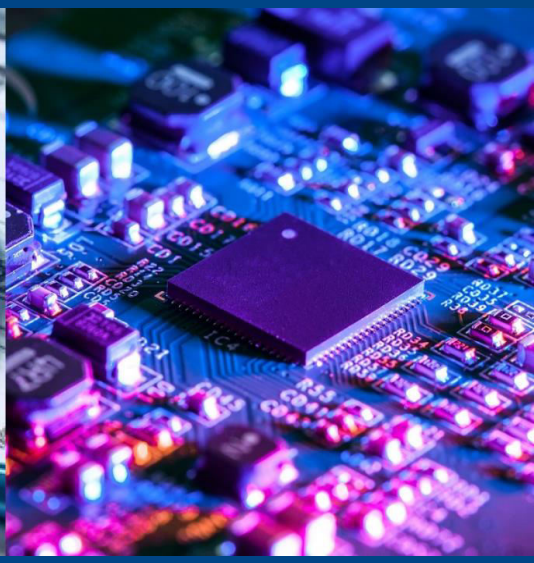
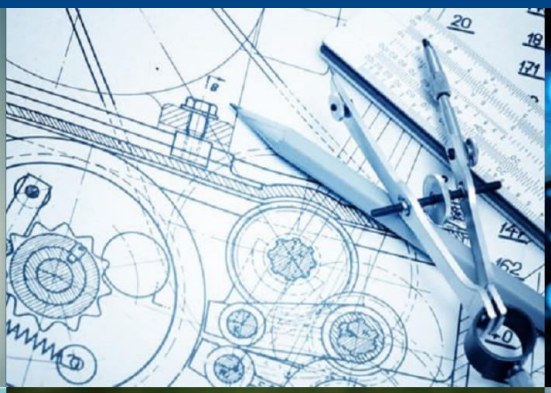
ISSN: 2582-7219

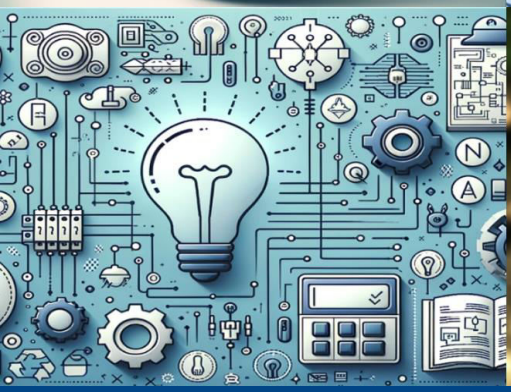




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 9.864

Volume 9, Issue 6, June 2026

© 2026 IJMRSET | Volume 9, Issue 6, June 2026| DOI:10.15680/IJMRSET.2026.0906022

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

AI-Powered System for an Efficient and Effective Cyber Incidents Detection and Response

M.Kasthuri[1], Dr. J. Lourdu Xavier[2]

PG Scholar, Department of Master of Computer Applications, R.V.S. College of Engineering, Dindigul, Tamil Nadu, India[1]

Head & Professor, Department of Master of Computer Applications, R.V.S. College of Engineering, Dindigul, Tamil Nadu, India[2]

ABSTRACT: The growing complexity and frequency of cyber threats in cloud environments call for innovative and automated solutions to maintain effective and efficient incident response. This study introduces a cutting edge AI-driven cyber incident response system for cloud platforms, employing advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques to provide accurate, scalable integration with platforms like Google Cloud and Microsoft Azure. An automated pipeline integrates Network Traffic Classification, Web Intrusion Detection, and Post-Incident Malware Analysis into a cohesive framework via a Flask application. Validated on NSL-KDD, UNSW-NB15, and CIC-IDS-2017, the Random Forest model achieved accuracies of 90%, 75%, and 99% respectively, with 96% precision for malware analysis. A neural network-based malware model achieved 99% accuracy. Containerisation ensures scalability and portability across diverse cloud environments. This research makes a significant contribution to the field of AI-powered cybersecurity by showcasing the powerful combination of AI models and cloud infrastructure to fill critical gaps in cyber incident response. Our findings emphasize the superior performance of Random Forest and deep learning models in accurately identifying and classifying cyber threats, setting a new standard for real-world deployment in cloud environments.

KEYWORDS: Cyber incident, digital forensics, artificial intelligence, machine learning, cloud security, incident response, NSL-KDD, UNSW-NB15, CIC-IDS-2017.

I. INTRODUCTION

In recent years, the proliferation of cyber attacks targeting organisations across various industries has reiterated the critical need for robust incident response capabilities. According to the UK government's Cybersecurity Breaches Survey in 2024, a significant percentage of businesses and charities have experienced breaches or attacks, with alarmingly low adoption rates of formal incident response capabilities (IR). Consequently, there is a pressing demand for organisations to invest in incident response capabilities to protect against data breaches and cyber threats.

Organisations with well-tested Incident Response (IR) capabilities and high levels of AI and ML integration for threat detection and response demonstrated substantially lower data breach costs, as highlighted by IBM's 2024 Cost of Data Breach report. This study investigates how AI contributes to cybersecurity and explores the potential to apply it in cloud environments to address associated challenges. The proposed system includes three main components: a network traffic classifier, a web intrusion detection system (WIDS), and a malware analysis system.

The proposed system stands out through its integration of real-time feature engineering, modular containerisation for scalability, and lightweight agents for efficient log collection in the WIDS. By dynamically adjusting contamination ratios based on domain-specific scenarios, it significantly reduces false positives while maintaining high accuracy in diverse cloud environments. The system leverages a honeypot subsystem for proactive threat detection, continually updating the models with real-world attack data. This seamless multi-cloud deployment strategy, supported by Docker and Kubernetes, ensures adaptability to emerging threats.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

II. EXISTING SYSTEM

Traditional cyber incident response systems primarily depend on rule-based detection and manual investigation by cybersecurity professionals. These conventional methods rely heavily on predefined signatures, handcrafted rules, and expert-driven analysis. The methodology involves log collection, network monitoring, manual triage, and forensic investigation of security incidents. Although these methods are operationally established, they are time-consuming, costly, and require highly skilled professionals. Traditional IDS tools such as Snort and Suricata rely on static signatures, while commercial SIEM platforms like Splunk require extensive manual tuning.

DISADVANTAGES

- **Time-Consuming and Costly:** Manual investigation and rule-based detection require significant human effort and expertise.
- **Prone to Human Error:** Manual analysis introduces inconsistency and risk of missed threats during investigation.
- **Limited Automation and Scalability:** Traditional systems cannot dynamically scale to handle modern cloud-scale threat volumes.
- **Reactive Rather Than Proactive:** Conventional tools detect threats only after signatures are defined, missing zero-day attacks.

III. PROPOSED SYSTEM

The proposed system presents an automated AI-powered cyber incident detection and response framework using Convolutional Neural Networks (CNNs), Random Forest classifiers, and Long Short-Term Memory (LSTM) networks implemented on cloud platforms. Unlike traditional methods that rely on manual diagnosis or rule-based features, the AI models automatically learn complex attack patterns directly from network traffic, HTTP logs, and malware binaries. The process includes data collection, preprocessing, feature extraction, model training, and real-time classification. This deep learning-based approach improves accuracy, speed, and reliability while reducing the workload of cybersecurity professionals. It provides a cost-effective and scalable solution deployable on Google Cloud, Microsoft Azure, and AWS using Docker and Kubernetes containerisation.

ADVANTAGES

- **High Accuracy and Reliability:** Random Forest achieves up to 99.82% accuracy; Keras LSTM achieves 99% in malware detection.
- **Time-Efficient and Cost-Effective:** Automated pipeline reduces incident response times and lowers operational costs significantly.
- **Scalability and Accessibility:** Containerised microservices enable horizontal and vertical scaling across cloud platforms.
- **Proactive Threat Detection:** Honeypot subsystem continuously feeds real-world attack data to retrain AI models dynamically.

© 2026 IJMRSET | Volume 9, Issue 6, June 2026| DOI:10.15680/IJMRSET.2026.0906022

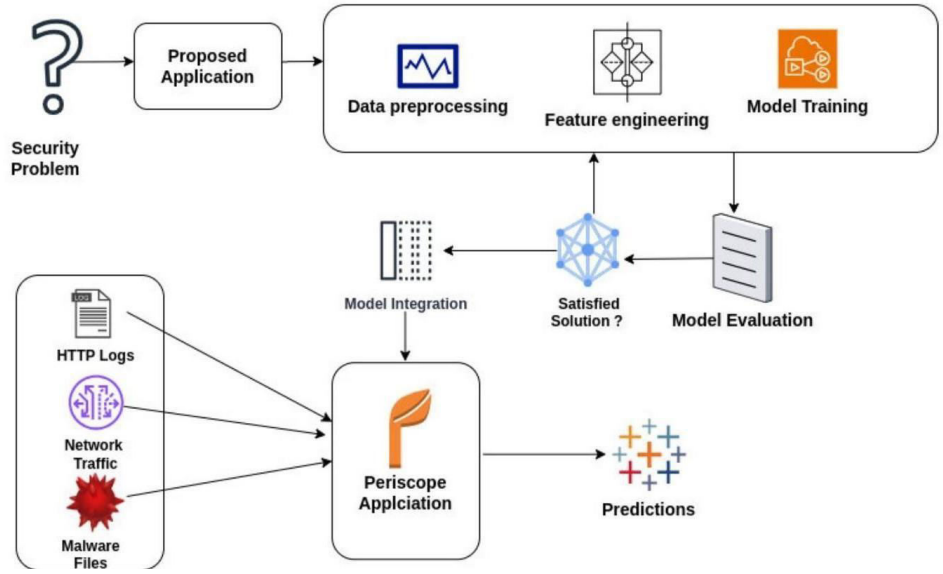
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

IV. SYSTEM ARCHITECTURE

FIGURE 1. Framework for data management and analysis.



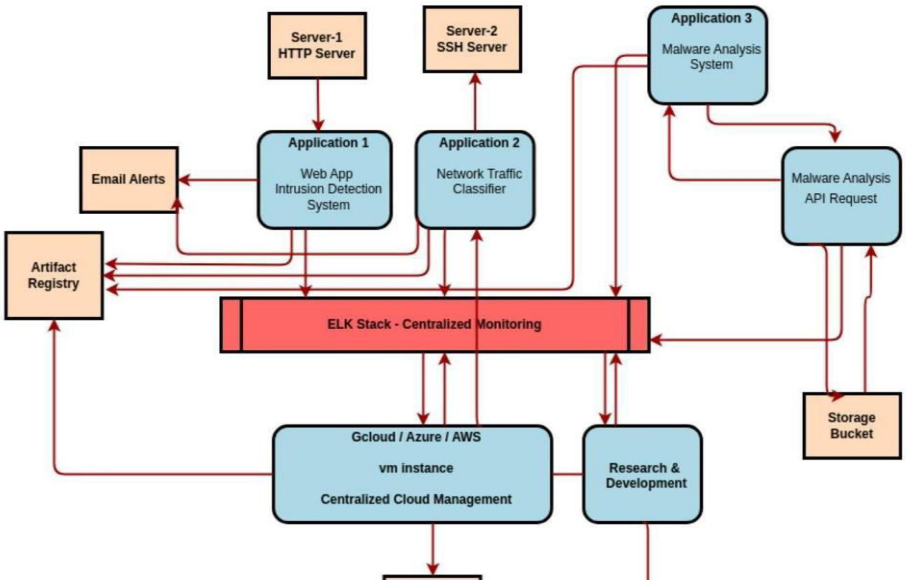


FIGURE 2. Proposed system data flow diagram.

V. MODULE DESCRIPTIONS

- Data Collection, Image Preprocessing ,Network Traffic Classification, Web Intrusion Detection System (WIDS) ,Malware Analysis System
- Cloud Deployment and Containerisation

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

DATA COLLECTION

Data collection is the first step in this project. In this stage, network traffic data, HTTP server logs, and malware/benign executable files are collected from publicly available cybersecurity datasets to train and test the deep learning model. The network traffic data is obtained from reliable benchmark sources such as the NSL-KDD Dataset, UNSW-NB15 Dataset, and CIC-IDS-2017 Dataset. These datasets contain thousands of labelled network flow records representing different types of cyber attacks including DoS, Brute Force, DDoS, Fuzzing, Backdoors, and Shellcode. For malware analysis, executable samples are sourced from VirusTotal.com. The training data for malware consists of 694 benign and 299 malicious samples, while network datasets range from 125,973 to over 2.8 million records.

IMAGE PREPROCESSING

Preprocessing is an important step in this project. In this stage, the collected raw data including network PCAP files, HTTP access logs, and executable binaries are prepared and improved before feeding them into the AI models. Network packets are captured using the Scapy library and stored as PCAP files, then parsed to extract connection-based statistical features. HTTP log files are converted into pandas DataFrames for feature extraction. Executable binaries undergo static analysis to extract string features, Import Address Table (IAT) characteristics, and PE header attributes. Noise and irrelevant features such as flags, protocols, and services are dropped. Features are standardised using StandardScaler to ensure uniform input dimensions. These preprocessing steps improve data quality and ensure uniformity, which helps the model learn more effectively.

NETWORK TRAFFIC CLASSIFICATION

Network traffic classification is a core component of this system. The preprocessed network flow data is fed into a Random Forest classifier trained on NSL-KDD, UNSW-NB15, and CIC-IDS-2017 datasets. The system is containerised into three distinct engines: the Capture Engine (captures live PCAP data using Scapy), the Feature Engine (extracts statistical features from PCAP files), and the Model Classifier (applies the pre-trained Random Forest model for real-time attack labelling). The classifier can identify a wide range of attacks including DoS, DDoS, Brute Force, Port Scanning, SQL Injection, and Exploits. By classifying incoming traffic in real-time, the system enables prompt identification and mitigation of potential cyberattacks and triggers alerts to security analysts upon detecting anomalous activity.

WEB INTRUSION DETECTION SYSTEM (WIDS)

Web intrusion detection focuses on detecting suspicious behaviour in web traffic to prevent unauthorised access. This is achieved by extracting informative features from standard HTTP server logs. Lightweight agents deployed on each web server collect and forward logs to the centralised WIDS container. The Isolation Forest algorithm is used for unsupervised anomaly detection due to its effectiveness in highdimensional datasets. The system extracts five key feature categories: IP-level access statistics, URL string aberrations, unusual referrer patterns, sequence of accesses to endpoints, and user agent patterns. A contamination ratio of 0.01 is selected as the optimal threshold, achieving a recall of 91.3% while keeping false positives at 5.2%. Alerts are triggered only when the number of detected anomalies exceeds a predefined threshold, based on the assumption that real-world attacks involve rapid bursts of activity.

MALWARE ANALYSIS SYSTEM

Malware analysis encompasses the investigation of malicious software's functionality, purpose, origin, and potential impact. The proposed system automates this process using a dual-model hybrid architecture. The primary model is a Random Forest classifier trained on features extracted from executable binaries including strings, Import Address Table (IAT) characteristics, PE headers, and callback servers. If the Random Forest model predicts a probability above 0.7, the file is immediately classified as Malicious and a detailed PDF analysis report is generated. For files with uncertain classification (probability 0.5 to 0.7), a secondary Keras TensorFlow LSTM deep learning model is invoked for refined binary classification. Both models were trained on a dataset obtained from VirusTotal.com. The system is deployed as a Flask application on Kubernetes Engine.

CLOUD DEPLOYMENT AND CONTAINERISATION

The proposed system leverages containerisation technologies (Docker and Kubernetes) for deployment on public cloud platforms including Google Cloud, Microsoft Azure, and AWS. The architecture comprises three distinct Virtual Private Cloud (VPC) environments: the Production VPC which hosts critical customer infrastructure and mirrors traffic to DFIR, the Honeypot VPC which uses T-Pot to attract and capture real-world attack data, and the DFIR VPC which is

© 2026 IJMRSET | Volume 9, Issue 6, June 2026| DOI:10.15680/IJMRSET.2026.0906022

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

the central analysis hub housing trained AI models, ELK Stack for SIEM visualisation, and the Research and Development subnet for continuous model retraining. The ELK Stack (Elasticsearch, Logstash, and Kibana) provides centralised storage and visualisation of security events across all environments.

VI. OUTPUT SCREENSHOTS & RESULTS

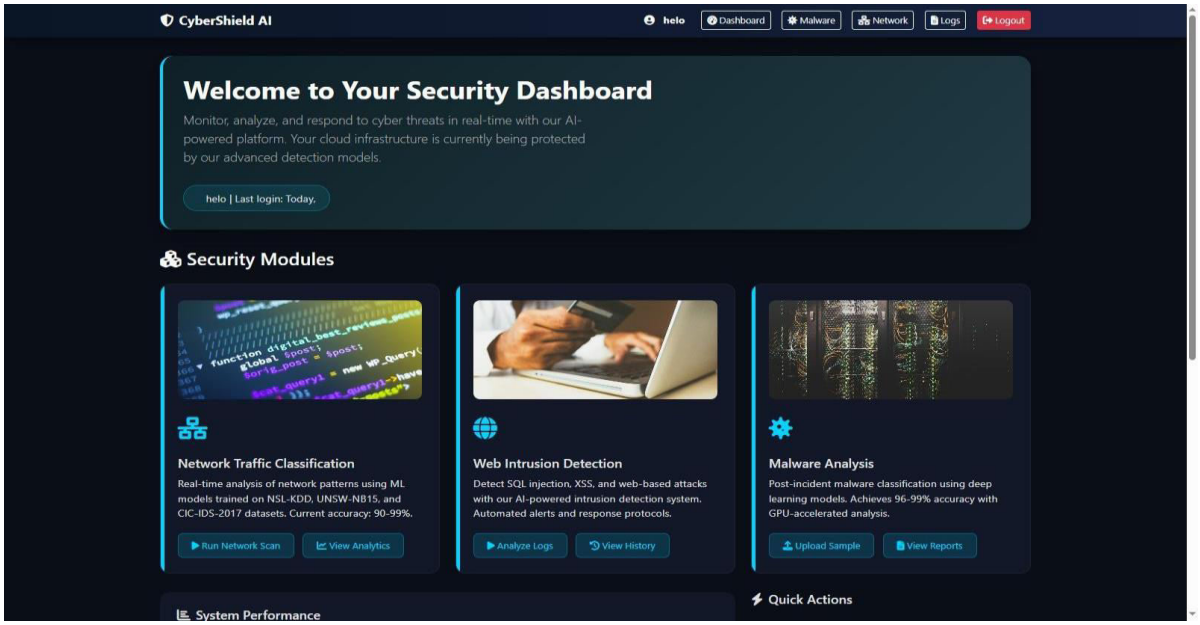


Figure 1: Dashboard

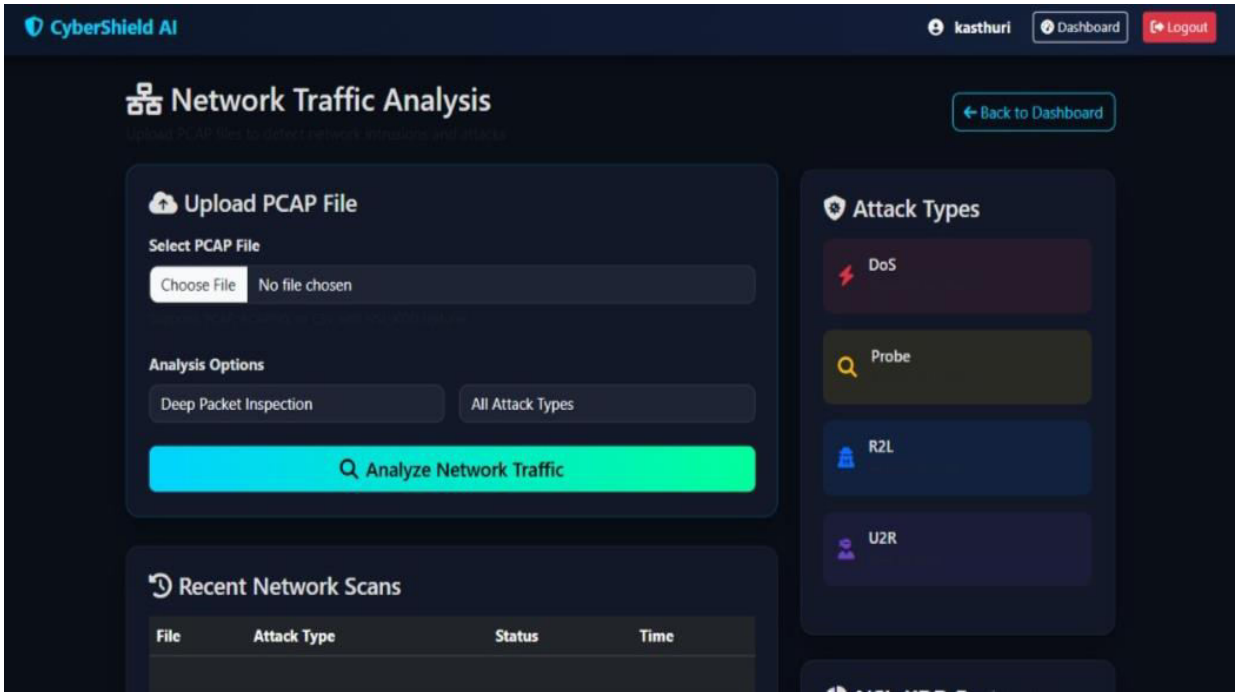


Figure 2: Network traffic Analysis

© 2026 IJMRSET | Volume 9, Issue 6, June 2026| DOI:10.15680/IJMRSET.2026.0906022

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

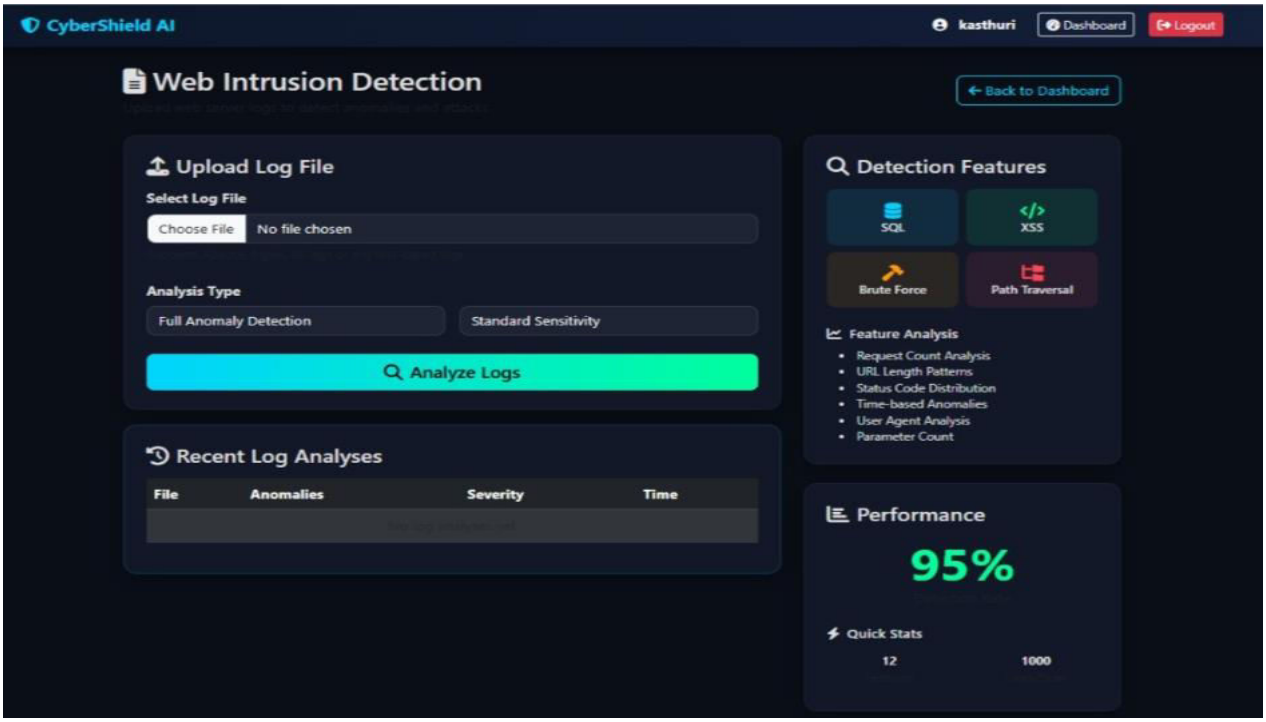


Figure 3: Web Intrusion Detection

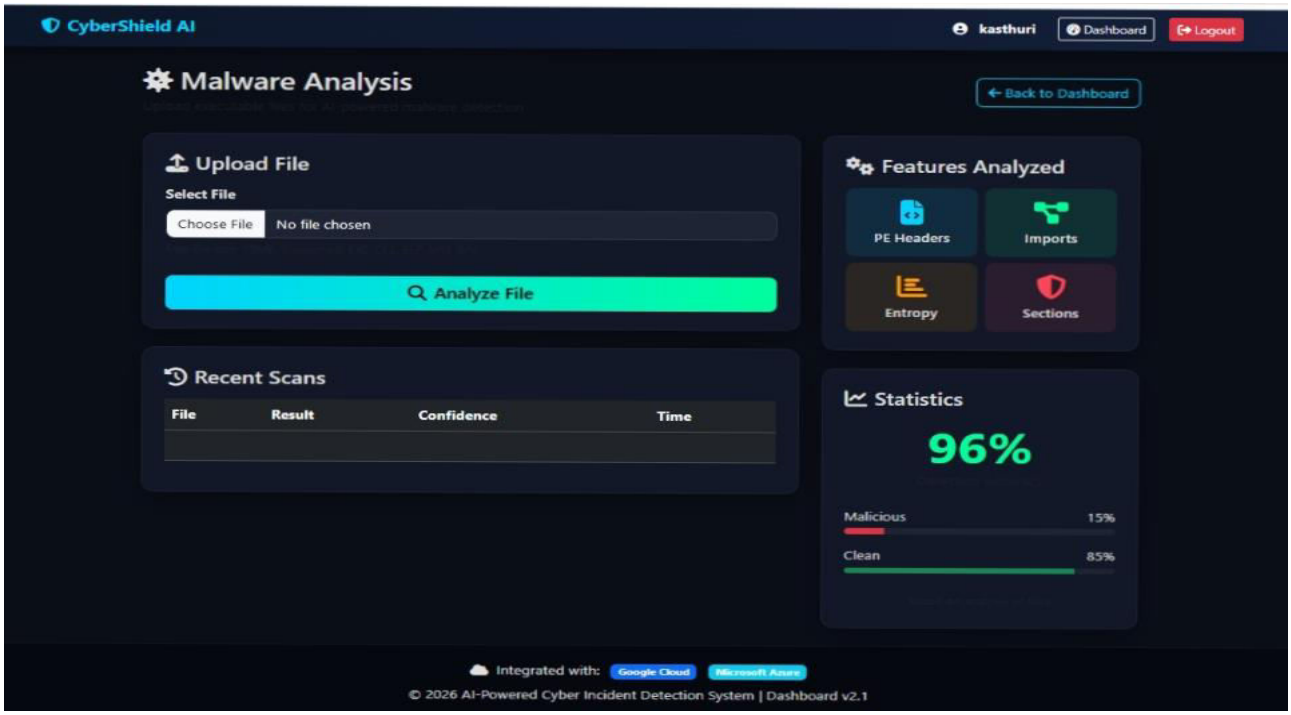


Figure 4: Malware Analysis

© 2026 IJMRSET | Volume 9, Issue 6, June 2026| DOI:10.15680/IJMRSET.2026.0906022

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

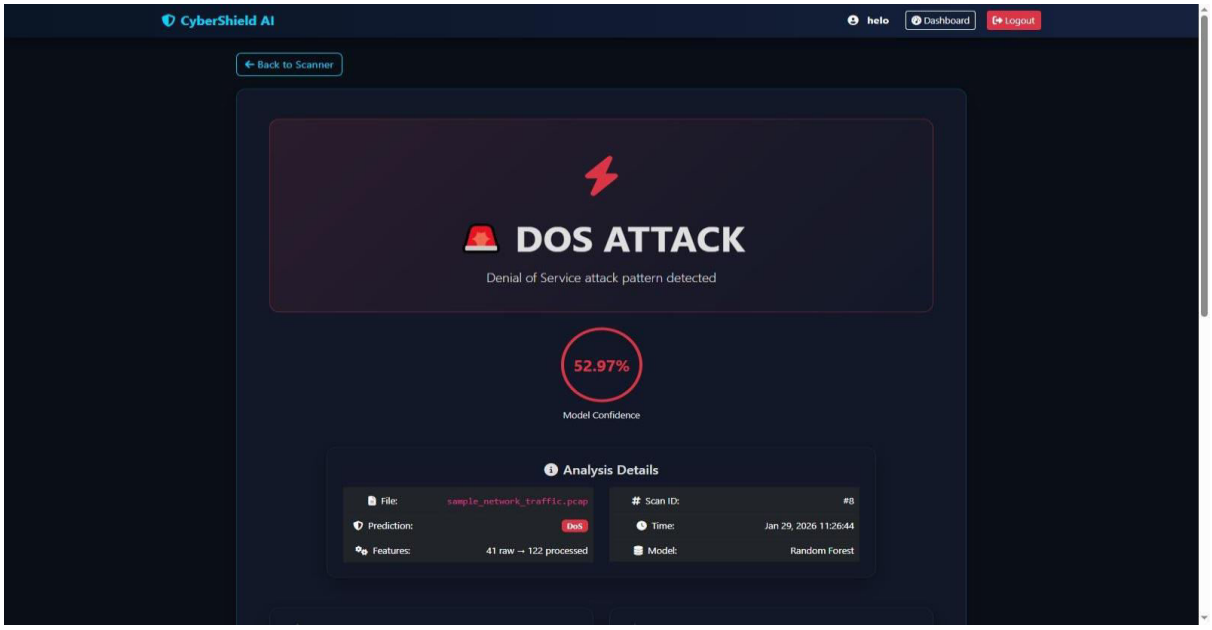


Figure 5: Dos Attack Analysis Result

Figure 6: Web Log Analysis Report

VII. CONCLUSION

In conclusion, the AI-Powered Cyber Incident Detection and Response system uses advanced deep learning and machine learning techniques to identify and respond to cyber threats in cloud environments. The system involves several stages such as data collection, preprocessing, network traffic classification, web intrusion detection, and malware analysis. A combination of Random Forest and Keras LSTM deep learning models are trained using large labelled cybersecurity datasets to learn the patterns of different attack types. By analysing important features extracted

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 9.864| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

from network packets, HTTP logs, and executable binaries, the models can accurately classify whether network traffic or files are malicious or benign.

The proposed CNN and Random Forest-based cyber incident detection system implemented on Google Cloud and Microsoft Azure provides a fast, non-invasive, and reliable method for classifying network traffic and malware. By incorporating preprocessing, feature engineering, and data augmentation techniques, the model improves accuracy and robustness while reducing false positives. Compared to traditional rule-based intrusion detection, this approach offers quicker detection and lowers manual workload for security analysts. The modular and containerised architecture ensures efficient deployment and scalability across cloud environments, allowing real-time traffic analysis and threat detection.

VIII. FUTURE ENHANCEMENTS

In future, the system can be improved using larger cybersecurity datasets to increase detection accuracy. Advanced deep learning models like Transformers and GNNs can be added for better threat detection.
Explainable AI techniques such as SHAP and LIME may help analysts understand predictions clearly.
The system can also integrate real-time threat intelligence platforms like MITRE ATT&CK. Multi-cloud automated deployment and real-world SOC testing can further improve scalability and performance.

- Use of large-scale and diverse cybersecurity datasets for better training
- Implementation of real-time threat detection using streaming data
- Development of web/mobile-based dashboards for easy monitoring
- Integration with cloud security tools and (SIEM)

REFERENCES

[1] GOV.U.K. (Apr. 19, 2024). Official Statistics Security Breaches Survey 2024. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024
[2] IBM. (2024). Cost of a Data Breach Report. [Online]. Available: http://www.ibm.com/reports/data-breach
[3] J. N. Angelis, R. S. Murthy, T. Beaulieu, and J. C. Miller, Better angry than afraid: The case of post data breach emotions on customer engagement, IEEE Trans. Eng. Manag., vol. 71, pp. 2593-2605, 2022.
[4] D. Cotroneo, A. Paudice, and A. Pecchia, Empirical analysis and validation of security alerts filtering techniques, IEEE Trans. Depend. Secure Comput., vol. 16, no. 5, pp. 856-870, Sep. 2019.
[5] N. Moustafa and J. Slay, UNSW-NB15: A comprehensive data set for network intrusion detection systems, in Proc. MilCIS, Canberra, Australia, Nov. 2015, pp. 1-6.
[6] A. Boukhamla and J. C. Gaviro, CICIDS2017 dataset: Performance improvements and validation, Int. J. Inf. Comput. Secur., vol. 16, no. 1, p. 20, 2021.
[7] C. Stelly and V. Roussev, SCARF: A container-based approach to cloud-scale digital forensic processing, Digit. Invest., vol. 22, pp. S39-S47, Aug. 2017.
[8] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, A comprehensive analysis of the role of AI and ML in modern digital forensics and incident response, Forensic Sci. Int., Digit. Invest., vol. 48, Mar. 2024.
[9] OWASP Found. (2023). OWASP Top 10-2023. [Online]. Available: https://owasp.org/Top10/
[10] ENISA. (2020). Threat Landscape. [Online]. Available: http://enisa.europa.eu/topics/cyber-threats/threats-and-trends
[11] M. Ashfaaq M. Farzaan, M. Chahine Ghanem, A. El-Hajjar, and D. N. Ratnayake, AI-enabled system for efficient and effective cyber incident detection and response in cloud environments, 2024, arXiv:2404.05602.
[12] Deutsche Telekom Security GmbH (2024). T-Pot 24.04.0. [Online]. Available: https://github.com/telekom-security/tpotce

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com