NETWORK INTRUSION DETECTION SYSTEM

A PROJECT REPORT – PHASE I

Submitted by

U.ROHITH(9920004138)

K.PARAMESH(9920004808)

U.ANIL KUMAR(9920004263)

P.LAKSHMI CHAITANYA(9920004261)

In partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

Computer Science and Engineering

SCHOOL OF COMPUTING DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(Deemed to be University)

Academic Year 2023-2024

Kalasalingam Academy of Research and Education

KRISHNANKOIL 626 126

DECLARATION BY THE STUDENT

I/We hereby declare that this project **"NETWORK INTRUSION DETECTION SYSTEM"** is my/our genuine work and no part of it has been reproduced from any other works.

U.Rohith
(9920004138)

U.Anil Kumar
(9920004263)

K.Paramesh
(9920004808)

P.Lakshmi Chaitanya
(9920004261)

Date:

KALASALINGAM UNIVERSITY

(Kalasalingam Academy of Research and Education)

KRISHNANKOIL 626 126

BONAFIDE CERTIFICATE

Certified that this project report **"NETWORK INTRUSION DETECTION SYSTEM"** is the bonafide work of "**U.Rohith(9920004138) ,k.Paramesh(9920004808) ,U.Anil Kumar(9920004263),P.Lakshmi Chaitanya(9920004261)"** who carried out the project work under my supervision.

HEAD OF THE DEPARTMENT

Dr.N.Suresh Kumar
Professor & Head Of The Department
Computer Science and Engineering
Kalasalingam Academy of Research and Education
Krishnankoil 626126

SUPERVISOR

Dr.R.Sumathi
Assistant Professor
Computer Science and Engineering
Kalasalingam Academy of Research and Education
Krishnankoil 626126

Submitted for the Project Viva-voce examination held on

Internal Examiner **External Examiner**

ACKNOWLEDGEMENT

First and foremost, I wish to thank the **Almighty God** for his grace and benediction to complete this Project work successfully. I would like to convey my special thanks from the bottom of my heart to my dear **Parents** and affectionate **Family members** for their honest support for the completion of this Project work.

I express deep sense of gratitude to "Kalvivallal" Thiru. **T. Kalasalingam** B.com., Founder Chairman, "Ilayavallal" **Dr. K. Sridharan,** Ph.D., Chancellor, **Dr. S. Shasi Anand**, Ph.D., Vice President(Academic), **Mr. S. Arjun Kalasalingam** M.S., Vice President(Administration) , **Dr. S. Narayanan**, Vice-Chancellor, **Dr. V. Vasudevan,** Ph.D., Registrar , **Dr. P. Deepalakshmi,** Ph.D., Dean (School of Computing) and **Dr.N.Suresh Kumar** Head, Department of CSE, Kalasalingam Academy of Research and Education for granting the permission and providing necessary facilities to carry out Project work.

I would like to express my special appreciation and profound thanks to my enthusiastic Project Supervisor **Dr.R.Sumathi**, Assistant Professor/CSE of Kalasalingam Academy of Research and Education [KARE] for his inspiring guidance, constant encouragement with my work during all stages. I am extremely glad that I had a chance to do my Project under my Guide, who truly practices and appreciates deep thinking. I will be forever indebted to my Guide for all the time he has spent with me in discussions. And during the most difficult times when writing this report, he gave me the moral support and the freedom I needed to move on.

Besides my Project guide, I would like to thank the rest of Class committee members and all faculty members and Non-Teaching staff for their insightful comments and encouragement. Finally, but by no means least, thanks go to all my school and college teachers, well wishers, friends for almost unbelievable support.

ABSTRACT

Network intrusion discovery technology plays an important part in maintaining network security, the main work is to continuously descry the current network status, through the discovery of abnormal geste in the network state, timely warning to warn network directors. The punctuality and delicacy of the intrusion discovery system(IDS) is critical to the vacuity and trustability of the current network. In response to the problems of high false alarm rate, low discovery effectiveness and limited functions generally set up in IDS. With the growing reliance on networked systems and the adding complication of cyber pitfalls, the need for robust network intrusion discovery systems(NIDS) has come consummate. We're going to apply a Network Intrusion Discovery System that leverages both traditional machine learning and deep learning algorithms to enhance network security.collecting and preprocessing network traffic data, which serves as the foundation for training and testing the intrusion detection models. The objective of a project on a Network Intrusion Detection System (NIDS) using machine learning algorithms such as Decision Tree Classifier(DTC),K Nearest Neighbours(KNN),Linear Regression(LR),MultiNomialNavieBayes(MNB),Random Forest Classifier(RFC),Support Vector Classifier(SVC) and deep learning algorithms such as convulutional neural networks(CNN),recurrent neural networks(RNN) and Feed forward neural networks(FNN)is to develop a system that can effectively detect the attack type Use machine learning and deep learning algorithms to identify abnormal patterns and behaviors in network traffic dataset.Identification of Intrusions: Detect and classify different types of network intrusions, such as malware attacks, 'apache2', 'back', 'buffer_overflow', 'ftp_write' and other malicious attacks and compare the accuracies of ml and dl algorithms.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DTC	Decision Tree Classifier
KNN	K Nearest Neighbours
LR	Linear Regression
MNB	MultiNomial NavieBayes
RFC	Random Forest Classifier
SVC	Support Vector Classifier
CNN	Convulutional Neural Networks
RNN	Recurrent Neural Networks
FNN	Feed Forward Neural Networks
AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning

CHAPTER I: INTRODUCTION

1.1 Overview

A Network Intrusion Detection System (NIDS) is a pivotal component in safeguarding digital networks. Its primary function is to continuously monitor and analyze network traffic for signs of malicious or unauthorized activities. By scrutinizing incoming and outgoing packets, a NIDS aims to detect various anomalies or patterns that could indicate potential security threats or breaches.

NIDS can be categorized into two main types:

Signature-Based Detection: This method involves comparing network traffic against pre-defined patterns or signatures of known attacks. When a match is found, it triggers an alert or takes predefined action.

Anomaly-Based Detection: Anomaly-based systems establish a baseline of normal network behavior and flag any deviations from this standard as potential threats. These anomalies could be unusual traffic patterns, unexpected protocols, or unusual packet sizes.

The core goal of a NIDS is to swiftly identify and respond to suspicious activities, reducing the risk of data breaches, unauthorized access, or other cyber threats. The system's effectiveness lies in its ability to accurately differentiate between normal and abnormal network behavior while minimizing false positives and negatives.

Continual advancements in machine learning, deep learning, and data analysis techniques have enabled more sophisticated NIDS models capable of adapting to evolving cyber threats and enhancing network security.

CHAPTER II : LITERATURE SURVEY

Several studies have significantly contributed to the field of network intrusion detection. One survey offers an extensive overview of intrusion detection techniques, emphasizing their respective strengths and weaknesses. Another study focuses on anomaly-based detection using autoencoders, showcasing their effectiveness in identifying network anomalies. Furthermore, deep learning methods, including CNNs and LSTMs, have been extensively reviewed for their potential in handling complex attacks. Comparative studies have evaluated the accuracy and computational aspects of various machine learning algorithms for intrusion detection. Additionally, specific network architectures like LSTM networks and stacked autoencoders have been explored for capturing temporal patterns and feature extraction. Lastly, a survey outlines the evolutionary shift towards machine learning and deep learning methods in intrusion detection systems.

In recent advancements within Network Intrusion Detection Systems (NIDSs), a multi-stage optimized framework has been proposed to reduce computational needs while maintaining tracking efficacy. Referenced as [6], this ML-based structure significantly diminishes training sample dimensions (by 74%) and feature set sizes (by 50%) using datasets like CICIDS 2017 and UNSW-NB 2015.

Another avenue, highlighted in [7], emphasizes the limitations of existing datasets in adapting to evolving threats. This study underscores the absence of genuine network threats in recent datasets, hindering the effectiveness of machine learning-based IDS techniques. The paper advocates for a categorization and dataset analysis approach to enhance current research landscapes and combat sophisticated threats, acknowledging the necessity for dataset improvements to align with modern attack patterns and bolster system defenses.