www.ijarp.com ISSN 2456-9992 Page: 01-08

International Journal Advanced Research Publications

Review Article

Volume: 02
Issue: 08

INTRUSION DETECTION SYSTEM WITH FORENSIC DATA LOGGING USING MACHINE LEARNING

G. P. Hegde*[1], Pradeep G. S.[2]

[1]Department of Information Science and Engineering

[2]Department of Computer Science and Enginering

SDM Institute of Technology, Ujire, Karnataka, India.

Article Received: 23 June 2026, Article Revised: 13 July 2026, Published on: 01 August 2026

***Corresponding Author: G. P. Hegde**

Department of Information Science and Engineering, SDM Institute of Technology, Ujire, Karnataka, India.

Doi: https://doi-doi.org/101555/ijarp.4877

ABSTRACT

The increasing dependence on digital networks and internet-based services has resulted in a significant rise in cyber threats and malicious activities. Traditional Intrusion Detection Systems (IDS) primarily rely on signature-based approaches, which are often ineffective against emerging and unknown attacks. This paper presents a Machine Learning-based Intrusion Detection System integrated with Forensic Data Logging for enhanced network security and post-incident analysis. The proposed system analyzes network traffic data using machine learning algorithms such as K-Nearest Neighbors (KNN) and Random Forest (RF) to classify network activities as normal or malicious. In addition to intrusion detection, the system maintains detailed forensic logs containing attack information, timestamps, protocol details, and prediction confidence scores. The system also generates real-time alerts and email notifications to facilitate rapid incident response. Experimental results demonstrate that the proposed approach effectively identifies suspicious activities while maintaining a comprehensive audit trail for forensic investigation. The integration of machine learning and forensic logging provides a scalable, intelligent, and legally supportive framework for modern cybersecurity environments.

KEYWORDS: Intrusion Detection System, Machine Learning, Network Security, Forensic Logging, K-Nearest Neighbors, Random Forest, Cybersecurity.

1. INTRODUCTION

Cybersecurity has become one of the most critical concerns in modern information systems due to the rapid growth of networked infrastructures, cloud computing, and Internet of Things (IoT) devices. Organizations continuously face threats such as malware attacks, denial-of-service attacks, unauthorized access, and data breaches. Traditional Intrusion Detection Systems (IDS) employ rule-based or signature-based techniques to detect known attacks; however, they struggle to identify new and evolving threats. Machine learning techniques have emerged as effective solutions for intrusion detection because of their ability to learn patterns from historical data and recognize anomalies in network traffic. Furthermore, forensic data logging is essential for preserving digital evidence, understanding attack patterns, and supporting post-incident investigations. This work proposes an intelligent Intrusion Detection System that combines machine learning-based threat detection with forensic data logging. The system provides real-time monitoring, intrusion classification, evidence collection, and automated alert generation, thereby enhancing overall cybersecurity preparedness.

2. Related Work

Several researchers have explored machine learning and deep learning approaches for intrusion detection systems. Yiping et al. [1] developed a Random Forest-based IDS integrated with reinforcement learning techniques and achieved an average detection accuracy of 96.93%. Jabez et al. [2] proposed an outlier detection approach using the Neighborhood Outlier Factor (NOF) to identify unknown attacks with reduced computational complexity. Kanimozhi et al. [3] introduced a cloud intrusion detection framework using Oppositional Tunicate Fuzzy C-Means clustering and achieved 80% detection accuracy. Al-Yaseen et al. [5] proposed a hybrid multi-level IDS combining Support Vector Machine (SVM) and Extreme Learning Machine (ELM) for hierarchical attack classification. Xiao et al. [8] utilized Principal Component Analysis (PCA), Auto-Encoders, and Convolutional Neural Networks (CNN) to improve intrusion detection accuracy on benchmark datasets. Vinayakumar et al. [14] designed a Deep Neural Network (DNN)-based IDS that demonstrated scalability across multiple intrusion detection datasets. Although these approaches improve detection performance, many existing systems lack integrated forensic logging capabilities. The proposed work addresses this limitation by combining intelligent intrusion detection with detailed forensic evidence collection.

3. Proposed Methodology

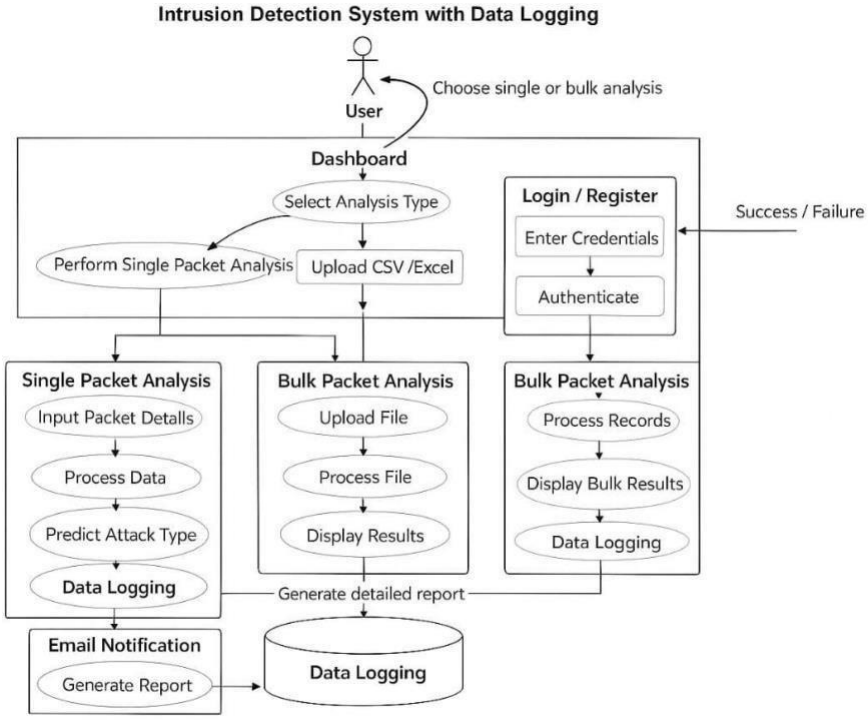

Figure 1: Proposed Frame Work.

The proposed work shown in Figure 1 focuses on the development of an intelligent Intrusion Detection System (IDS) integrated with forensic data logging using machine learning techniques. The system is designed to continuously monitor network traffic, identify malicious activities in real time, and maintain detailed forensic records for post-incident investigation. Unlike traditional signature-based IDS solutions, the proposed system is capable of detecting both known and previously unseen attacks by learning patterns from network traffic data. The implementation begins with the collection of network traffic from live network interfaces or benchmark datasets containing both normal and malicious activities. The collected data undergoes preprocessing, where irrelevant information is removed, missing values are handled, and important network features such as source IP address, destination IP address, protocol type, port numbers, packet size, connection duration, and traffic flags are extracted. The processed data is then normalized and converted into a suitable format for machine learning algorithms. To improve intrusion detection accuracy, machine learning algorithms such as K-Nearest Neighbors (KNN) and Random Forest (RF) are trained using labeled datasets. These models learn to distinguish between legitimate and malicious network behavior and classify incoming traffic accordingly. During real-time operation, newly captured network traffic is analyzed by the trained model, which predicts

whether the activity is normal or represents a cyberattack. The Intrusion Detection System interprets these predictions and identifies suspicious or confirmed intrusion attempts. A key contribution of the proposed system is the integration of a forensic data logging module. Whenever an intrusion is detected, the system automatically records comprehensive forensic evidence, including timestamps, source and destination IP addresses, protocol information, attack category, prediction confidence, and other relevant network parameters. These tamper-resistant logs provide valuable evidence for incident investigation, auditing, compliance verification, and future model improvement. Additionally, the system generates real-time alerts through the user dashboard and automatically sends email notifications to the network administrator, enabling rapid response to security incidents. To enhance usability, a secure login module restricts access to authorized administrators, while an intuitive graphical interface allows users to upload datasets, monitor network activities, view prediction results, manage forensic logs, retrain the machine learning model, and configure alert settings. The overall system combines intelligent intrusion detection with comprehensive forensic capabilities, providing an effective and scalable cybersecurity solution that supports both proactive threat detection and post-incident analysis.

Figure 2 shows the Single-Entry Prediction page of the Intrusion Detection System, where users can manually input network features. The interface provides options to predict intrusions using either the KNN or Random Forest algorithm. After submitting the values, the system displays the prediction result, indicating whether the connection is normal or intrusive.

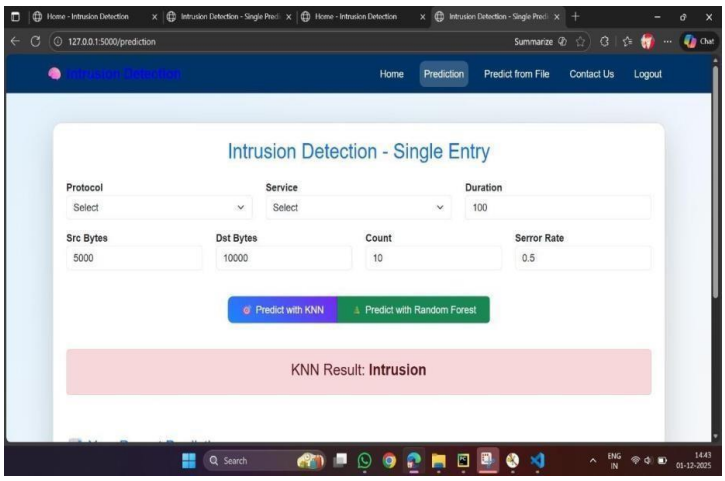

Figure 2: Manual Packet Entry.

Figure 3 shows the Data Logging section of the Intrusion Detection System, where recent prediction results are recorded. It displays key details such as date, algorithm used, protocol, service, prediction outcome, and probability. This feature helps users track previous analyses and maintain a history of intrusion detection activity.

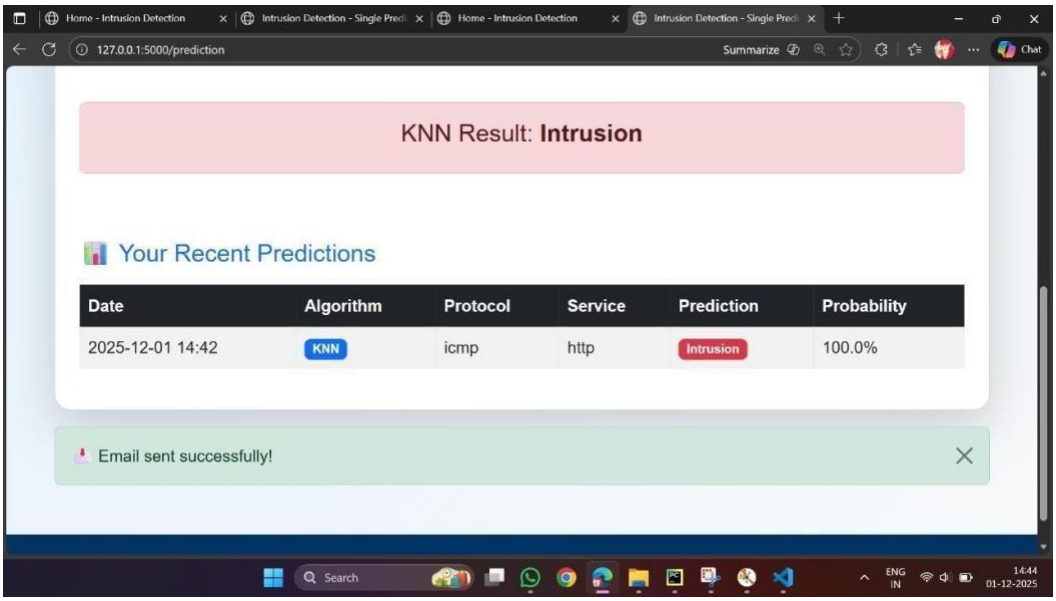

Figure 3: Data Logging.

Figure 4 shows the CSV File Prediction page of the Intrusion Detection System, allowing users to upload dataset files. It provides an option to select a CSV file containing network records for bulk intrusion analysis. After uploading, the system processes the data and predicts whether each entry is normal or intrusive.

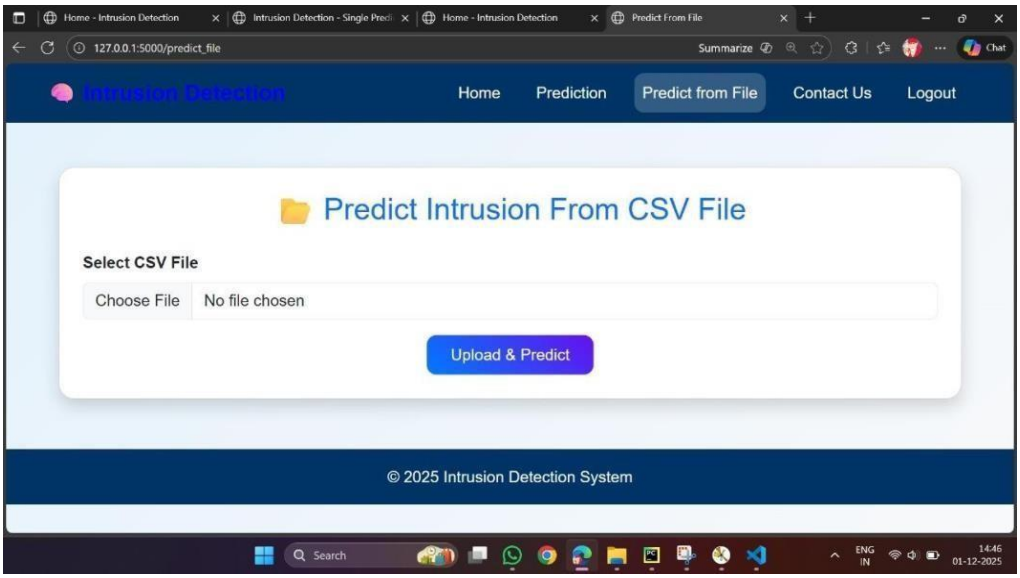

Figure 4: File Upload Page.

Figure 5 shows the CSV Prediction Results page of the Intrusion Detection System after a dataset is uploaded. The system displays a detailed table containing network feature values along with the predicted class for each entry. This allows users to analyze multiple records at once and identify normal and intrusive activities efficiently.

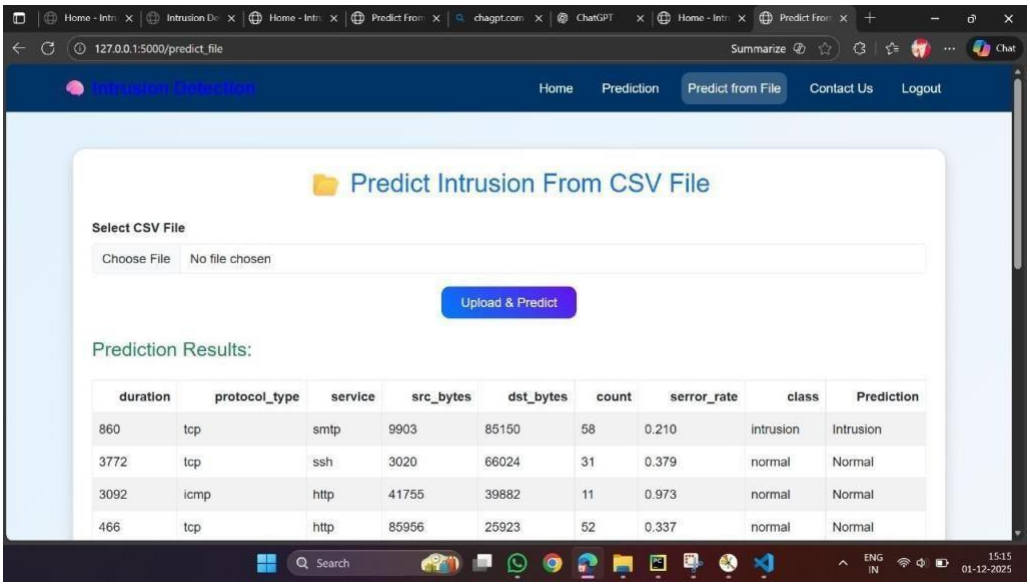

Figure 5: File Upload Prediction Results.

Figure 6 shows the email notification feature of the Intrusion Detection System, which sends prediction results to the user. The email includes the algorithm used and the intrusion detection outcome for the submitted data. This feature ensures users receive immediate alerts about potential security threats.

4. Experimental Results and Discussion

The proposed machine learning-based Intrusion Detection System (IDS) with integrated forensic data logging was successfully implemented using Python, Flask, Scikit-learn, Pandas, NumPy, and MySQL. The system provides secure user authentication, real-time intrusion detection, and automated forensic evidence collection through an intuitive web interface. Network traffic can be analyzed either by manually entering traffic parameters or by uploading CSV files, and both K-Nearest Neighbors (KNN) and Random Forest (RF) models accurately classify traffic as normal or malicious. Whenever an intrusion is detected, the system records detailed forensic information, including the prediction result, confidence score, protocol details, timestamp, and algorithm used, enabling effective incident investigation and historical analysis. In addition, automated email notifications promptly alert administrators about suspicious activities, allowing timely response to potential cyber threats.

Experimental evaluation demonstrates that the integration of machine learning with forensic logging enhances intrusion detection performance while providing reliable evidence for cybersecurity auditing and post-incident analysis. Overall, the proposed framework offers an efficient, scalable, and practical solution for modern network security applications.

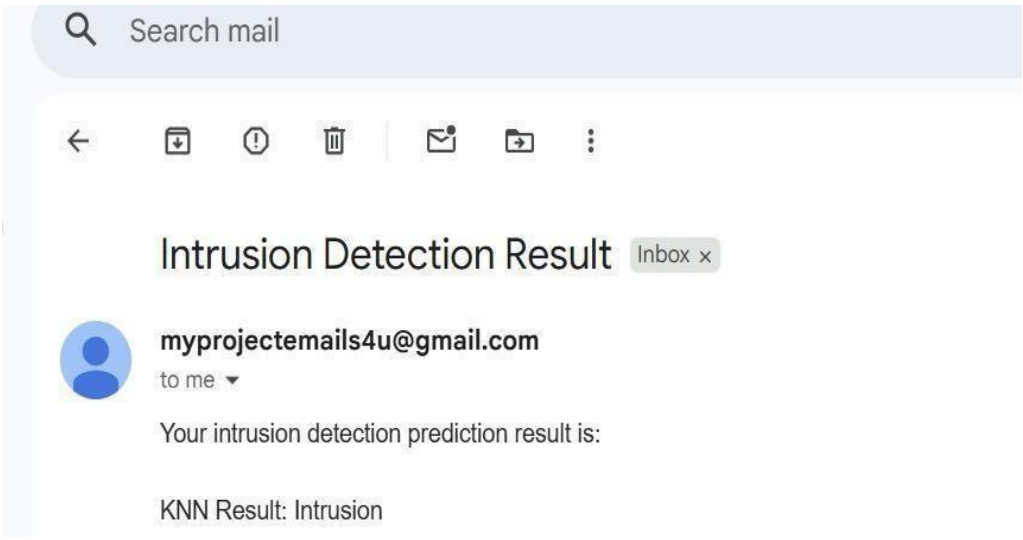

Figure 6: Alert Mail.

5. CONCLUSION AND FUTURE WORK

This paper presented a Machine Learning-based Intrusion Detection System integrated with forensic data logging for enhanced cybersecurity monitoring. The proposed system effectively detects malicious network activities using KNN and Random Forest algorithms while maintaining comprehensive forensic records for post-incident analysis. The inclusion of automated alerts and email notifications improves incident response capabilities.

Future work will focus on incorporating advanced deep learning techniques such as CNN, RNN, and LSTM models for improved detection accuracy. Additional enhancements include blockchain-based forensic logging, cloud deployment, IoT security integration, and automated threat response mechanisms.

REFERENCES

1. Yiping et al., “Intrusion Detection System for Wireless Networks Using Random Forest Algorithm,” 2023.
2. Jabez et al., “Outlier Detection-Based Intrusion Detection System,” Journal of Cybersecurity Research, 2022.
3. Kanimozhi et al., “Cloud Intrusion Detection Using Oppositional Tunicate Fuzzy C-Means,” International Journal of Computer Security, 2021.

4. Rohit et al., “Ensemble Learning for Network Intrusion Detection,” Springer Publications, 2019.
5. Al-Yaseen et al., “A Multi-Level Hybrid Intrusion Detection Model Using SVM and ELM,” Applied Computing Journal, 2018.
6. Gu et al., “Improved SVM-Based Intrusion Detection Using Naïve Bayes Feature Selection,” Cybersecurity Applications, 2020.
7. Pan et al., “Cloud-Based Wireless Network Intrusion Detection,” Symmetry, 2019.
8. Xiao et al., “CNN-Based Intrusion Detection Using PCA and Autoencoders,” IEEE Access, 2020.
9. Gao et al., “Ensemble Machine Learning for Intrusion Detection,” Symmetry, 2023.
10. Shone et al., “Deep Learning-Based Intrusion Detection Using Autoencoders and Random Forest,” Computers & Security, 2018.
11. Ali et al., “Fast Learning Network for Network Anomaly Detection,” University of Essex, 2018.
12. Dong et al., “Hybrid Clustering and SVM-Based Intrusion Detection,” Neural Computing, 2019.
13. Marir et al., “Deep Belief Networks for Intelligent Intrusion Detection,” Applied Intelligence, 2019.
14. Vinayakumar et al., “Deep Learning Approach for Intelligent Intrusion Detection Systems,” IEEE Access, 2019.
15. Elhefnawy et al., “Hybrid Nested Genetic-Fuzzy Algorithm for Attack Detection,” Lancaster University, 2022.