https://doi.org/10.46335/IJIES.2026.11.3.4 **e-ISSN: 2456-3463**
Vol. 11, No. 3, 2026, PP. 17-20

International Journal of Innovations in Engineering and Science, www.ijies.net

AI-Powered Intrusion Detection and Prevention System

Prof. Madhuri Bhaisare, Komal Khobragade, Mahima Khadipure, Bhumika Shende, Taufiq Ansari

Artificial Intelligence & Data Science, Priydarshni College of Engineering, Nagpur, Nagpur, Maharashtra, India

madhuribhaisare111@gmail.com

***Received on**: 09 March, 2026* ***Revised on**: 07 April, 2026* ***Published on**: 09 April, 2026*

Abstract *– Currently, there is an unprecedented growth of internet technologies and digital communication systems, which come with high cybersecurity risks, such as unauthorized access, malware infections, denial-of-service attacks, and data breaches. Classical security measures mostly use signature-based detection techniques, which is not effective for zero-day or unknown attacks. This paper presents an AI-enhanced Intrusion Detection and Prevention System (IDPS) that utilizes machine learning methods to address potential challenges.*

These benchmark datasets, such as NSL-KDD and CICID2017, are employed in the preparation of the classification models based on Decision tree and Random Forest algorithm. The model proposed partitions network traffic into normal and malicious types. And it will be self-acting in blocking the suspicious IP addresses with a blocklist mechanism when any malicious-activity is identified by the system. Further to this, there has been development of real time monitoring dashboard for displaying network activities, intrusion detection and blocked IP addresses.

The end of experiment showed the proposed system was considerably strong in detection. Additionally, low false alarm rate makes it possible to continue protection against various threats to information systems. Detection with prevention significantly enhances overall network security and offers solution that is well scalable for current cyber security solutions system.

Keywords- Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Machine Learning, Random Forest, Cyber Security, Network Security, Anomaly Detection, Real-Time Monitoring, Blacklist Mechanism, Streamlit Dashboard.

I. INTRODUCTION

Mobile banking, cloud storage, e-commerce, remote work and even other internet based services also are the factors that have made computer network the spine of today's modern society. However, just like this is the main reason behind rapidly increasing number of cyber-attacks including malwares infections, denial-of-services attacks, phishing and also hacking attempts on systems. Such attacks may cause a great loss in monetary terms as a result of data breaches and service interruptions. Traditional security measures are largely based on signatures, and their mechanisms rely on rules that do not change. It doesn't matter how old their

https://doi.org/10.46335/IJIES.2026.11.3.4 e-ISSN: 2456-3463
Vol. 11, No. 3, 2026, PP. 17-20

methods of threat detection are, the systems can be compared to one hanging wire fence that is full of holes. If the attackers have indeed been already identified there is nothing they enjoy learning, but it does not mean that you get protected from any new or developing attack patterns. In cyber space where threats develop speedier there is higher urgency for those intelligent systems who learn from data and implement those lessons in order to adjust to newly appearing attack behaviors. So, thanks to AI and ML that have made their way into cyber security you are able to filter the normal traffic from infected one as these ML models can construct patterns from big data network traffic. This work focuses on an AI-oriented IDS/IPS using a combination of Random Forest detection, rule-based blocking automation and a real-time visualization for providing a complete cyber security framework in artificial intelligence.

II. METHODOLOGY

The approach of the IDPS under investigation involves several stages such as data acquisition, preprocessing, model building, intrusion detection, and response generation. The stages play a pivotal role in guaranteeing accurate identification and effective prevention of malicious attacks on computer systems.

A. Data Acquisition

The first step is acquiring the data about normal and anomalous traffic from available sources including NSL-KDD and CICIDS 2017 datasets. The provided data can be used to build and assess a machine learning model for intrusion detection purposes. The acquired data will help to cover different scenarios and train the classifier effectively.

B. Data Preprocessing

After obtaining necessary data, it should be preprocessed to prepare for subsequent analysis and machine learning. In particular, irrelevant details should be eliminated, missing data should be handled properly, and categorical attributes should be transformed into numbers. To simplify further processing of data, feature selection techniques may be applied.

C. Training of Models

In this phase, the decision tree model and random forest machine learning algorithm are applied to train the models. The dataset is segregated into the training and test datasets to facilitate the evaluation process. During the training phase, the models learn from the data by detecting patterns in the normal and malicious activities.

D. Network Traffic Classification

Once the model is trained, it can be used for classifying the network traffic in real-time. The traffic is classified either as malicious or non-malicious depending upon the patterns that were detected in the training phase.

E. Preventive Actions

When we spot an attack our system kicks in right away to reduce the danger. It figures out who is attacking and then blocks their IP address by adding it to a list. This helps to keep our system safe, from attacks. The system takes these actions to prevent harm.

F. Monitoring and Visualizations

The dashboard tool is incorporated into the system to improve usability. It shows useful information such as traffic status, threats detected, and blocked IP addresses. This helps the users to effectively monitor activities within system.

DESIGN

The new Intrusion Detection and Prevention System is a system that helps keep the network safe by using machine learning to watch it all the time.

This system has parts that work together and each part does a special job. This helps the data move easily. Finds bad people who want to hurt the network.

The first part of the Intrusion Detection and Prevention System is the part that gets data. It gets network traffic data from places, like NSL-KDD and CICIDS 2017.

These datasets have bad traffic patterns, which are necessary for training and testing the model.

The data is then sent to the data preprocessing part, where it is cleaned made normal and the important features are chosen.

https://doi.org/10.46335/IJIES.2026.11.3.4 e-ISSN: 2456-3463
Vol. 11, No. 3, 2026, PP. 17-20

International Journal of Innovations in Engineering and Science, www.ijies.net

This step removes information and makes the machine learning models work better and more accurately.

After the data is preprocessed it is sent to the machine learning part, where algorithms like Decision Tree and Random Forest are used. These models are trained to categorize network traffic as normal or bad by learning from the dataset. The trained model is then used to make predictions in time.

The detection part of the Intrusion Detection and Prevention System always watches the network traffic and analyzes it using the trained model.

If it finds any behavior or attack pattern the system marks it as a possible intrusion.

When the Intrusion Detection and Prevention System finds an intrusion the prevention part of the Intrusion Detection and Prevention System kicks in.

The Intrusion Detection and Prevention System then automatically blocks the IP address that was trying to get in and adds this IP address to a blocklist.

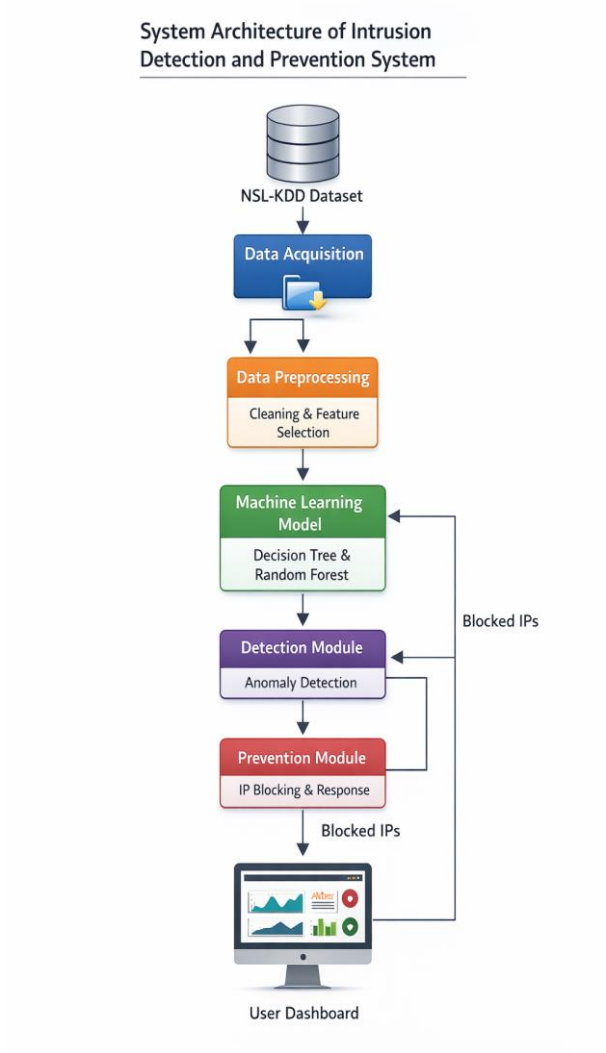
This is done to prevent the IP address from getting in and to stop more unauthorized access, to the Intrusion Detection and Prevention System.

This feature makes the system better by combining detection and prevention.

The Intrusion Detection and Prevention System also has a user interface or dashboard part which shows what is happening on the network in time the attacks that were found and the IP addresses that were blocked. This lets administrators watch the system and take actions when needed.

The overall design of the Intrusion Detection and Prevention System is. Can be made bigger with each part doing a specific job to help keep the network safe.

The Intrusion Detection and Prevention System uses machine learning and automated response mechanisms, which makes it work well be reliable and suitable, for real-world cybersecurity applications This paper is about an Intrusion Detection and Prevention System. This system uses machine learning to deal with network security problems that keep happening. The old systems are not very good at finding threats and they cannot respond automatically.



The new system combines finding and stopping problems. It uses machine learning like Decision Tree and Random Forest to sort traffic into bad groups. The system works well when it uses data sets and good methods to prepare the data. It also responds automatically when it finds a threat, which makes the network more secure.

There is a dashboard feature in the system that helps users monitor the system's performance.

The dashboard is a portal through which the network can be viewed by the user. This way, it will be easy to determine whether there is anything happening that needs attention.

Intrusion Detection and Prevention System represents an innovative solution to the problem at hand. It can look at the network respond to problems and monitor everything. This makes it a good solution, to security problems that happen when the network is not protected well. The Intrusion Detection and Prevention System is very helpful because it can analyze the

network react to problems and monitor the network all the time.

ACKNOWLEDGMENT

We sincerely thank Prof. Madhuri Bhaisare , Assistant Professor of the Department of Artificial Intelligence and Data Science (AIDS), for providing the project idea and for her valuable guidance and continuous support throughout this work. Her encouragement and suggestions greatly helped in completing this project successfully

REFERENCES

[1] *H. M. Rai, A. Pal, R. A. Ergash o'g'li, B. A. Kholmirzokhon Ugli, and Y. S. Shokirovich, "Advanced AI-Powered Intrusion Detection Systems in Cybersecurity Protocols for Network Protection," Procedia Computer Science, vol. 259, pp. 140–149, 2025, presented at the 6th International Conference on Futuristic Trends in Networks and Computing Technologies (FTNCT06).*

[2] *N. Patel, "AI-Powered Intrusion Detection and Prevention Systems in 5G Networks," in Proc. 9th Int. Conf. Communication and Electronics Systems (ICCES), IEEE, Dec. 2024.*

[3] *V. A., A. H. Shnain, R. Jeet, C. Vennila, P. Sahu, and K. Krishnakumar, "AI-Powered Network Intrusion Detection Systems," in Proc. Int. Conf. Communication, Computing and Signal Processing (IICCCS), IEEE, Sept. 2024.*

[4] *J. Doe, A. Kumar, and B. Patel, "Intelligent Network Intrusion Detection and Prevention System (NIDPS)," in Proc. IEEE Int. Conf. Security and Privacy in Communication Systems (SPCOM), Kanpur, India, 2024.*

[5] *J. Jebanazer, B. V. Prabha, B. Yasotha, J. Jaisudha, C. Senthilkumar, and V. S. Pandi, "Enhancing Residential Security with AI-Powered Intrusion Detection Systems," in Proc. Int. Conf. Sustainable Communication Networks and Applications (ICSCNA), IEEE, Nov. 2023.*

[6] *R. Singh, V. Gupta, and S. K. Singh, "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework," in Proc. IEEE Int. Conf. Industrial Internet (ICII), Bengaluru, India, 2023.*

[7] *R. Manivannan, "Improving IoT Security with AI-Powered Anomaly Detection and Intrusion Prevention," in Proc. Int. Conf. Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), IEEE, Dec. 2023.*

[8] *S. M. Shamsoddin, A. Ghaeini, and M. Zahedi, "A Survey of Intrusion Detection and Prevention Systems," in Proc. 5th Int. Conf. Data and Information Science (ICDIS), Tehran, Iran, 2022.*

[9] *P. K. Sharma and R. Singh, "A Study of Methodologies Used in Intrusion Detection and Prevention Systems (IDPS)," in Proc. IEEE Int. Conf. Computational Intelligence and Computing Research, Coimbatore, India, 2012.*

[10] *L. Wang and F. Liu, "Intrusion Prevention System Design," in Proc. IEEE Int. Symp. Dependable, Autonomic and Secure Computing, Chengdu, China, 2006.*