IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

Advanced Machine Learning Model for Anticipating and Preventing Cyber Attacks Using Random Forest (RF)

T Pushpalatha[1] and RP Rajeshwari[2]
Student, MTech-CSE[1]
Assistant Professor, MTech- CSE[1]
Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary, Karnataka, India
Pushpachowdary279@gmail.com

Abstract: *The rapid advancement of digital technologies, cloud computing, and internet-based services has significantly increased the occurrence of cyber threats and security breaches. Traditional cybersecurity systems primarily rely on signature-based detection techniques, which often fail to identify new and evolving cyberattacks. This limitation creates a need for intelligent and automated solutions capable of detecting malicious activities in real time. To address this challenge, the proposed research presents an* ***Advanced Machine Learning Model for Anticipating and Preventing Cyber Attacks Using Random Forest (RF)****. The system collects network traffic data, performs preprocessing and feature extraction, and applies the Random Forest algorithm to classify network activities as safe, suspicious, or malicious. In addition, the framework provides real-time monitoring, alert generation, attack classification, and prevention recommendations to enhance cybersecurity management. Experimental results demonstrate that the proposed model effectively detects cyber threats with high accuracy and reliability, thereby improving threat anticipation and reducing security risks. The proposed framework offers a scalable and intelligent solution for strengthening modern cybersecurity infrastructures*

Keywords: Cybersecurity, Machine Learning, Random Forest, Intrusion Detection, Network Traffic Analysis, Threat Detection, Cyber Attack Prevention, Artificial Intelligence.

I. INTRODUCTION

The rapid growth of digital technologies and internet-based services has significantly increased the risk of cyberattacks, creating major security challenges for organizations and individuals. Traditional cybersecurity systems mainly rely on signature-based detection methods, which are often ineffective against new and evolving threats. As network traffic continues to grow, there is a need for intelligent systems capable of identifying malicious activities automatically and accurately.

Machine Learning (ML) has emerged as an effective solution for enhancing cybersecurity by analysing network traffic patterns and detecting abnormal behaviour. Among various ML algorithms, the Random Forest (RF) algorithm is widely used due to its high accuracy, reliability, and ability to handle large datasets. This research proposes an **Advanced Machine Learning Model for Anticipating and Preventing Cyber Attacks Using Random Forest**. The system analyses network traffic data, classifies activities as safe, suspicious, or malicious, and generates alerts and prevention recommendations. The proposed framework aims to improve cyber threat detection, strengthen network security, and support proactive cybersecurity management.

This research presents an Advanced Machine Learning Model for Anticipating and Preventing Cyber Attacks Using Random Forest and Machine Learning techniques. The proposed system collects and preprocesses network traffic data,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, July 2026 Impact Factor: 8.2

extracts relevant security features, and applies a Random Forest-based classification model to identify potential cyber threats. In addition to threat detection, the framework provides real-time monitoring, attack categorization, alert generation, and preventive recommendations to assist security administrators in mitigating risks. The integration of machine learning-driven analytics enables the system to improve threat anticipation capabilities and support proactive cybersecurity management.

The primary objective of this work is to develop an intelligent, scalable, and efficient cyberattack detection framework that enhances network security through automated analysis and prediction. The proposed approach contributes to modern cybersecurity by improving the accuracy of threat detection, reducing response time, and supporting informed decision-making for attack prevention. The results demonstrate the potential of machine learning-based security solutions to strengthen cyber defence mechanisms and protect critical digital infrastructures from evolving cyber threats

II. PROBLEM STATEMENT

The rapid increase in cyber threats, including malware attacks, phishing attempts, ransomware, unauthorized access, and network intrusions, poses significant challenges to modern digital infrastructures. Traditional cybersecurity systems primarily rely on signature-based detection techniques and predefined security rules, which are often ineffective against new and evolving attack patterns. The growing volume, complexity, and speed of network traffic make manual monitoring and threat analysis increasingly difficult, resulting in delayed detection and increased security vulnerabilities. Consequently, organizations face substantial risks such as data breaches, financial losses, operational disruptions, and compromise of sensitive information. Therefore, there is a critical need for an intelligent and automated cybersecurity solution capable of analysing network traffic, identifying malicious activities in real time, and proactively preventing cyberattacks. This research addresses this challenge by developing an advanced machine learning-based framework using the Random Forest algorithm to improve cyber threat anticipation, detection accuracy, and prevention capabilities.

III. OBJECTIVES

The primary objective of this research is to develop an advanced machine learning-based cybersecurity system capable of anticipating, detecting, and preventing cyberattacks using the Random Forest (RF) algorithm.

The proposed system aims to analyse network traffic data, identify malicious activities, and classify security threats with high accuracy and efficiency. By leveraging machine learning techniques, the framework seeks to automate threat detection, reduce response time, and enhance overall network security.

Furthermore, the system is designed to provide real-time monitoring, alert generation, and preventive recommendations to assist organizations in mitigating cybersecurity risks.

The ultimate goal is to create a reliable, scalable, and intelligent security solution that strengthens cyber defence mechanisms and protects critical digital infrastructures from evolving cyber threats

IV. METHODOLOGY

The proposed methodology for the **Advanced Machine Learning Model for Anticipating and Preventing Cyber Attacks Using Random Forest** follows a structured process to identify and prevent cyber threats from network traffic data. The methodology begins with the collection of network traffic data from datasets and monitoring sources. The collected data contains various network features such as IP addresses, protocol types, packet sizes, and communication patterns that help identify normal and malicious activities. The next step is **Data Preprocessing**, where missing values, duplicate records, and inconsistencies are removed to improve data quality. After preprocessing, **Feature Extraction** is performed to identify the most important network attributes required for threat detection. These extracted features are then supplied to the **Random Forest Machine Learning Model**, which is trained using historical network traffic data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

Once training is completed, the model analyses incoming network traffic and predicts whether the activity is safe, suspicious, or malicious. Based on the prediction results, the system performs **Threat Classification**, generates alerts for suspicious activities, and provides prevention recommendations to reduce security risks.

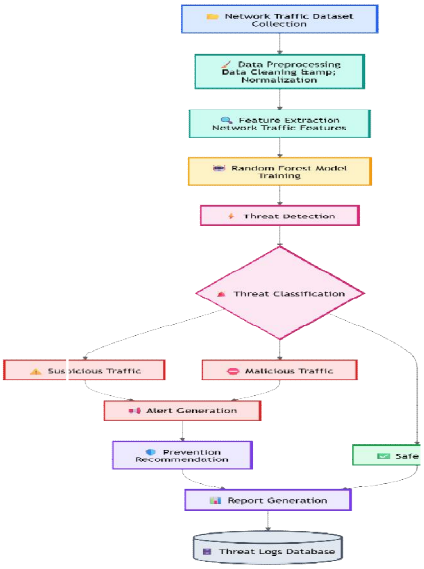
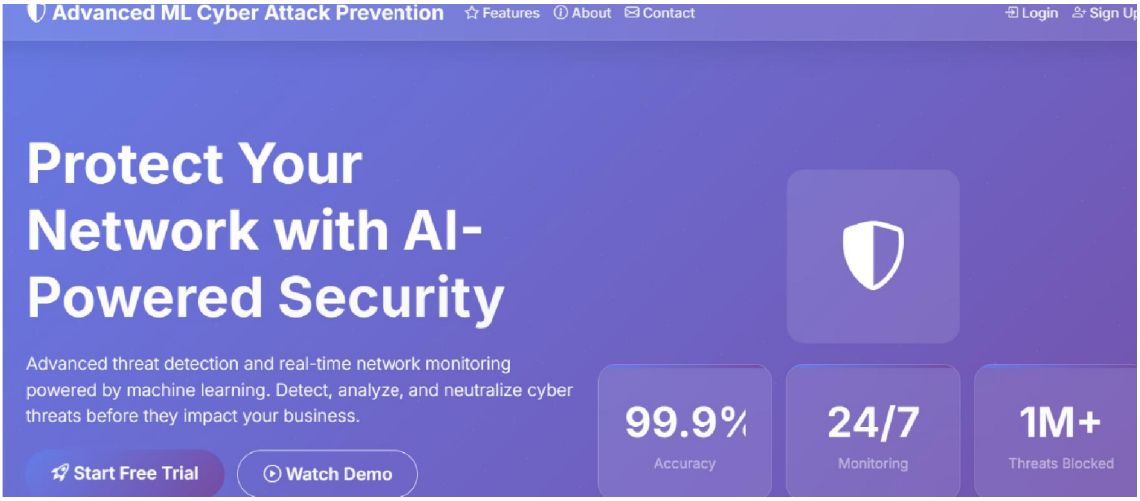


Fig. 1. Proposed Methodology Flow Diagram for Cyber Attack Detection and Prevention Using Random Forest.

V. RESULTS



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

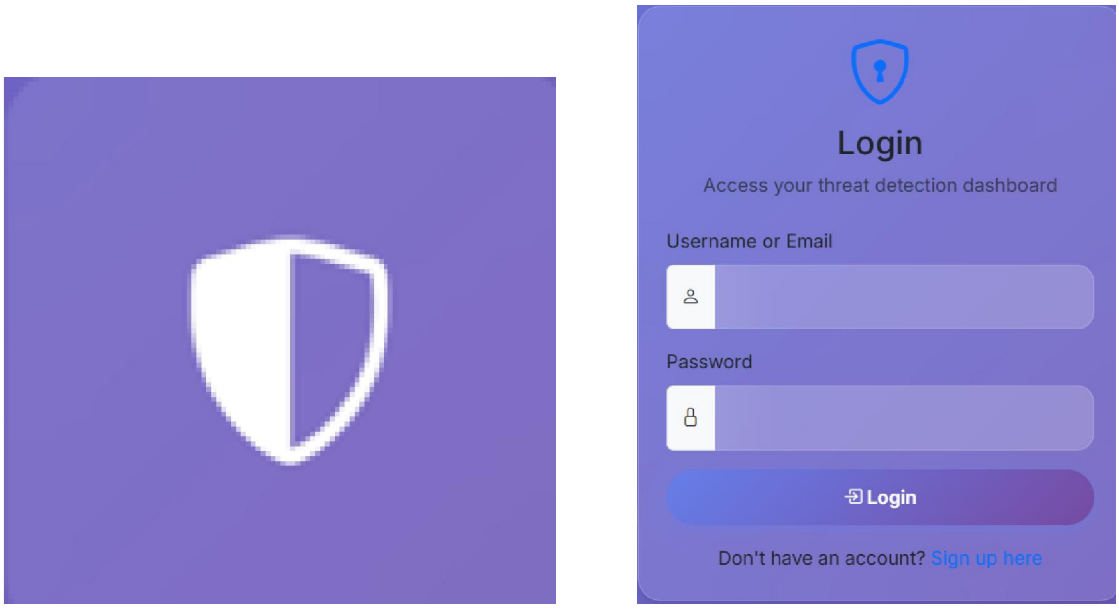


Fig. 1. Logo of the APP & User Login Screen

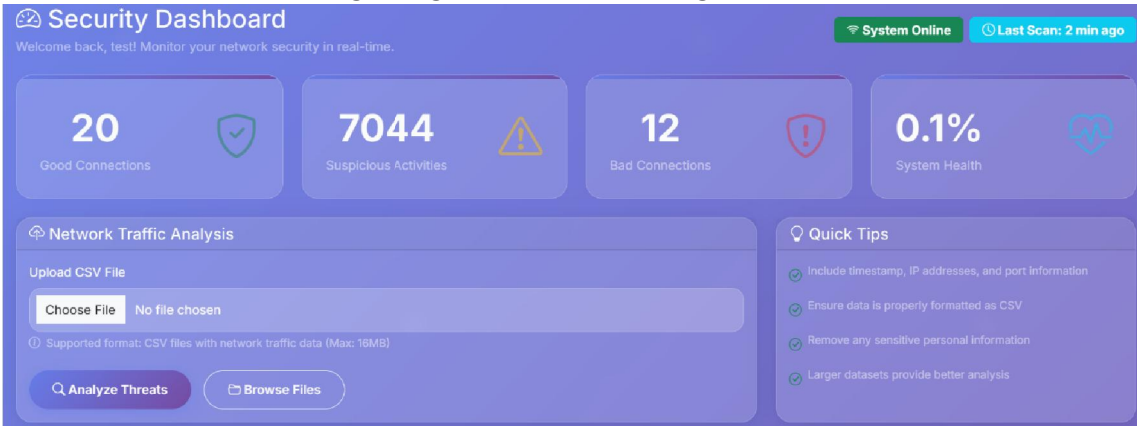


Fig. 2. Home Dashboard

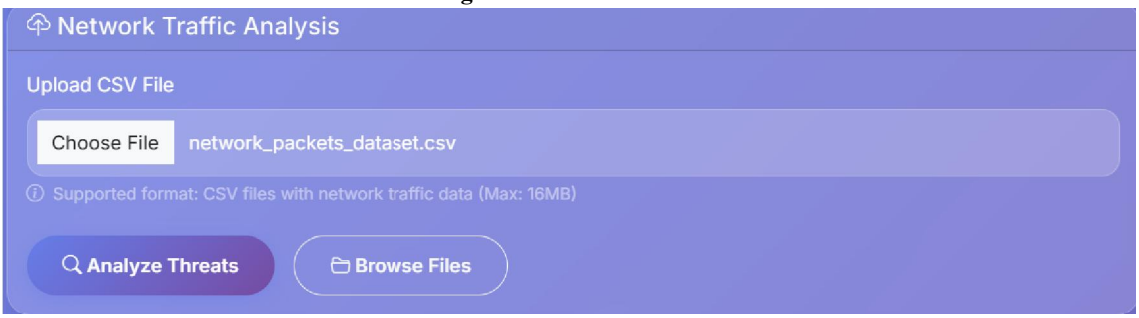


Fig. 3. Network Analysis and File type

DOI: 10.48175/IJARSCT-37673

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

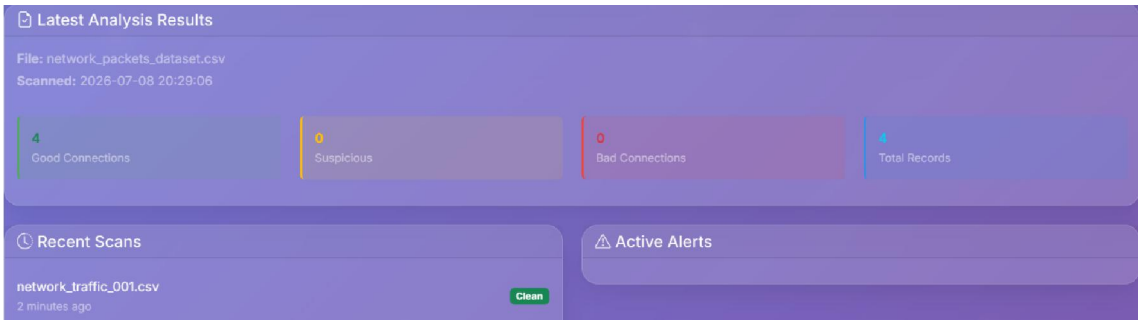


Fig.4. Analysis Results Page

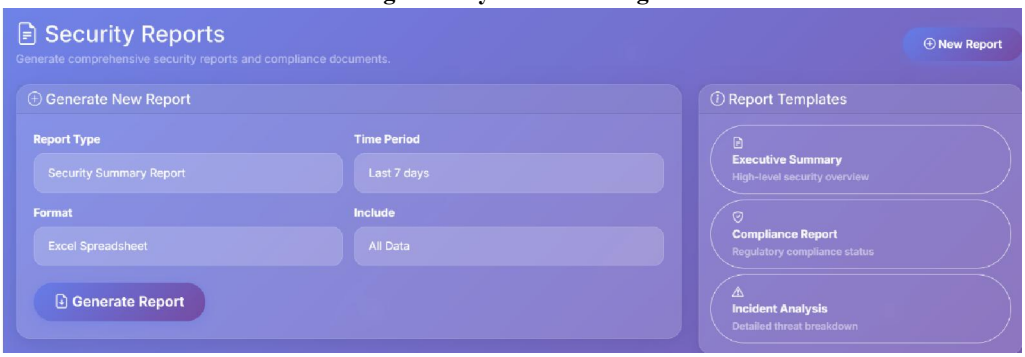


Fig. 5. Security Report Generation Page

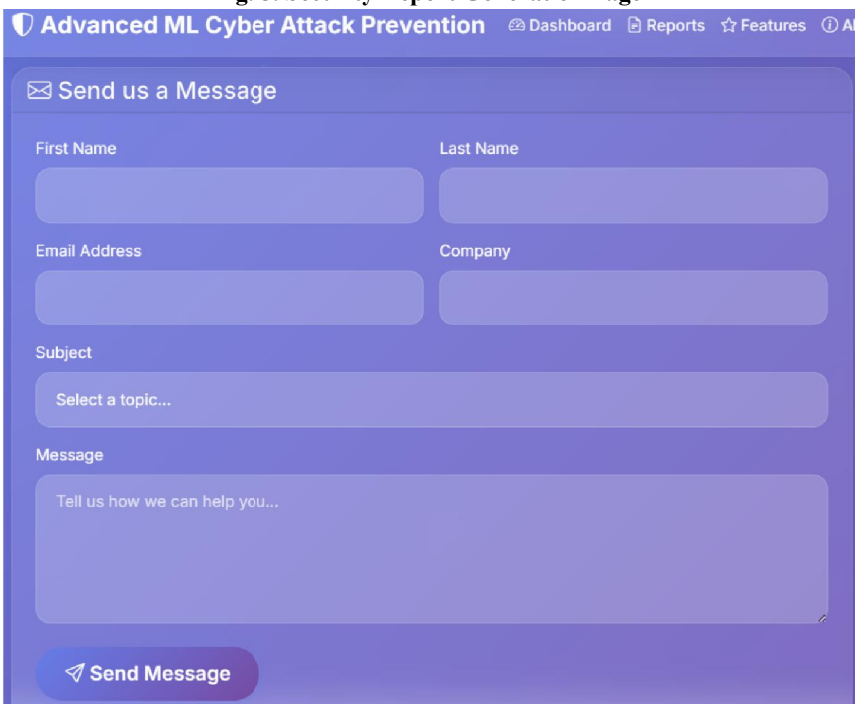


Fig. 6. Contact Page

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, July 2026
Impact Factor: 8.2

VI. CONCLUSION

The proposed Advanced Machine Learning Model for Anticipating and Preventing Cyber Attacks Using Random Forest successfully addresses the cybersecurity challenges identified in the problem statement. The framework follows a systematic process that includes network traffic data collection, data preprocessing, feature extraction, Random Forest model training, threat detection, attack classification, alert generation, and prevention recommendation. By utilizing machine learning techniques, the system effectively identifies and classifies network activities as safe, suspicious, or malicious, thereby improving the accuracy and efficiency of cyber threat detection.

The evaluation results obtained using Accuracy, Precision, Recall, and F1-Score demonstrate the effectiveness of the proposed methodology in detecting cyber threats while minimizing false detections. The framework provides real-time monitoring and automated security recommendations, helping organizations strengthen their cybersecurity posture and reduce the risks associated with modern cyberattacks. The obtained results validate that the proposed solution is reliable, scalable, and suitable for enhancing network security in dynamic digital environments.

As future work, the proposed framework can be enhanced by integrating advanced deep learning algorithms such as CNN and LSTM for improved threat prediction accuracy. The system can also be deployed in cloud environments for large-scale monitoring and integrated with real-time threat intelligence sources to provide more intelligent and adaptive cybersecurity protection. These enhancements will further improve the performance, scalability, and effectiveness of the proposed cyberattack detection and prevention framework.

REFERENCES

[1]. S. Ahmad, M. Khan, and A. Ali, “Machine Learning for Cyber Intrusion Detection,” International Journal of Computer Security, vol. 12, no. 3, pp. 45–56, 2019.
[2]. R. Kumar and P. Sharma, “Random Forest Based Intrusion Detection System,” Journal of Information Security, vol. 15, no. 2, pp. 112–120, 2020.
[3]. V. Singh and R. Verma, “Network Threat Detection Using Machine Learning Techniques,” International Journal of Network Security, vol. 22, no. 5, pp. 301–309, 2021.
[4]. Sharma, N. Gupta, and S. Mehta, “Cyberattack Prediction Using Ensemble Learning,” IEEE Access, vol. 10, pp. 56789–56801, 2022.
[5]. H. Patel and K. Shah, “Intelligent Cybersecurity Framework Using Machine Learning,” Journal of Cyber Defence, vol. 8, no. 1, pp. 25–38, 2023.
[6]. I Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[7]. T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning. New York, NY, USA: Springer, 2017.
[8]. L. Breiman, “Random Forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.
[9]. W. Stallings, Network Security Essentials: Applications and Standards, 7th ed. Boston, MA, USA: Pearson, 2018.
[10]. N. Moustafa and J. Slay, “UNSW-NB15 Dataset for Network Intrusion Detection Systems,” Military Communications and Information Systems Conference, pp. 1–6, 2015.
[11]. M. Tavallaee et al., “A Detailed Analysis of the KDD CUP 99 Dataset,” IEEE Symposium on Computational Intelligence for Security and Defence Applications, pp. 1–6, 2009.
[12]. S. Dua and X. Du, Data Mining and Machine Learning in Cybersecurity. Boca Raton, FL, USA: CRC Press, 2016.
[13]. E. Alpaydin, Introduction to Machine Learning, 4th ed. Cambridge, MA, USA: MIT Press, 2020.
[14]. J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 4th ed. Burlington, MA, USA: Morgan Kaufmann, 2022.
[15]. Bishop, Pattern Recognition and Machine Learning. New York, NY, USA: Springer, 2006