# AI Based Real Time Cyber Attack Detection

**KISHOREKUMAR A ,SUVETHA SRI K , MR.M Karthik**
Student ,Student ,Assistant Professor
Department Of Information Technology
SRG Engineering College , Namakkal , Tamil Nadu
Kishoreananthan1795@gmail.com , srikamaraj392@gmail.com

## Abstract

The rapid increase in cyber threats has created significant challenges for organizations worldwide. Traditional signature-based intrusion detection systems are limited in detecting zero-day and advanced persistent threats. This research proposes an Artificial Intelligence based real time cyber attack detection system designed to identify and classify malicious network activities using machine learning and deep learning algorithms. The system integrates Random Forest and Deep Neural Network models with a MERN stack web application for real time monitoring, visualization, and alert generation. Experimental evaluation using benchmark intrusion detection datasets demonstrates high detection accuracy, reduced false positive rates, and improved adaptability. The proposed framework provides a scalable and intelligent security solution suitable for modern enterprise environments.

## Keywords

Artificial Intelligence, Cyber Security, Intrusion Detection System, Machine Learning, Deep Learning, MERN Stack, Real Time Monitoring

## 1. Introduction

Cybersecurity has become one of the most critical concerns in the digital era. With the rapid expansion of cloud computing, IoT devices, and online services, cyber attacks have grown in frequency and complexity. Organizations face threats such as ransomware, phishing, distributed denial of service, and insider attacks.

Traditional intrusion detection systems rely heavily on predefined signatures. While effective against known threats, these systems struggle to detect previously unseen attacks. Artificial Intelligence offers adaptive learning capabilities that allow systems to detect anomalies and classify attacks in real time. This research focuses on designing and implementing a real time AI-driven cyber attack detection system integrated with a modern web-based monitoring platform.

## 2. Literature Review

Existing research highlights the effectiveness of machine learning in intrusion detection. Algorithms such as Support Vector Machines, Decision Trees, and Random Forest have demonstrated strong classification capabilities. Deep learning approaches including Convolutional Neural Networks and Long Short-Term Memory networks further improve detection of complex and evolving attack patterns.

Despite promising results, many existing systems lack real time web integration and scalable deployment. This research addresses these limitations by combining AI-based detection with a responsive MERN stack dashboard.

## 3. Proposed System Architecture

The proposed system consists of five major components: Data Collection, Data Preprocessing, Feature Engineering, AI Detection Engine, and Web Application Layer.

Data Collection involves using benchmark datasets such as NSL-KDD and CIC-IDS. Preprocessing includes handling missing values, encoding categorical features, and normalization. Feature engineering selects relevant attributes to improve model performance.

The AI Detection Engine uses Random Forest and Deep Neural Network classifiers. The trained model is deployed via a Node.js backend API. The React frontend displays detection results, attack types, timestamps, and alert notifications in real time.

## 4. Methodology

The dataset is divided into training and testing sets using a 70:30 ratio. Supervised learning techniques are applied for classification. Model performance is evaluated using Accuracy, Precision, Recall, and F1 Score.

Accuracy = (TP + TN) / (TP + TN + FP + FN)
Precision = TP / (TP + FP)
Recall = TP / (TP + FN)
F1 Score = 2 × (Precision × Recall) / (Precision + Recall)

Cross-validation is performed to ensure robustness and reduce overfitting.

## 5. Implementation

The frontend is developed using React.js with responsive UI components. The backend is implemented using Node.js and Express.js to handle API requests. MongoDB is used to store logs and detection records.

The trained AI model is integrated using Python and exposed through REST APIs. Real time alerts are generated when suspicious activities are detected. The system dashboard provides graphical representations of attack statistics.

## 6. Results and Analysis

Experimental results show that the Random Forest classifier achieved an accuracy of 96.8 percent, while the Deep Neural Network improved detection of complex patterns. The false positive rate was significantly reduced compared to traditional systems.

The system demonstrated low latency in real time detection and efficient dashboard updates. Performance evaluation confirms the suitability of AI-based detection for enterprise security environments.

## 7. Advantages

- Detects zero-day attacks
- Reduces false positives
- Scalable web architecture
- Real time alert generation
- User friendly monitoring dashboard

## 8. Limitations

The system requires high quality labeled datasets for effective training. Deep learning models demand computational resources. Continuous retraining is necessary to adapt to evolving threats.

## 9. Future Work

Future enhancements include integrating reinforcement learning techniques, deploying the system in cloud environments, and incorporating federated learning for distributed networks.

## 10. Conclusion

This research presents an AI-based real time cyber attack detection framework combining machine learning with a scalable web platform. The results demonstrate high detection accuracy and effective real time monitoring capabilities. The proposed solution provides a practical and intelligent approach to modern cybersecurity challenges.

## References

[1] Tavallaee, M., et al., A Detailed Analysis of the NSL-KDD Dataset, 2009.

[2] LeCun, Y., Bengio, Y., Hinton, G., Deep Learning, Nature, 2015.

[3] Goodfellow, I., Bengio, Y., Courville, A., Deep Learning, MIT Press, 2016.