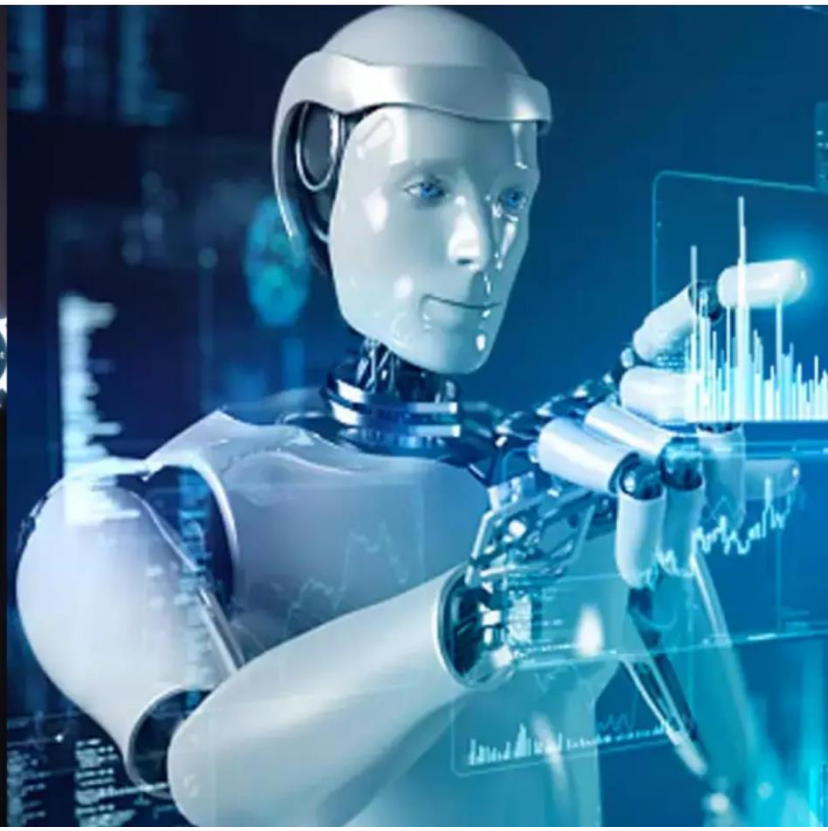
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 4, April 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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|

AI Driven Intrusion Detection and Prevention System (IDPS)

P. Srinivasa Rao[1], CH.Upendra[2], Y.Sai Prasad Reddy[3], N.Teja[4], D.Larshan[5]

Associate Professor, Department of CSE, ACE Engineering College, Hyderabad, India[1]

Department of CSE, ACE Engineering College, Hyderabad, India [2,3,4,5]

ABSTRACT: In recent years, the use of internet-based services and networked systems has increased rapidly. This growth has also led to a rise in cyber threats such as hacking, malware attacks, and unauthorized access. Because of this, securing network infrastructure has become a major concern for organizations and individuals. Traditional security tools like firewalls and rule-based intrusion detection systems are limited in their ability to detect new and unknown attacks. They mainly rely on predefined signatures and rules, which makes them ineffective against modern and evolving threats.

To address this issue, this project presents an Intrusion Detection and Prevention System (IDPS) based on machine learning. The system uses the XGBoost algorithm to analyze network traffic and classify it as normal or malicious. It continuously monitors packets flowing through the network and extracts key features such as IP address, protocol type, and traffic patterns.

When suspicious activity is detected, the system automatically blocks the attacker's IP address and sends alerts to the administrator. A web-based dashboard is developed using Flask to display real-time network activity and alerts. The system also maintains logs for further analysis and security improvement.
This approach increases detection accuracy, reduces response time, and provides better protection against both known and unknown cyber threats.

I. INTRODUCTION

With the advancement of technology, computer networks have become an essential part of everyday life. People and organizations use networks for communication, storage, and various business operations. However, this increased dependence also makes systems more vulnerable to cyberattacks.

Cyber threats such as phishing, malware, denial-of-service attacks, and unauthorized access are becoming more common. Traditional security systems like firewalls and signature-based intrusion detection systems are not sufficient to handle these modern threats. These systems can only detect attacks that match known patterns and fail when new types of attacks occur.

To overcome these limitations, there is a need for intelligent systems that can learn and adapt. Machine learning provides a powerful solution by analyzing patterns in data and identifying unusual behavior.

In this project, we design and implement an Intrusion Detection and Prevention System using machine learning. The system continuously monitors network traffic, analyzes data, and detects suspicious activities in real time. Once a threat is identified, it automatically takes action to prevent damage.The system also includes a user-friendly dashboard for monitoring network activity and alerts. This improves both security and usability.

II. EXISTING SYSTEM

Existing network security solutions mainly depend on firewalls and signature-based intrusion detection systems. These systems work by comparing incoming traffic with a database of known attack signatures.
Although these systems are effective for detecting known threats, they have several limitations:

- They cannot detect new or unknown attacks

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|

- They depend heavily on predefined rules
- They require frequent updates to stay effective

Another drawback is the lack of behavior analysis. These systems do not analyze how traffic behaves over time, making it difficult to identify unusual patterns.

In addition, most existing systems only generate alerts when a threat is detected. They do not take automatic action to stop the attack. This means administrators must manually respond, which can delay the response and increase the risk of damage.

Because of these limitations, traditional systems are not suitable for modern cybersecurity needs.

.

III. PROPOSED SYSTEM

The proposed system introduces a smart Intrusion Detection and Prevention System using machine learning techniques. Unlike traditional systems, this model does not depend only on predefined rules. Instead, it learns from data and identifies abnormal patterns in network traffic.

The system performs the following tasks:

- Continuously monitors network traffic
- Extracts important features from data
- Uses XGBoost algorithm for classification
- Detects both known and unknown attacks

Once a threat is detected:

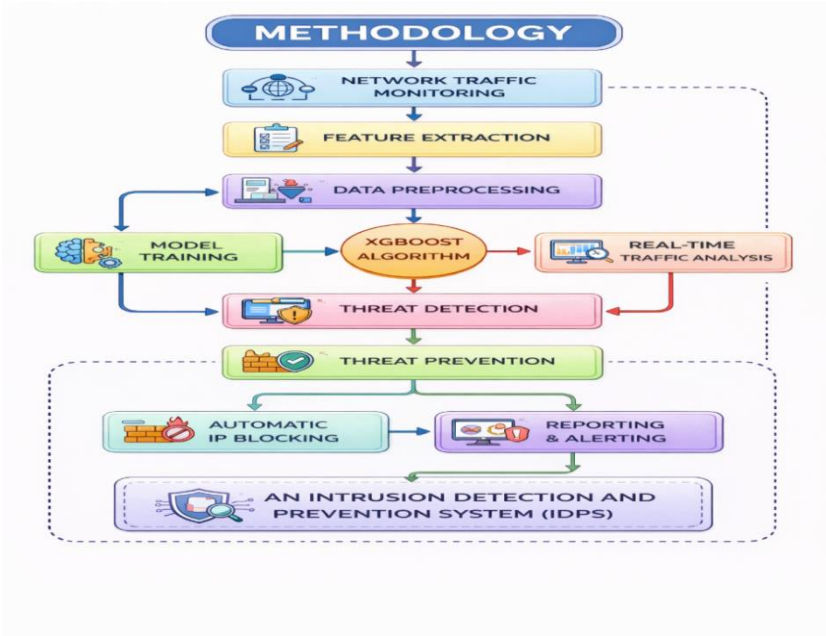
- The attacker's IP address is blocked automatically
- Alerts are sent to the administrator
- Attack details are stored for future analysis

A web dashboard is provided to visualize:

- Network traffic
- Alerts
- System performance

This system improves detection accuracy, reduces manual effort, and provides faster response to attacks.

IV. METHODOLOGY



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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|

i. Network Traffic Monitoring

The system continuously monitors all incoming and outgoing traffic. It captures packets and collects information such as:

- Source IP
- Destination IP
- Protocol type
- Packet size

This step helps in identifying unusual activities.

ii. Feature Extraction

After collecting data, important features are extracted. These include:

- Packet length
- Connection time
- Port numbers
- Traffic patterns

These features help the model understand the behavior of the network..

iii. Data Preprocessing

Before training, the data is cleaned and prepared:

- Duplicate data is removed
- Missing values are handled
- Data is converted into numerical form

This improves the performance of the machine learning model..

iv. Model Training

In this stage, the prepared dataset is used to train the machine learning model so that it can correctly identify normal and malicious network traffic.

First, the dataset is divided into two parts:

- **Training data** – used to train the model
- **Testing data** – used to check the model performance

The XGBoost algorithm is then applied to the training data. It learns patterns by analyzing different features such as packet size, protocol type, and connection duration. The model builds multiple decision trees step by step, where each new tree improves the accuracy of the previous one.

During training, the model adjusts its internal parameters to reduce errors in prediction. This process continues until the model reaches a good accuracy level.

After training is completed, the model is tested using unseen data to evaluate how well it can detect attacks. Performance metrics such as:

- Accuracy
- Precision
- Recall
- F1-score

are used to measure how effectively the model works.

This training process helps the system become intelligent and capable of identifying both normal and malicious traffic.

v. XGBoost Algorithm

XGBoost (Extreme Gradient Boosting) is a powerful machine learning algorithm used for classification and prediction tasks.

It works by combining multiple weak models (decision trees) to create a strong model. Each tree focuses on correcting the mistakes made by the previous trees. This process improves the overall accuracy of the system.

The main advantages of using XGBoost are:

- High accuracy in prediction
- Fast processing speed
- Ability to handle large datasets

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|

- Works well with structured data

In this project, XGBoost analyzes network traffic features and predicts whether the traffic is normal or an attack. Because of its efficiency and reliability, it is widely used in cybersecurity applications.

vi. Real-Time Traffic Analysis

After the model is trained, it is applied to real-time network traffic.The system continuously captures incoming packets and sends them to the trained model. The model analyzes each packet instantly and checks for abnormal behavior.

This process happens very fast, allowing the system to detect threats without delay. Real-time analysis is important because it helps stop attacks before they cause damage.The system keeps running continuously, ensuring constant monitoring of the network.

vii. Threat Detection

When the model detects unusual or suspicious behavior, it classifies the traffic as a threat.
The detection process is based on:

- Deviation from normal patterns
- Abnormal traffic flow
- Suspicious IP activity

The system may also identify the type of attack, such as:

- Unauthorized access
- Malware activity
- Network scanning

Once a threat is detected, the system immediately marks it and prepares for further action.

viii. Threat Prevention

After detecting a threat, the system takes immediate action to prevent damage.
Unlike traditional systems that only generate alerts, this system actively blocks harmful activity. Prevention actions may include:

- Stopping malicious packets
- Blocking suspicious connections
- Restricting access to the network

This automatic response reduces the time taken to handle attacks and improves overall security.

ix. Automatic IP Blocking

One of the key features of this system is automatic IP blocking.
When a malicious source is identified, the system adds the attacker's IP address to a block list using firewall rules. This prevents the attacker from sending further requests to the network.
This process is fully automatic and does not require human intervention. It helps in quickly stopping repeated attacks from the same source.

x. Reporting and Alerting

The system keeps a complete record of all detected threats and actions taken.
It generates:

- Logs of network activity
- Details of detected attacks
- Information about blocked IPs

Alerts are sent to the administrator through:

- Dashboard notifications
- Email alerts (if configured)

These reports help administrators understand attack patterns and improve security measures in the future.

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

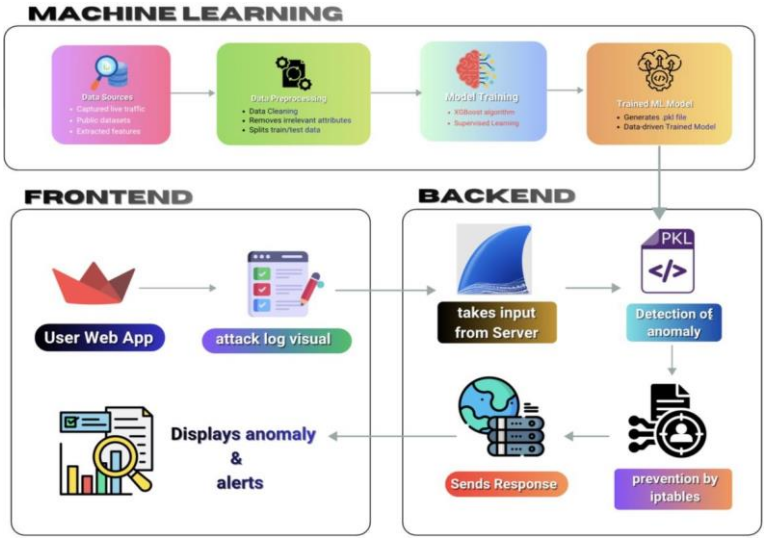
Impact Factor 8.699

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

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|

V. SYSTEM ARCHITECTURE

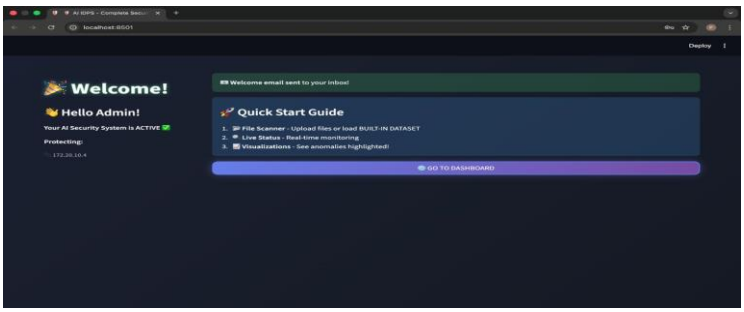


The system architecture of the Intrusion Detection and Prevention System (IDPS) is designed to provide real-time monitoring, analysis, and protection of network traffic using machine learning techniques. The architecture begins with a user-friendly web application through which the administrator can interact with the system. This interface displays important information such as attack logs, detected anomalies, and overall network activity in a clear and visual format. The web application communicates with the backend server, which acts as the central processing unit of the system.

The backend server receives data either from the network or user inputs and processes it before sending it to the trained machine learning model. The model, stored as a serialized (.pkl) file, is loaded into the system and used for prediction. It analyzes the incoming data using the XGBoost algorithm and determines whether the traffic is normal or malicious. If any abnormal behavior is detected, it is classified as an anomaly.

Once an anomaly is identified, the system triggers appropriate actions such as generating alerts and preparing for preventive measures like blocking the attacker's IP address. All detected threats and related information are stored in a database for future reference, analysis, and auditing. This stored data helps in understanding attack patterns and improving the system over time.Finally, the processed results, including detected anomalies and alerts, are sent back to the web application and displayed to the administrator. This allows continuous monitoring and quick decision-making. Overall, the architecture ensures smooth data flow between components, accurate threat detection using machine learning, and immediate response to potential cyber threats, making the system efficient and reliable for modern network security.

VI. RESULTS AND OUTPUT



SYSTEM INITIALIZATION

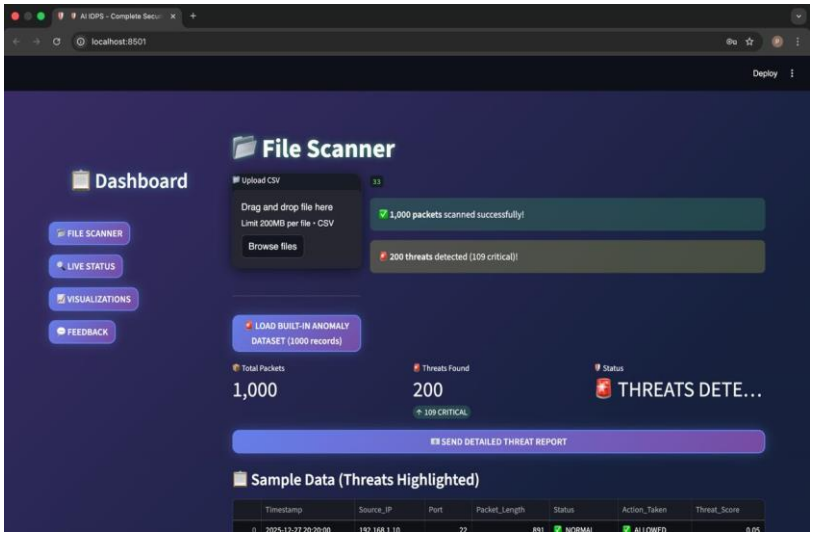
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

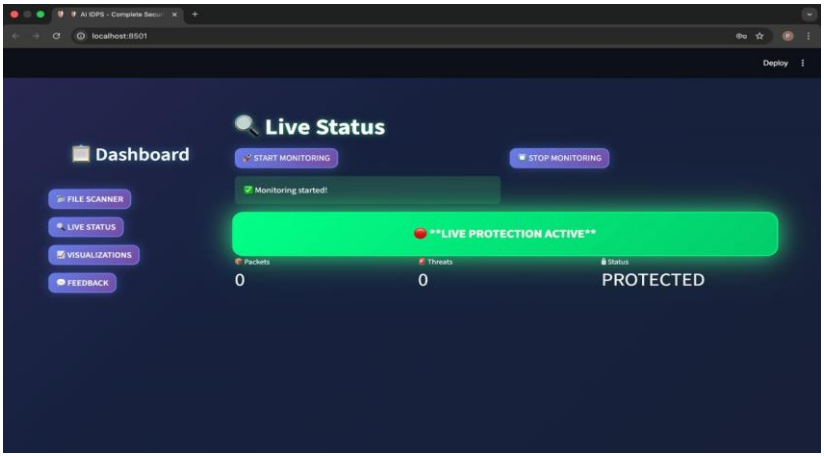
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

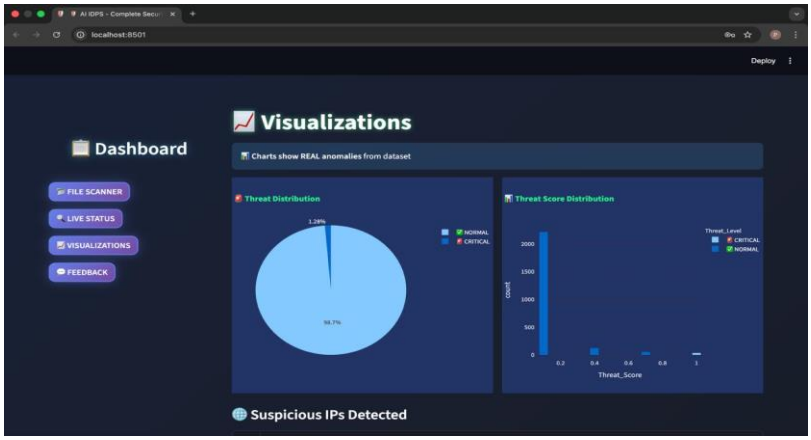
|DOI: 10.15680/IJIRSET.2026.1504037|



PACKET THREAT SCANNING



REAL-TIME MONITORING



THREAT ANALYSIS VISUALIZATION

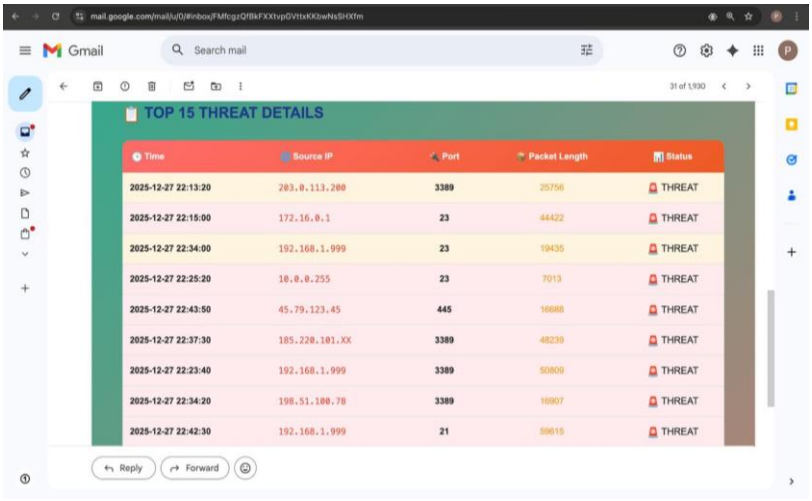
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

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

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|



EMAIL THREAT NOTIFICATION

VII. CONCLUSION AND FUTURE SCOPE

The Intrusion Detection and Prevention System (IDPS) developed in this project provides a smart and efficient solution for handling modern network security challenges. As cyber threats continue to grow in number and complexity, traditional security systems are no longer sufficient. This project successfully demonstrates how machine learning can be used to improve the detection and prevention of cyberattacks.

The system continuously monitors network traffic and analyzes it using the XGBoost algorithm. By learning patterns from data, it can accurately distinguish between normal and malicious activities. One of the key advantages of this system is its ability to detect not only known attacks but also new and unseen threats based on abnormal behavior.

Another important feature of the system is its automated response mechanism. When a threat is detected, the system immediately blocks the attacker's IP address and generates alerts for the administrator. This reduces the time required to respond to attacks and minimizes potential damage. The logging feature also helps in storing detailed information about attacks, which can be useful for future analysis and improving security strategies.

The web-based dashboard plays a significant role in making the system user-friendly. It provides real-time visualization of network traffic, detected anomalies, and system performance. This allows administrators to easily monitor the system and take necessary actions when required.

Overall, the proposed IDPS improves detection accuracy, reduces manual work, and provides faster response to threats. It is a reliable and scalable solution that can be used in different network environments. The project clearly shows how integrating machine learning with security systems can enhance protection against cyber threats.

Even though the current system performs effectively, there are many opportunities to enhance its capabilities in the future.
One possible improvement is the use of advanced deep learning techniques such as Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), or Recurrent Neural Networks (RNN). These models can analyze more complex patterns in network traffic and improve detection accuracy, especially for sophisticated attacks.

The system can also be extended to support large-scale and distributed environments such as cloud computing and enterprise networks. By integrating with cloud platforms, the system can monitor traffic from multiple sources and provide centralized security management.

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 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504037|

Another important enhancement is the integration of real-time threat intelligence. By connecting the system with external security databases and threat feeds, it can stay updated with the latest attack patterns and vulnerabilities. This will help the system adapt quickly to new cyber threats.

The user interface can also be improved further by adding advanced visualization tools, interactive dashboards, and mobile notifications. This will make it easier for administrators to monitor the system remotely and respond to threats quickly.In addition, the system can be integrated with Security Information and Event Management (SIEM) tools. This will allow better coordination between different security systems and provide a more comprehensive security solution.

Another future enhancement is the implementation of adversarial learning techniques. This will make the model more robust against attackers who try to bypass detection systems by manipulating input data.

Finally, the system can be optimized for better performance by reducing processing time and improving resource efficiency. This will make it suitable for real-time applications with high network traffic.With these improvements, the proposed IDPS can become a more powerful, intelligent, and scalable solution for protecting modern networks from evolving cyber threats.

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).
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