}{\#\text{ samples assigned to class}} = \frac{\text{TC}}{\text{TC} + \text{FC}}$$

- **F1 score:** Te F1 score is the harmonic mean of precision and recall, meaning that it penalizes extreme values of either. This metric is not symmetric between the classes, i.e., it depends on which class is defined as positive and negative. (Hicks et al. [2022])

$$\text{F1} = 2 \times \frac{\textit{precision} \times \textit{recall}}{\textit{precision} + \textit{recall}} = \frac{2 \times \text{TP}}{2 \times \text{TP} + \text{FP} + \text{FN}}$$

- **Mean Squared Error:** This is one of the most widely used metrics for evaluation which is the average squared difference between the predicted and the actual target values within a dataset. ["Mean Square Error", www.encord.com]

Chapter 6

PROFESSIONAL, LEGAL, ETHICAL AND SOCIAL ISSUES

Professional Issues

The author will write and test the code while adhering to British Computing Society (BCS) code of conduct. Code will be written to a high standard and commented throughout for clarity. There will be adequate documentation presented. All third-party software, libraries, and other goods will only be utilized if their licenses let it. Any citations or outside data will be properly referenced.

Legal Issues

PD diagnosis requires the use of sensitive patient data, so the author will ensure proper data privacy and security measures are followed in accordance with GDPR UK.

Ethical Issues

In general, when working with the data obtained from real subjects, it is crucial to take ethical factors such as informed consent, data privacy, data security, fairness, and transparency into account (Lamba et al., 2022). In particular, the author will ensure that –

- the research is conducted with integrity and transparency.
- the data is managed carefully, respecting the rights of test subjects, supervisors, and Heriot Watt University as well as their right to privacy.
- the participants' data is kept confidential.
- the information is securely kept and guarded against unauthorized access or disclosure.
- Finally, the author will need to ensure that the data gathering process is handled responsibly and in accordance with GDPR UK.

Social Issues

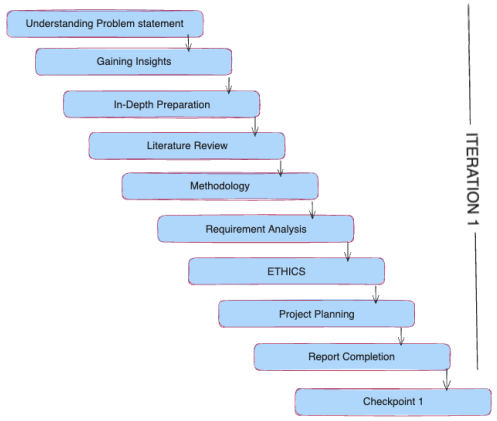
As there is no direct communication with the satellite organisation so the project does not come across any social issues.

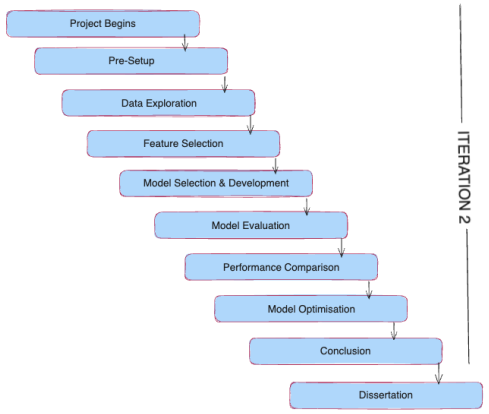
Chapter 7

Project Planning

7.1 Gantt Chart

A well-designed plan with a timeline to accomplish the result of the project. Although, minor modifications can be made based on the circumstances.





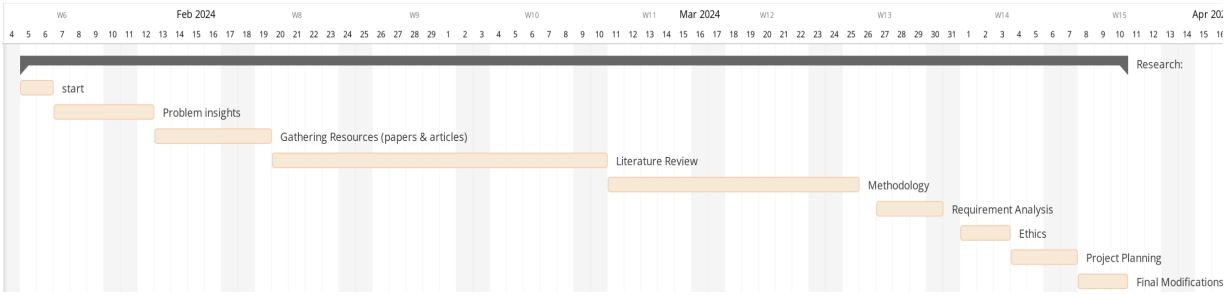


FIGURE 7.1: Research

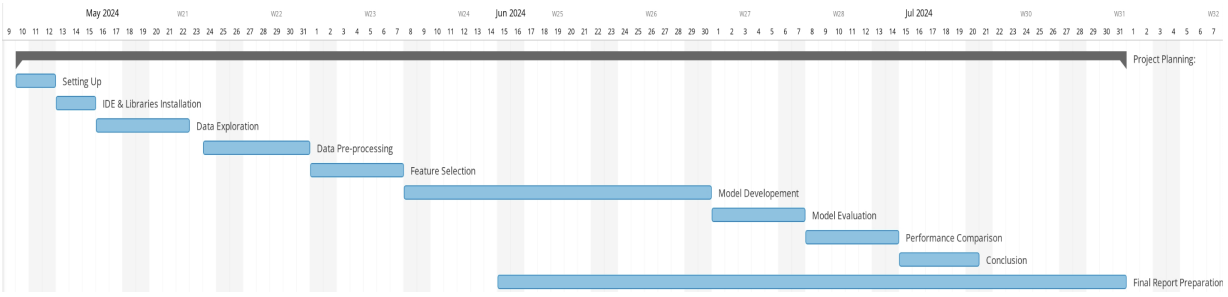


FIGURE 7.2: Project Planning

7.2 Risk Management

Dinu [2015] defines risk management as anything that threatens or limits the goals, objectives or deliverables of a project is a project risk. Identifying the potential risks is essential. On the other hand Yim et al. [2015] defines project risk management as a process for systematically identifying, evaluating, and mitigating risks to improve the likelihood of project success.

Risk	Likelihood of occurrence	Impact	Avoidance Strategy
Lack of proper data	***Low***	***High***	Find the other ones
Loosing the data	***Low***	***High***	Backing up the data on weekly basis
Feedback delays	***Low***	***Medium***	Setting up online meets with supervisor permission.
Low accuracy	***Medium***	***High***	Performing hyper parameter tuning and selection of better subset of features.
Challenges while programming	***Medium***	***Medium***	Asking supervisor for assistance
Loosing the code	***Low***	***High***	Pushing the code to version control systems like Gitlab/ Github frequently
Health issues	***Low***	***Medium***	Working remotely

Appendix A

Appendix Title Here

Write your Appendix content here.

Bibliography

Ahamed, K. I. and Akthar, D. S. [2016], 'A study on neural network architectures', *Internation Institute Of Science, Technology and Education* **29**.

Ali, J., Khan, R., Ahmad, N. and Maqsood, I. [2012], 'Random forests and decision trees', *International Journal of Computer Science Issues (IJCSI)* **9**(5), 272.

Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F. and Rasool, N. [2022], 'A deep learning-based smart framework for cyber-physical and satellite system security threats detection', *Electronics* **11**(4), 667.

Devan, P. and Khare, N. [2020], 'An efficient xgboost–dnn-based classification model for network intrusion detection system', *Neural Computing and Applications* **32**(16), 12499–12514.

Dinu, A.-M. [2015], 'The importance of risk management in projects', *Calitatea* **16**(S3), 162.

Dubey, S. R., Singh, S. K. and Chaudhuri, B. B. [2022], 'Activation functions in deep learning: A comprehensive survey and benchmark', *Neurocomputing* **503**, 92–108.

Farnaaz, N. and Jabbar, M. [2016], 'Random forest modeling for network intrusion detection system', *Procedia Computer Science* **89**, 213–217.

Fernandez Jr, P. L., Co, J. M. et al. [2017], 'Time-series link prediction using support vector machines'.

Ghosh, P. and Mitra, R. [2015], Proposed ga-bfss and logistic regression based intrusion detection system, *in* 'Proceedings of the 2015 third international conference on computer, communication, control and information technology (C3IT)', IEEE, pp. 1–6.

Gurung, S., Ghose, M. K. and Subedi, A. [2019], 'Deep learning approach on network intrusion detection system using nsl-kdd dataset', *International Journal of Computer Network and Information Security* **11**(3), 8–14.

Hicks, S. A., Strümke, I., Thambawita, V., Hammou, M., Riegler, M. A., Halvorsen, P. and Parasa, S. [2022], 'On evaluation metrics for medical applications of artificial intelligence', *Scientific reports* **12**(1), 5979.

Jha, J. and Ragha, L. [2013], 'Intrusion detection system using support vector machine', *International Journal of Applied Information Systems (IJAIS)* **3**, 25–30.

Kaelbling, L. P., Littman, M. L. and Moore, A. W. [1996], 'Reinforcement learning: A survey', *Journal of artificial intelligence research* **4**, 237–285.

Khan, J. A., Rehman, I. U., Khan, Y. H., Khan, I. J. and Rashid, S. [2015], 'Comparison of requirement prioritization techniques to find best prioritization technique', *International Journal of Modern Education and Computer Science* **7**(11), 53.

Kralik, L., Jasek, R., Zacek, P. and Senkerik, R. [2019], 'Agile approach in multi-criterial decision making', *International Journal of Manufacturing Technology and Management* **33**(3-4), 256–267.

Kriegeskorte, N. and Golan, T. [2019], 'Neural network models and deep learning', *Current Biology* **29**(7), R231–R236.

Kumari, K. and Yadav, S. [2018], 'Linear regression analysis study', *Journal of the practice of Cardiovascular Sciences* **4**(1), 33–36.

Li, K., Zhou, H., Tu, Z., Wang, W. and Zhang, H. [2020], 'Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning', *IEEE Access* **8**, 214852–214865.

Maleki, F., Muthukrishnan, N., Ovens, K., Reinhold, C. and Forghani, R. [2020], 'Machine learning algorithm validation: from essentials to advanced applications and implications for regulatory certification and deployment', *Neuroimaging Clinics* **30**(4), 433–445.

Miranda, E. [n.d.], 'Moscow rules: A quantitative exposé (working paper jan 2nd, 2022)'.

Nagesh Singh Chauhan, N. B. A. E. Y. N. t. K. W. D. [n.d.], 'Url https://www.kdnuggets.com/2020/06/naive-bayes-algorithm-everything.html', *KDnuggets* .

Network Layer Services- Packetizing, Routing and Forwarding [n.d.], https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/. Accessed: 16 April 2024.

Obaid, H. S., Dheyab, S. A. and Sabry, S. S. [2019], The impact of data pre-processing techniques and dimensionality reduction on the accuracy of machine learning, *in* '2019 9th annual information technology, electromechanical engineering and microelectronics conference (iemecon)', IEEE, pp. 279–283.

Panda, M. and Patra, M. R. [2007], 'Network intrusion detection using naive bayes', *International journal of computer science and network security* **7**(12), 258–263.

Roddy, D. [2006], *Satellite Communications*, McGraw-Hill.

Sarker, I. H. [2021], 'Machine learning: Algorithms, real-world applications and research directions', *SN computer science* **2**(3), 160.

Satellite Communication - Quick Guide [n.d.], https://www.tutorialspoint.com/satellite_communication/satellite_communication_quick_guide.htm. Accessed: 16 April 2024.

Support Vector Machine Algorithm [n.d.], https://www.javatpoint.com/machine-learning-support-vector-machine-algorithm. Accessed: 16 April 2024.

Theng, D. and Bhoyar, K. K. [2024], 'Feature selection techniques for machine learning: a survey of more than two decades of research', *Knowledge and Information Systems* **66**(3), 1575–1637.

Understanding Random Forest [n.d.], https://towardsdatascience.com/understanding-random-forest-58381e0602d2. Accessed: 16 April 2024.

Veropoulos, K., Cristianini, N. and Campbell, C. [1999], 'The application of support vector machines to medical decision support: a case study', *Advanced Course in Artificial Intelligence* pp. 1–6.

Yim, R., Castaneda, J., Doolen, T., Tumer, I. and Malak, R. [2015], 'A study of the impact of project classification on project risk indicators', *International Journal of Project Management* **33**(4), 863–876.

Yin, C., Zhu, Y., Fei, J. and He, X. [2017], 'A deep learning approach for intrusion detection using recurrent neural networks', *Ieee Access* **5**, 21954–21961.

Zhu, J. and Wang, C. [2019], Satellite networking intrusion detection system design based on deep learning method, *in* 'Communications, Signal Processing, and Systems: Proceedings of the 2017 International Conference on Communications, Signal Processing, and Systems', Springer, pp. 2295–2304.