Volume 10, Issue 4, April – 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

Learning-Based Intrusion Detection and Prevention System (LIDPS)

M V V Gopala Krishna Murthy[1]; D Lahari[2]; Ch Lakshmi Pujitha [3]; P Lakshmi Pranamya[4]; T Harsha Tri Lakshmi[5]; S Sai Durga Lavanya[6]

[1]Assistant Professor; [2,3,4,5,6] B.Tech. Student

[1,2,3,4,5,6] Department of CSE, Sri Vasavi Engineering College(A), Pedatadepalli, Tadepalligudem – 534101

Publication Date: 2025/05/07

Abstract; The increasing number of cyber threats and security breaches has necessitated the development of intelligent, automated, and proactive cybersecurity mechanisms. This project focuses on designing and implementing an Intrusion Detection and Prevention System (IDPS) that leverages Machine Learning (ML) techniques to detect and prevent network intrusions in real-time. The system continuously monitors incoming network traffic, extracts meaningful features, and classifies it as normal or malicious using a trained Random Forest algorithm, ensuring high detection accuracy and minimal false positives. If an attack is detected, the system automatically blocks the attacker's IP address, preventing further malicious activity and enhancing network security. The backend is developed using Flask, while MySQL is utilized for storing attack logs, detected intrusions, and blocked IPs, ensuring an efficient and well-structured database management system. The user-friendly dashboard, designed with an intuitive UI, enables real-time monitoring and management of intrusion events, providing detailed logs and analytics to help security administrators analyze attack patterns and refine network defenses. The system is trained using 17 critical network features, allowing it to differentiate between normal and anomalous traffic with high precision. It is designed to function efficiently in large-scale network environments, making it suitable for organizations, enterprises, and cloud-based infrastructures that require robust cybersecurity measures. Additionally, the integration of automated response mechanisms ensures that threats are mitigated instantly without manual intervention, significantly reducing the risk of security breaches. The implementation of machine learning algorithms such as Support Vector Machine (SVM), Random Forest enhances the system's ability to adapt to evolving cyber threats. This IDPS system not only provides real-time threat prevention but also contributes to cybersecurity intelligence by offering insights into intrusion trends, attacker behavior, and potential vulnerabilities in the network. With cyberattacks becoming increasingly sophisticated, the need for such an advanced intrusion prevention mechanism is more crucial than ever. This project represents a highly scalable, efficient, and reliable approach to proactive network defense, providing organizations with a powerful security solution to safeguard their digital assets from emerging cyber threat.

Keywords: *Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Network Security, Machine Learning, Cyber Threat Detection, IP Blocking, Flask Web Application, Real-Time Monitoring, Automated Response, Anomaly Detection, Email Notification, MySQL Database.*

How to Cite: M V V Gopala Krishna Murthy; D Lahari; Ch Lakshmi Pujitha ; P Lakshmi Pranamya; T Harsha Tri Lakshmi; S Sai Durga Lavanya (2025). Learning-Based Intrusion Detection and Prevention System (LIDPS). *International Journal of Innovative Science and Research Technology*, 10(4), 2562-2571. https://doi.org/10.38124/ijisrt/25apr945

I. INTRODUCTION

In today's hyper-connected digital world, where technology is an integral part of our daily lives, ensuring cybersecurity has become more critical than ever before. The rapid growth of the internet and the increasing dependence on network-based applications have brought about numerous benefits. However, they have also opened the door to a wide range of cyber threats and malicious activities. Organizations and individuals alike are now more vulnerable to various forms of intrusions, such as denial-of-service attacks, unauthorized access, phishing, and malware infections, which can lead to data breaches, financial loss, and reputational damage.

Traditional security systems often operate based on predefined rules and signatures to detect threats. While these systems are effective against known attacks, they struggle to identify new or evolving threats that do not match predefined patterns. This limitation creates a pressing need for more intelligent, adaptive, and automated security solutions that can analyze network traffic in real-time, detect anomalies, and take swift action to mitigate threats before they escalate.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

To address this challenge, our project introduces a Machine Learning-based Intrusion Detection and Prevention System (IDPS), designed to monitor network traffic, identify suspicious behaviors, and proactively block malicious IP addresses. Our system is developed as a Flask-based web application that leverages a trained machine learning model to analyze real-time data using 17 essential features. Once abnormal activity is detected, the system automatically logs the event into a MySQL database and updates a list of blocked IPs to prevent further damage. Additionally, it sends immediate email alerts to notify administrators of the threat, ensuring quick awareness and response.

The IDPS not only aims to improve detection accuracy through intelligent algorithms but also simplifies the process of incident handling by automating the entire workflow—from detection to prevention and notification. This automation reduces human intervention, enhances operational efficiency, and minimizes the potential for human error in critical security operations.

This research paper explores the system architecture, methodologies, and machine learning techniques employed in our IDPS. It highlights how combining classification models with robust data preprocessing and feature scaling can significantly boost the detection rate of intrusions. Furthermore, the paper discusses the importance of transparent, real-time threat tracking and the role of automated prevention mechanisms in strengthening an organization's cybersecurity posture.

Through the development and deployment of this IDPS, we aim to provide an accessible, efficient, and scalable solution to contemporary cybersecurity challenges. By incorporating real-time analytics and automatic IP blocking, our system not only detects intrusions but also ensures active protection against future attacks—offering peace of mind to users and promoting a safer digital environment.

II. LITERATURE REVIEW

In the ever-evolving landscape of cybersecurity, examining previous research acts as the bedrock for innovation. Understanding earlier approaches, technologies, and techniques enables researchers to build more efficient and secure systems. In this study, we have carefully explored several research papers that provide valuable insights into the development of Intrusion Detection and Prevention Systems (IDPS) using various machine learning techniques. Each of these works has contributed uniquely to the advancement of cybersecurity, laying the foundation for our proposed system.

M. Belouch et al. (2017) [1] proposed a two-stage classifier approach using the REPTree algorithm to improve the accuracy of intrusion detection. Their system utilized network traffic features to detect abnormal behavior in real-time, showcasing the importance of combining efficient algorithms with effective data preprocessing. Their research emphasizes the role of decision tree-based classifiers in reducing false positives and improving classification accuracy—an approach that has inspired components of our model design.

A. Iftikhar et al. (2018) [2] carried out a performance comparison among Support Vector Machine (SVM), Random Forest (RF), and Extreme Learning Machine (ELM) for intrusion detection purposes. Their comprehensive analysis revealed that Random Forest delivered better overall accuracy and detection rates when handling large-scale intrusion datasets. This comparative study helped establish a baseline for our project when selecting suitable models for our detection pipeline.

Jitti Annie Abraham and V. R. Bindu (2021) [3] presented a detailed review of both machine learning and deep learning approaches for intrusion detection and prevention. Their work highlighted the strengths and limitations of various learning models and stressed the need for hybrid systems that can adapt to modern network threats. Their observations validated the importance of our focus on machine learning-based IDPS as a practical and lightweight solution.

Sibi Amaran et al. (2022) [4] explored the application of machine learning algorithms in Wireless Sensor Networks (WSNs) for surveillance purposes. Their proposed model, optimized for energy efficiency and detection accuracy, serves as an ideal reference for integrating intelligent security systems in constrained environments. Their work reinforces the versatility and potential of machine learning in various domains of intrusion detection.

Ajmeera Kiran et al. (2023) [5] developed an IDPS using machine learning algorithms, focusing on real-time monitoring and detection. Their research emphasized the implementation of classification techniques for fast and accurate identification of threats. Their system design inspired several elements in our project, such as the real-time analysis engine and automated response mechanisms.

V. Ebenezer et al. (2023) [6] introduced an Intrusion Detection and Prevention System focused on malware detection using supervised machine learning models. They demonstrated how integrating prevention with detection can lead to proactive defense systems. This approach aligns closely with our project's core objective of not only detecting but also auto-blocking malicious IPs.

Mona Esmaeili et al. (2024) [7] discussed the role of machine learning in enhancing IoT security. Their system leveraged data analytics and classification models to detect anomalous behavior in IoT networks. Their findings support our project's goal of applying scalable and intelligent security solutions in both traditional and modern network environments.

Each of these studies brings forward critical advancements in the field of intrusion detection and prevention. They collectively emphasize the importance of using data-driven models, real-time analytics, and automated responses for stronger network security. Drawing inspiration

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

from these works, our proposed IDPS integrates real-time detection, IP blocking, email alerting, and web-based monitoring to offer a comprehensive and user-friendly cybersecurity solution.

III. PROPOSED SYSTEM

➢ *Problem Statement*

In today's increasingly connected world, the rise in cyber threats has exposed the limitations of traditional security methods that often rely on manual monitoring and reactive responses. These outdated approaches are time-consuming, prone to human error, and inadequate for detecting modern, complex intrusions that can cause significant damage. To address this challenge, our project proposes a Machine Learning-based Intrusion Detection and Prevention System (IDPS) that automates the detection and blocking of malicious activities in real time. Unlike conventional systems, our IDPS not only identifies threats with high accuracy but also instantly blocks malicious IP addresses, sends real-time alerts, and logs detailed IP information such as location, user agent, and ISP for further analysis. This automated and intelligent solution enhances security, reduces the risk of human oversight, and provides a scalable defense mechanism that adapts to evolving cyber-attack patterns, ensuring robust protection for modern networks.

➢ *System Architecture*

To overcome the limitations of traditional manual methods and static detection systems, our Intrusion Detection and Prevention System (IDPS) introduces a dynamic and automated architecture that enhances security, accuracy, and responsiveness. The system architecture (see Fig-1) is composed of several integral modules working in tandem to detect, analyze, and respond to potential network intrusions in real-time.

At the center of the architecture is the App Module, which orchestrates the overall system operations. This module integrates a Machine Learning Model for detecting anomalies, a Standard Scaler for normalizing incoming data, and a MySQL database that stores vital logs and blocked IPs. The Email Handler Module is responsible for sending immediate alerts to the system administrator when suspicious activity is detected. The IP Manager Module handles IP address verification, blocking, and retrieving lists of blocked sources. Meanwhile, the Logger Module ensures detailed logging of all detected intrusions for analysis and auditing.

The architecture emphasizes modularity, allowing each component to operate independently while communicating through a centralized backend application. This design ensures scalability, security, and efficiency in handling large volumes of network traffic.

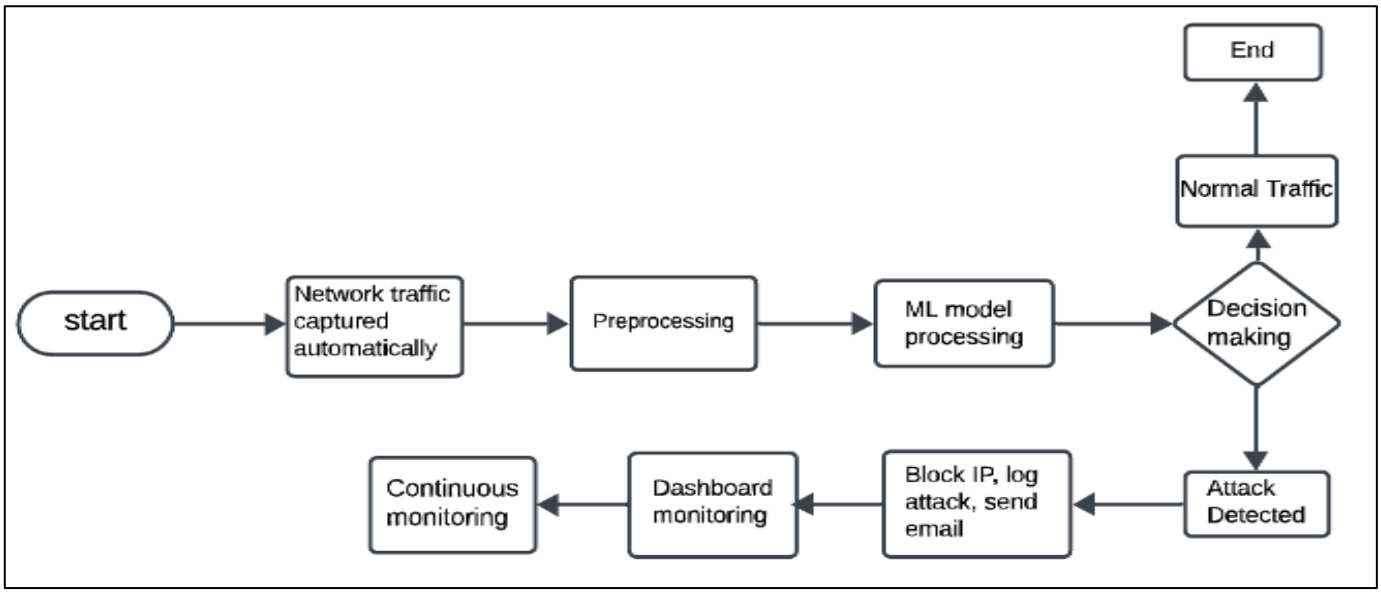

Fig 1 Proposed System Architecture

Our application comprises core components and their interactions to detect and mitigate threats effectively. The Class Diagram (see Fig-2) highlights key classes such as App, EmailHandler, IPManager, and Logger, detailing their attributes and methods. This structure provides a blueprint of how system entities collaborate to execute tasks like monitoring, blocking, logging, and alerting.Additionally, the Activity Diagram (see Fig-3) outlines the flow of operations from data collection to threat prevention. It captures the sequence of processes including real-time traffic analysis, ML-based intrusion prediction, decision-making, and corresponding actions such as blocking IPs or allowing access. This diagram ensures a clear understanding of the runtime behavior and helps visualize the logic behind every detection and response mechanism.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

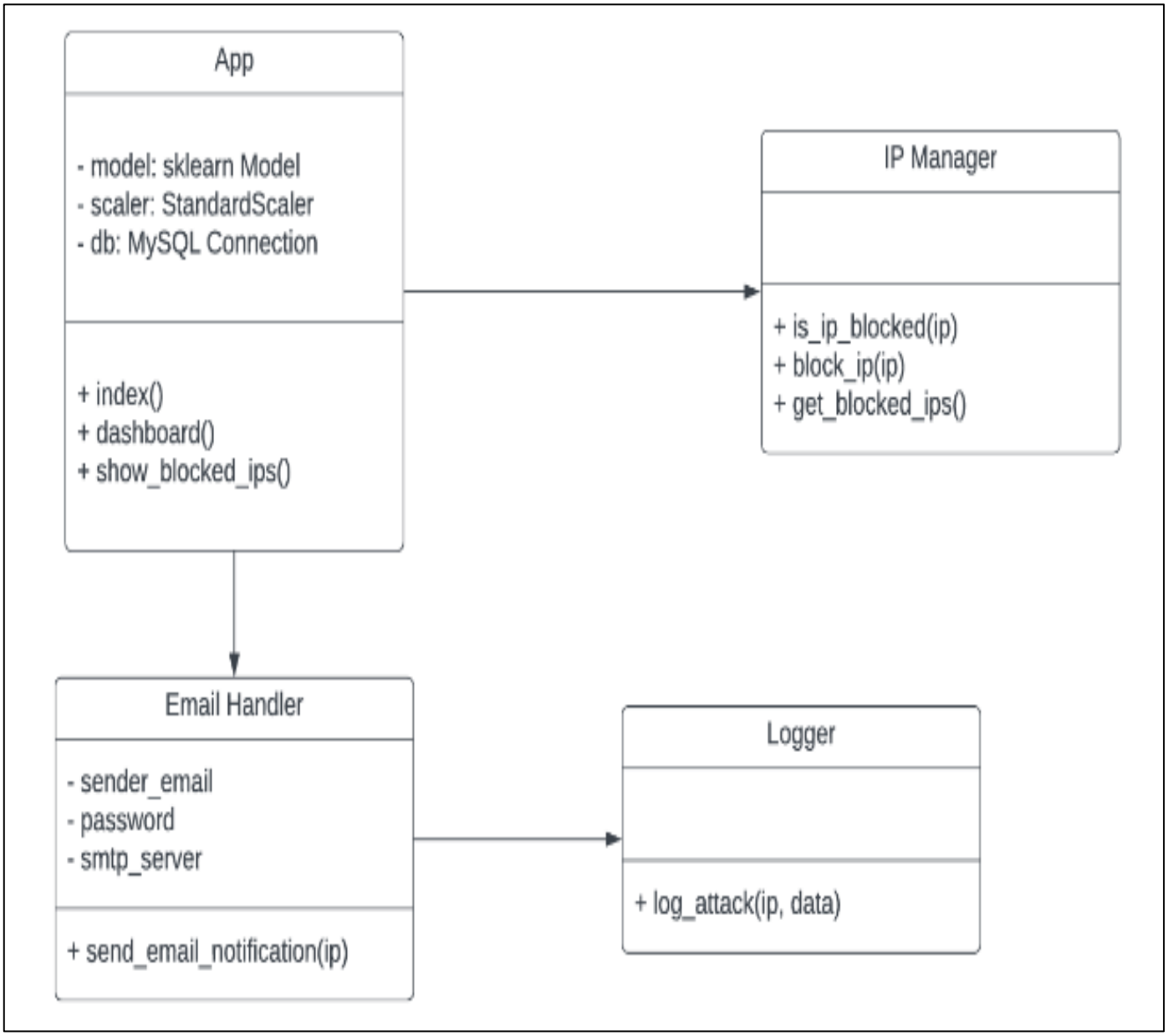

Fig 2 UML CLASS Diagram

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

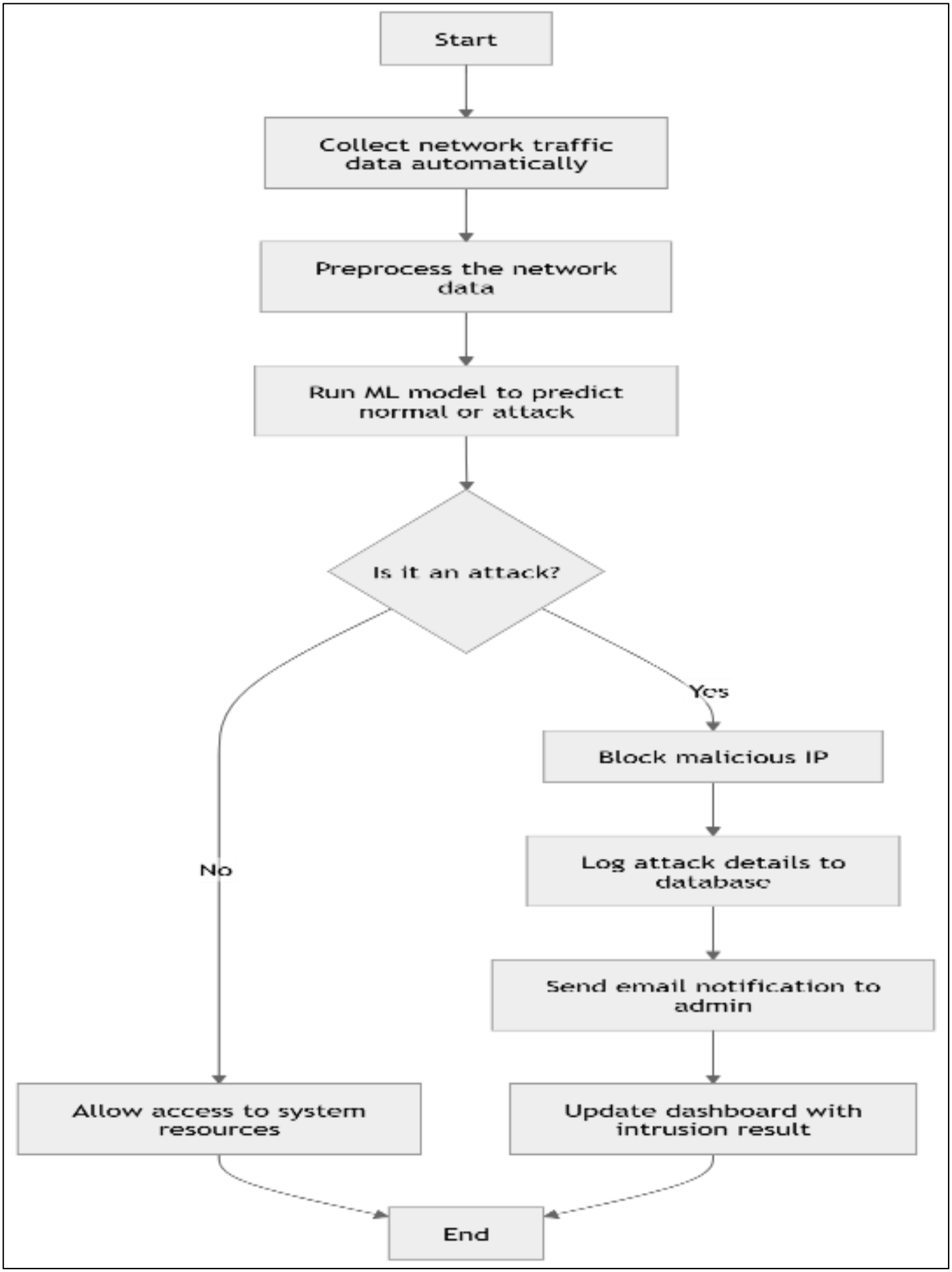

Fig 3 Activity Diagram

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

IV. METHODOLOGY

This section provides a comprehensive overview of the architecture and functional workflow behind the implementation of our Flask-based Intrusion Detection and Prevention System (IDPS). The methodology integrates Machine Learning for threat detection, real-time logging, auto-blocking mechanisms, and administrator notification via email—all of which work together to ensure a proactive defense against cyber intrusions. The system is trained on 17 key features from the KDD dataset and is built using Python, Flask, MySQL, and scikit-learn.

➢ *Data Monitoring and Feature Preparation*

Incoming network traffic is continuously monitored and converted into feature vectors. For simulation, the system randomly generates 16 numerical features to mimic real-world data. One feature is dynamically adjusted to simulate either normal or attack-like behavior. These vectors are then processed through a StandardScaler, which was saved during the training phase, ensuring that the format and scale match what the model expects. This step ensures consistency and prepares the data for accurate real-time prediction.

features_scaled = scaler.transform([features])[0]

➢ *Intrusion Detection Model*

The heart of the system lies in a pre-trained ML model (idps_model.pkl) which takes the scaled features and outputs a binary prediction:

- 0 for normal traffic
- 1 for intrusion

This model is trained on the NSL-KDD dataset using supervised learning techniques, leveraging 17 numerical and categorical features (encoded via protocol_type, service, and flag encoders). The prediction process is seamlessly integrated into the Flask /dashboard route for real-time web-based interaction.

prediction = model.predict([features_scaled])[0]

➢ *Attack Logging Module*

Whenever an intrusion is detected (prediction == 1), the system logs the associated IP address and feature data into the attacks1 table within the idps_db MySQL database. This log includes:

- The attacking IP
- The feature vector (saved as a string)
- The email used by the system (for traceability)

This module provides a historical audit trail for future analysis and threat intelligence.

The use case diagram (Fig-4) that explains this workflow is as follows:

query = "INSERT INTO attacks1 (ip_address, features, email) VALUES (%s, %s, %s)"

The Use Case Diagram (see Fig-4) outlines the primary interactions between the administrator and the IDPS system. It captures core functionalities such as monitoring traffic, detecting intrusions, blocking malicious IPs, logging attack data, and sending alert notifications, providing a clear view of the system's intended behavior.

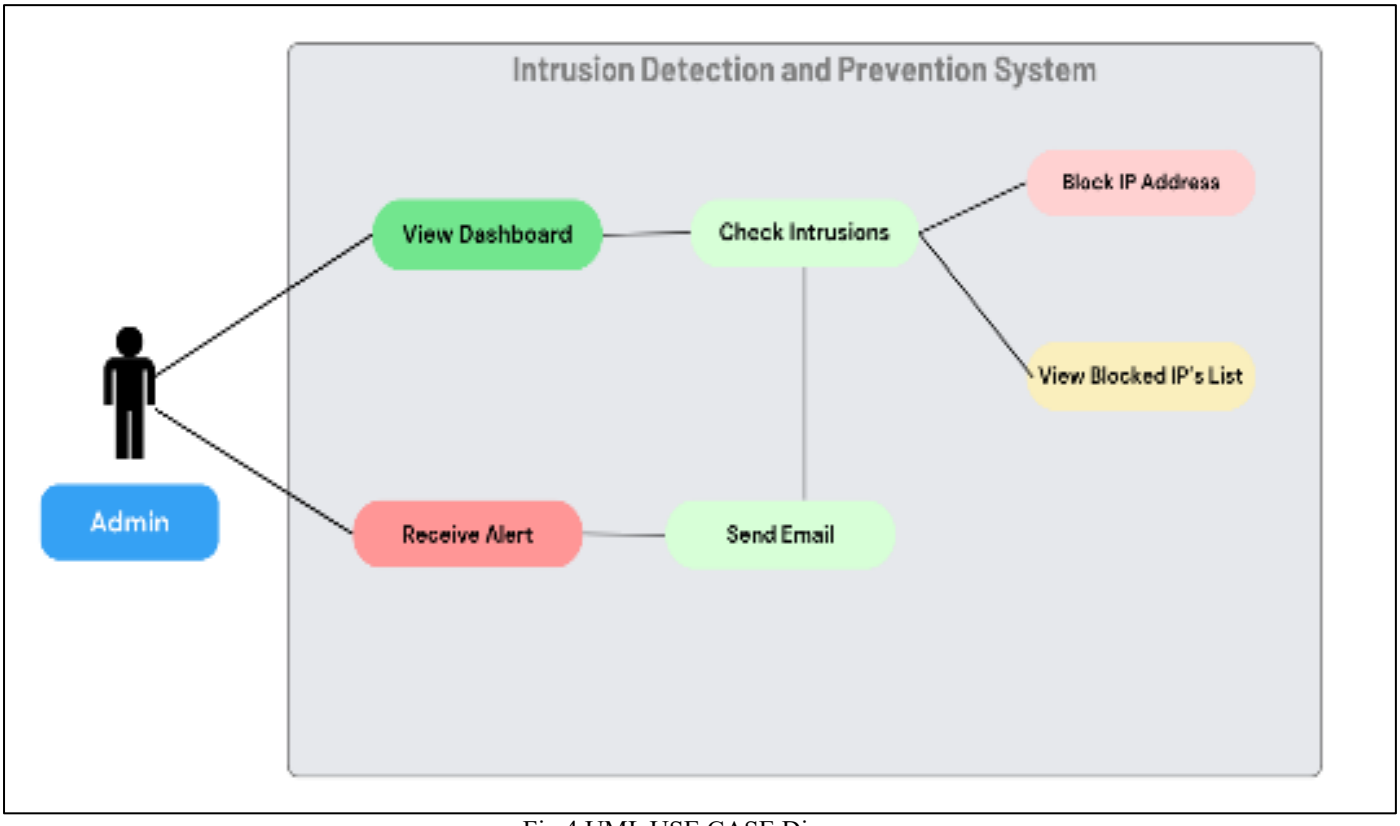

Fig 4 UML USE CASE Diagram

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

➢ *Auto IP Blocking Mechanism*

A core feature of the IDPS is its ability to automatically block any IP address associated with a detected attack. When an IP is flagged, it is added to the blocked_ips1 table along with:

- IP address
- Timestamp of the block
- The source email

Before inserting, the system checks to ensure that the IP hasn't already been blocked. This logic is crucial to prevent redundant actions and database bloat.

```
if not is_ip_blocked(ip):

cursor.execute("INSERT INTO blocked_ips1 (...) VALUES (...)")
```

➢ *Email Notification System*

The system includes an SMTP-based email alert mechanism. When an attack is detected and an IP is blocked, an alert email is sent to the administrator with the IP address and timestamp. This ensures administrators remain informed in real-time, allowing for quick human inspection or manual override if needed. The email is composed using the MIMEMultipart and MIMEText libraries, and delivered securely through Gmail's SMTP service with TLS encryption.

```
send_email_notification(ip)
```

➢ *Admin Dashboard*

The /dashboard route provides a live web interface where the administrator can view current detection results, including:

- Simulated IPs and traffic
- Real-time alerts (Attack Detected & Blocked / Normal Traffic)
- A table of all currently blocked IPs

Additionally, the /blocked_ips route renders a complete list of blocked IP addresses with timestamps, offering full transparency and control over the system's actions.

V. RESULTS AND DISCUSSION

Captured in this image is the homepage of the IDPS application, where the system initiates monitoring of network traffic and user interactions (see Fig-5). It forms the foundation for the real-time detection and prevention of malicious activities.

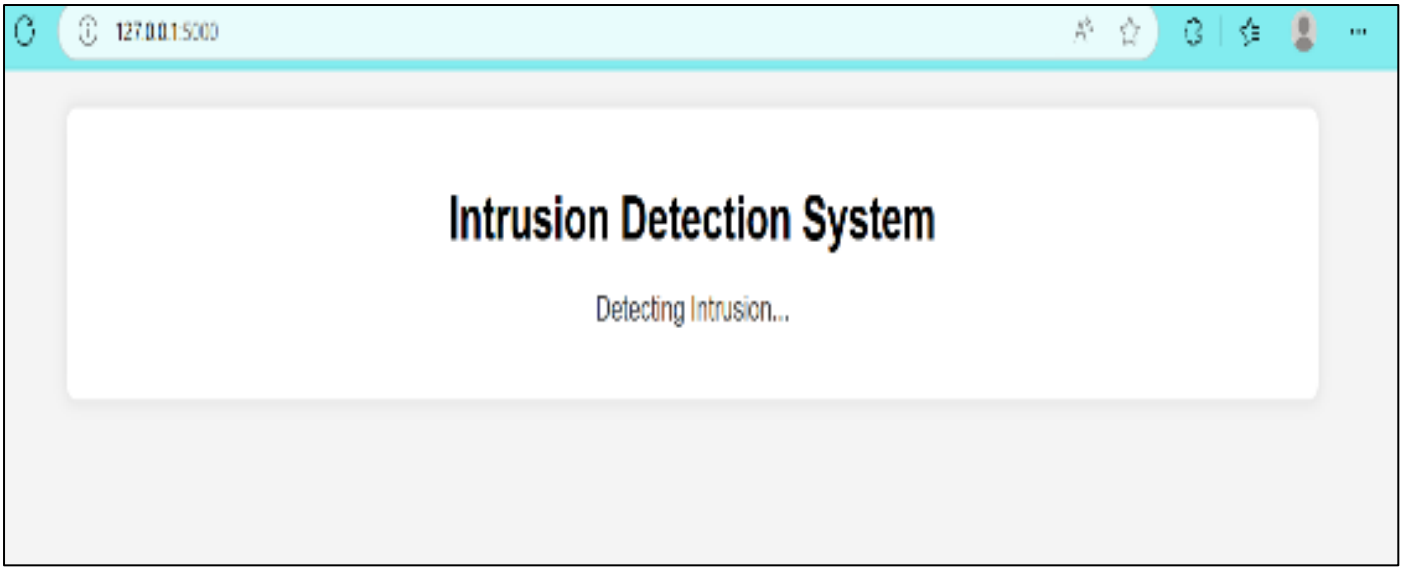

Fig **5** Homepage of IDPS Application

Here, we showcase the live dashboard of the IDPS, which dynamically simulates traffic patterns and displays the system's detection results (see Fig-6). This interface illustrates how the system intelligently distinguishes between normal and suspicious traffic, marking detected threats with appropriate alerts and immediately responding through preventive measures like IP blocking and logging.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

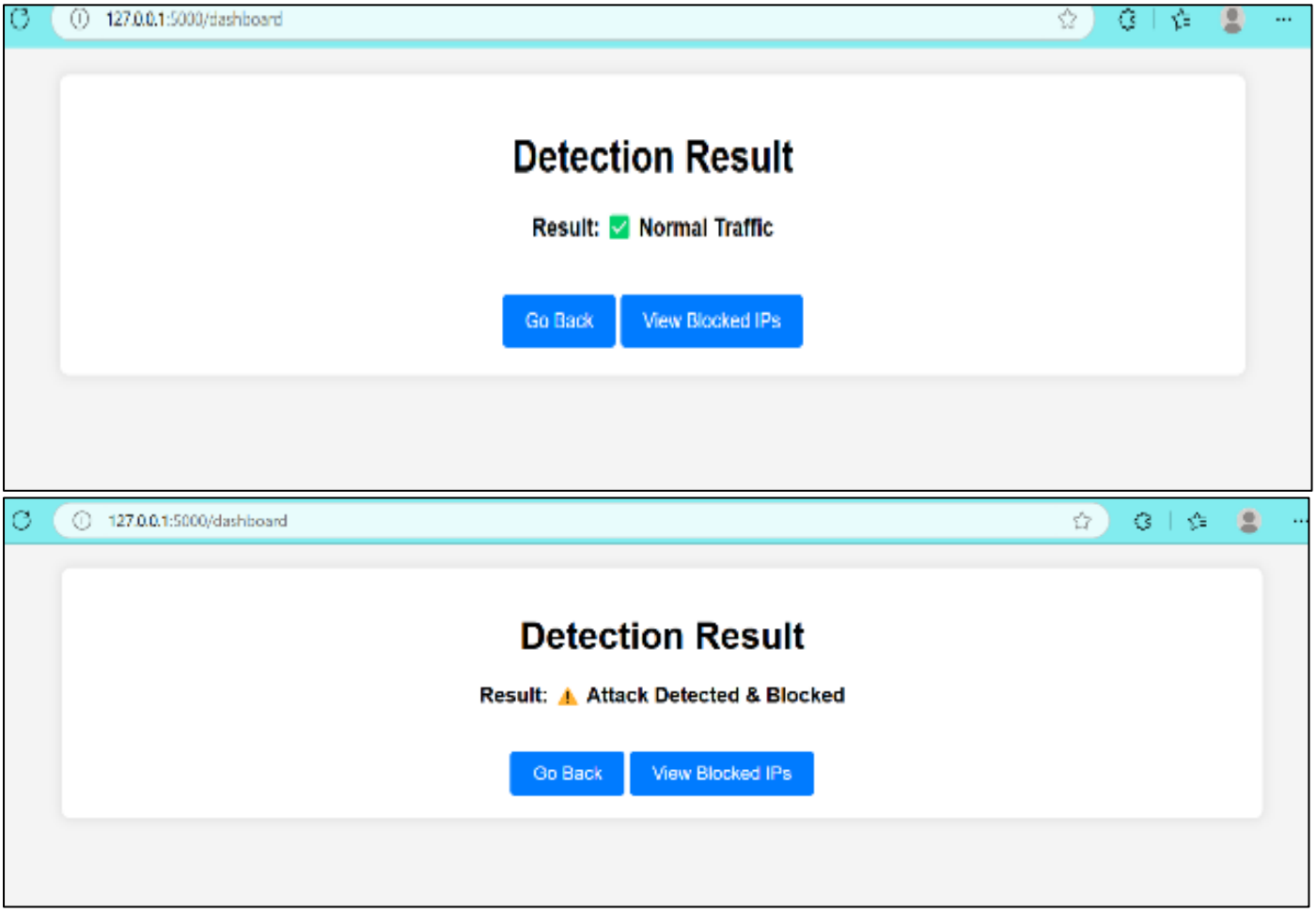

Fig 6 IDPS Live Dashboard

The interface shown below (Fig-7) highlights the Blocked IPs page, where all suspicious IP addresses identified by the system are automatically added. Each entry is timestamped, providing administrators with an audit trail and allowing for detailed review and incident analysis.

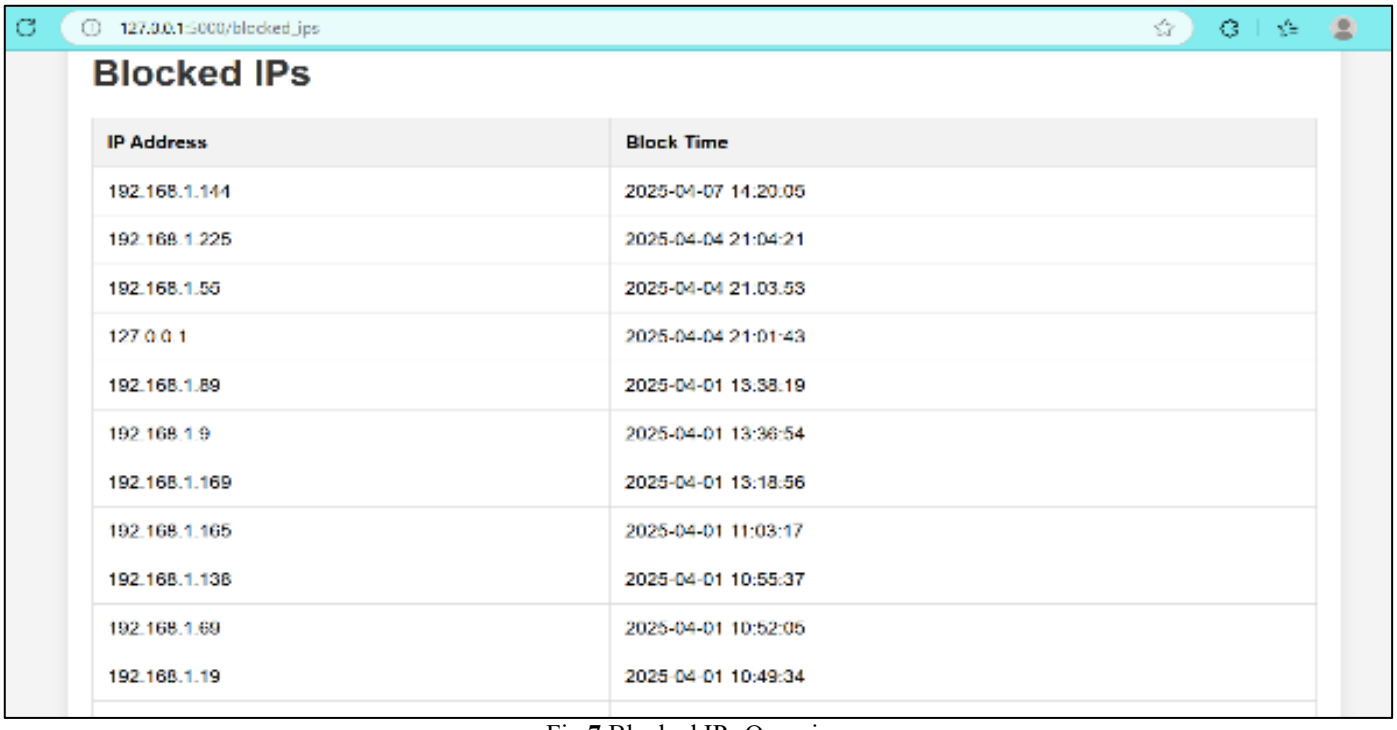

Fig 7 Blocked IPs Overview

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

When an intrusion is detected, the system triggers an automatic alert mechanism. As shown in Fig-8, an email notification is sent to the system administrator, containing vital information like the blocked IP address and the timestamp. This instant alert ensures quick awareness and enhances the overall responsiveness of the security team.

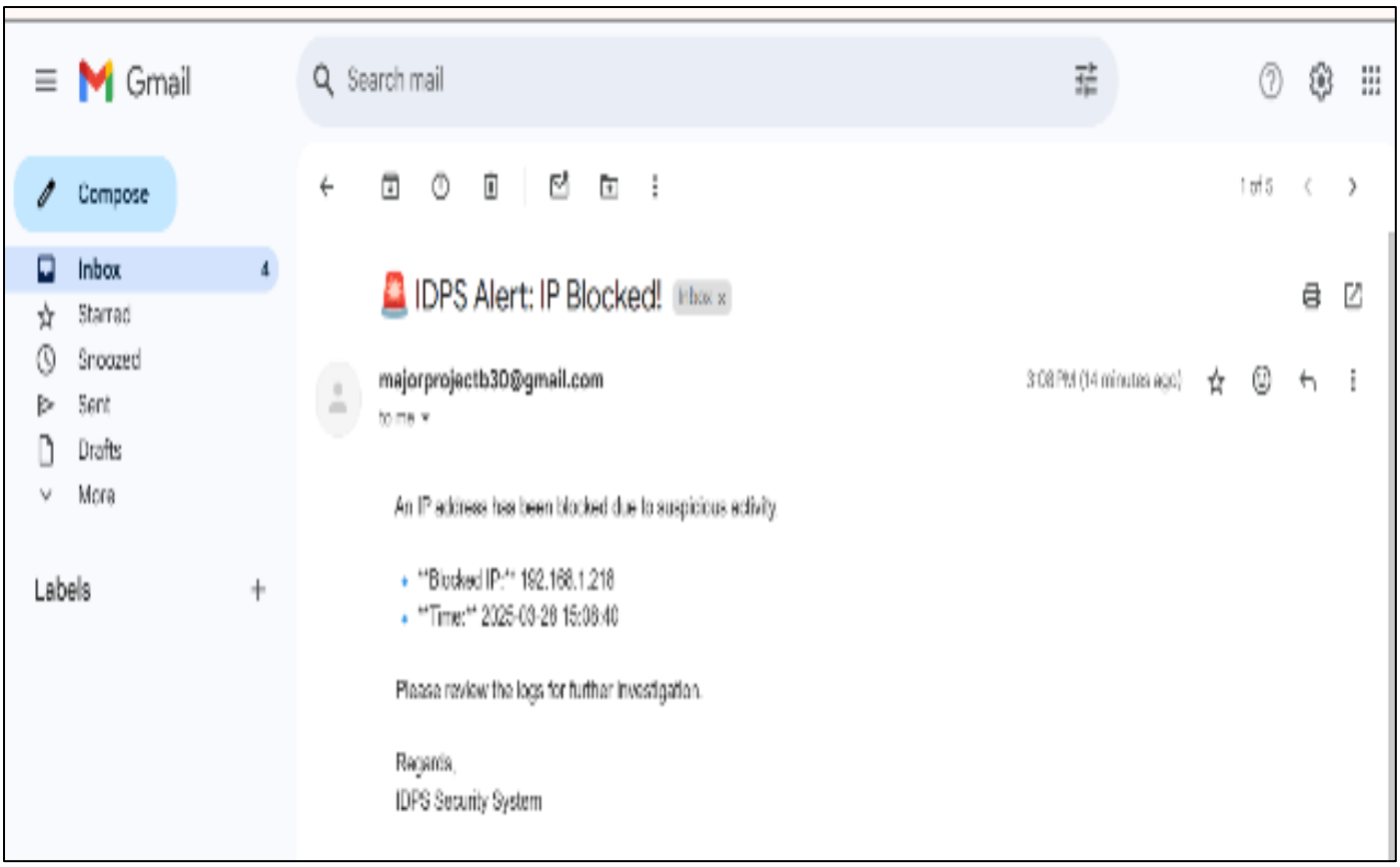

Fig 8 Email Alert Notification

VI. CONCLUSION

Our Intrusion Detection and Prevention System (IDPS) stands as a robust and intelligent solution to the evolving landscape of cybersecurity threats. Leveraging machine learning algorithms and real-time analytics, the system effectively identifies malicious activities, blocks unauthorized IP addresses, and notifies administrators instantly through automated alerts. The user-friendly interface ensures seamless interaction, while the backend handles complex threat detection processes with accuracy and speed. By integrating live attack monitoring, automatic IP blocking, and email notifications, the system offers a proactive defense mechanism against network intrusions, making it a valuable asset for maintaining secure digital environments.

Looking ahead, the future prospects of our IDPS system are both exciting and impactful. Plans include incorporating geo-IP tracking to visualize attack origins, enhancing detection models using deep learning for higher accuracy, and introducing a centralized admin panel for managing threat reports, IP whitelisting, and incident response. These additions will further elevate the system's ability to adapt, respond, and protect against sophisticated cyber threats, marking a significant step toward a smarter and more secure cyberspace.

ACKNOWLEDGEMENT

We extend our heartfelt gratitude to Dr. Jaya Kumari, Head of the Department of Computer Science and Engineering, Sri Vasavi Engineering College, for her constant support, valuable insights, and encouragement throughout this project. Her expert guidance was instrumental in shaping the direction of our work. We also sincerely thank our faculty and mentors who provided technical assistance and motivation during every phase of development. Their contributions have been crucial in turning our project into a successful and fulfilling endeavor.

REFERENCES

[1]. M. Belouch , S. El Hadaj , M. Idhammad,"A Two-Stage Classifier Approach Using REPTree Algorithm for Network Intrusion Detection",2017.
[2]. A. Iftikhar, M. Basheri, M. Javed Iqbal, A. Raheem, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection",2018.
[3]. Jitti Annie Abraham,V. R. Bindu,"Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review",2021.
[4]. Sibi Amaran, Ramalingam Madhan Mohan, Rethnaraj Jebakumar," Optimal Machine Learning Based

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr945

Intrusion Detection System in Wireless Sensor Networks for Surveillance Applications",2022.

[5]. Ajmeera Kiran; S. Wilson Prakash; B Anand Kumar; Likhitha; Tammana Sameeratmaja; Ungarala Satya Surya Ram Charan ," Intrusion Detection System Using Machine Learning",2023.

[6]. V. Ebenezer; Rosebel Devassy; G. Jaspher W. Kathrine," Intrusion Detection and Prevention System to Analyse and Prevent Malware using Machine Learning",2023.

[7]. Mona Esmaeili, Morteza Rahimi, Hadise Pishdast, Dorsa Farahmandazad, Matin Khajavi, Hadi Jabbari Saray ," Machine Learning-Assisted Intrusion Detection for Enhancing Internet of Things Security" ,2024.