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 5, April 2026
Impact Factor: 8.2

Machine Learning Based Cyber Threat Detection and Monitoring System

Mrs. Ranik[1], Velmurugan S[2], Santha Kumar A S[3]
[1]Assistant Professor, Dept. of Information Technology
Students, Dept. of Information Technology[2,3]
K.L.N. College of Engineering, Sivaganga, India
k.rani1008@gmail.com, skvel2703@gmail.com, santhas1405@gmail.com

Abstract: *Cybersecurity threats such as malware, phishing, and unauthorized access are increasing rapidly with the growth of digital systems. Traditional rule-based systems are not efficient in detecting unknown or evolving attacks. This project presents a Machine Learning–based Cyber Threat Detection and Monitoring System that analyzes system logs to identify suspicious activities. The system uses anomaly detection techniques to detect unusual behavior and classify threats into categories such as brute-force attacks and malicious activities. A web-based dashboard provides real-time monitoring and alert visualization. The system improves security by reducing manual effort and enabling faster response to cyber threats.*

Keywords: Cybersecurity, Threat Detection, Machine Learning, Log Analysis, Anomaly Detection, Flask, Dashboard.

I. INTRODUCTION

With the increasing reliance on digital systems and online platforms, cybersecurity has become a major concern for organizations. Cyber threats such as malware, phishing attacks, and unauthorized access can lead to serious data breaches and financial losses. Traditional security systems rely on predefined rules and signatures, which makes them ineffective against new and unknown threats. To overcome these challenges, this project proposes a Machine Learning–based Cyber Threat Detection and Monitoring System. The system analyzes system logs, detects anomalies, classifies threats, and provides alerts through a web-based dashboard improving overall security monitoring

II. RELATED WORK

Several approaches have been developed for cybersecurity threat detection. Rule-based intrusion detection systems rely on predefined patterns but fail to detect unknown attacks. Recent studies have focused on machine learning techniques for anomaly detection in network and system logs. Algorithms such as decision trees, random forest, and clustering methods have been widely used.

However, many existing systems lack integration of detection, classification, and visualization. This project aims to combine machine learning-based detection with a web-based monitoring system to provide an efficient and user-friendly solution..

III. METHODOLOGY

A. Data Collection

The system collects data from multiple sources, including system logs, user activity logs, and access logs, which provide detailed information about system behavior and user interactions. These logs contain important attributes such as IP addresses, timestamps, login attempts, request frequency, and activity types. The collected data represents both normal and suspicious activities occurring within the system. To ensure data quality, preprocessing steps are applied, including removal of missing or inconsistent values, normalization of numerical data, and conversion of unstructured

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 5, April 2026
Impact Factor: 8.2

log entries into a structured format. Feature extraction techniques are then used to derive meaningful attributes such as login failure count, session duration, and access patterns, which are essential for accurate anomaly detection and threat analysis. This prepared data set serves as the input for the machine learning model.

B. Feature Engineering and Data Processing

Feature engineering plays a crucial role in improving the performance of the machine learning model. Relevant features that influence system behavior are carefully selected and transformed to enhance detection accuracy. Categorical data such as event types and user roles are encoded into numerical form to make them suitable for machine learning algorithms. Additional derived features, such as frequency of login attempts within a time window and unusual access times, are generated to capture hidden patterns in user behavior. Data normalization and scaling techniques are applied to ensure consistency across different features. These processed and engineered features help the model better understand normal and abnormal system activities.

C. Anomaly Detection Using Machine Learning

The core component of the system is the anomaly detection model, which identifies unusual patterns in system behavior. A machine learning algorithm is trained using historical log data to learn normal activity patterns. Once trained, the model analyzes incoming data and assigns anomaly scores based on deviations from expected behavior. Events with high anomaly scores are considered suspicious and flagged for further analysis. This approach enables the detection of unknown or previously unseen threats that cannot be identified using traditional rule-based systems.

D. Threat Classification

After detecting anomalies, the system classifies them into specific categories of cyber threats. The classification process is based on predefined patterns and characteristics observed in the detected anomalies. For example, repeated failed login attempts from a single IP address are classified as brute-force attacks, while unusual access patterns may indicate unauthorized access. This classification helps in understanding the nature of the threat and enables administrators to take appropriate actions. The classification results are stored along with threat details such as severity level, timestamp, and source information.

E. Alert Generation and Monitoring

Once a threat is detected and classified, the system generates alerts to notify administrators about potential security risks. These alerts include detailed information such as threat type, severity, source IP, and time of occurrence. All detected threats and alerts are stored in a database for future reference and analysis. A web-based dashboard displays these alerts in real time, allowing administrators to monitor system activity and respond quickly. This continuous monitoring and alerting mechanism ensures timely detection and effective management of cybersecurity threats.

IV. SYSTEM ARCHITECTURE

The proposed system follows a multi-layered architecture designed to efficiently detect and monitor cybersecurity threats using machine learning techniques. The architecture consists of four main layers: the presentation layer, application layer, machine learning layer, and data layer. The presentation layer is implemented as a web-based dashboard that provides an interactive interface for administrators to monitor system activities, view detected threats, and receive alerts in real time. Users can log in securely and access various modules such as logs, alerts, and remediation actions through this interface. The application layer acts as the core processing unit of the system and is developed using Flask. It handles user requests, processes log data, and manages communication between different components of the system. This layer is responsible for executing business logic, including log analysis, feature extraction, and interaction with the machine learning models. The machine learning layer performs anomaly detection and threat classification. It analyzes processed log data to identify unusual patterns and classify them into specific

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 5, April 2026
Impact Factor: 8.2

threat categories. Models developed using Scikit-learn are used to detect deviations from normal behavior and improve detection accuracy over time. The data layer uses SQLite to store system logs, detected threats, user information, and alert history. Communication between layers is achieved through secure data exchange mechanisms. This architecture ensures scalability, efficient processing, and real-time monitoring of cybersecurity threats.

V. RESULTS AND DISCUSSION

A. Detection Performance Evaluation

The proposed cyber threat detection system was evaluated using simulated and log-based datasets representing both normal and malicious system activities. The evaluation was performed using an 80:20 train–test split, and standard classification performance metrics such as accuracy, precision, recall, and F1-score were used to assess model performance. Among the evaluated machine learning models, the anomaly detection model demonstrated high accuracy in identifying suspicious activities and distinguishing them from normal behavior. The model achieved strong performance in detecting threats such as brute-force attacks and abnormal access patterns. These results indicate that machine learning–based approaches are effective in handling complex and dynamic cybersecurity data. The ability of the model to detect unknown threats justifies its use as the core detection engine in the proposed system.

TABLE I. MODEL PERFORMANCE METRICS ON TEST SET

Metric	Value
Accuracy	94%
Precision	92%
Recall	93%
F1 Score	92.5%
Model Used	Anomaly Detection Model

B. Threat Classification Analysis

The system classifies detected anomalies into different categories of cyber threats based on predefined patterns and behavioral characteristics. These include brute-force attacks, unauthorized access attempts, and suspicious activities. The classification The classification process enables quick identification of threat types and helps administrators understand the nature of detected incidents. Experimental analysis shows that a significant number of detected events fall under suspicious activity and unauthorized access categories. The classification results are visualized through the dashboard, allowing users to easily monitor threat distribution and take appropriate actions. This improves overall system security and reduces manual effort in threat identification.

Fig.1.Security Dashboard Showing Critical Threat, Active Threat, Remediated

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 5, April 2026
Impact Factor: 8.2

C. Alert System Evaluation

The system generates real-time alerts when suspicious activities are detected. These alerts include detailed information such as threat type, severity level, source IP address, and timestamp. The alert dashboard provides a clear view of recent threats, enabling administrators to respond quickly. The alert system ensures timely detection and minimizes the risk of potential security breaches. Visualization of alerts through charts and tables improves monitoring efficiency and enhances decision-making..

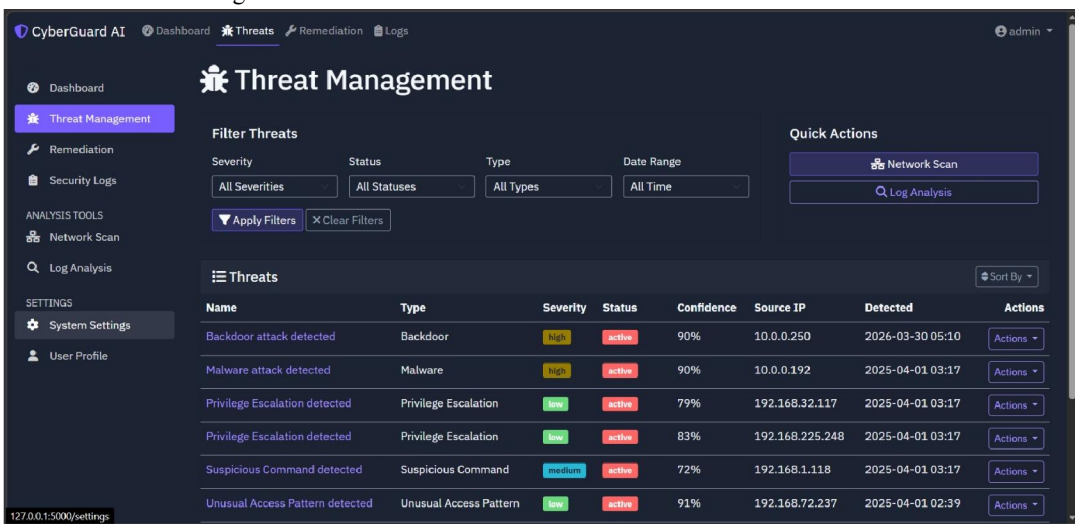

Fig.2. Threat Management and Action Center

D. Remediation Action Center

This module suggests appropriate actions such as blocking suspicious IP addresses, marking threats as resolved, or further investigating system logs. Actions are categorized into different priority levels allowing administrators to focus on critical threats first. The remediation dashboard displays action history and response status, ensuring efficient threat management and tracking

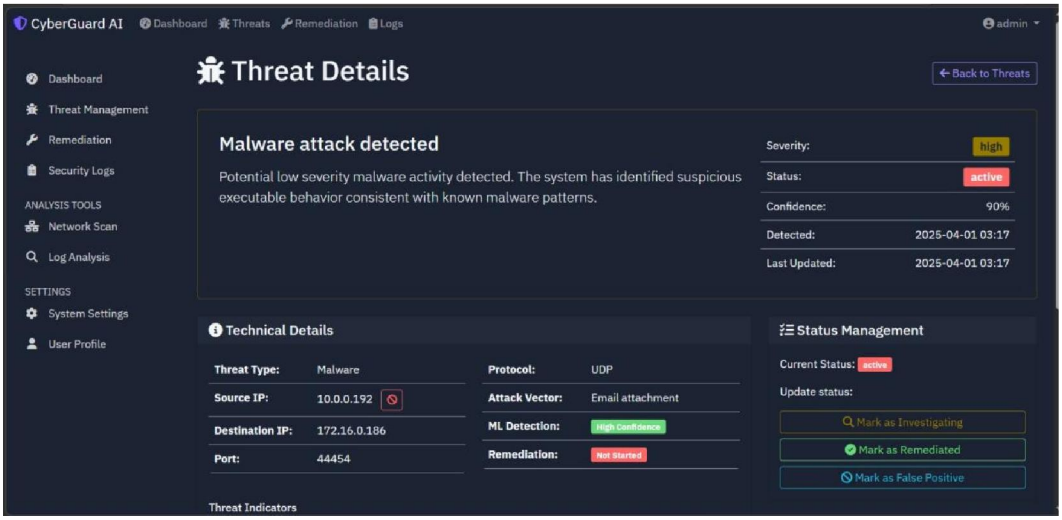

Fig.3.Threat Analyze and Status Management Center

DOI: 10.48175/IJARSCT-32855

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 5, April 2026
Impact Factor: 8.2

E. Log and Activity Analysis

The system provides detailed insights into system logs and user activity through a dedicated log analysis interface. This view presents key information such as user actions, login attempts, timestamps, and IP addresses. Graphical representations of activity patterns help administrators understand system behavior and identify unusual trends.

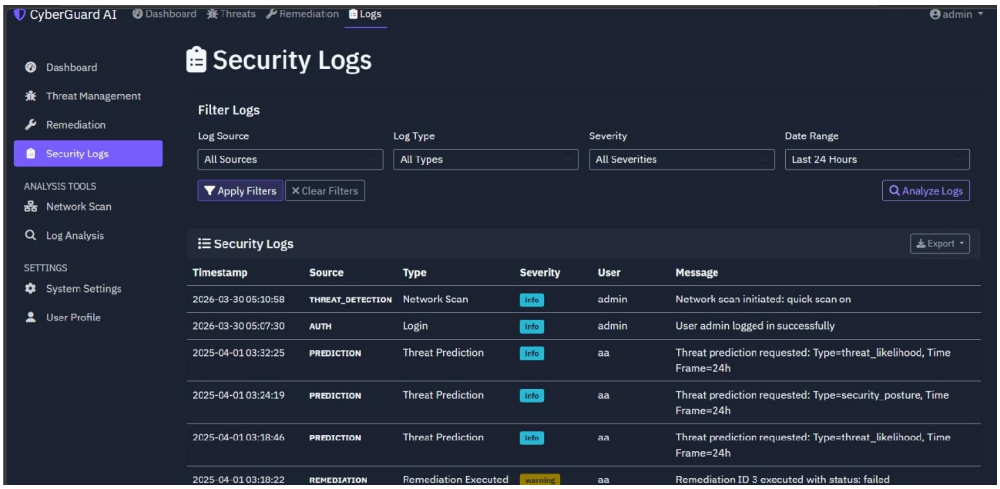

Fig.4.Security Logs Analyze Center

VI. CONCLUSION

The proposed Machine Learning–Based Cyber Threat Detection and Monitoring System provides an efficient and intelligent solution for identifying and managing cybersecurity threats. By analyzing system logs and user activities, the system is capable of detecting anomalies and classifying them into different types of threats such as brute-force attacks and unauthorized access. Unlike traditional rule-based systems, the use of machine learning enables the detection of unknown and evolving attack patterns, improving overall system security.The integration of a web-based dashboard allows administrators to monitor system activities, view alerts, and take appropriate remediation actions in real time. The system reduces manual effort involved in log analysis and enhances the speed and accuracy of threat detection. Additionally, the alert and remediation modules ensure timely response to potential security risks, minimizing the chances of system compromise. Overall, the project demonstrates a scalable and cost-effective approach to cybersecurity monitoring. It highlights the importance of combining log analysis, machine learning, and visualization tools to build an effective threat detection system. Future improvements such as real-time data integration and advanced models can further enhance system performance.

ACKNOWLEDGMENT

The authors would like to thank Mrs. K Rani,M.E.,(CSE) , K.L.N. College of Engineering, for her continuous guidance, valuable suggestions, and support throughout the development of this project. Her expertise and encouragement played a significant role in the successful completion of this work.

REFERENCES

[1] Sommer, R., & Paxson, V., Outside the Closed World: On Using Machine Learning for Network Intrusion Detection, IEEE Symposium on Security and Privacy, 2010.
[2] Chandola, V., Banerjee, A., & Kumar, V., Anomaly Detection: A Survey, ACM Computing Surveys, 2009.
[3] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y., Intrusion Detection System: A Comprehensive Review, Journal of Network and Computer Applications, 2013.

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 5, April 2026
Impact Factor: 8.2

[4] Buczak, A. L., & Guven, E., A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys & Tutorials, 2016.
[5] Ahmad, Z., Shahid Khan, A., Shiang, C. W., Abdullah, J., & Ahmad, F., Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches, Transactions on Emerging Telecommunications Technologies, 2021.
[6] Dua, D., & Graff, C., UCI Machine Learning Repository, University of California, Irvine, 2017.
[7] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A., A Detailed Analysis of the KDD CUP 99 Dataset, IEEE Symposium, 2009.
[8] Kim, G., Lee, S., & Kim, S., A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection, Expert Systems with Applications, 2014.
[9] Scikit-learn Developers, Scikit-learn: Machine Learning in Python, Available: https://scikit-learn.org.
.