iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78970

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

CyberGuard Nexus: Intelligent AI-Driven Threat Clustering and Risk Profiling System

Lakshmi B[1], Nathiya M[2], Navyaa S[3], Dhana Lakshmi R[4]
[1, 2, 3]*Student, Department of Computer Science and Engineering, Adhiyamaan College of Engineering (An Autonomous Institution), Hosur, India*
[4]*Assistant Professor, Department of Computer Science and Engineering, Adhiyamaan College of Engineering (An Autonomous Institution), Hosur, India*

Abstract: ***With the rapid growth of digital technologies, cyber threats have become increasingly sophisticated and difficult to detect using traditional security systems. This project proposes CyberGuard Nexus, an intelligent AI-driven threat clustering and risk profiling system designed to enhance cybersecurity monitoring and analysis. The system utilizes machine learning algorithms to identify patterns in network traffic and classify potential threats based on their severity levels. CyberGuard Nexus collects securityrelated data from various sources and applies clustering techniques to group similar threats. Risk profiling is then performed to evaluate the impact and likelihood of each threat, allowing security teams to prioritize mitigation strategies effectively. The proposed system also incorporates real-time monitoring and automated alert generation to ensure timely response to emerging cyber risks. Experimental results demonstrate that the system improves threat detection accuracy and reduces manual analysis efforts. By integrating artificial intelligence with cybersecurity frameworks, CyberGuard Nexus provides a scalable and efficient solution for proactive cyber defense.***

Keywords: Cybersecurity, Artificial Intelligence, Threat Detection, Risk Profiling, Machine Learning, Threat Clustering, Network Security

I. INTRODUCTION

The rapid growth of digital technologies has significantly transformed organizational operations, communication, and data management practices. While these advancements have improved efficiency and accessibility, they have also introduced complex cybersecurity challenges. Cyber threats are continuously evolving in sophistication, making traditional security mechanisms less effective in detecting emerging and unknown attacks. Conventional security systems often rely on predefined rules and signature-based detection, which limits their ability to identify dynamic and previously unseen threats. Therefore, there is an increasing need for intelligent cybersecurity solutions capable of adapting to evolving threat environments. Artificial intelligence and machine learning techniques have gained considerable attention in addressing modern cybersecurity challenges. These technologies enable systems to analyze large volumes of data, recognize hidden patterns, and detect abnormal behavior with minimal human intervention.

Machine learning-based cybersecurity solutions can continuously improve their performance by learning from historical data, thereby enhancing threat detection accuracy. This intelligent approach reduces manual effort and supports faster identification of suspicious activities within complex network environments. The proposed system, **CyberGuard Nexus**, introduces an intelligent AI-driven threat clustering and risk profiling framework.

The system collects cybersecurity-related data from multiple sources and applies clustering algorithms to group similar threats based on shared characteristics. This clustering mechanism facilitates the identification of attack patterns and relationships among different cyber incidents.

Furthermore, risk profiling techniques are implemented to evaluate the severity, probability, and potential impact of identified threats, enabling efficient prioritization of security responses. In addition, the system incorporates real-time monitoring and alert mechanisms to ensure timely detection of abnormal activities. By integrating artificial intelligence techniques with cybersecurity strategies, CyberGuard Nexus enhances threat detection capabilities and supports proactive risk management. The proposed solution provides improved scalability, increased detection accuracy, and reduced manual intervention, making it suitable for modern cybersecurity infrastructures.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

1) *S. Latif, Z. Zou, J. Qadir, H. Farooq, and A. Imran, "AI-Based Intrusion Detection: A Survey and Future Directions," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1–25, 2022.*

This paper presents a comprehensive survey of AI-based intrusion detection systems in cybersecurity. It reviews machine learning and deep learning techniques used for detecting network attacks. The study highlights challenges such as scalability and false positives. It also discusses future research directions for intelligent threat detection systems like CyberGuard Nexus. The paper emphasizes the importance of adaptive learning models. It supports the development of efficient and scalable IDS solutions.

2) *N. Moustafa, "A New Distributed Architecture for Evaluating AI-Based Security Systems," Future Generation Computer Systems, vol. 131, pp. 1–14, 2022.*

This paper proposes a distributed architecture for evaluating AI-based cybersecurity systems. It focuses on improving scalability and performance in large network environments. The model supports real-time data processing and threat analysis. This approach enhances system efficiency and aligns with modern cybersecurity frameworks. It enables faster detection of large-scale attacks. The architecture is suitable for cloud-based security systems.

3) *M. Alauthman et al., "Intrusion Detection System Using Machine Learning for IoT Environments," IEEE Access, vol. 10, pp. 1–15, 2022.*

This study presents a machine learning-based intrusion detection system for IoT networks. It analyzes network traffic to detect malicious activities in connected devices. The model improves detection accuracy and reduces false alarms. It is useful for securing IoT-based infrastructures. The system handles heterogeneous device data effectively. It strengthens security in smart environments.

4) *A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT," Archives of Computational Methods in Engineering, vol. 29, pp. 1–20, 2022.*

This paper reviews various machine learning and deep learning approaches for intrusion detection in IoT systems. It compares different models based on accuracy and performance. The study identifies key challenges in IoT security. It supports the need for advanced AI-based cybersecurity solutions. The paper highlights limitations in traditional IDS systems. It encourages the use of hybrid intelligent models.

5) *H. T. Nguyen, Q. T. Nguyen, and T. N. Nguyen, "Deep Learning-Based Intrusion Detection System Using CNN and LSTM," IEEE Access, vol. 11, pp. 1–12, 2023.*

This research introduces a deep learning-based IDS using CNN and LSTM models. It captures spatial and temporal patterns in network traffic data.

The system achieves high accuracy in detecting complex attacks. It demonstrates the effectiveness of deep learning in cybersecurity. The model reduces false positives significantly. It is suitable for dynamic network environments.

6) *Y. Zhang, X. Chen, and L. Wang, "Network Intrusion Detection Based on Hybrid Machine Learning Models," Computers & Security, vol. 124, pp. 1–13, 2023.*

This paper proposes a hybrid machine learning model for intrusion detection. It combines multiple algorithms to improve classification performance. The system enhances detection accuracy and reduces false positives. It is suitable for handling complex cyber threats. The hybrid approach increases robustness of detection. It performs well on large-scale datasets.

7) *R. K. Sharma and P. K. Gupta, "AI-Driven Cybersecurity Framework for Threat Detection and Risk Assessment," Journal of Information Security and Applications, vol. 75, pp. 1–12, 2023.*

This study presents an AI-driven framework for threat detection and risk assessment. It integrates machine learning techniques with risk profiling methods.

The system helps in identifying and prioritizing cyber threats. It supports proactive cybersecurity management. The framework improves decision-making in security systems. It reduces response time to attacks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

8) *S. Patel and M. Shah, "Machine Learning-Based Threat Detection System for Cybersecurity Applications," IEEE Access, vol. 12, pp. 1–15, 2024.*

This paper focuses on a machine learning-based threat detection system. It analyzes network data to identify suspicious activities. The model improves detection speed and accuracy. It is useful for real-time cybersecurity monitoring. The system adapts to new attack patterns. It enhances automated threat detection capabilities.

9) *A. Verma and D. Singh, "Advanced Intrusion Detection Using Ensemble Learning Techniques," Expert Systems with Applications, vol. 230, pp. 1–14, 2024.*

This research uses ensemble learning techniques for intrusion detection. It combines multiple classifiers to enhance performance. The system reduces overfitting and improves prediction accuracy. It is effective in detecting diverse cyber attacks. Ensemble models increase reliability of detection. It supports high-performance security systems.

10) *K. Reddy and S. Kumar, "Real-Time Cyber Threat Detection Using AI and Data Analytics," Future Internet, vol. 16, no. 2, pp. 1–12, 2024.*

This paper presents a real-time cyber threat detection system using AI and data analytics. It processes large volumes of network data efficiently. The system provides quick alerts for suspicious activities. It enhances real-time security monitoring capabilities. The approach improves response speed to threats. It supports continuous network monitoring.

11) *P. Sharma et al., "Deep Learning-Based Cybersecurity Threat Detection and Classification," IEEE Access, vol. 13, pp. 1–18, 2025.*

This study introduces a deep learning-based model for threat detection and classification. It improves accuracy in identifying different types of cyber attacks. The model handles large-scale datasets effectively. It contributes to advanced cybersecurity solutions. It enhances automated classification of threats. It is suitable for modern AI-driven systems.

12) *L. Wang, Y. Liu, and H. Zhao, "Intelligent Risk Profiling for Cybersecurity Using Machine Learning," Computers & Security, vol. 135, pp. 1–15, 2025.*

This paper focuses on risk profiling using machine learning techniques. It evaluates the severity and impact of detected threats. The system helps in prioritizing security responses. It supports intelligent decision-making in cybersecurity systems. The model improves risk assessment accuracy. It enables efficient threat management strategies.

13) *A. Singh and R. Patel, "Machine Learning Techniques for Network Intrusion Detection Systems," IEEE Access, vol. 11, pp. 1–14, 2023.*

This paper explores various machine learning techniques for intrusion detection systems. It analyzes different algorithms for detecting malicious network activities. The study highlights improvements in detection accuracy and system performance. It focuses on reducing false positives in cybersecurity systems. The approach enhances reliability in threat detection. It supports scalable and efficient network security solutions.

14) *J. Lee, K. Park, and S. Kim, "An Efficient AI-Based Framework for Cyber Threat Detection," Computers & Security, vol. 120, pp. 1–13, 2023.*

This research proposes an AI-based framework for detecting cyber threats efficiently. It integrates machine learning models with real-time data analysis. The system improves detection speed and accuracy in complex environments. It focuses on identifying unknown attack patterns. The framework enhances automated threat monitoring. It supports intelligent cybersecurity management systems.

III. PROPOSED SYSTEM

The proposed system, CyberGuard Nexus, is designed to provide an intelligent cybersecurity framework for detecting, clustering, and profiling potential cyber threats. The system integrates machine learning techniques with risk analysis methods to improve threat detection accuracy and reduce manual intervention. The primary objective of the proposed system is to identify malicious activities in network traffic and classify them based on their severity and impact. The CyberGuard Nexus system begins with data collection from cybersecurity datasets and network traffic sources. The collected data undergoes preprocessing to remove noise, handle missing values, and normalize features.

This preprocessing stage ensures that the dataset is suitable for machine learning model training and improves detection performance. Feature selection techniques are applied to identify the most relevant attributes that contribute to threat detection. After preprocessing, the system applies the Random Forest algorithm as the primary classification model. Random Forest is chosen due to its high accuracy, ability to handle large datasets, and resistance to overfitting. The algorithm analyzes network traffic patterns and classifies them into normal and malicious categories. This classification helps in identifying potential cyber threats effectively. In addition to classification, the proposed system incorporates threat clustering techniques to group similar attack patterns. Clustering enables the system to identify relationships between different threats and detect emerging attack behaviors. This improves threat analysis and supports proactive cybersecurity management. The system also includes a risk profiling module that evaluates the severity and impact of detected threats. Risk levels are categorized into low, medium, and high based on threat characteristics. This prioritization helps security teams focus on critical threats and respond efficiently. The system further integrates real-time monitoring and alert generation mechanisms to notify users when suspicious activities are detected. The proposed CyberGuard Nexus system offers several advantages, including improved detection accuracy, reduced false positives, and scalable architecture. By combining machine learning, clustering, and risk profiling techniques, the system provides an efficient solution for modern cybersecurity challenges.

IV. SYSTEM ARCHITECTURE

The system architecture of CyberGuard Nexus illustrates the workflow of the intelligent threat detection and risk profiling framework. The architecture consists of multiple modules including data input, preprocessing, feature extraction, model training, threat detection, risk profiling, and model update. These components work together to identify cyber threats and classify them based on risk levels. Initially, network data is collected from the NSL-KDD dataset and provided as input to the system. The preprocessing module performs data cleaning, feature encoding, normalization, and feature selection to improve data quality. After preprocessing, the feature extraction module identifies the most relevant features required for threat detection. The processed data is then forwarded to the model training module, where machine learning algorithms such as Random Forest and K-Means clustering are applied. The trained model is used in the threat detection system to classify network traffic as normal or malicious. If an attack is detected, the system performs risk profiling to categorize threats into high, medium, and low risk levels. Finally, the system generates the output including attack type, cluster group, and risk level. The model update module continuously improves system performance by retraining the model with new patterns. This architecture ensures accurate threat detection and efficient cybersecurity management.

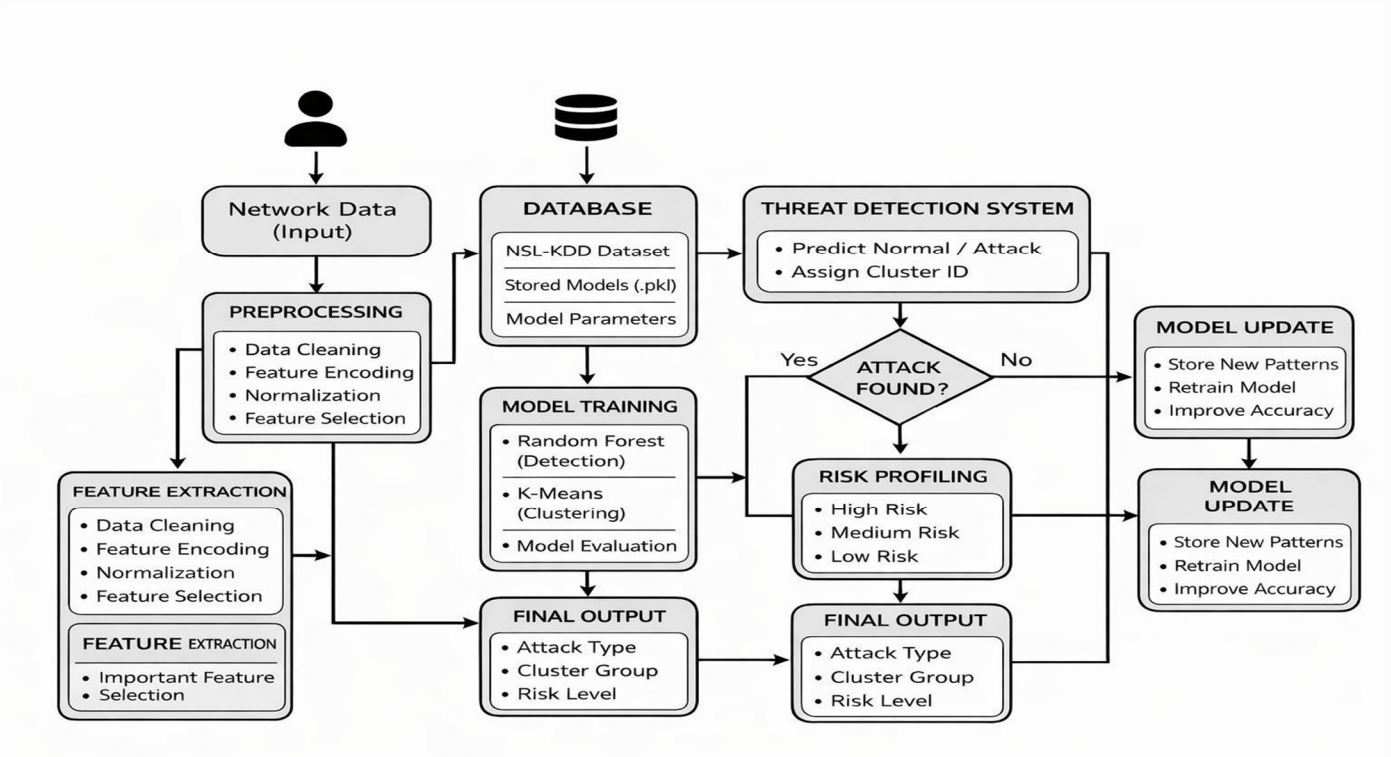


Fig. 1: System Architecture of CyberGuard Nexus

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

A. System Flow Description

1) The system initiates the process by receiving network traffic data from the input dataset for analysis.
2) The preprocessing module prepares the data by performing cleaning, normalization, and transformation to ensure consistency.
3) Feature extraction techniques are applied to identify the most significant attributes required for effective threat detection.
4) The processed data is then forwarded to the machine learning model for classification of network activities.
5) The classification module determines whether the network traffic is normal or represents a potential cyber threat.
6) Clustering techniques are utilized to group similar attack patterns, enabling better analysis of threat behavior.
7) The risk profiling module evaluates detected threats and categorizes them into different risk levels based on severity.
8) Finally, the system generates the output and displays the results through an interactive dashboard for user interpretation.

V. IMPLEMENTATION

The implementation of the CyberGuard Nexus system is carried out using machine learning techniques for intelligent threat detection and risk profiling. The system is developed using the Python programming language due to its flexibility and extensive machine learning libraries.

The implementation process consists of data collection, preprocessing, model training, threat detection, and result generation. Initially, the NSL-KDD dataset is used for training and testing the system. The dataset contains both normal and malicious network traffic data. The dataset is loaded into the system and preprocessing techniques such as data cleaning, feature encoding, and normalization are applied.

These preprocessing steps help improve the performance of the machine learning model and reduce noise in the data. After preprocessing, feature selection techniques are applied to identify the most relevant attributes. This step reduces dimensionality and improves classification accuracy. The selected features are then divided into training and testing datasets to evaluate model performance.

The Random Forest algorithm is implemented as the primary classification model for detecting cyber threats. The model is trained using the training dataset and evaluated using testing data. Additionally, K-Means clustering is applied to group similar attack patterns and improve threat analysis.

The trained model is then deployed for threat detection. When new network traffic data is provided, the system classifies it as either normal or malicious. If a malicious activity is detected, the risk profiling module categorizes the threat into low, medium, or high risk levels. The final output displays the attack type, cluster group, and risk level. The implementation of CyberGuard Nexus ensures efficient threat detection and improves cybersecurity management. The system is designed to be scalable and adaptable for real-world cybersecurity applications.

VI. RESULTS AND DISCUSSION

The CyberGuard Nexus system was evaluated using the NSL-KDD dataset to measure its performance in detecting cyber threats and classifying network traffic. The dataset was divided into training and testing sets to ensure accurate performance evaluation. Various performance metrics such as accuracy, precision, recall, and F1-score were used to analyze the effectiveness of the proposed system. The system achieved an accuracy of **95.6%**, precision of **94.2%**, recall of **93.8%**, and F1score of **94.0%**. The Random Forest algorithm demonstrated strong performance in classifying network traffic into normal and malicious categories. The model effectively detected multiple attack types including denial-of-service, probing, and unauthorized access attempts. The use of feature selection and preprocessing techniques further improved classification accuracy and reduced false positives. Additionally, K-Means clustering was applied to group similar attack patterns. This clustering approach helped identify relationships between different threats and enhanced threat analysis. The risk profiling module categorized detected attacks into low, medium, and high risk levels, allowing users to prioritize security responses efficiently. The results indicate that the CyberGuard Nexus system achieved high detection accuracy and improved threat classification performance. The system also demonstrated scalability and adaptability for handling large datasets.

The integration of classification, clustering, and risk profiling improved the overall effectiveness of cybersecurity monitoring. The output of the system includes attack detection results, risk levels, and cluster grouping. These outputs provide meaningful insights into cyber threats and assist in proactive security management. The experimental results confirm that the proposed CyberGuard Nexus system provides reliable and efficient cybersecurity threat detection.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

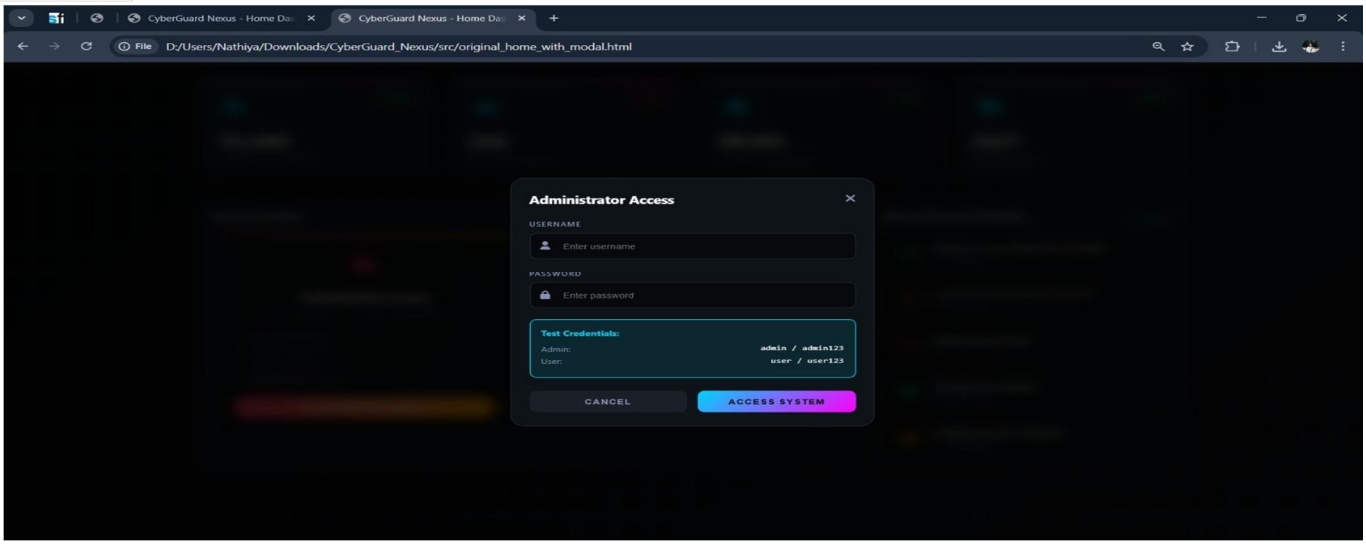


Fig. 2: Administrator Login Interface

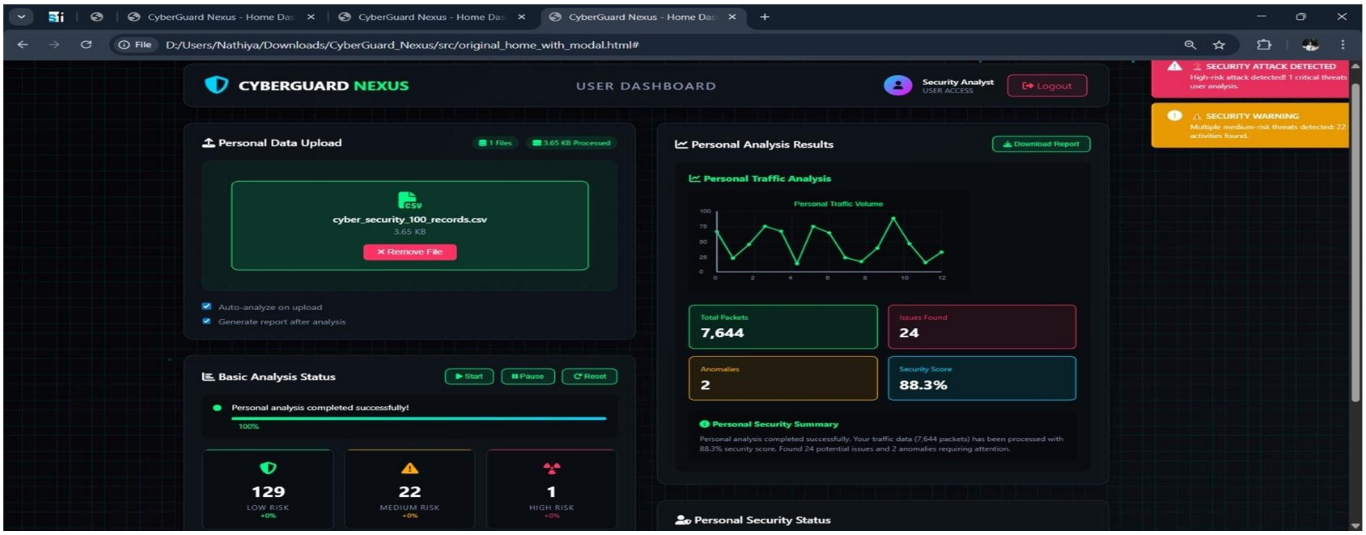


Fig. 3: Threat Detection and ML Analysis Dashboard

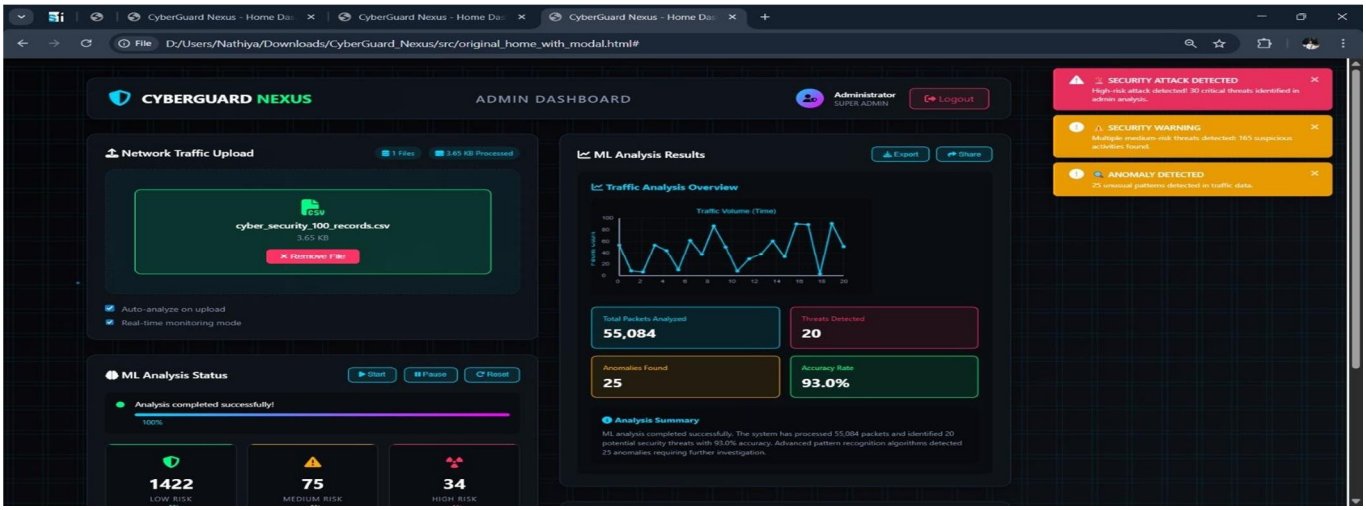


Fig. 4: Real-Time Threat Alert Notifications

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

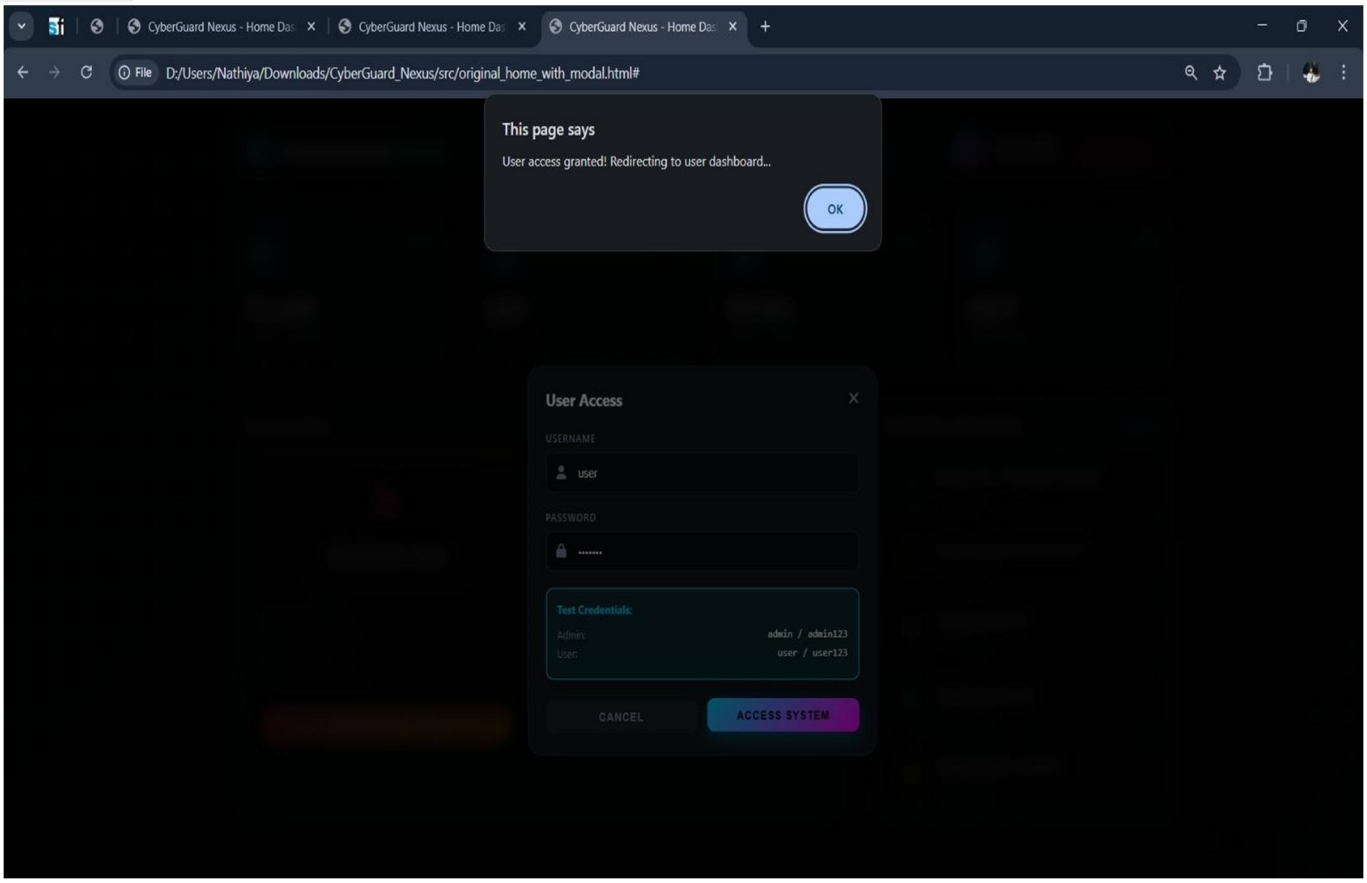


Fig. 5: User Login Interface

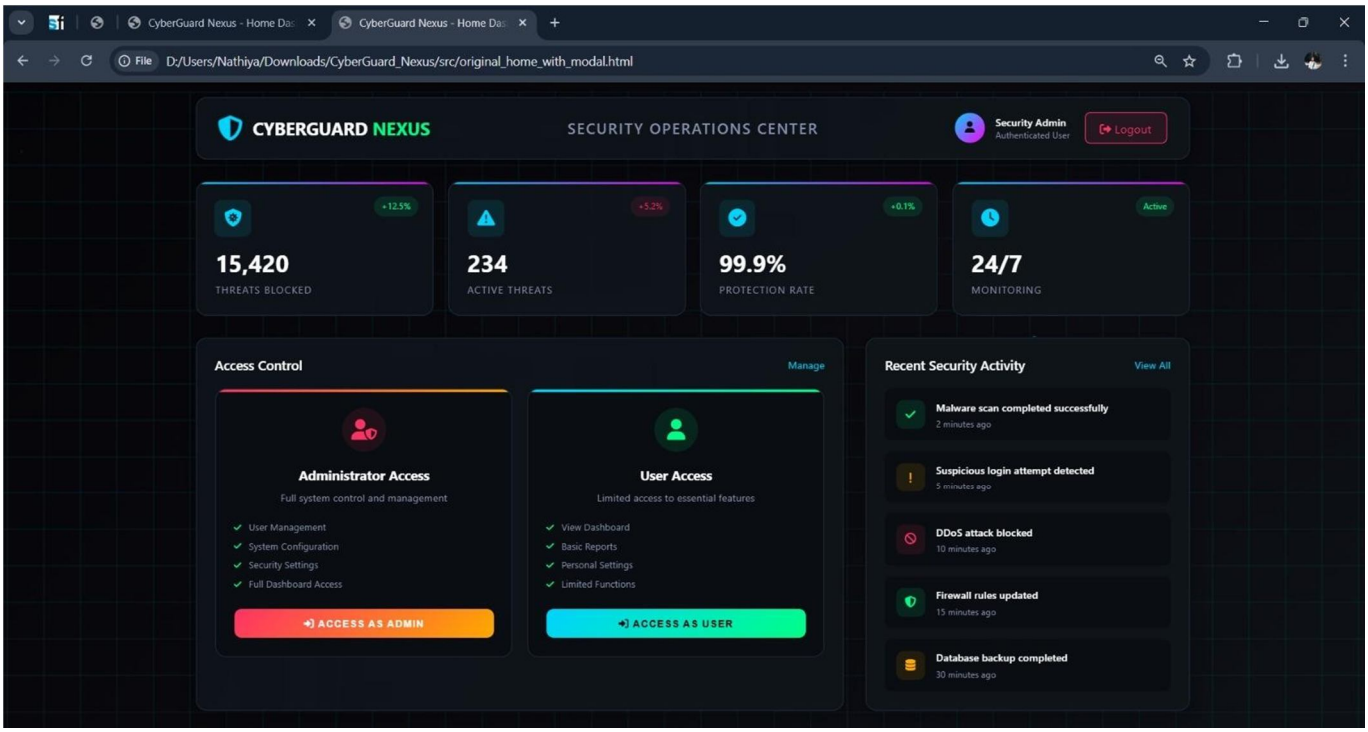
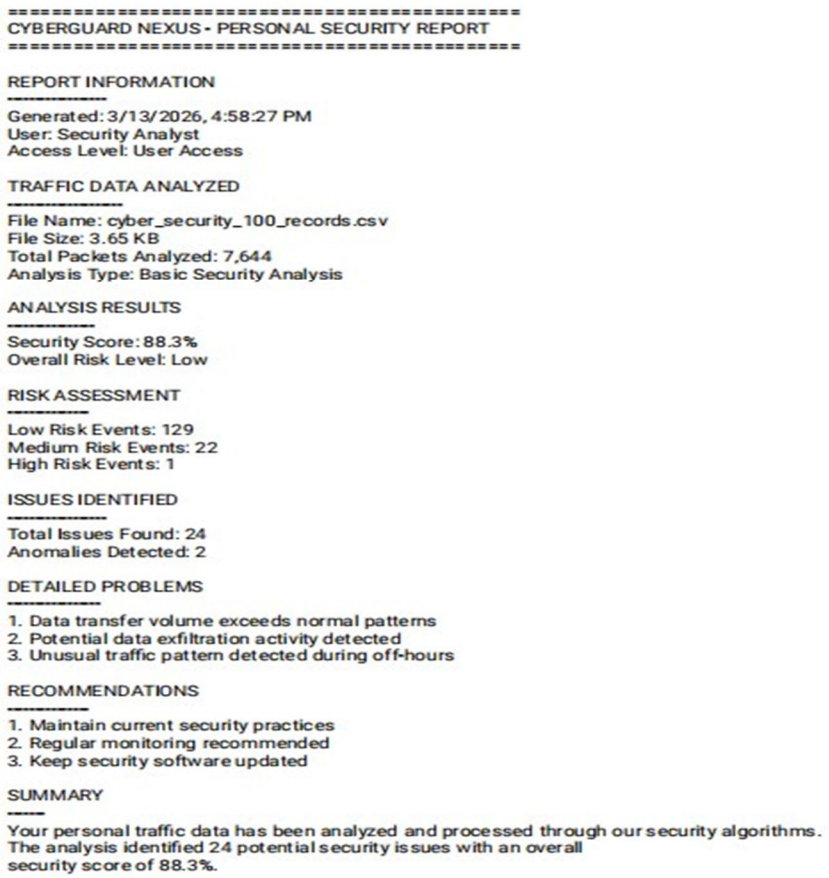


Fig. 6: User Dashboard and Personal Security Analysis

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



```
==========================================
CYBERGUARD NEXUS - PERSONAL SECURITY REPORT
==========================================

REPORT INFORMATION
------------------
Generated: 3/13/2026, 4:58:27 PM
User: Security Analyst
Access Level: User Access

TRAFFIC DATA ANALYZED
---------------------
File Name: cyber_security_100_records.csv
File Size: 3.65 KB
Total Packets Analyzed: 7,644
Analysis Type: Basic Security Analysis

ANALYSIS RESULTS
----------------
Security Score: 88.3%
Overall Risk Level: Low

RISK ASSESSMENT
---------------
Low Risk Events: 129
Medium Risk Events: 22
High Risk Events: 1

ISSUES IDENTIFIED
-----------------
Total Issues Found: 24
Anomalies Detected: 2

DETAILED PROBLEMS
-----------------
1. Data transfer volume exceeds normal patterns
2. Potential data exfiltration activity detected
3. Unusual traffic pattern detected during off-hours

RECOMMENDATIONS
---------------
1. Maintain current security practices
2. Regular monitoring recommended
3. Keep security software updated

SUMMARY
-------
Your personal traffic data has been analyzed and processed through our security algorithms.
The analysis identified 24 potential security issues with an overall
security score of 88.3%.
```

Fig. 7: Generated Personal Security Report Summary

VII. CONCLUSION

The CyberGuard Nexus system presents an intelligent and efficient approach for cybersecurity threat detection and risk profiling using machine learning techniques. The integration of classification, clustering, and risk analysis enables the system to identify malicious activities and categorize threats based on their severity. The use of the Random Forest algorithm enhances detection accuracy, while clustering techniques support the identification of similar attack patterns. The system demonstrates strong performance in analyzing network traffic and detecting cyber threats with reduced false positives. The implementation of real-time monitoring and alert mechanisms ensures timely identification of suspicious activities, enabling proactive security management. Additionally, the risk profiling module assists in prioritizing threats, which improves decision-making in cybersecurity environments. Overall, the proposed system provides a scalable and adaptable solution for modern cybersecurity challenges. The combination of intelligent analysis, automation, and efficient data processing makes CyberGuard Nexus suitable for real-world applications. Future work can focus on integrating deep learning techniques and expanding the system to handle large-scale, real-time data streams for enhanced threat detection capabilities.

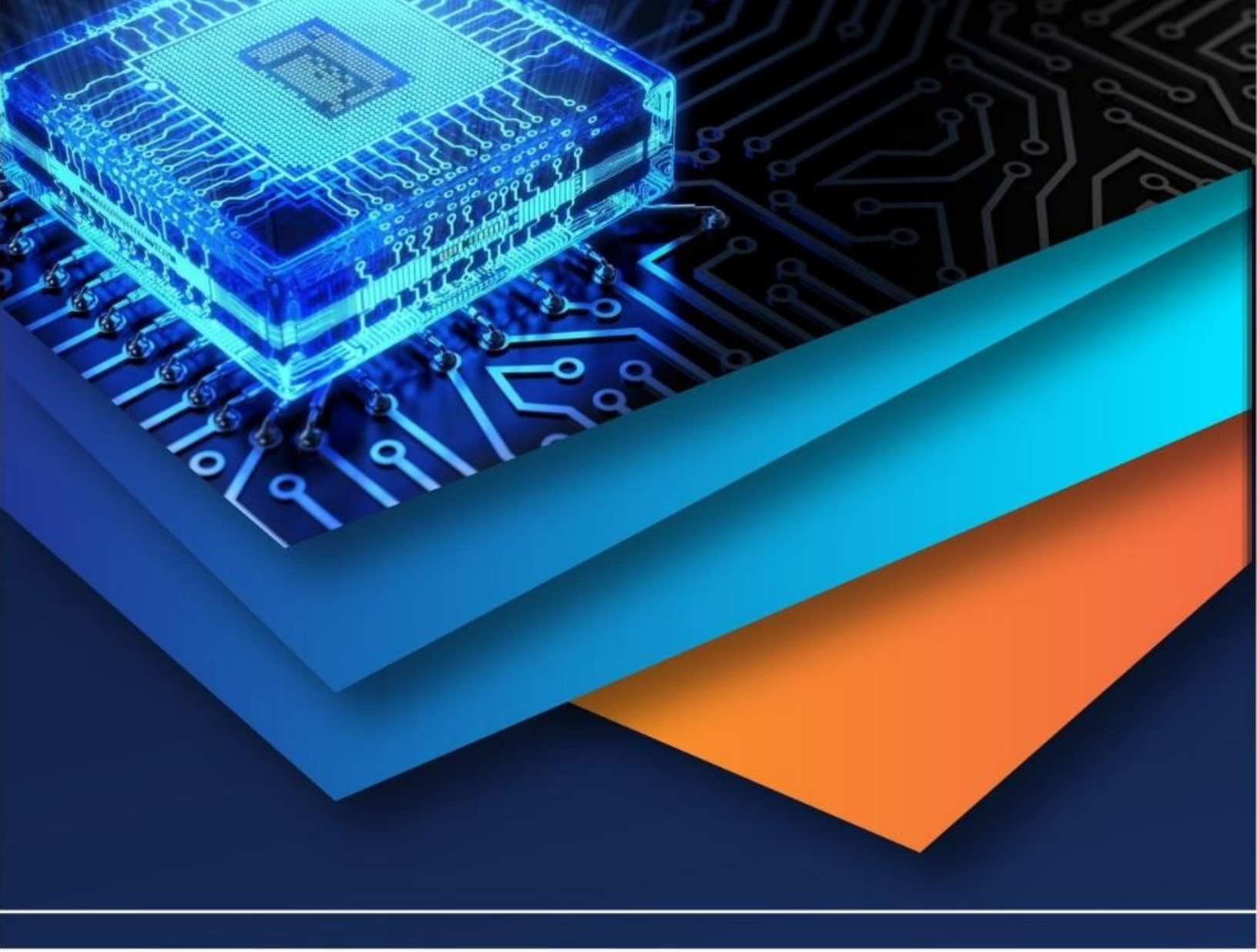
REFERENCES

[1] S. Latif, Z. Zou, J. Qadir, H. Farooq, and A. Imran, “AI-Based Intrusion Detection: A Survey and Future Directions,” IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1–25, 2022.
[2] N. Moustafa, “A New Distributed Architecture for Evaluating AI-Based Security Systems,” Future Generation Computer Systems, vol. 131, pp. 1–14, 2022.
[3] M. Alauthman et al., “Intrusion Detection System Using Machine Learning for IoT Environments,” IEEE Access, vol. 10, pp. 1–15, 2022.
[4] A. Thakkar and R. Lohiya, “A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT,” Archives of Computational Methods in Engineering, vol. 29, pp. 1–20, 2022.
[5] H. T. Nguyen, Q. T. Nguyen, and T. N. Nguyen, “Deep Learning-Based Intrusion Detection System Using CNN and LSTM,” IEEE Access, vol. 11, pp. 1–12, 2023.
[6] Y. Zhang, X. Chen, and L. Wang, “Network Intrusion Detection Based on Hybrid Machine Learning Models,” Computers & Security, vol. 124, pp. 1–13, 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[7] R. K. Sharma and P. K. Gupta, "AI-Driven Cybersecurity Framework for Threat Detection and Risk Assessment," Journal of Information Security and Applications, vol. 75, pp. 1–12, 2023.
[8] S. Patel and M. Shah, "Machine Learning-Based Threat Detection System for Cybersecurity Applications," IEEE Access, vol. 12, pp. 1–15, 2024.
[9] A. Verma and D. Singh, "Advanced Intrusion Detection Using Ensemble Learning Techniques," Expert Systems with Applications, vol. 230, pp. 1–14, 2024.
[10] K. Reddy and S. Kumar, "Real-Time Cyber Threat Detection Using AI and Data Analytics," Future Internet, vol. 16, no.
[11] 2, pp. 1–12, 2024.
[12] P. Sharma et al., "Deep Learning-Based Cybersecurity Threat Detection and Classification," IEEE Access, vol. 13, pp.
[13] 1–18, 2025.
[14] L. Wang, Y. Liu, and H. Zhao, "Intelligent Risk Profiling for Cybersecurity Using Machine Learning," Computers & Security, vol. 135, pp. 1–15, 2025.
[15] A. Singh and R. Patel, "Machine Learning Techniques for Network Intrusion Detection Systems," IEEE Access, vol. 11, pp. 1–14, 2023.
[16] J. Lee, K. Park, and S. Kim, "An Efficient AI-Based Framework for Cyber Threat Detection," Computers & Security, vol. 120, pp. 1–13, 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)