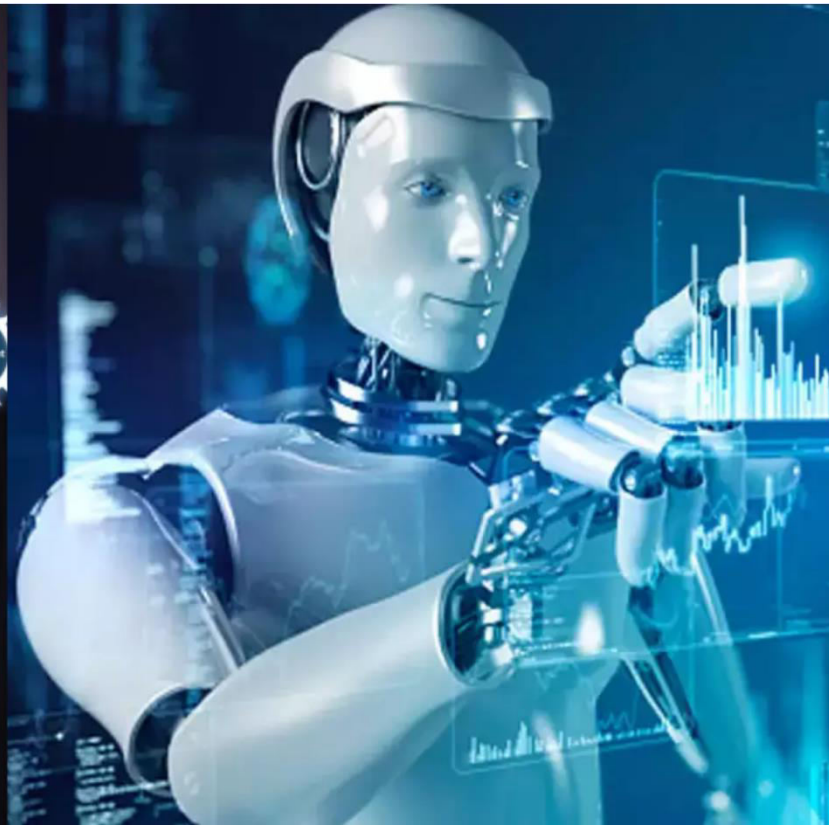
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|

An Intrusion Detection and Prevention System (IDPS)

Mr. Shaik Nagur Vali [1], P. Sai Nikhil[2], Ch. Sathwika[3], M. Sameer[4], G. Himadweep[5]

Assistant Professor, Department of CSE (Data Science), ACE Engineering College, Hyderabad, India[1]

IV B. Tech, Department of CSE (Data Science), ACE Engineering College, Hyderabad, India[2,3,4,5]

ABSTRACT: The rapid growth of digital networks has increased the risk of cyberattacks, making network security a critical concern. Traditional security systems such as firewalls and signature-based intrusion detection systems are limited in identifying new and unknown threats. This project proposes an An Intrusion Detection and Prevention System (IDPS) to enhance network security through intelligent threat detection and automated prevention. The system uses machine learning techniques, specifically the XGBoost algorithm, to analyze network traffic and classify it as normal or malicious. It continuously monitors network packets, extracts important features such as IP address, protocol type, and packet behavior, and detects suspicious patterns. When a threat is identified, the system automatically blocks the attacker's IP address and sends alerts to the administrator. A web-based dashboard developed using Flask provides real-time visualization of network activity and detected threats. The system also maintains logs for further analysis and security auditing. By integrating machine learning with automated response mechanisms, the proposed IDPS improves detection accuracy and reduces response time. This approach enables proactive protection against both known and unknown cyber threats. Overall, the system provides a scalable and intelligent solution for modern cybersecurity environments.

I. INTRODUCTION

The rapid advancement of computer networks and internet technologies has significantly increased the risk of cyber threats and security attacks. Organizations and individuals rely heavily on digital systems for communication, data storage, and business operations, making network security an essential requirement. Traditional security mechanisms such as firewalls and signature-based intrusion detection systems are limited in detecting new and unknown attacks. These systems mainly rely on predefined rules and signatures, which makes them ineffective against evolving cyber threats and zero-day attacks.

This project focuses on developing An Intrusion Detection and Prevention System (IDPS) that uses machine learning techniques to detect malicious activities in network traffic. The system analyzes network packets and identifies abnormal behavior using advanced algorithms such as XGBoost. By continuously monitoring network activity, the system can detect suspicious patterns in real time. Once an intrusion is detected, the system automatically blocks the attacker's IP address and sends alerts to the administrator. The proposed system also provides a web-based dashboard for monitoring network traffic, viewing alerts, and analyzing attack patterns. This approach improves detection accuracy, reduces response time, and enhances overall network security.

II. EXISTING SYSTEM

The existing network security systems mainly rely on traditional mechanisms such as firewalls and signature-based Intrusion Detection Systems (IDS) to protect networks from cyber threats. These systems work by comparing network traffic with predefined attack signatures and rules. While they are effective in detecting known attacks, they are unable to identify new or unknown threats such as zero-day attacks. As cyberattacks are continuously evolving, static rule-based systems struggle to adapt to new attack patterns. Another limitation of the existing system is the lack of intelligent behavioral analysis. Traditional IDS does not analyze the behavior of network traffic deeply, which makes it difficult to detect abnormal patterns that do not match known signatures. This often results in a high number of false alerts or missed attacks. Additionally, most existing systems only generate alerts without taking automatic preventive actions. Administrators must manually analyze these alerts and take necessary actions, which delays the response time during active attacks. This reactive approach makes the network more vulnerable to serious security breaches.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

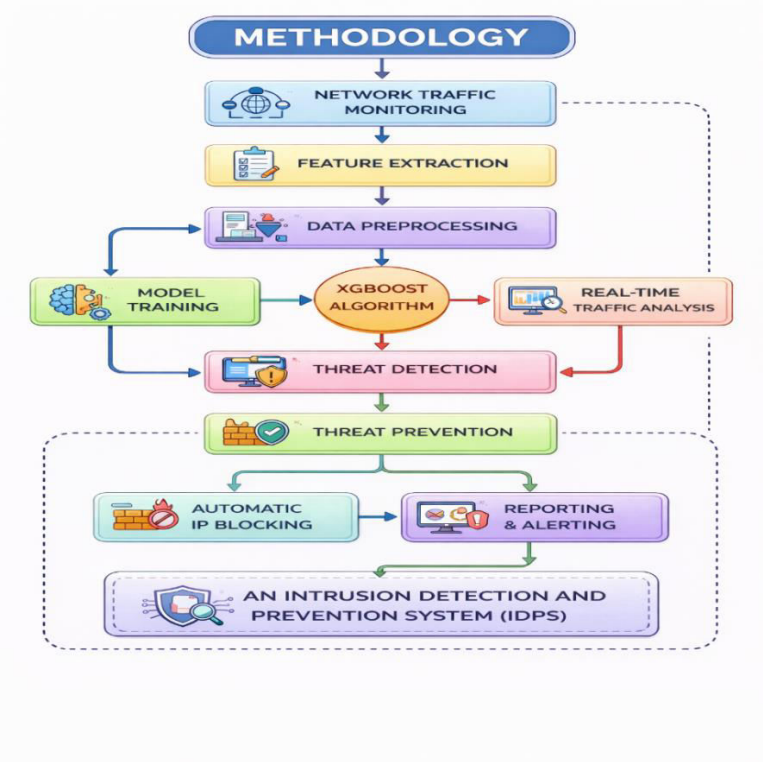
|DOI: 10.15680/IJIRSET.2026.1503114|

III. PROPOSED SYSTEM

The proposed system introduces an An Intrusion Detection and Prevention System (IDPS) designed to improve network security by detecting and preventing cyber threats in real time. Unlike traditional systems that rely on static rules and predefined signatures, the proposed model uses machine learning techniques to analyze network behavior and identify suspicious activities. The system continuously monitors network traffic and collects packet information such as IP addresses, protocols, and data flow patterns. These features are processed and analyzed using the XGBoost machine learning algorithm, which classifies the traffic as either normal or malicious. By using behavioral analysis, the system can detect both known attacks and previously unseen threats such as zero-day attacks. When malicious activity is detected, the system automatically blocks the attacker's IP address using firewall rules.

The system also sends real-time alerts to the administrator and stores all attack information in secure logs for future analysis. A web-based dashboard is provided to visualize network traffic, intrusion alerts, and system performance. This intelligent and automated approach improves detection accuracy, reduces response time, and provides proactive protection against modern cyber threats.

IV. METHODOLOGY



i. Network Traffic Monitoring

This step involves continuously monitoring network traffic to capture data packets flowing through the network. Tools such as packet sniffers or network monitoring software collect information like source IP address, destination IP address, protocol type, and packet size. This real-time monitoring helps in identifying unusual or suspicious activities occurring in the network.

ii. Feature Extraction

After capturing the network traffic, important features are extracted from the collected packets. These features include attributes such as packet length, connection duration, protocol type, source and destination ports, and traffic flow patterns. Feature extraction helps convert raw network data into meaningful parameters that can be used by machine learning algorithms for analysis.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|

iii. Data Preprocessing
In this stage, the extracted data is cleaned and prepared for model training. Data preprocessing involves removing duplicate records, handling missing values, converting categorical values into numerical form, and normalizing data. This step ensures that the dataset is accurate, consistent, and suitable for machine learning analysis.

iv. Model Training
The processed dataset is used to train the machine learning model. In this project, the XGBoost algorithm is used to learn patterns between normal network traffic and malicious activities. During training, the model analyzes historical data and builds decision trees that help classify future traffic as normal or malicious.

v. XGBoost Algorithm
The XGBoost algorithm acts as the core intelligence of the system. It analyzes network traffic features and predicts whether the incoming data represents normal behavior or a potential intrusion. XGBoost is chosen because it provides high accuracy, fast processing, and better performance when dealing with large datasets.

vi. Real-Time Traffic Analysis
Once the model is trained, it is applied to live network traffic. Incoming packets are analyzed in real time using the trained model. The system continuously checks for abnormal patterns or suspicious behavior that may indicate cyberattacks such as unauthorized access or malware activity.

vii. Threat Detection
If the machine learning model identifies malicious behavior, the system flags it as a threat. The detection module classifies the type of attack based on the network behavior patterns. This step helps the system quickly identify intrusions and generate alerts for further action.

viii. Threat Prevention
After detecting a threat, the system immediately performs prevention actions to protect the network. These actions may include blocking suspicious connections, stopping malicious packets, or restricting access from the attacker's IP address. This step ensures that attacks are stopped before they cause serious damage.

ix. Automatic IP Blocking
The system automatically blocks the IP address of the attacker using firewall rules or security policies. This prevents the attacker from sending further malicious traffic to the network and helps maintain network security.

x. Reporting and Alerting
All detected attacks and prevention actions are logged in the system. The system sends alerts to administrators through the dashboard or notifications. These reports help administrators analyze attack patterns and improve network security strategies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

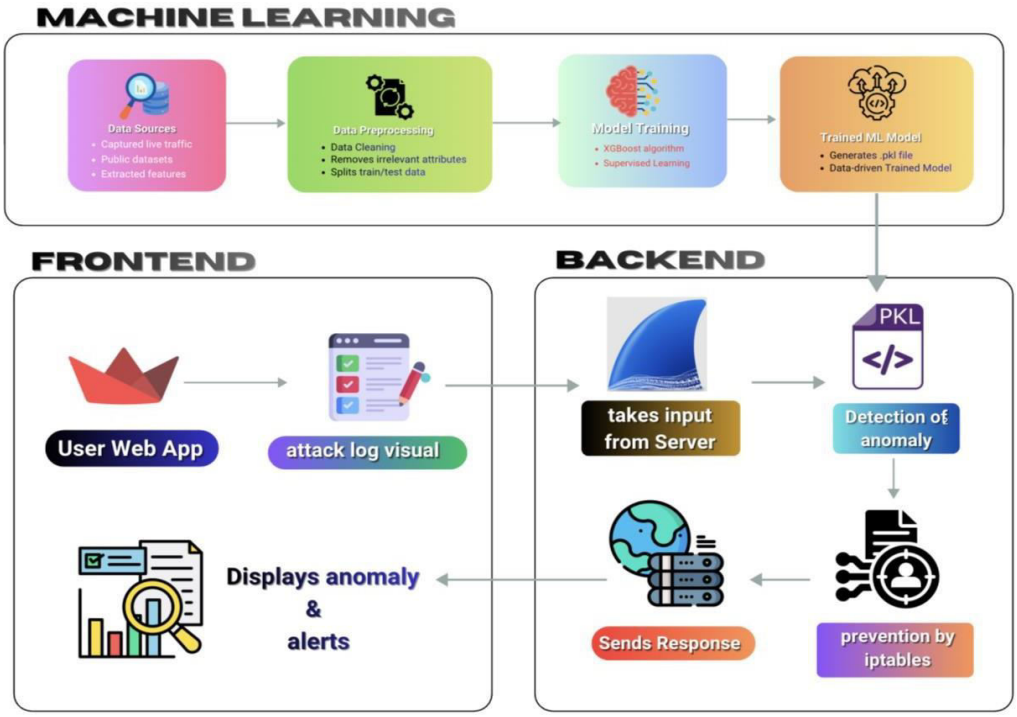
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|

V. SYSTEM ARCHITECTURE



The system architecture of the Intrusion Detection and Prevention System (IDPS) is designed to monitor, analyze, and protect network traffic in real time. The architecture begins with the network traffic monitoring module, which captures incoming and outgoing packets from the network. The system architecture diagram illustrates the overall structure and workflow of the Intrusion Detection and Prevention System (IDPS). The architecture is divided into three major components: machine learning layer, backend processing, and frontend interface. In the machine learning layer, the system performs tasks such as data preprocessing, feature extraction, and model training using the XGBoost algorithm. This trained model is responsible for analyzing network traffic and detecting anomalies or malicious activities.

The backend module processes incoming network traffic data and sends it to the trained model for prediction. Based on the prediction results, the system determines whether the traffic is normal or malicious. If a threat is detected, the backend activates the prevention mechanism, which blocks the attacker's IP address using firewall rules and generates security alerts. The system also logs intrusion details for further analysis and monitoring.

The frontend module provides a web-based dashboard for administrators. It displays network traffic statistics, detected anomalies, and attack logs in real time. Through this interface, administrators can monitor system performance, view alerts, and analyze threat patterns. This integrated architecture ensures efficient data processing, intelligent threat detection, and automated prevention, making the system capable of providing proactive network security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

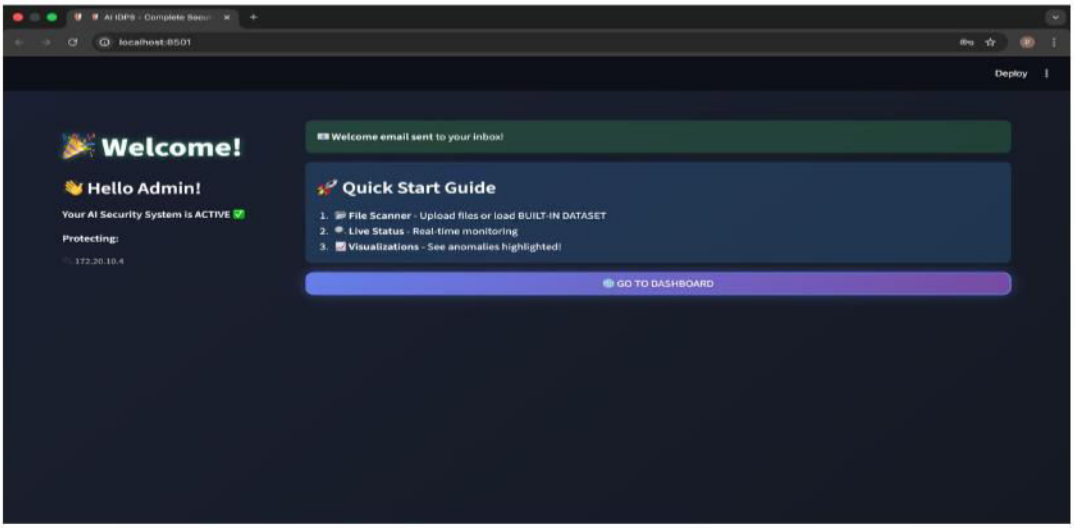
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

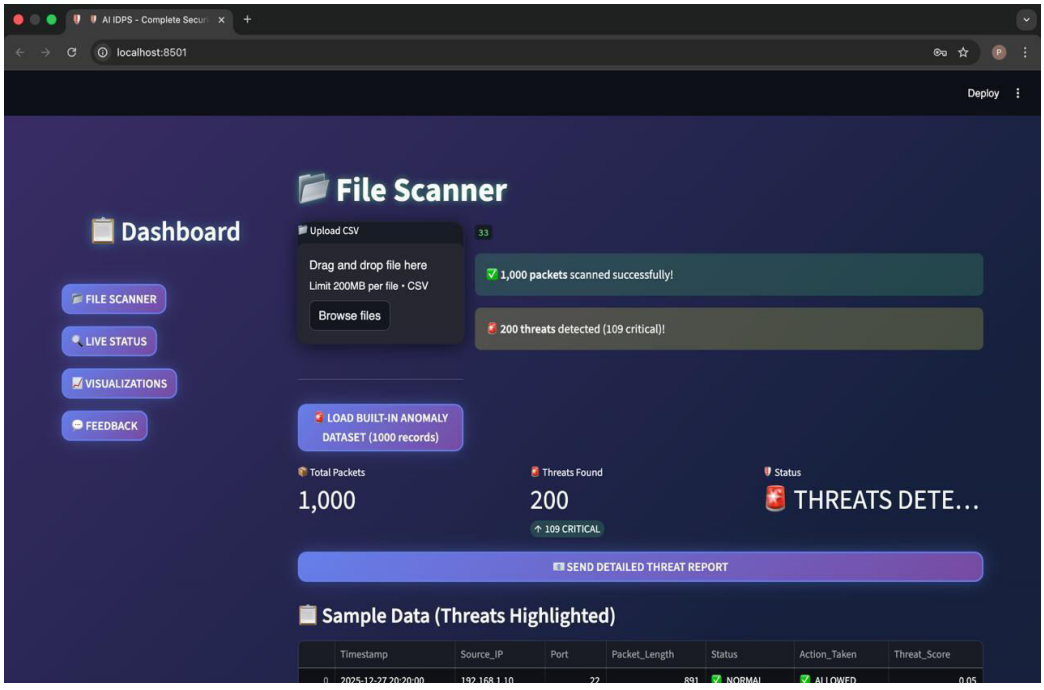
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|

VI. RESULTS AND OUTPUT



SYSTEM INITIALIZATION



PACKET THREAT SCANNING

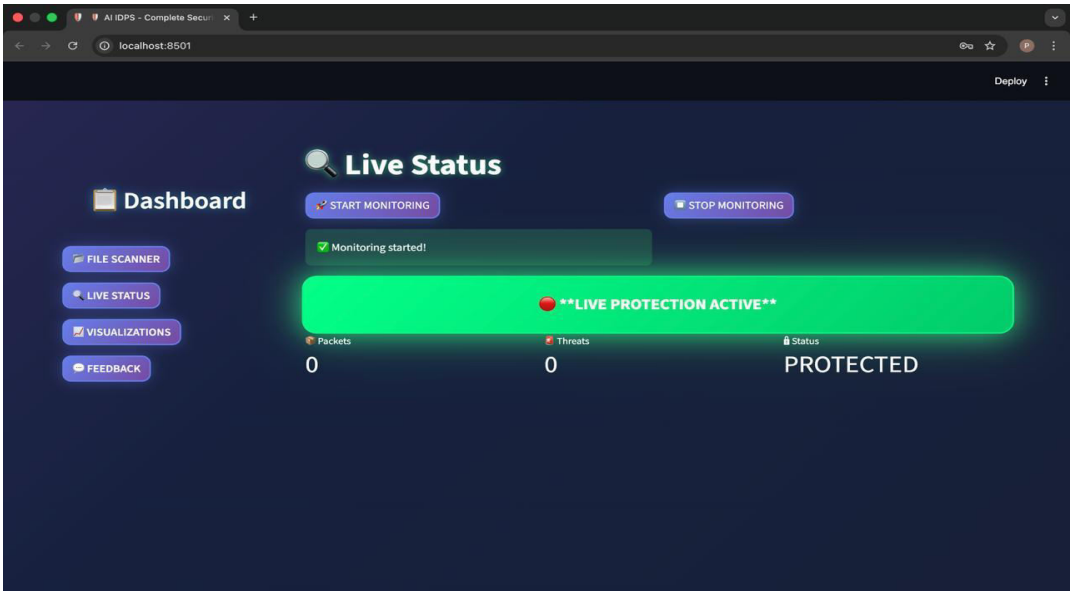
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

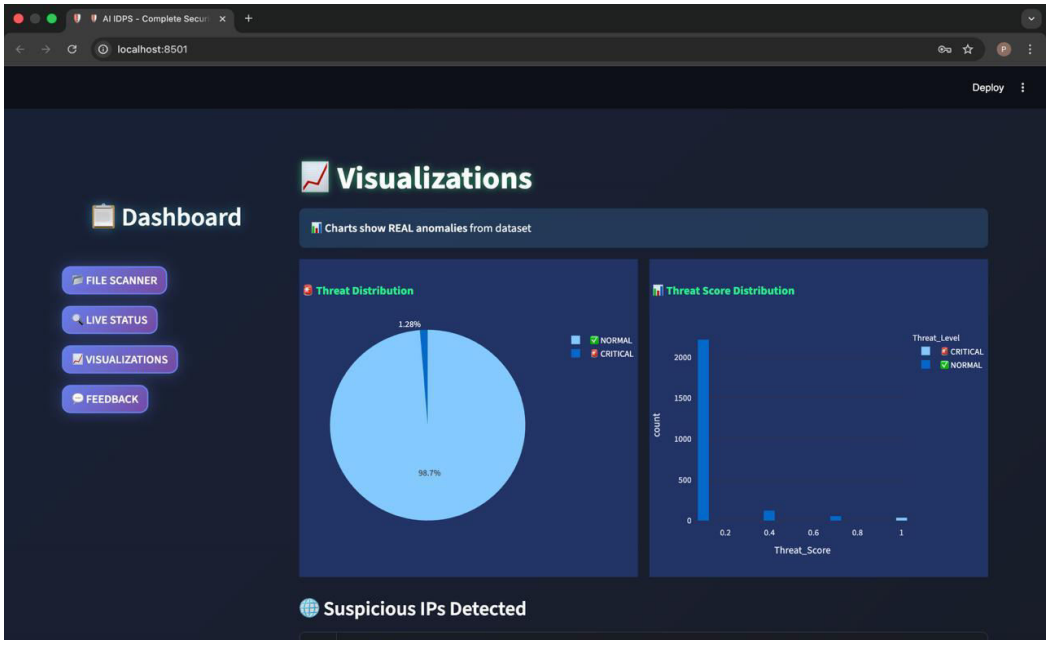
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|



REAL-TIME MONITORING



THREAT ANALYSIS VISUALIZATION

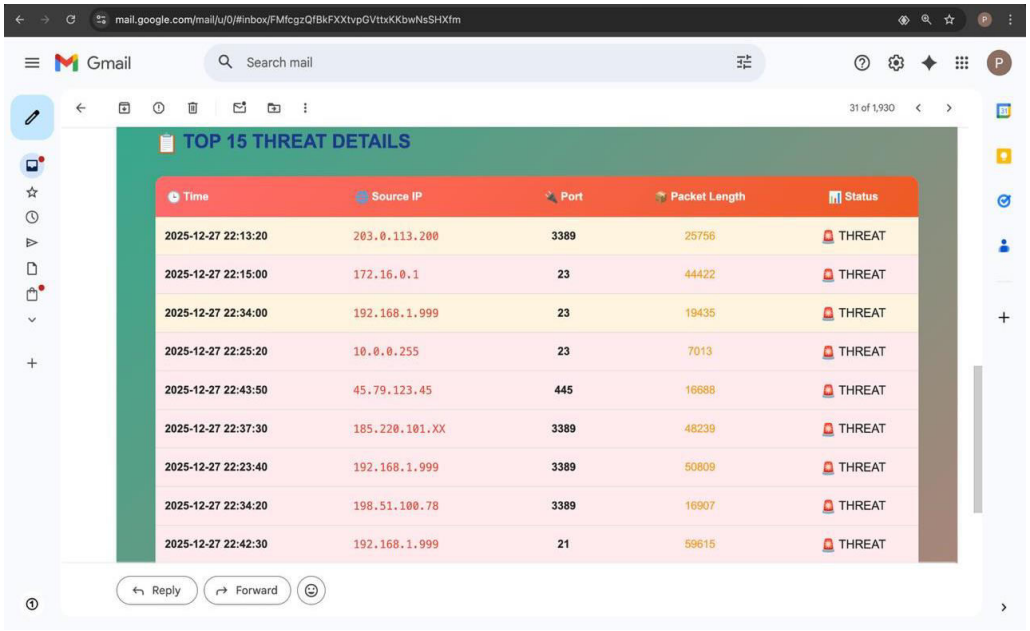
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|



EMAIL THREAT NOTIFICATION

VII. CONCLUSION AND FUTURE SCOPE

The Intrusion Detection and Prevention System (IDPS) developed in this project addresses the increasing challenges of network security and cyber threats in modern digital environments. By integrating machine learning techniques with real-time network monitoring, the system provides a proactive solution for detecting and preventing malicious activities. The use of the XGBoost algorithm enables accurate analysis of network traffic patterns and helps classify traffic as normal or malicious based on behavioral characteristics. The system also includes automated prevention features such as blocking attacker IP addresses, generating alerts, and maintaining detailed logs for analysis and auditing. In addition, the web-based dashboard provides administrators with clear visualization of network activity and detected threats. Overall, the proposed IDPS offers an efficient, scalable, and intelligent approach to improving network security and protecting systems from potential cyberattacks. Although the proposed IDPS demonstrates effective detection and prevention capabilities, it can be further enhanced in several ways. Future improvements may include integrating advanced machine learning and deep learning techniques such as neural networks or random forest models to improve detection accuracy and identify more complex attack patterns. The system can also be expanded to support large-scale enterprise networks and cloud environments, allowing it to monitor traffic from multiple distributed sources. Incorporating real-time threat intelligence and external security databases can enable the system to continuously learn and adapt to new cyber threats. Additionally, future versions may include enhanced visualization dashboards, mobile alerts, and integration with Security Information and Event Management (SIEM) systems to provide faster response and stronger cybersecurity management.

REFERENCES

[1] Chen, T., & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.
https://doi.org/10.1145/2939672.2939785
[2] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. IEEE Symposium on Computational Intelligence for Security and Defense Applications.
https://doi.org/10.1109/CISDA.2009.5356528
[3] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503114|

https://doi.org/10.5220/0006639801080116
[4] 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
[5] Scapy Development Team (2023). Scapy: Packet Manipulation for Network Security Monitoring.https://scapy.net

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details