

**Tribhuvan University**

Institute of Engineering

Purwanchal Campus

[Subject Code: **CT** **654**]

A PROPOSAL ON

“**NETWORK INTRUSION DETECTION USING**

**MACHINE LEARNING**”

Submitted by:

Abdullah Waqar (BCT/074/002)

Sandesh Chudal (BCT/074/035)

Sarthak Parajuli (BCT/074/039)   
Srijan Chaudhary (BCT/074/043)

Submitted to:

**Department of Computer and Electronics Engineering**

**Mangsir-2078**

Table of Contents

[1 INTRODUCTION 3](#_Toc134779188)

[1.1 Background 3](#_Toc134779189)

[1.2 Statement of Problem 3](#_Toc134779190)

[1.3 Objectives 3](#_Toc134779191)

[1.4 Applications 3](#_Toc134779192)

[1.5 Project Features: 4](#_Toc134779193)

[1.6 Feasibility 4](#_Toc134779194)

[1.6.1 Technical feasibility 4](#_Toc134779195)

[1.6.2 Economic feasibility 4](#_Toc134779196)

[1.6.3 Social feasibility 4](#_Toc134779197)

[1.6.4 Time feasibility 4](#_Toc134779198)

[1.7 System Requirement 4](#_Toc134779199)

[2 LITERATURE REVIEW 5](#_Toc134779200)

[2.1 Introduction 5](#_Toc134779201)

[2.2 Existing Researches 5](#_Toc134779202)

[2.3 Recent Techniques for Intrusion Detection 5](#_Toc134779203)

[3 METHODOLOGY 6](#_Toc134779204)

[3.1 Block Diagram 7](#_Toc134779205)

[4 5. REFERENCES 9](#_Toc134779206)

# INTRODUCTION

With the rapid advancement and growing importance of technology in today's interconnected world, security is one of the most pressing concerns. Intrusion detection systems (IDS) are one of the best systems for detecting various types of attacks among many options. We are proposing to develop a Network Intrusion detection system (NIDS) technique using Machine Learning (ML). We've highlighted the latest NIDS techniques that use machine learning techniques and approaches, as well as the common attacks that they can detect and their issues.

## Background

At the moment, the usage of digital technology in all areas, particularly business, is fast increasing. Along with the good influence and expansion of the internet for worldwide communication, its evil side could be overlooked. As the number of networked devices increases, so do the number of attacks; networks are constantly vulnerable to malicious attackers. Security is among the most important aspects of any organization. Based on recent researches, we have pointed out various method of intruder detection using machine learning techniques and approached. The purpose of our project is to identify the network intrusion and its prevention.

## Statement of Problem

Network Intrusion Detection system will be designed to overcome the network attacks by identifying the threat, attempting to block it and informing system administrator about breaches. It will be vital for system administrator to monitor the abnormalities on the network which is very tedious task, NIDS will be using effective machine learning techniques to detect anomalies on network, identify suspicious tasks and take effective action to overcome it.

## Objectives

The objectives of Network Intrusion Detection System are:

1. To monitor network anonymously

2. To use machine learning models to analyse the monitored packets and identify any intrusion attempts

3. To log all packets and notify the system administrator when the intrusion occurs.

## Applications

It can be implemented on home network, organisational network, and servers in order to effectively identify network intrusion and mitigate any damages.

## Project Features:

Our project will feature the following functionalities:

1. Easy to use GUI
2. Use of effective machine learning algorithms to detect intrusion
3. Alert notification in case of intrusion

## Feasibility

### Technical feasibility

Our project would be technically feasible as we are proposing to use python. Our project will would work explicitly on a single device attached on a network.

### Economic feasibility

Our project is economically feasible since it doesn’t necessarily require any extra device to work since it can be implemented on any computer on a home/enterprise network or directly in a server computer.

### Social feasibility

Due to the growing demand of Cyber security, our project with some more enhancement can sustain itself in cybersecurity field.

### Time feasibility

Our system is supposed to be completed in time i.e., 5 months from the start of the day of the project (acceptance of project proposal).

## System Requirement

The minimum system requirements of the project are:

1. Modern PC/laptop/server
2. Network Interface Card capable of packet capturing.
3. Active internet connection

The minimum Operating System and Browser Requirements are:

1. OS:
2. For Windows: Microsoft Windows XP or higher
3. Kali Linux – Latest release
4. Ubuntu/Ubuntu-server latest release
5. Hardware requirements:
6. NIC capable of packet capturing

# LITERATURE REVIEW

## Introduction

Literature review is searching similar system and identifying the difference between researcher’s projects with existing systems. This helps to get a deep idea of the project. It provides the combination of theoretical, methodological and current knowledge of findings according to subject. There is need to gather the information according to the project. This chapter describes how this app is different from other similar system.

## Existing Researches

With the advancement in technology, cybersecurity is an integral part of our daily online activities. The increased ratio in attacks is also becoming more powerful and difficult to mitigate. Security researchers and hackers are always in a war to win. The mitigation of sophisticated attacks requires high-end hardware or a well-developed software-based system. Existing tools for detection and prevention requires constant maintenance to counter recent attacks. Maintaining mentioned systems also include updating and checking logs on daily basis, which is quite hectic for security experts. Since the internet world is advanced with technology, the attacker’s strategies also change which ultimately makes the traditional tools vulnerable. Such liabilities allow intruders to bypass and evade security systems and allowing the intruders to perform malicious activities2, 3. R. Thornton4 have proposed a model that uses Machine Learning (ML) and Deep learning (DL) approaches to detect unknown attacks. Authors discussed various ML & DL techniques that comes under supervised and unsupervised learning techniques. In the papers3, 5, 6, authors have proposed a model in which different data sources such as logs, packets flow, and sessions are collected and presented to ML algorithms. Although, to achieve high accuracy a proper standardized data-set must be available. As per the different reviewed papers for the study, 2017 was the year in which maximum number of publications in journals and conferences were on DL and ANN. This trend is still ongoing with increasing number of publications related to ML or DL techniques. The study shows that the most broadly used methods for NIDS are DL and ANN. While the most common dataset for NIDS evaluations are KDD199 and NSL KDD respectively.

## Recent Techniques for Intrusion Detection

The IDS by function can be divided into types; signature-based IDS and the anomaly-based IDS. The signature-based IDS requires the **signature** patterns available in its **signature database** to be compared with the packet signature received by the sensor for the intrusion detection. For this type of system it needs to be up to date with due respect to time, and also its only effective for the known attacks. However, on the other side, the **anomaly** detection-based Intrusion Detection is effective for the detection of **unknown** attacks or **intrusions**.

It relies on the **behavior** of the system and **compares** the system’s **normal** behavior with the deviated behavior if attacked by any threat actor. The set of features are used to identify the network connections such as; service, protocol, number of login attempts, packets per flow, bytes per flow, source address, destination address, source port, destination port, and others. The features values are recorded by the model and any deviation in recorded values will be marked as anomalous by the anomaly detection engine. Techniques in anomaly detection can be categorized into three types; Machine Learning, Statistical Techniques and Finite State Machine.

# METHODOLOGY

Intrusion detection systems (IDS) are security systems that are used to detect security threats to computer systems and computer networks. These systems are configured to detect and respond to security threats automatically there by reducing the risk to monitored computers and networks. Intrusion detection systems use different methodologies such as signature based, anomaly based and a hybrid system that combines some or all of the other systems to detect and respond to security threats.

For our project development the following aspects are used:

**Packet Analyser**

A packet analyser or packet sniffer is a computer program or computer hardware such as a packet capture appliance that can intercept and log traffic that passes over a computer network or part of a network. Packet capture is the process of intercepting and logging traffic.

**Multiple levels of security –**

Intrusion prevention system- firewalls, content filtering, antivirus, malware, filtering router policies, honeypots are used. Fails to impede such attacks and they become common clause. Intrusion still happens regardless of how many precautions are taken. Therefore it is desirable to be Detected and dealt properly

**IDS - Intrusion Detection System**

Device or software that monitors network activities for malicious users and produces report to managing station. Main role- prepare computer system/network to deal with network attacks to have secure data communication in the network``

**Model used for the project are SVM and/or Random Forest**

**SVM**

Support Vector Machines (SVM) are the classifiers which were originally designed for binary classification. The classification applications can solve multi-class problems. Decision-tree-based support vector machine which combines support vector machines and decision tree can be an effective way for solving multi-class problems. This method can decrease the training and testing time, increasing the efficiency of the system. The different ways to construct the binary trees divides the data set into two subsets from root to the leaf until every subset consists of only one class .The construction order of binary tree has great influence on the classification performance. In this paper we are studying an algorithm, Tree structured multiclass SVM, which has been used for classifying data. This paper proposes the decision tree based algorithm to construct multiclass intrusion detection system.

**3.2 Random Forest (RF)**

Random forest (RF) is an ensemble classifier used to improve the accuracy. Random forest consists of many decision trees. Random forest has low classification error compared to other traditional classification algorithms. Number of trees, minimum node size and number of features used for splitting each node. Advantages of RF are listed below.

1) Generated forests can be saved for future reference.

2) Random forest overcomes the problem over fitting.

3) In RF accuracy and variable importance is automatically generated. When constructing individual trees in random forest, randomization is applied to select the best node to split on. This value is equal to √A, where A is no. of attributes in the data set. However, RF will generate many noisy trees, which affect accuracy and wrong decision for new sample

## Block Diagram

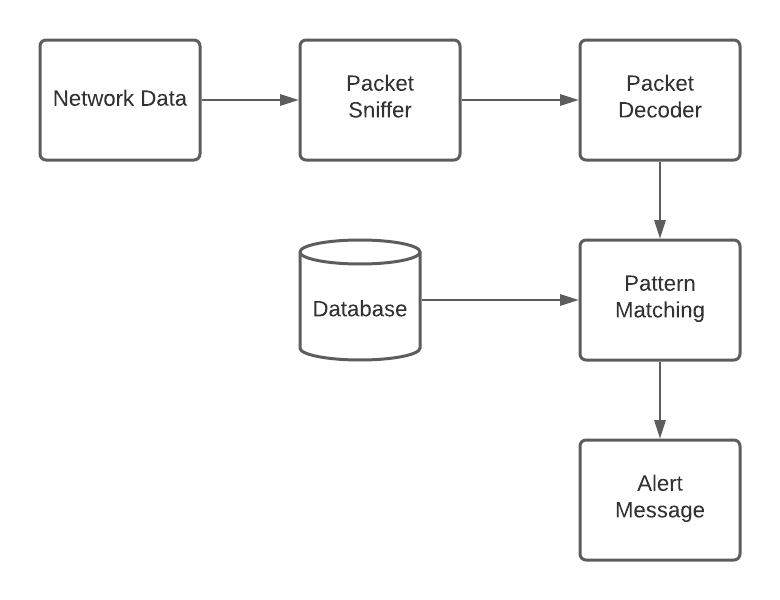


  Figure 3.1 Block diagram of Intrusion Detection System

**3.2 Use Case Diagram**

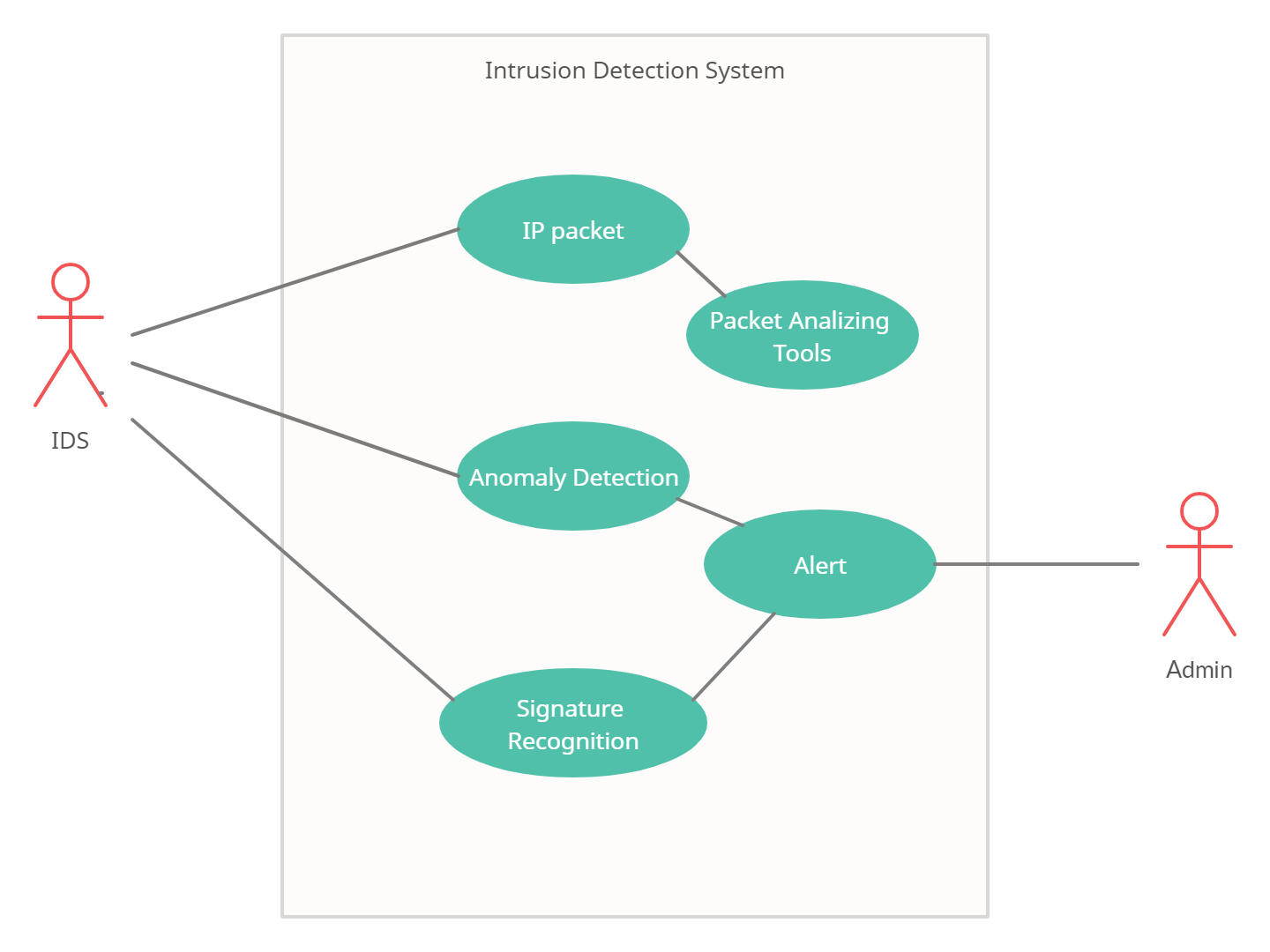


Figure 3.2 Use Case Diagram of Intrusion Detection System

# 5. REFERENCES

1. <https://www.sciencedirect.com/topics/computer-science/network-based-intrusion-detection-system>
2. <https://www.gispp.org/2021/01/25/network-intrusion-detection-techniques-using-machine-learning/>
3. B. Mukherjee et al., “Network intrusion detection”, IEEE Network, vol.8, no.3,pp.26–41,1994.
4. <https://www.barracuda.com/glossary/intrusion-detection-system>
5. <https://www.upguard.com/blog/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise>