Anomalies in Network detection

Minor Project-II

(ENSI252)

Submitted in partial fulfilment of the requirement of the degree of

BACHELOR OF TECHNOLOGY

to

K.R Mangalam University

by

Kashish Negi (2301730287)

Under the supervision of

Supervisor Name
<Ms.Megha >
Faculty
K.R Mangalam University

Supervisor Name
<Mr.Ashish Goguvan>
Data Scientist
Deloitte

Department of Computer Science and Engineering
School of Engineering and Technology
K.R Mangalam University, Gurugram- 122001, India

April 2

CERTIFICATE

This is to certify that the Project Synopsis entitled, "**anomalies in network intusion** " submitted by "**Kashish Negi(2301730287)**" to **K.R Mangalam University, Gurugram, India,** is a record of bonafide project work carried out by them under my supervision and guidance and is worthy of consideration for the partial fulfilment of the degree of **Bachelor of Technology** in **Computer Science and Engineering** of the University.

Type of Project (Tick One Option)

√

Industry/Research/University Problem

Megha

<Signature of Internal supervisor>
<Ms. Megha , Faculty at K.R Mangalam University>

Signature of Project Coordinator

Date: 30th April 2025

INDEX

ABSTRACT

In today's digital world, network security has become a critical concern as cyber-attacks and intrusion attempts continue to rise. Traditional security systems often fail to detect sophisticated threats in real-time, leaving organizations vulnerable. Many existing solutions either lack intelligent threat detection or are too complex and costly for broader deployment. This gap highlights the need for a lightweight, smart, and user-friendly Network Intrusion Detection System (NIDS) that can quickly identify and respond to malicious activities.

In this project, we developed a Machine Learning-based NIDS designed to detect network intrusions with high accuracy. Leveraging a Random Forest Classifier model, Flask for backend integration, and HTML, CSS, and JavaScript for the frontend, our system enables real-time detection, alert generation, and easy visualization of network threats. The platform offers an intuitive dashboard, graphical analytics, live alerts, and customizable settings, ensuring a streamlined and accessible security monitoring experience.

With the increasing demand for efficient cybersecurity solutions, this NIDS project serves as a practical, deployable system for monitoring network health and identifying potential attacks. By combining machine learning techniques with an interactive web interface, it enhances security awareness and supports faster decision-making. As cybersecurity threats continue to evolve, intelligent, real-time detection systems like this NIDS project are vital in building resilient digital infrastructures.

KEYWORDS: Network Security, Intrusion Detection, Machine Learning, Random Forest, Flask, Real-Time Monitoring, Cybersecurity

INTRODUCTION

The rapid shift to digital learning has highlighted significant challenges in virtual education. Traditional classroom-based learning methods are increasingly being replaced by online platforms, yet most existing solutions fall short of providing an engaging, interactive, and structured environment for students and teachers alike. The lack of real-time interaction, inefficient communication tools, limited collaborative features, and rising security concerns have made it difficult to replicate the rich, dynamic experience of a physical classroom in a virtual setting.

While platforms like Zoom, Microsoft Teams, and Google Meet have offered basic solutions for video communication, they are primarily designed for general meetings and corporate environments. They often lack features specifically tailored for education, such as structured classroom management, interactive participation tools, easy resource sharing, and session monitoring. This gap has led to reduced engagement levels among students, challenges in maintaining discipline, and difficulties for teachers in delivering effective lessons online..

To bridge this gap, we introduce **ClassBridge**, a comprehensive real-time virtual learning platform built specifically to address the unique needs of online education. **ClassBridge** leverages modern web technologies such as **WebRTC**, **Socket.io**, and **Express.js** to facilitate seamless, low-latency communication between students and teachers. The platform offers a secure, engaging, and structured virtual classroom experience with features like:

- **Live video and audio sessions**
- **Real-time chat and instant messaging**
- **Screen sharing for better explanation of concepts**
- **Session tracking and attendance monitoring**
- **Secure authentication and encrypted communication**

By integrating these functionalities into a single platform, **ClassBridge** aims to revolutionize the way online education is conducted. Whether used in schools, universities, or professional training programs, **ClassBridge** is designed to make virtual learning more effective, secure, and truly student-centered.

MOTIVATION

In recent years, the digital world has faced a surge in cyber attacks, causing severe financial, reputational, and operational damages to individuals and organizations. Despite the deployment of security systems, networks remain highly vulnerable due to sophisticated intrusion techniques and zero-day attacks.

Existing systems often rely on static rules and signatures, which struggle to identify new or modified threats. Moreover, manual analysis of network traffic is time-consuming and prone to human error, making it inadequate for large-scale environments.

This motivates the need for an intelligent, real-time monitoring system that can dynamically adapt to emerging threats. Our project proposes a **machine learning-based NIDS** that bridges this gap, offering proactive intrusion detection and helping to secure network infrastructures more effectively and efficiently.

LITERATURE REVIEW

1. **Using Machine Learning for Intrusion Detection**

   Author(s): Sommer, R., & Paxson, V.

   Summary: This paper discusses how machine learning techniques, such as supervised and unsupervised learning, can enhance intrusion detection by identifying complex attack patterns that static signature-based systems often miss.
   Relevance to NIDS: Our project uses machine learning algorithms to classify network traffic as normal or malicious, improving detection accuracy over traditional rule-based systems.

---

2. **Challenges in Network Intrusion Detection Systems**

   Author(s): Bridges, S. M., & Vaughn, R. B.

   Summary: The study highlights challenges like high false-positive rates, scalability issues, and the evolving nature of threats that affect the efficiency of NIDS.
   Relevance to NIDS: Our system addresses these challenges by optimizing feature selection and model training to reduce false positives and enhance detection rates.

---

3. **Deep Learning Approaches for Network Traffic Analysis**

   Author(s): Yin, C., et al.

   Summary: This paper explores the application of deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), in detecting network anomalies and intrusions.
   Relevance to NIDS: It provides insights into advanced techniques that we can incorporate into our system for future upgrades.

---

4. **Security Evaluation of Machine Learning-Based NIDS**

   Author(s): Cybersecurity Research Journal (2022)

   Summary: Focuses on the vulnerabilities of ML-based NIDS, including adversarial attacks and data poisoning, emphasizing the need for robust model training and secure data pipelines.

Relevance to NIDS: Reinforces the importance of using secured and clean datasets, like CICIDS, for training and testing our models.

5. **The Importance of Feature Engineering in NIDS**

   Author(s): Information Security Journal (2023)

   Summary: This study stresses the importance of selecting relevant features from network traffic to improve model performance and detection accuracy.

   Relevance to NIDS: In our project, feature selection plays a critical role in optimizing machine learning models for better intrusion detection.

Gap Analysis

- Despite the existence of traditional intrusion detection systems, many suffer from limitations like high false alarm rates, delayed detection, and poor adaptability to unknown threats. Most signature-based IDS systems fail to detect novel attacks and are ineffective in high-speed network environments.
- Our project addresses these gaps by building an **ML-based NIDS** that can learn from historical traffic patterns and accurately detect anomalies in real time. By integrating efficient machine learning models, robust feature engineering, and secure data handling, our solution overcomes the limitations of conventional systems and provides an adaptive, scalable, and accurate network protection system.
- Despite the availability of various video conferencing tools, current platforms have several limitations when it comes to supporting virtual education:

Existing Tools (Zoom, Google Meet, MS Teams)	**Gaps in Functionality for Education**
Designed primarily for corporate meetings	Lack of education-specific features like attendance tracking and session scheduling
Limited real-time interaction beyond video/audio	No tools for live participation tracking, quizzes, or classroom engagement
Complex interfaces for teachers and students	Poor user experience for non-technical users in academic settings
No built-in analytics for academic monitoring	No insights into student engagement or learning progress
Security concerns (Zoombombing, unauthorized access)	Lack of robust authentication and encryption tailored for education
These gaps highlight the need for a dedicated platform that understands the specific requirements of a digital classroom, and not just a generic meeting space.	

PROBLEM STATEMENT

Current network intrusion detection methods, largely based on signature matching, often fail to detect unknown or evolving threats. Additionally, traditional systems suffer from issues like:

- High false positive rates.
- Inability to scale with high-volume traffic.
- Delayed detection and response.

There is a pressing need for an intelligent system that can monitor network traffic in real time, distinguish between normal and abnormal behavior, and adapt to emerging threats dynamically.

To design and develop a secure, real-time virtual classroom platform tailored specifically for educational use, addressing the limitations of existing video conferencing tools by integrating features such as attendance tracking, screen sharing, live chat, secure authentication, and session management—thereby enhancing the quality, engagement, and accessibility of online education."

This problem statement emphasizes both the **technical** and **educational** goals of the project, while aligning it with real-world needs of students and educators.

Our project aims to develop a **machine learning-based NIDS** that enhances detection capabilities, reduces false alarms, and improves overall cybersecurity readiness.

OBJECTIVES

1. To develop a machine learning-based NIDS capable of detecting a wide range of network intrusions in real-time.
2. To select and preprocess network traffic datasets (such as CICIDS) for effective model training and evaluation.
3. To implement supervised machine learning algorithms like Random Forest, Decision Trees, and Logistic Regression for traffic classification.
4. To design an intuitive dashboard to display alerts, analytics, and detailed session histories.
5. To achieve high detection accuracy while maintaining low false positive rates.
6. To ensure the system is scalable and can handle large volumes of real-time traffic.
7. To validate and improve the NIDS performance through rigorous testing on different network conditions.

8.Develop a Real-Time Virtual Classroom Platform : Create a lightweight, easy-to-use web-based application that allows teachers and students to conduct live classes seamlessly through video, audio, and screen-sharing capabilities.

9.Ensure Secure and Reliable Communication : Implement robust authentication mechanisms to ensure only authorized users can join sessions, and provide encrypted data transmission to maintain the confidentiality and integrity of online classes.

10. Enhance Classroom Engagement : Integrate real-time features such as live chat, hand-raising, polling, and participation tracking to foster an interactive and collaborative virtual classroom environment.

Tools/Technologies Used

Programming Languages: Python (for machine learning models and backend)

Libraries/Frameworks:

- Scikit-learn (for ML algorithms)
- Pandas and NumPy (for data preprocessing)
- Matplotlib and Seaborn (for data visualization)
- Flask (for backend server and dashboard integration)

Dataset: CICIDS2017 / CICIDS2018 (Intrusion detection datasets)

Reasons for Selecting these Tools:

- **Python**: Versatile, easy-to-use, and has extensive ML libraries.
- **Scikit-learn**: Offers simple yet powerful ML model implementations.
- **Flask**: Lightweight web framework, perfect for creating a custom dashboard.
- **Pandas/NumPy**: Essential for handling large datasets and feature engineering.
- **CICIDS dataset**: Offers a wide range of labeled real-world network traffic.

METHODOLOGY

1. DATA COLLECTION & PREPROCESSING

- We used the CICIDS dataset, which contains labeled data for normal and attack traffic.
- Preprocessing involved data cleaning, feature scaling, encoding categorical features, and handling missing values.

2. MODEL TRAINING & EVALUATION

- Applied supervised learning techniques: Random Forest, Decision Tree, Logistic Regression.
- Split the dataset into training and testing sets to validate model performance.
- Evaluation Metrics: Accuracy, Precision, Recall, F1 Score, Confusion Matrix.

3. DASHBOARD DEVELOPMENT

- Created using Flask and Bootstrap for a responsive and user-friendly UI.
- Features:
    - Alerts on detected intrusions.
    - Real-time traffic monitoring.
    - Analytics and session history display.

4. DEPLOYMENT

- The final model was deployed with the backend server, capable of processing real-time network packets (simulated during testing).

REFERENCES

Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2010.25

Bridges, S. M., & Vaughn, R. B. (2000). Intrusion Detection via Fuzzy Data Mining. Proceedings of the 12th Annual Canadian Information Technology Security Symposium.

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961.

Cybersecurity Research Journal. (2022). Security Challenges in Machine Learning-Based Intrusion Detection Systems.

Information Security Journal. (2023). Feature Engineering for Improving Intrusion Detection System Accuracy.