International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Insider Threat Detection Using Machine Learning

Prof. Tanuja Zende[1], Tanuja Zende[2], Krishna Wagh[3], Asfahan Shaikh[4]

MIT Art Design and Technology
Department of Computer Engineering, MIT Art, Design and Technology University, Pune, India
[3]krishnaw.official@gmail.com, [4]asfahan786786@gmail.com

Abstract
Insider threats represent one of the most significant cybersecurity challenges in modern organizations. These threats originate from individuals within the organization who have authorized access to sensitive systems and data. This research paper presents an intelligent system for Insider Threat Detection using Machine Learning (ML) techniques. The system employs user behavior analytics, real-time log monitoring, and anomaly detection to identify suspicious activities. The proposed framework integrates a Flask-based web interface with a backend SQLite database and leverages scikit-learn for anomaly detection. The model effectively detects unauthorized access, abnormal data transfer, and unusual system usage patterns. The paper discusses methodology, implementation, challenges, and future enhancements involving deep learning and blockchain-based security measures.

Keywords
Insider Threats, Machine Learning, Cybersecurity, Anomaly Detection, User Behavior Analytics

I. INTRODUCTION

. In today's digital era, organizations across all sectors are increasingly dependent on information technology and interconnected systems to manage their daily operations. While this digital transformation enhances efficiency, accessibility, and scalability, it simultaneously exposes organizations to a wide range of cybersecurity threats. Traditionally, cybersecurity efforts have focused on defending against external adversaries such as hackers, cybercriminals, and nation-state actors. However, one of the most dangerous and often overlooked categories of threats originates from within the organization itself — **insider threats**.

An insider threat refers to a security risk posed by individuals who have legitimate access to an organization's systems, data, or networks but misuse that access intentionally or unintentionally. Such individuals may include employees, contractors, business partners, or former staff members who exploit their privileges for malicious purposes such as data theft, sabotage, fraud, or espionage. According to industry reports, insider-related incidents account for a significant percentage of all cybersecurity breaches, often leading to severe financial and reputational damage because these threats are difficult to detect and mitigate using traditional security mechanisms.

Unlike external attacks, insider threats are challenging to identify because the malicious activities are performed by authorized users who already possess the required permissions to access critical systems. Traditional rule-based or signature-based detection methods often fail in these scenarios since insiders can operate within normal behavioral boundaries, making anomalies subtle and context-dependent. Hence, there is a critical need for **intelligent detection mechanisms** that can analyze user behavior patterns and distinguish between legitimate and suspicious activities in real-time.

This research focuses on developing a **Machine Learning (ML)-based Insider Threat Detection System** that leverages advanced data analytics and behavioral modeling to identify potential threats from within an organization. The system collects and analyzes system logs, user activities, file access behavior, USB usage, and network connections to build comprehensive user profiles. Using these profiles, the ML model detects deviations from normal behavior, flags anomalies, and triggers alerts before any significant damage occurs.

Furthermore, the system incorporates a **Flask-based web interface** and an **SQLite database** for real-time monitoring, visualization, and data storage. The use of open-source libraries such as **pandas, NumPy, and scikit-learn** enables efficient data preprocessing and model training. By employing anomaly detection algorithms, the system aims to reduce false positives, improve accuracy, and enhance overall security posture.

The motivation behind this project stems from the increasing frequency and sophistication of insider-related incidents in both corporate and government environments. The proposed system not only aids in proactive threat detection but also serves as a scalable and adaptable solution that can evolve with changing behavioral dynamics. The outcomes of this study are expected to contribute significantly to the field of cybersecurity, especially in the domain of user behavior analytics and predictive threat intelligence.

II. LITERATURE REVIEW

Several studies have explored insider threat detection using various approaches, including rule-based systems, statistical analysis, and machine learning. Traditional rule-based methods rely on predefined patterns of malicious behavior but struggle to detect zero-day threats or new attack types. Machine Learning, however, can learn user activity patterns and detect anomalies dynamically. Previous works, such as those presented in IEEE and MDPI journals, have utilized datasets like the CERT Insider Threat Dataset to train models capable of identifying unauthorized access and data exfiltration.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

The proposed system architecture integrates multiple components for data collection, analysis, and visualization. It consists of the following modules:

1. Data Collection: Logs user activities such as login attempts, file access, USB usage, and network connections.

2. Data Storage: Uses SQLite database to store user logs and risk scores.

3. Machine Learning Module: Employs scikit-learn algorithms to detect anomalies in behavioral data.
4. Flask API: Handles communication between the backend ML model and the web-based dashboard.
5. Admin Dashboard: Visualizes alerts, user scores, and activity reports in real-time.

IV. IMPLEMENTATION DETAILS

The system was implemented using Python programming language. Flask framework was used for building APIs and the web dashboard, while SQLite served as the backend database. The psutil library and bash scripts were employed to collect system logs and process data. Data preprocessing was handled using pandas and NumPy, and the machine learning models were built using scikit-learn. The model training focused on anomaly detection by evaluating deviations in user activities from normal behavior.

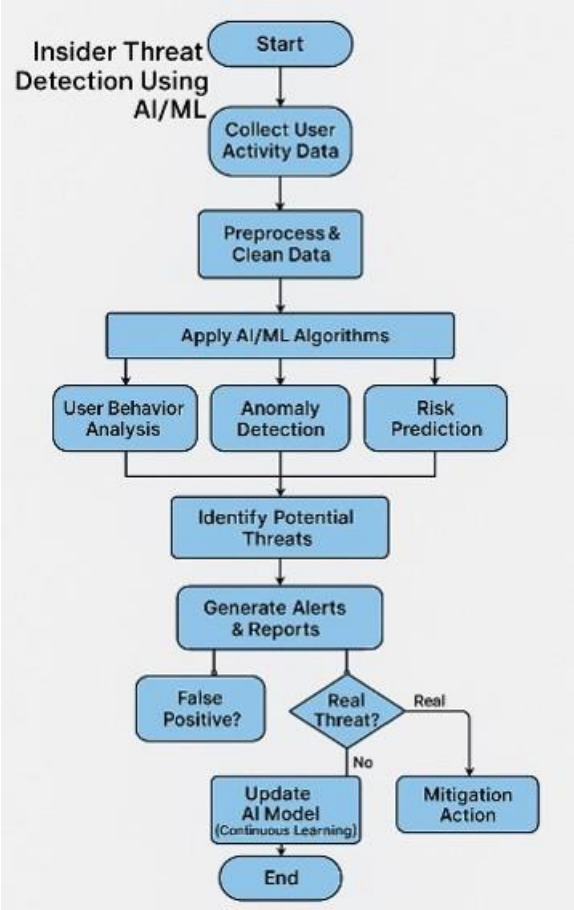
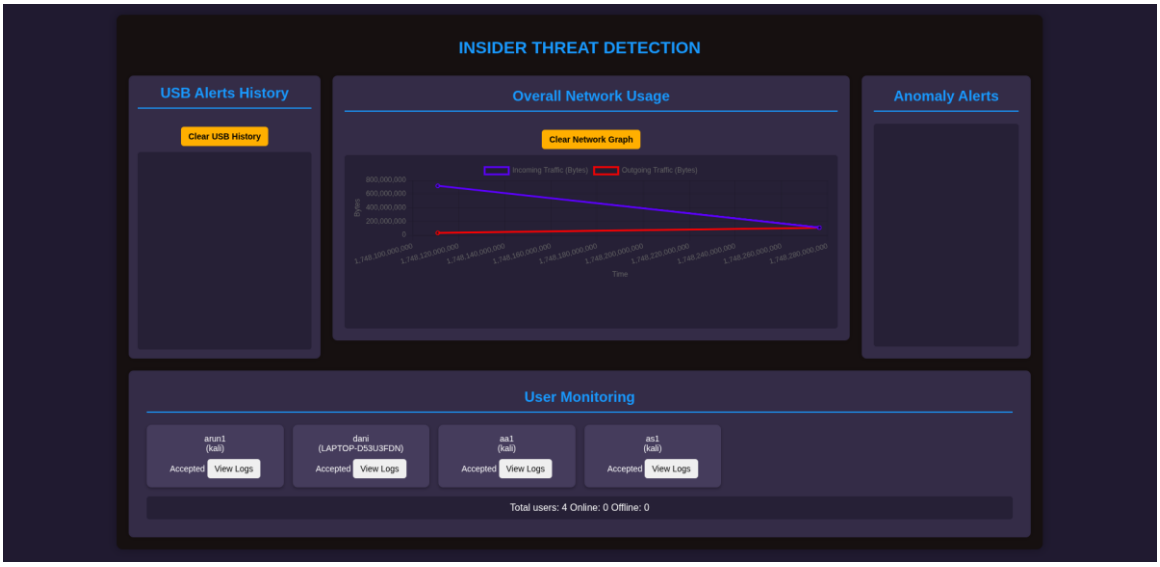
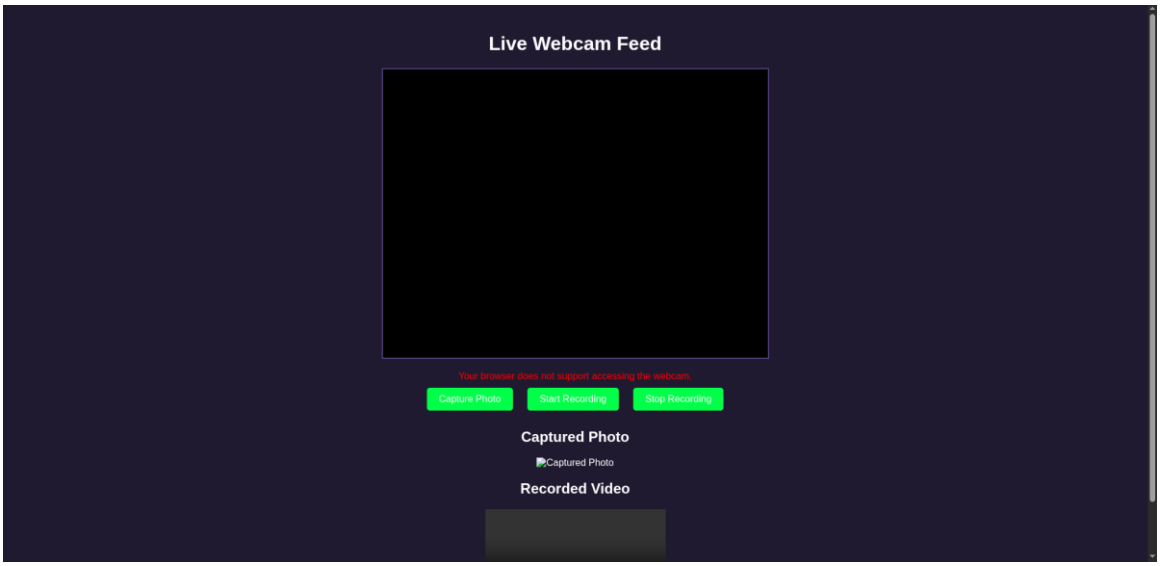


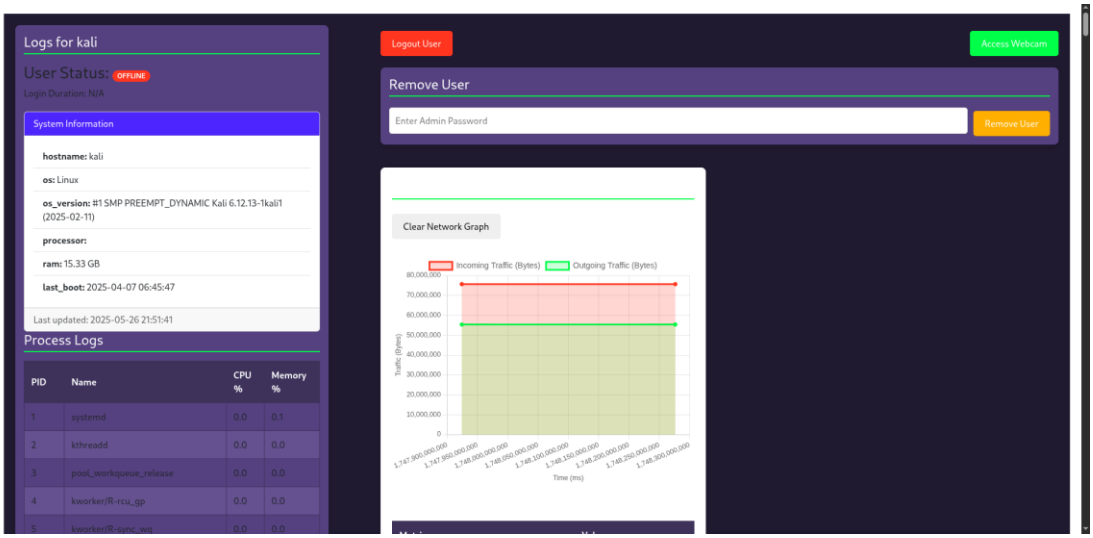
Fig. 1 – Implementation Workflow

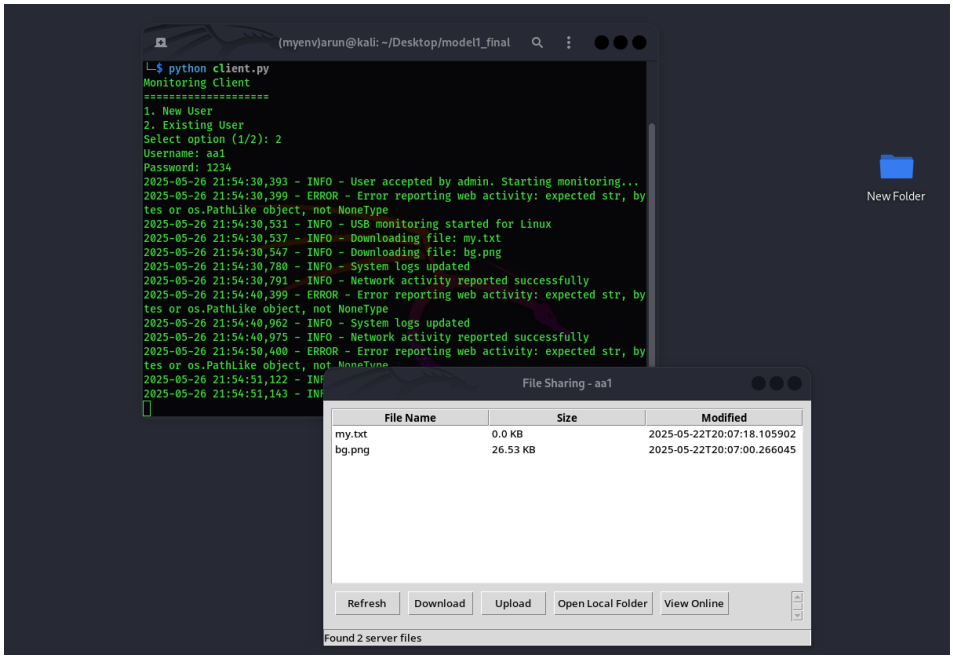
V. RESULTS AND DISCUSSION

The developed system successfully detected abnormal patterns such as unusual login times, unauthorized file transfers, and external device access. Real-time alerts were generated for anomalies based on predefined thresholds. The results demonstrated that machine learning algorithms, specifically anomaly detection models, effectively reduced false positives compared to traditional rule-based systems. The system's efficiency was tested using the CERT Insider Threat Dataset, and the model achieved high accuracy in detecting malicious activities.


INSIDER THREAT DETECTION
USB Alerts History
Clear USB History
Overall Network Usage
Clear Network Graph
Incoming Traffic (Bytes)
Outgoing Traffic (Bytes)
Anomaly Alerts
User Monitoring
arun1 (kali)
dani (LAPTOP-D53U3FDN)
aa1 (kali)
as1 (kali)
Accepted
View Logs
Total users: 4 Online: 0 Offline: 0


Live Webcam Feed
Your browser does not support accessing the webcam.
Capture Photo
Start Recording
Stop Recording
Captured Photo
Captured Photo
Recorded Video


Logs for kali
User Status:
OFFLINE
System Information
hostname: kali
os: Linux
processor:
ram: 15.33 GB
Process Logs
PID
Name
CPU %
Memory %
Logout User
Access Webcam
Remove User
Enter Admin Password
Remove User
Clear Network Graph
Incoming Traffic (Bytes)
Outgoing Traffic (Bytes)



VI. CONCLUSION AND FUTURE SCOPE

The Insider Threat Detection System using Machine Learning provides an efficient approach to identifying and mitigating cybersecurity risks originating from within an organization. By integrating machine learning algorithms, user behavior analytics, and real-time monitoring, the system enhances the organization's ability to detect suspicious activities early. In the future, the system can be expanded using deep learning for better accuracy and blockchain for secure log management. Additionally, automation in threat response could further strengthen system resilience.

ACKNOWLEDGMENT

The authors express their gratitude to MIT Art, Design and Technology University, Pune, for providing the necessary infrastructure and support for this research. The guidance of faculty members and peers was instrumental in the successful completion of this project.

REFERENCES

1. https://ieeexplore.ieee.org/abstract/document/10695344
2. https://ieeexplore.ieee.org/document/10421133
3. https://scholar.google.com/scholar?q=10.1109%2FICAIBD57115.2023.10206282
4. https://www.mdpi.com/2076-3417/10/15/5208