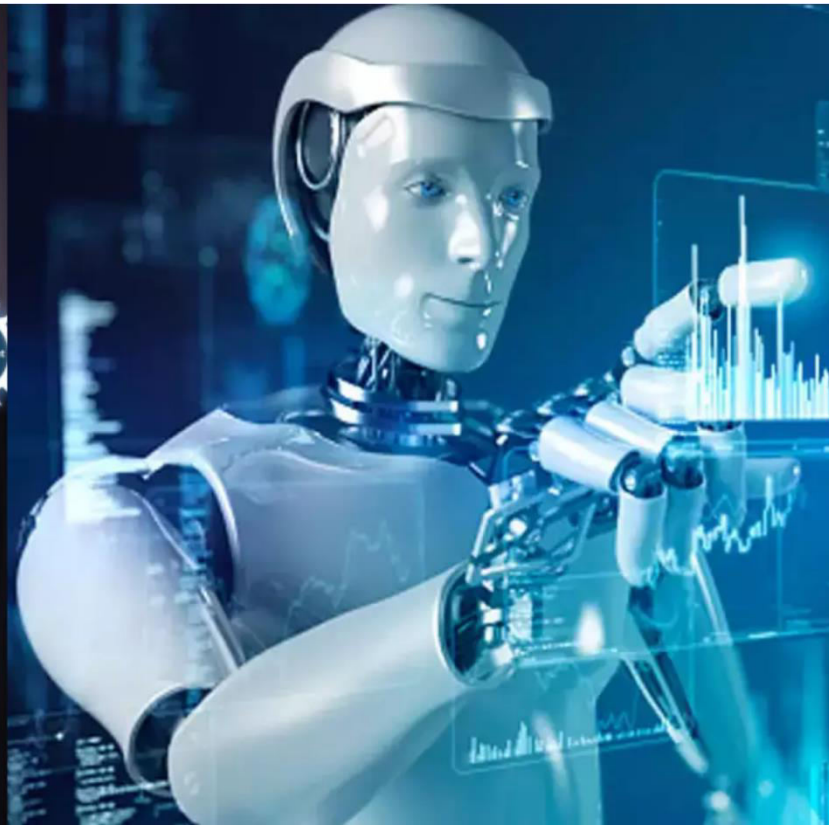
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411179|

AI-Powered Cyber Threat Detection and Defense system

Shruthi M K, Aishwarya Veerendra Bellad, Harshitha Malahal M P, Navyashree C, Nikitha C M

Associate Professor, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India

ABSTRACT: In today's digital era, the increasing dependence on technology has made cyber threats more sophisticated and frequent. Traditional cybersecurity approaches, which often rely on predefined rules and static signature-based detection systems, are becoming inadequate against advanced persistent threats, zeroday attacks, and evolving malware. This growing challenge has led to the integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity, resulting in more intelligent, adaptive, and proactive defense mechanisms. It uses data collected from multiple sources such as system logs, network traffic, and user behavior to train ML models. These models can identify deviations from normal patterns and classify potential threats with high accuracy. For instance, supervised learning algorithms like decision trees and support vector machines (SVM) can be trained to detect malware or phishing attempts based on labeled datasets, while unsupervised learning techniques such as clustering and anomaly detection can help identify novel threats that have no prior labels or signatures.

KEYWORDS: Cybersecurity, Artificial Intelligence (AI), Machine Learning (ML), Cyber Threats, Advanced Persistent Threats (APT), Zero-Day Attacks, Malware Detection, Rule-Based Systems, Signature-Based Detection, Data Analysis, System Logs, Network Traffic, User Behavior, Supervised Learning, Unsupervised Learning, Decision Trees, Support Vector Machine (SVM), Clustering, Anomaly Detection, Threat Classification, Adaptive Defense, Proactive Security, AI-Powered Cybersecurity..

I. INTRODUCTION

The AI-Powered Cyber Threat Detection and Defense System is a comprehensive solution designed to protect organizations from evolving cyber threats. This system leverages advanced machine learning algorithms and deep learning techniques to detect and respond to malware, phishing attacks, and malicious URL links in real-time. The malware detection module uses machine learning to identify and classify malicious software, including Trojans, ransomware, and other types of malware. The phishing detection module employs natural language processing to identify suspicious emails and messages, while the URL link detection module analyzes web links to identify potential threats. The system also integrates with firewalls to block malicious traffic and prevent unauthorized access to the network. By analyzing patterns and anomalies in system behavior, network traffic, and user activity, the system can identify potential threats and alert security teams. The AI-powered system can learn from experience and adapt to new threats, reducing the risk of false positives and improving incident response. With its advanced threat detection capabilities and automated incident response, the system provides comprehensive protection against cyber threats, helping organizations safeguard their sensitive data and assets. The system can be integrated with existing security infrastructure, including security information and event management (SIEM) systems, to provide a robust defense against cyber threats. By leveraging AI-powered analytics, the system can stay ahead of emerging threats, reducing the risk of breaches and cyber attacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411179|

II. LITERATURE SURVEY

One of the foundational areas where AI has shown significant promise is in the development of Intrusion Detection Systems (IDS). Early works such as those by Mukkamala et al. (2002) demonstrated the viability of using Support Vector Machines (SVM) and Artificial Neural Networks (ANN) for detecting malicious activities within network traffic. This, later studies explored the use of decision trees, k-nearest neighbors (KNN), and ensemble learning to improve detection accuracy. While these traditional machine learning models provided good results, their reliance on manual feature extraction limited their scalability and adaptability. To address this, researchers began employing deep learning techniques. Kim et al. (2016) introduced the use of deep neural networks (DNNs) in intrusion detection and achieved notable improvements in classification accuracy and false positive rates. These models were particularly effective in learning hierarchical representations of raw data, reducing the need for domain-specific feature engineering.

III. METHODOLOGY

The proposed AI-powered cyber threat detection and defense system follows a structured methodology. Initially, raw network traffic and system logs are collected from diverse sources such as firewalls, servers, endpoints, and IoT devices. Data preprocessing eliminates noise and extracts meaningful features. A machine learning model, trained using labeled datasets, identifies malicious patterns and unknown threats through anomaly detection. Deep learning techniques enhance real-time prediction accuracy. Detected threats trigger an automated response module that isolates affected nodes, blocks suspicious IPs, and alerts security administrators. Continuous model retraining and feedback improve system performance and adaptability to emerging cyber-attacks.

To enhance system intelligence, the model utilizes continuous monitoring techniques to track abnormal behavior trends over time. Threat intelligence feeds and global cybersecurity databases are integrated to update new attack signatures and zero-day vulnerabilities. The defense engine applies dynamic rule updates and adaptive filtering to strengthen system resilience. A reinforcement learning component optimizes decision-making based on outcomes of previous threat responses. The system includes a real-time dashboard for visual analytics, enabling administrators to observe threat patterns and system health. Finally, extensive testing, such as penetration testing and simulation of cyber-attacks, is performed to validate model accuracy, robustness, and reliability.

IV. RESULTS

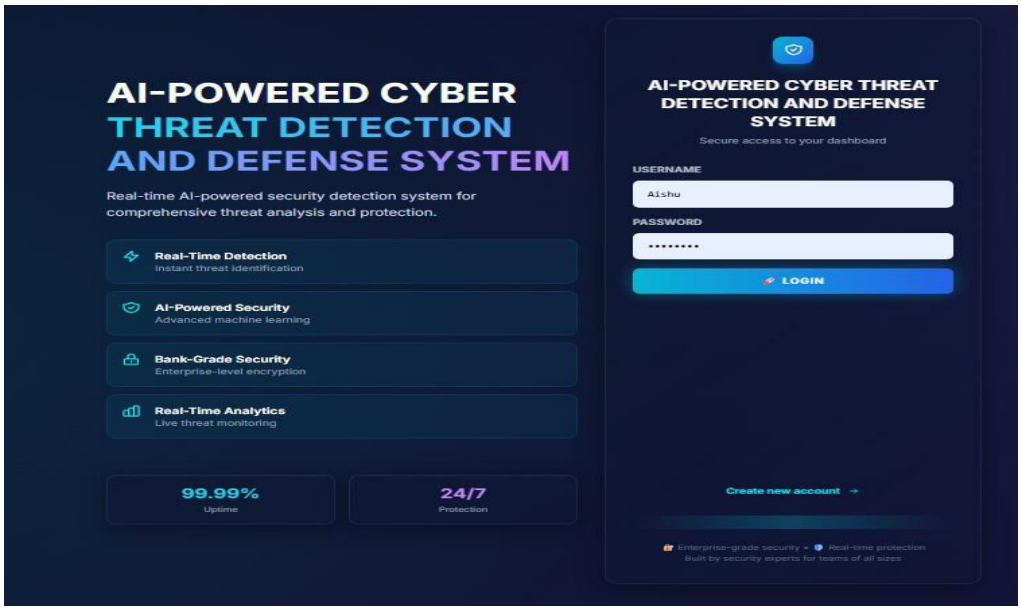


Fig-1 Home page

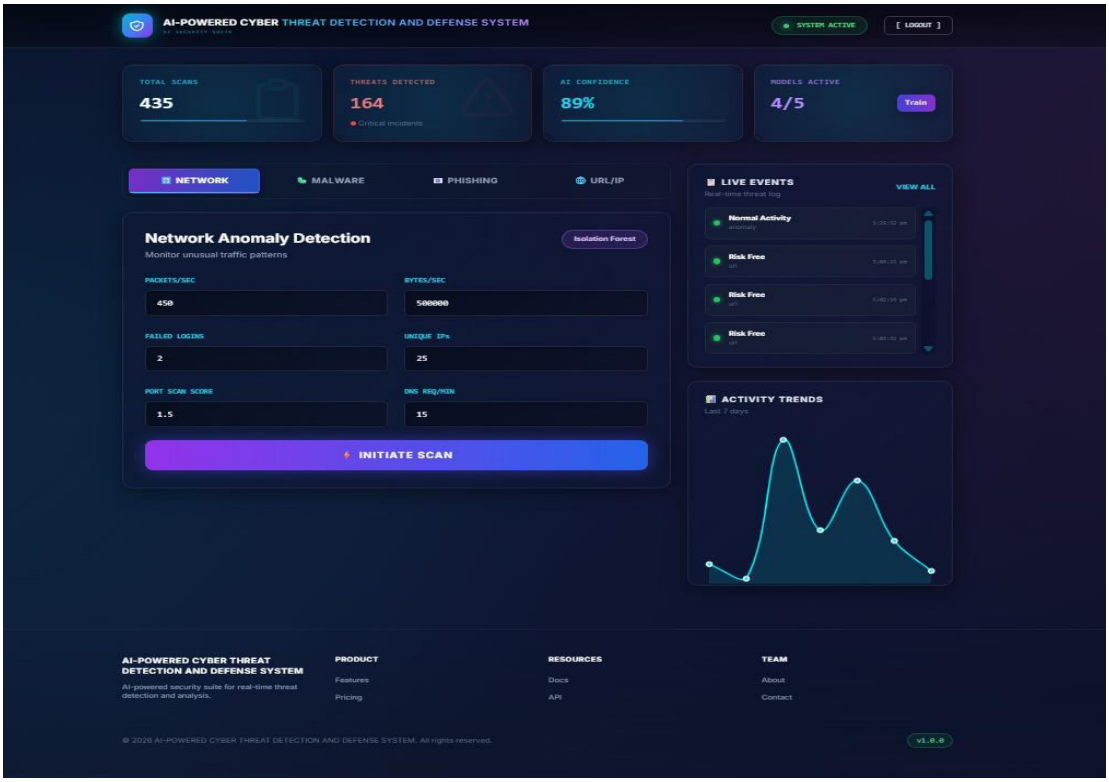
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411179|



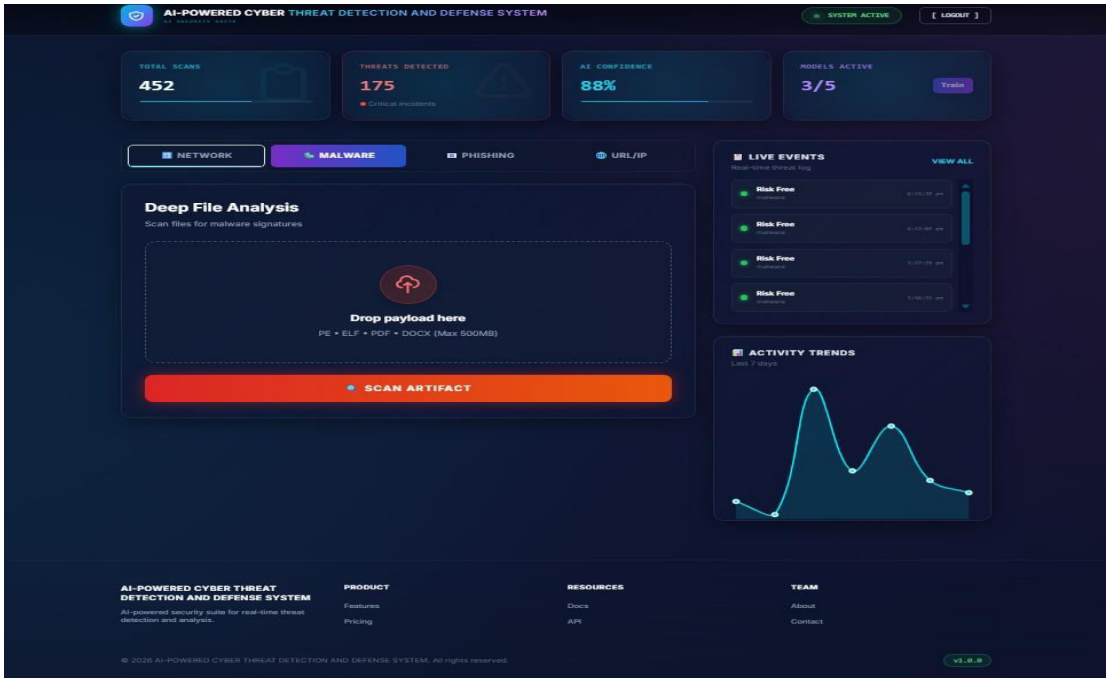


Fig-2 Network Anamoly Detector

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411179|

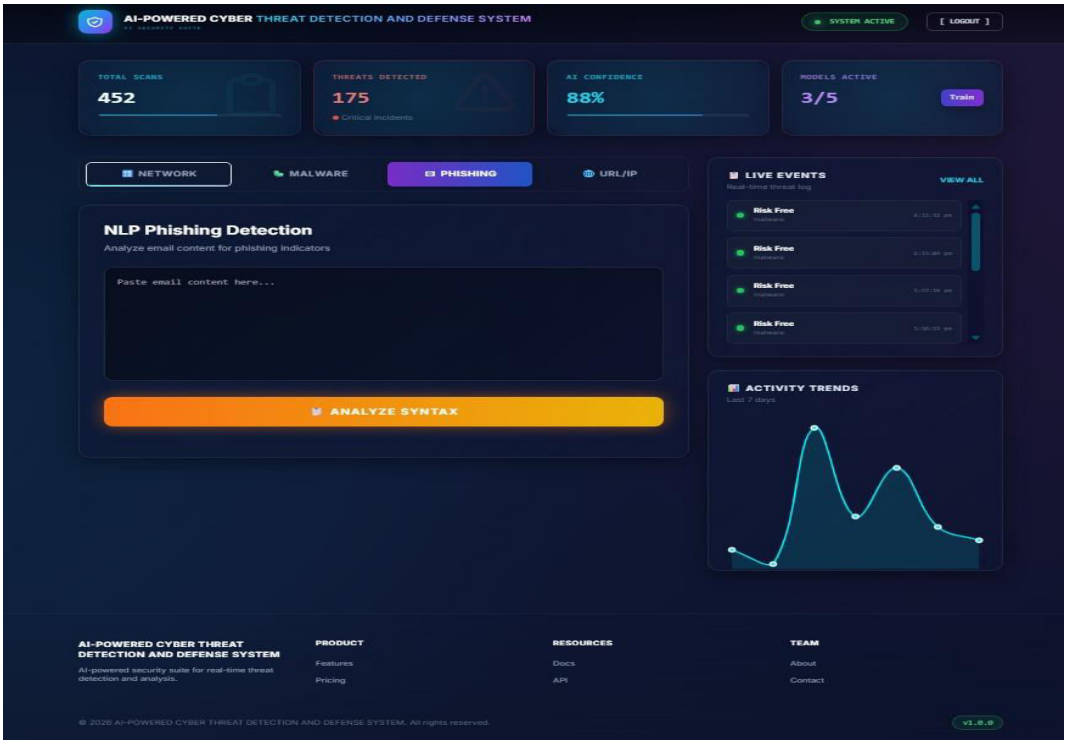


Fig-3 Deep File Analysis Detector

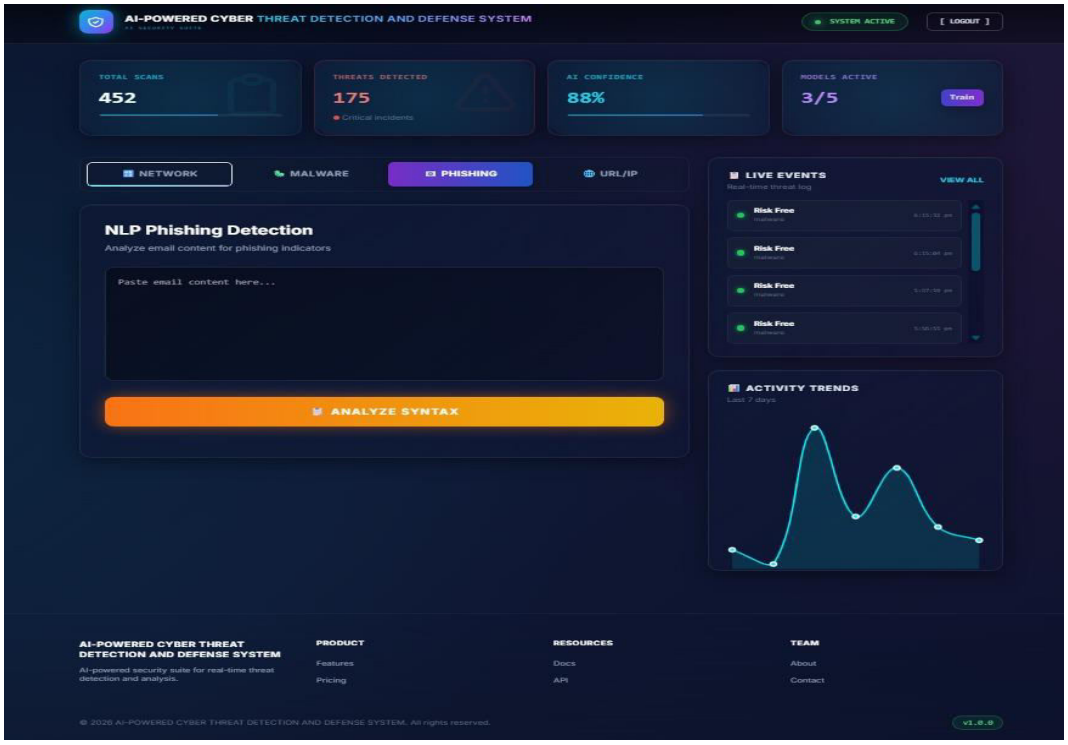


Fig-4 Phishing Detector

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411179|

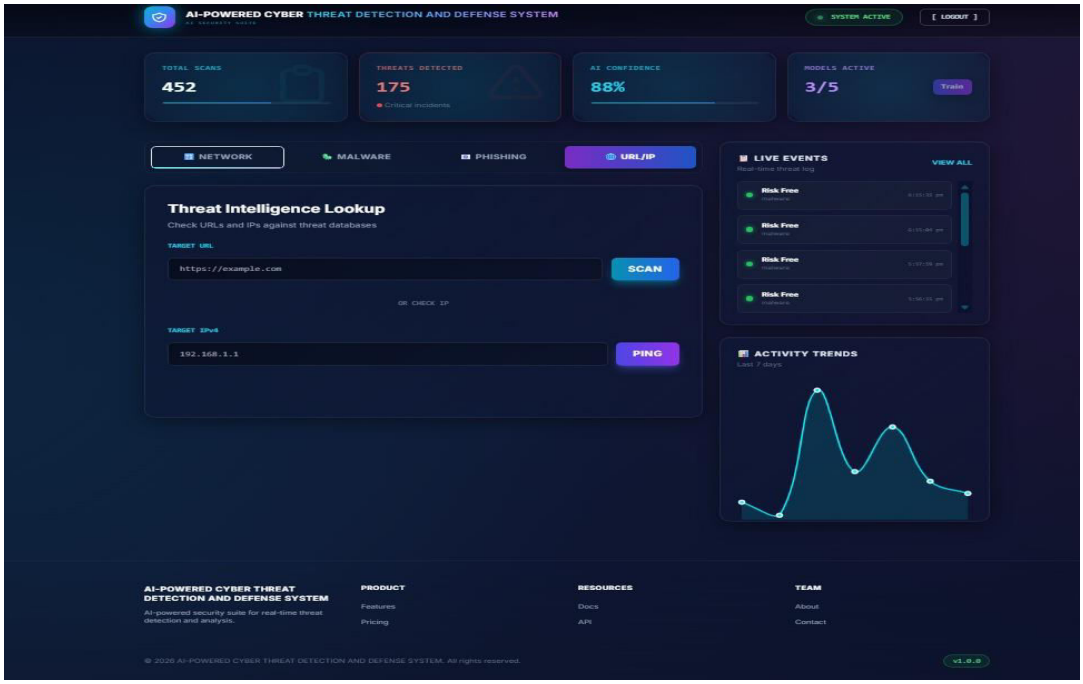


Fig -5 URL/IP Detector

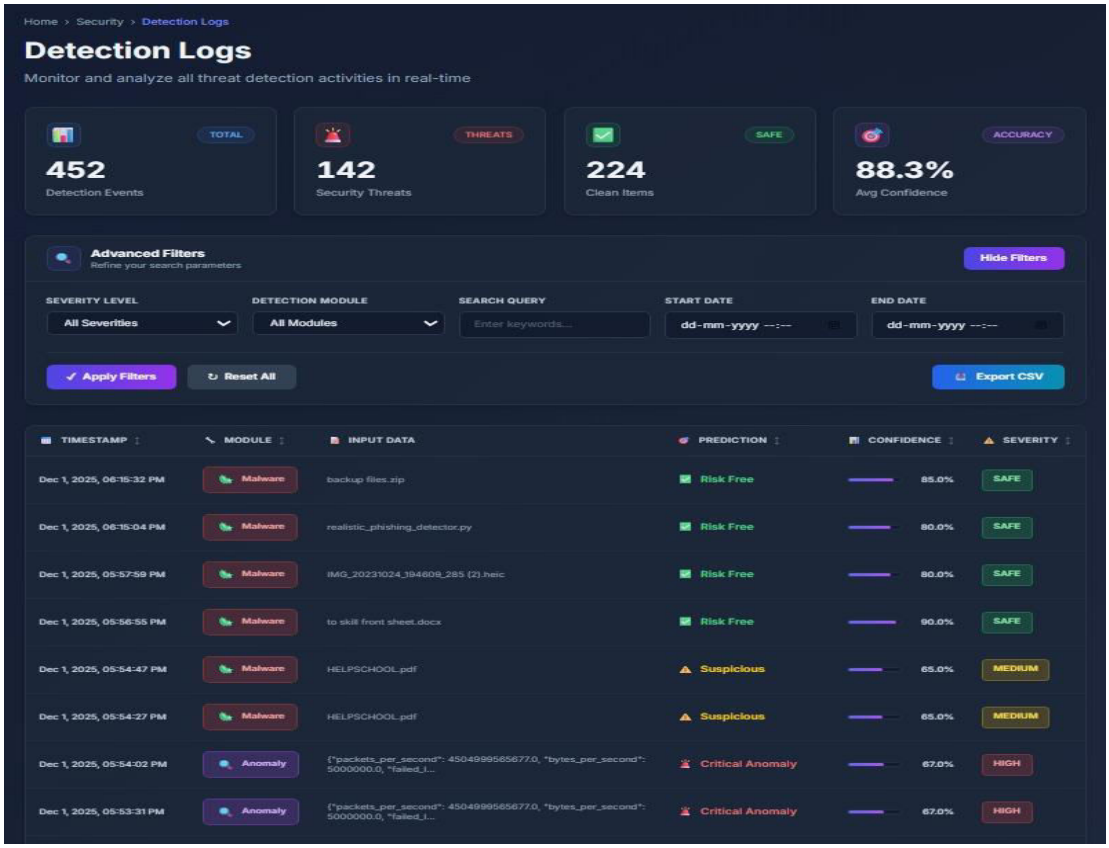


Fig-6 Detection Logs Page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411179|

V. CONCLUSION

The AI-Powered Cyber Threat Detection and Defense System successfully demonstrates an intelligent and automated approach to securing digital infrastructures against rapidly evolving cyber threats. Traditional security solutions are often limited by static rule-based mechanisms, delayed response times, and inability to detect unknown attacks. In contrast, this system integrates machine learning and deep learning algorithms to analyze network traffic patterns, detect anomalies, and identify threats in real time with high accuracy. Through automated response mechanisms, the system minimizes human intervention, reduces risk exposure, and ensures faster containment of malicious activities. Continuous model training enhances adaptability, enabling the system to learn from new attack behavior and emerging vulnerabilities.

The integration of analytics dashboards and alert mechanisms helps security administrators visualize threat trends and make informed decisions. Testing and performance evaluation confirm system reliability, scalability, and applicability across various domains such as enterprise networks, cloud platforms, and IoT environments. Overall, the project proves that artificial intelligence is a highly effective strategy for building proactive and intelligent cybersecurity defenses, capable of providing robust protection against advanced persistent threats, zero-day attacks, and ransomware. The system can be further expanded through federated learning, improved dataset variety, and integration with blockchain to enhance security transparency and trust.

REFERENCES

[1].Miles Brundage, Shahar Avin, Jasmine Wang, et al. Toward trustworthy ai development: Mechanisms for supporting verifiable claims. Xiv pre printer Xiv:2004.07213, 2020.
[2]. Nicholas Carlini and David Wagner. Evaluating the robustness of machine learning models to adversarial examples. IEEE Transactions on Information Forensics and Security, 15:2483–2497, 2020.
[3]. Finale Doshi-Velez and Been Kim. Considerations for differential privacy with machine learning. Nature Machine Intelligence, 2(7):391–400, 2020.
[4]. Micah Goldblum, Nicholas Carlini, and Tom Goldstein. Dataset security for machine learning: A survey. Advances in Neural Information Processing Systems (Neur IPS), 2022.
[5]. Peter Kairouz, Brendan McMahan, Brendan Avent, et al. Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2):1–210, 2021.
[6]. A. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[7]. M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang and L. Shu, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," Journal of Information Security and Applications, vol. 50, pp. 1–16, 2020.
[8]. S. Revathi and A. Malathi, "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques," International Journal of Engineering Research & Technology (IJERT), vol. 2, issue 12, pp. 1848–1853, 2013.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details