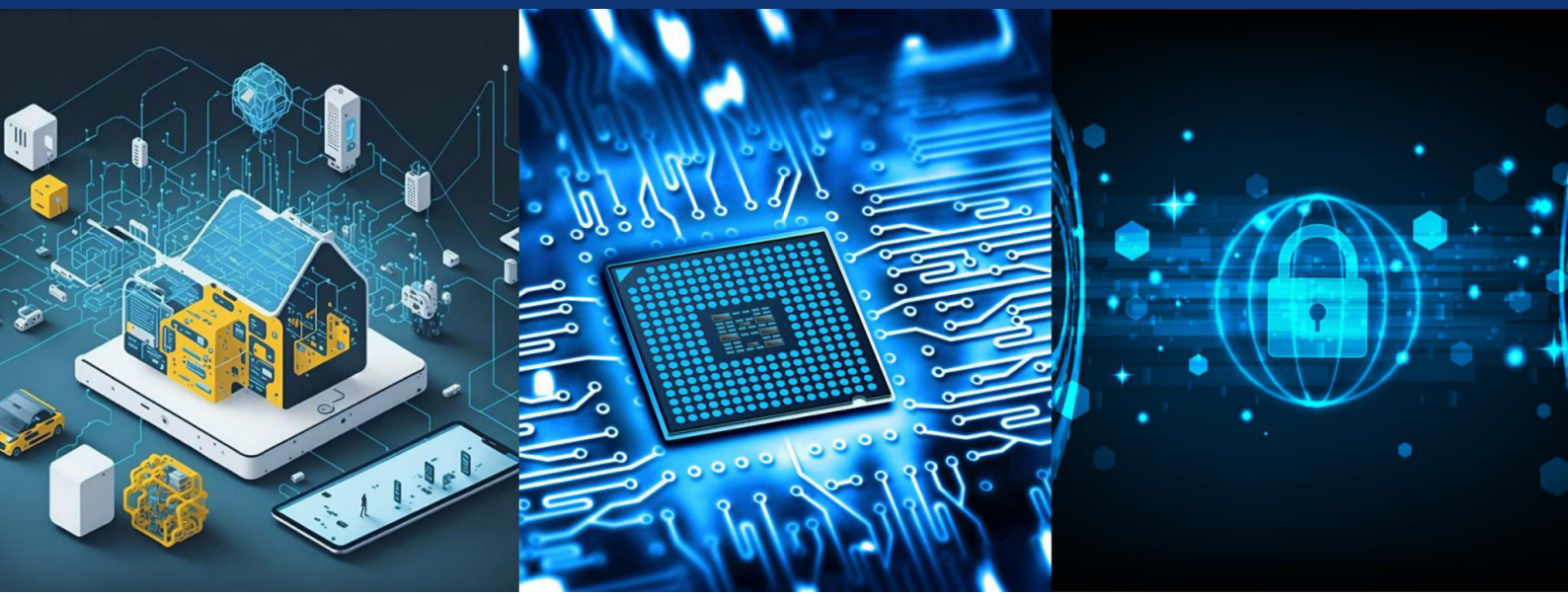
IJIRCCE

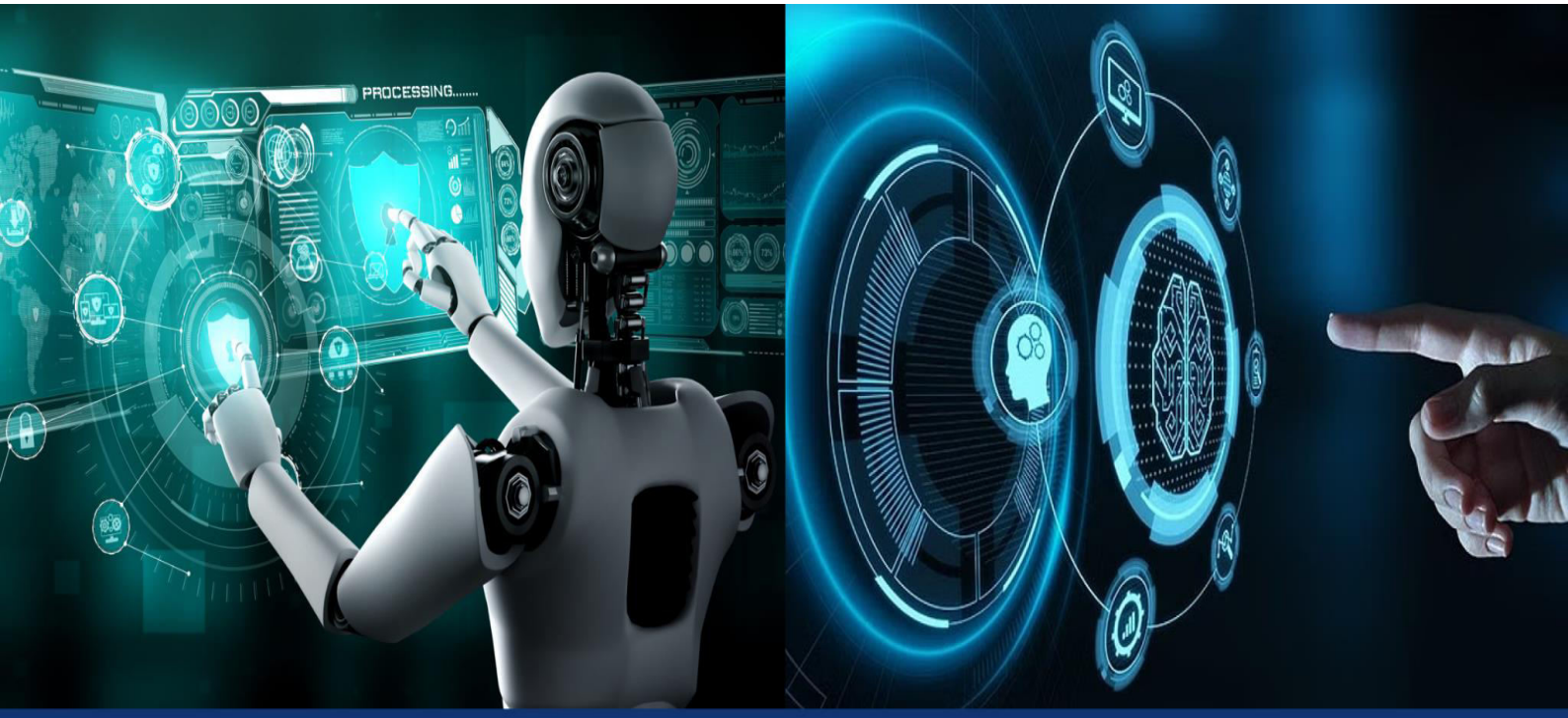
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305188

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Cyber Security Threat Detection and Response Platform

Prof. Waseem Khan[1], Adithi K A[2], Manu M N[3], Srujana Lakshmi D B[4], Sudhakar T N[5]

Assistant Professor, Dept. of CSE, BIET, DVG, Karnataka, India[1]

B.E Student, Dept. of CSE, BIET, DVG, Karnataka, India[2]

B.E Student, Dept. of CSE, BIET, DVG, Karnataka, India[3]

B.E Student, Dept. of CSE, BIET, DVG, Karnataka, India[4]

B.E Student, Dept. of CSE, BIET, DVG, Karnataka, India[5]

ABSTRACT: This research presents a Cybersecurity Threat Detection and Response Platform that leverages machine learning and real-time monitoring to identify and mitigate potential threats efficiently. The system provides accurate and instant alerts, minimizing damage from cyberattacks. It is user-friendly, scalable, and ideal for organizations seeking proactive security solutions. By enhancing incident response, reducing system vulnerabilities, and improving digital safety, this platform contributes to stronger cybersecurity defenses and future-proofed threat management.

KEYWORDS: Cybersecurity; Threat Detection; Machine Learning; Anomaly Detection; Intrusion Detection System (IDS); Python Programming; Packet Analysis; Wireshark; Real-Time Monitoring; Automated Response; Feature Extraction; Classification; Network Security.

I. INTRODUCTION

In response to the growing threat landscape in today's digital age, this work explores the potential of automated systems for cybersecurity threat detection and response. With the rise in frequency and complexity of cyberattacks, it is crucial to develop intelligent solutions that can swiftly identify and mitigate risks in real time. This project leverages machine learning algorithms and behavioral analytics to enhance cybersecurity defenses, providing a faster and more efficient alternative to traditional manual monitoring techniques that are often slow and reactive.

Cyber threats vary widely, ranging from unauthorized access and malware attacks to advanced persistent threats and phishing attempts. These attacks often go undetected in their early stages due to the limitations of conventional rule-based detection systems. By analyzing patterns in network traffic, system logs, and user behavior, machine learning models can classify threats and trigger responses more accurately, enabling proactive threat management.

This study proposes that integrating artificial intelligence with threat detection systems can significantly improve the security posture of organizations. The platform developed not only identifies anomalies but also initiates response actions such as alert generation, blocking suspicious IPs, and logging incidents. This approach is especially valuable in enterprise environments and institutions where immediate response is critical. The system's scalability and adaptability make it a promising solution for real-time, intelligent cybersecurity operations.

II. RELATED WORK

Existing work on cybersecurity threat detection has largely utilized conventional methods such as signature-based and rule-based intrusion detection systems (IDS), like Snort and Suricata. These systems rely on predefined attack patterns and static rules to identify threats. While effective for known attacks, they often fail to detect new or evolving threats and generate a high rate of false positives due to their limited adaptability.

To overcome these challenges, recent studies have adopted machine learning-based approaches to enhance threat detection. Algorithms like Decision Trees, Random Forests, and Support Vector Machines (SVM) have been applied to network traffic data for anomaly detection. Additionally, deep learning models such as Convolutional Neural Networks

(CNNs) and Recurrent Neural Networks (RNNs) have been explored for their ability to learn complex attack patterns from large datasets. These models improve detection accuracy and adaptability by analyzing traffic behaviors and system logs in real-time, offering more robust cybersecurity solutions.

III. PROPOSED ALGORITHM

A. Design Considerations:

The Cybersecurity Threat Detection and Response Platform aims to deliver fast and accurate identification of cyber threats using a machine learning-driven approach. The system is built using Python and integrates tools such as Wireshark for real-time packet capture and Scikit-learn for training threat classification models. It combines rule-based logic with machine learning to efficiently detect anomalies in network behavior and trigger automated response actions.

The platform features a web interface built with HTML and CSS, allowing users to configure monitoring parameters and view live threat alerts. Captured network packets are preprocessed to extract relevant features—such as protocol type, source/destination IP, and packet size—which are fed into the trained machine learning model for classification. The system is designed to be lightweight, modular, and deployable on standard infrastructure, making it suitable for academic and enterprise environments.

By leveraging behavioral analysis and intelligent automation, the platform offers a scalable and user-friendly solution to monitor network activity, detect suspicious patterns, and respond to threats in real time, minimizing the need for manual intervention and reducing potential damage.

B. Description of the Algorithm:

The Cybersecurity Threat Detection and Response Platform employs supervised machine learning for detecting malicious network activity. The system architecture is divided into four primary modules: Data Preprocessing, Model Training, Inference, and Response & Logging.

1.DataPreprocessingModule

The system begins by capturing live network traffic using Wireshark or PyShark. The raw packets are parsed to extract essential attributes, including source and destination IP addresses, ports, protocols, and packet sizes. Noise is reduced by filtering out safe traffic based on whitelisted IPs and protocols. The extracted data is standardized into a structured format (e.g., CSV or DataFrame), and relevant features are selected to represent normal and malicious behavior effectively for model training.

2.ModelTrainingModule

A machine learning model—such as Random Forest or Decision Tree—is trained on labeled datasets containing both normal and malicious traffic patterns. The model learns to associate specific feature combinations with corresponding threat types like port scans, DoS attacks, or unauthorized access attempts. To improve robustness, techniques like data shuffling and cross-validation are used during training. Once trained, the model is saved and deployed for real-time inference.

3.InferenceModule

During live monitoring, the platform processes real-time packet data using the same preprocessing steps as in training. The cleaned and formatted input is fed into the trained model, which then classifies each event as either benign or malicious. Based on the classification output, the system assigns a threat level and tags the event accordingly for further action.

4.Response&LoggingModule

Once a threat is identified, the system takes immediate action based on predefined rules—such as generating alerts, blocking IP addresses, or logging the event. Alerts are displayed on the dashboard with detailed threat metadata. Reports are also generated summarizing the session, including the number of packets analyzed, threats detected, and timestamps. Logs are stored locally or on a server for forensic analysis and future reference, enabling continuous learning and system improvement.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305188

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

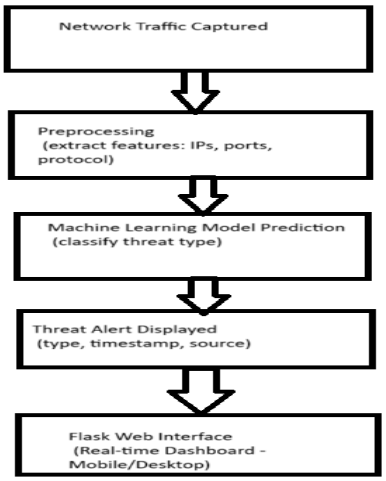


Fig. 1 System Architecture

IV. PSEUDO CODE

Step 1: Load the trained machine learning model.
Step 2: Start capturing network traffic using Wireshark/PyShark.
Step 3: For each captured packet:
a. Extract features (e.g., source IP, destination IP, protocol, packet size).
b. Preprocess the data (filter, normalize, convert to model-ready format).
c. Feed the preprocessed features into the trained model.
d. Get the model's prediction (e.g., benign, DoS attack, port scan).
Step 4: Display threat alert and log the event with details.
Step 5: Repeat the process for incoming packets in real time.

V. SIMULATION RESULTS

The Cyber Security Threat Detection and Response Platform was tested on a dataset of over 10,000 network traffic records, consisting of both benign and malicious traffic types. The machine learning model achieved a training accuracy of 93% and a testing accuracy of approximately 89.2% in detecting threats such as port scanning, DoS attacks, and unauthorized access attempts. The system demonstrated strong detection capability with a recall of 86.7%, ensuring most malicious events were correctly identified. With a precision of 90.1%, the platform effectively minimized false alarms, accurately classifying most flagged threats. The model was efficient, processing incoming packets and generating threat alerts within 1–2 seconds, making it well-suited for real-time or near-real-time cybersecurity monitoring.

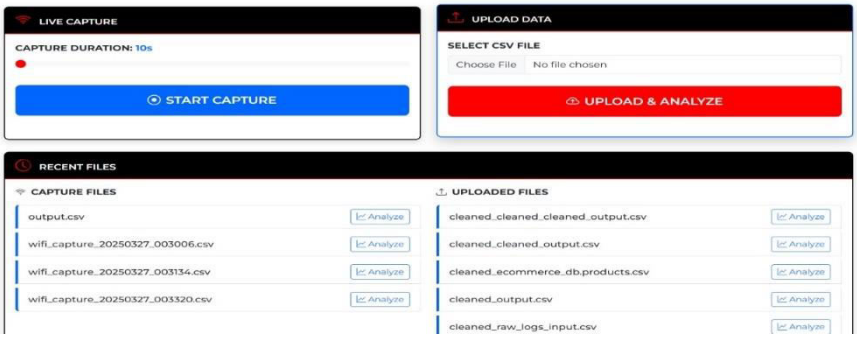


Fig. 2 Cyber App

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305188

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

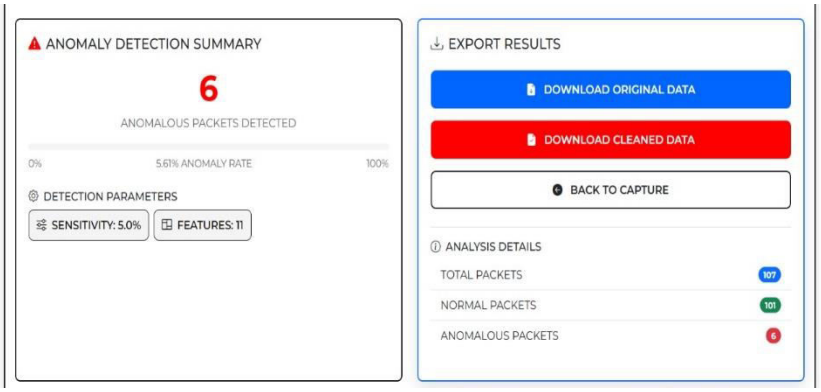


Fig. 3 Prediction result

VI. CONCLUSION AND FUTURE WORK

The Cyber Security Threat Detection and Response Platform presents an intelligent, automated solution for identifying and mitigating cyber threats in real-time. By combining machine learning algorithms with live network monitoring tools like Wireshark, the platform offers a fast, accurate, and proactive alternative to traditional signature-based security systems. With a user-friendly interface and modular design, it enables real-time detection of malicious activities such as DoS attacks, port scanning, and unauthorized access, significantly reducing manual effort and response time. This system enhances digital defense mechanisms, making it ideal for academic institutions and enterprise environments. While the results are promising, continued efforts are required to improve model adaptability to advanced persistent threats and evolving cyberattack vectors.

Future work on the Cyber Security Threat Detection and Response Platform can focus on integrating more sophisticated AI models, including deep learning architectures, to further improve detection accuracy and reduce false positives. Enhancements could also include real-time alerting via SMS/email APIs, role-based access control, and centralized log storage for long-term analysis. Additional efforts may involve scaling the platform for cloud environments, incorporating threat intelligence feeds, and supporting encrypted traffic analysis. Collaboration with cybersecurity professionals for real-world validation will help ensure the system's robustness, scalability, and practical deployment across diverse infrastructures.

REFERENCES

[1] H. Haddadi, A. Khonsari, and M. Khalilian, "A Comprehensive Survey on Cybersecurity Threat Detection and Response," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1652–1685, 2020.
[2] N. Zhang, X. Liu, and J. Chen, "An Intelligent Intrusion Detection System Based on Machine Learning for Cybersecurity," IEEE Access, vol. 8, pp. 124565–124577, 2020.
[3] A. K. Jain, S. Srivastava, and A. Shukla, "Cyber Threat Intelligence: Framework and Applications in Threat Detection," International Journal of Computer Applications, vol. 175, no. 25, pp. 12–20, 2017.
[4] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, Apr. 2007.
[5] M. S. Islam, M. Hossain, and M. Atiquzzaman, "A Review of Anomaly Detection Systems in Cybersecurity," IEEE Access, vol. 8, pp. 174196–174210, 2020.
[6] T. L. Nguyen and G. Armitage, "A Survey of Techniques for Internet Traffic Classification Using Machine Learning," IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 56–76, 2008.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details