# AI-Powered Intrusion Detection System Using Machine Learning

**Gandham Rohan, Ch Harsha Vardhan Rao, *Dr. D. Koteswara Rao, Dr. D. Deepika***
*Department of Computer Science and Engineering (Data Science)*
*Mahatma Gandhi Institute of Technology, Hyderabad*
Emails: gandhamrohan19@gmail.com, harshachengalva@gmail.com, dkoteswararao_cse@mgit.ac.in, ddeepika_cse@mgit.ac.in

## Abstract

Cybersecurity is a worry today because digital communication systems, cloud platforms and network-based services are growing really fast. Old Intrusion Detection Systems (IDS) mostly use -defined signatures and static rules which makes them not very good at stopping new and changing cyber threats like DDoS attacks, probing attacks and people trying to get in without permission. These old systems have some limitations so we need smarter and more flexible security solutions. This paper talks about an AI-Powered Intrusion Detection System that uses Machine Learning to spot network traffic in real time. The system we propose uses Random Forest and Decision Tree algorithms to look at network traffic features and figure out if an attack is happening. We also have a web-based dashboard that lets you monitor traffic do batch analysis with CSV files see attack visualizations and get reports on predictions. We trained our system using known datasets like NSL-KDD, UNSW-NB15 and CIC-IDS2017. Our test results show that our system can detect attacks accurately with fewer false alarms and classify attacks more efficiently. The way our system is set up is modular and scalable which makes it good, for cybersecurity applications.

**Keywords**: *Intrusion Detection System, Machine Learning, Random Forest, Decision Tree, Cybersecurity, Network Traffic Analysis, DDoS Detection, Anomaly Detection, Real-Time Monitoring.*

## 1. Introduction

Computer networks and digital systems need cybersecurity to stay safe. Organizations are using cloud computing and online communication more and more so they are sending a lot of data over the internet. This means cyberattacks are happening often and are getting more complicated.

Traditional systems that detect intrusions mainly look for patterns and use fixed rules to find attacks.. These systems cannot find new threats or attacks that are changing.

New cyberattacks like Distributed Denial of Service and other types of attacks are always changing, which makes traditional security systems not work well. Also many security tools that companies use are expensive and hard to set up. They need experts to run them.

To fix these problems this paper talks about a kind of Intrusion Detection System that uses Artificial Intelligence and Machine Learning. The Cybersecurity system looks at network traffic. Tries to predict bad activities in real time. It uses Random Forest and Decision Tree algorithms to make sure it detects attacks correctly and does not give alarms. The system also has a web dashboard where you can see what is happening live look at CSV files see what attacks are happening and get reports on what it predicts.

The new Intrusion Detection System is a solution for schools and companies because it is affordable and can be used by many people, which makes it a good option for Cybersecurity. The proposed system is a cost- solution, for Cybersecurity environments.

## 2. Related Work

Machine Learning techniques have been used a lot in research about finding intruders over the ten years. At first people looked at data. Used statistics to find bad traffic patterns. Wu and his team came up with a system that could tell bad network activities apart using groups and types.

Shrivas and Dewangan made a model that used Random Forest and picked the features from the KDD99 and NSL-KDD datasets. Their model was better at finding intruders. Did not need as much computer power. Gaikwad and Thool made a system that used models together to improve how well it could classify attacks even when the data was not balanced.

Kasongo and Sun proposed a system that picked the features and used Machine Learning on the UNSW-NB15 dataset, which made it better, at classifying and working with new data. Hassan and his team later used a way to add more data to improve how well it could find rare attacks.

Although many systems can find intruders well there are still some problems like finding things that are not really there not being able to adapt quickly and using too much computer power. The new system wants to fix these problems by using Machine Learning models and a dashboard that is easy to use and it uses Machine Learning to make it work better.

## 3. System Design and Methodology

The AI-Powered Intrusion Detection System is designed using a modular and scalable architecture that enables efficient traffic analysis, attack prediction, and network monitoring. The system focuses on accurate detection, reduced false alarms, and real-time usability.

### 3.1 System Architecture

The proposed system consists of three major layers:

**Presentation Layer**

The presentation layer provides a web-based dashboard developed using Streamlit. It allows administrators to:

- Monitor network traffic
- Perform manual predictions
- Upload CSV files for batch analysis
- View attack reports and prediction results
- Analyze confidence scores

**Application Layer**

The application layer contains:

- Traffic preprocessing modules
- Feature extraction modules
- Machine Learning prediction engine
- Real-time capture modules
- CSV analysis modules

The Machine Learning engine uses Random Forest and Decision Tree algorithms for attack classification.

**Data Layer**

The data layer stores:

- Network traffic datasets
- Extracted features
- Trained Machine Learning models
- Prediction reports
- Historical prediction records

This architecture improves scalability, maintainability, and efficient data processing.

### 3.2 Data Preprocessing and Feature Extraction

Raw network traffic data is collected and converted into structured feature vectors. Important traffic-related features such as packet rate, byte rate, SYN flag count, forward packet length, backward packet length, and average packet size are extracted.

The preprocessing stage includes:

- Data cleaning
- Missing value handling
- Feature normalization

- Feature selection
- Label encoding

Feature importance ranking is performed using Random Forest feature importance analysis to select the most relevant network attributes for classification.

### 3.3 Machine Learning Detection Engine

The detection engine is developed using supervised Machine Learning algorithms, mainly:

- Random Forest Classifier
- Decision Tree Classifier

The Random Forest model is used as the primary prediction model because of its high accuracy, robustness, and ability to handle large datasets efficiently. Decision Tree algorithms assist in traffic classification and feature analysis.

The system is trained using benchmark cybersecurity datasets including:

- NSL-KDD
- UNSW-NB15
- CIC-IDS2017

The trained model can detect multiple cyberattacks such as:

- DDoS attacks
- DoS attacks
- Probe attacks
- R2L attacks
- U2R attacks
- SQL Injection attacks

The model continuously analyzes incoming traffic data and predicts whether the traffic is benign or malicious.

### 3.4 Alert Management and Dashboard

The proposed system includes a web-based dashboard developed using Streamlit for monitoring and analyzing network traffic predictions. The dashboard provides an easy-to-use interface where administrators can perform live predictions, upload CSV files for batch analysis, and visualize attack distributions.

The dashboard supports:

- Manual network traffic prediction
- CSV batch prediction
- Real-time traffic monitoring
- Attack severity visualization
- Prediction confidence analysis
- Downloadable prediction reports
- Secure login access

The system also maintains prediction logs and historical records for future analysis and evaluation.

## 4. Results and Discussion

The AI-Powered IDS was tested using benchmark cybersecurity datasets and deployed through a Streamlit-based web application. The system supports both single-input prediction and batch CSV analysis.

The single prediction module allows users to manually enter network traffic values and obtain:

- Attack prediction
- Confidence score

- Attack category
- Cause of attack
- Prevention methods
- Severity level

The batch prediction module processes uploaded CSV files containing multiple traffic records and generates prediction reports efficiently.

The proposed system successfully detected several cyberattacks including:

- DDoS attacks
- DoS attacks
- Probe attacks
- R2L attacks
- U2R attacks
- SQL Injection attacks

The Random Forest model achieved high classification accuracy with reduced false-positive rates. The dashboard interface simplified network monitoring and attack analysis, making the system suitable for practical cybersecurity applications.

**Table 1: Comparison of Related IDS Approaches**

| S.No | Method | Dataset | Architecture | Key Feature |
|---|---|---|---|---|
| 1 | Shrivas et al. | KDD99, NSL-KDD | Random Forest | Feature selection |
| 2 | Gaikwad et al. [8] | NSL-KDD | Bagging Ensemble | Improved classification |
| 3 | Kasongo & Sun [11] | NSL-KDD, UNSW-NB15 | Stacked Autoencoder | High generalization |
| 4 | Hassan et al. [9] | Custom | GAN + Classifier | Rare attack detection |
| 5 | Proposed System | NSL-KDD, UNSW-NB15, CIC-IDS2017 | Ensemble (CNN+LSTM+AE) | Adaptive, real-time, full-stack |

The proposed system provides a balance between accuracy, real-time performance, scalability, and usability.

## 5. Conclusion

This paper is about an AI-Powered Intrusion Detection System that uses Machine Learning to find people on the internet in real time. The system uses Random Forest and Decision Tree algorithms to figure out what is a cyberattack and what is not.

The AI-Powered Intrusion Detection System does a lot of things including:

- It can predict attacks in real time
- It can look at a lot of data at the same time
- It can tell what kind of attack is happening
- It can tell how sure it is about the attack
- It can make reports that you can download
- It has a dashboard that you can use to monitor the network

When we tested the AI-Powered Intrusion Detection System we found out that it is very good at finding cyberattacks and it does not make many mistakes. The system is also very flexible so it can be used in different kinds of networks.

In the future we might make the AI-Powered Intrusion Detection System better by:

- Moving it to the cloud
- Making it better at finding strange things

- Making it able to look at secret messages
- Making it better, at watching the network in real time
- Making the Machine Learning algorithms even better

These changes can make the AI-Powered Intrusion Detection System work even better and be able to handle more things.

## References

[1] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Computers & Security, vol. 92, 2020.

[2] V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," Computer Networks, vol. 136, pp. 37–50, 2018.

[3] S.-Y. Wu, E. Yen, "Data mining-based intrusion detectors," Expert Systems with Applications, vol. 36, no. 3, pp. 5605–5612, 2009.

[4] A. K. Shrivas and A. K. Dewangan, "An ensemble model for classification of attacks with feature selection based on KDD99 and NSL-KDD data set," International Journal of Computer Applications, 2014.

[5] D. P. Gaikwad and R. C. Thool, "Intrusion detection system using bagging ensemble method of machine learning," Procedia Computer Science, 2015.

[6] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," Journal of Big Data, 2020.

[7] M. Hassan, A. Iqbal, and S. Rahman, "GAN-based intrusion detection with data augmentation for class imbalance," *Computer Networks*, 2024.