International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

Machine Learning-Powered Insider Threat Detection System for Organizational Security and Risk Mitigation

[1]Dr. Y.Chitti Babu,[2]Shaik Suffia Kowsar,[3]Vemparala Srilakshmi,[4]Sagiri Sravya

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

Insider threats pose a significant risk to organizational security, as malicious or negligent actions by authorized users can lead to data breaches, financial losses, and operational disruptions. Traditional security mechanisms such as rule-based monitoring and signature-based detection are often ineffective in identifying complex and evolving insider behaviours. This paper presents a Machine Learning-Powered Insider Threat Detection System that analyzes user behaviour patterns to detect potential insider threats accurately. The proposed system utilizes machine learning algorithms to evaluate behavioural attributes and classify activities as normal or malicious. A web-based interface is developed using Python, HTML, CSS, and JavaScript to allow easy interaction and real-time threat prediction. Experimental results demonstrate that the system effectively identifies insider threats and enhances organizational security by enabling proactive risk mitigation.

KEYWORDS: ***Insider threat detection, Machine Learning, Cyber security, Behavioural Analysis, Organizational Security***

INTRODUCTION

With the rapid growth of digital technologies and networked systems, organizations increasingly rely on internal users to access critical data and resources. While external cyberattacks receive significant attention, insider threats remain one of the most challenging security issues due to the legitimate access privileges held by insiders. Insider threats may arise from malicious intent, negligence, or

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

compromised credentials, making detection difficult using conventional security approaches.Traditional insider threat detection systems depend on predefined rules and static thresholds, which fail to adapt to evolving user behaviour patterns. Machine learning provides an effective solution by learning from historical data and identifying anomalous activities in real time. By analyzing user behaviour, access patterns, and operational metrics, machine learning models can distinguish between normal and suspicious actions. This paper proposes a machine learning-based insider threat detection system that improves accuracy, adaptability.

LITERATURE SURVEY

Several studies have explored machine learning approaches for cybersecurity and insider threat detection. Supervised learning techniques such as Decision Trees, Random Forest, and Support Vector Machines have been used to classify user behavior based on activity logs. These models offer high accuracy but require labeled datasets, which are often difficult to obtain in real-world environments. Unsupervised learning methods like clustering and anomaly detection have also been applied to identify deviations from normal behavior. However, these methods may produce high false-positive rates. Recent research focuses on hybrid approaches that combine multiple behavioral features and machine learning models to enhance detection performance. Despite these advancements, many existing systems lack real-time detection capabilities and user-friendly interfaces.

RELATED WORK

Insider threat detection has been studied using rule-based monitoring and traditional security policies, but these methods fail to detect complex user behavior patterns. To improve accuracy, researchers have applied machine learning techniques such as Decision Trees and Random Forest to classify insider activities based on behavioral data. Unsupervised and anomaly detection methods have also been explored, though they often produce high false positives. Recent deep learning approaches offer better detection capabilities but require high computational resources. The proposed system adopts an efficient machine learning approach that balances accuracy and practical implementation.

EXISTING METHOD

Traditional insider threat detection methods depend on predefined rules, access control

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

policies, and manual monitoring. These systems analyze login attempts, file access, and network usage using static thresholds. However, such approaches fail to detect subtle behavioural anomalies and are ineffective against evolving attack patterns. Additionally, manual analysis is time-consuming and prone to human error, resulting in delayed threat identification.

PROPOSED METHOD

The proposed system employs machine learning techniques to analyze user behavioural attributes and detect insider threats. Input parameters representing behavioral characteristics are processed and evaluated using trained machine learning models. The system classifies activities as either normal or malicious based on learned patterns.A web-based application is developed using Python for backend processing and HTML, CSS, and JavaScript for frontend interaction. Users can input behavioral parameters, and the system provides instant threat prediction results. This approach improves detection accuracy, reduces false positives, and enables proactive security management.

SYSTEM ARCHITECTURE

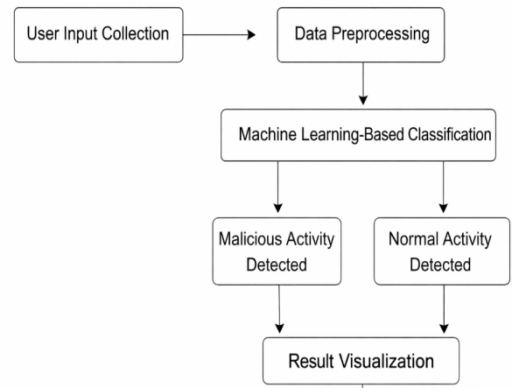

Fig 1: Architecture of the project

The system architecture consists of simple sequential blocks. User behaviour data is first collected through the input interface. This data is then preprocessed to remove inconsistencies and prepare it for analysis. The processed data is passed to the machine learning classification module, which analyzes behaviour patterns to identify insider threats. Based on the classification, the system determines whether the activity is normal or malicious. Finally, the prediction result is displayed to the user through the result visualization module.

RESULTS AND DISCUSSION

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

Fig 2: Home Page

The home page introduces the insider threat detection system and provides navigation options to access the threat identification module.

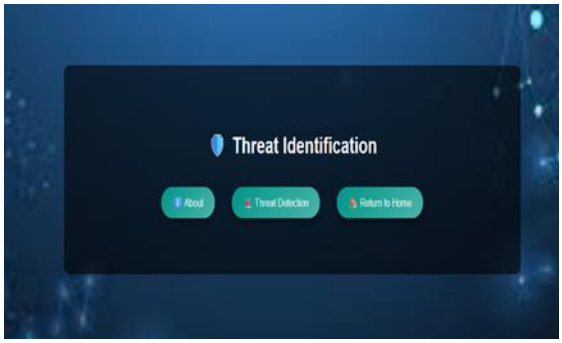

Fig 3: Threat Identification Page

Threat Identification page of the system. It acts as a navigation and control interface that allows users to access different modules of the application. The About option provides basic information about the system, the Threat Detection button directs the user to the input page for performing insider threat analysis, and the Return to Home option allows easy navigation back to the main page. This page helps users efficiently move between system functionalities and initiate threat detection.

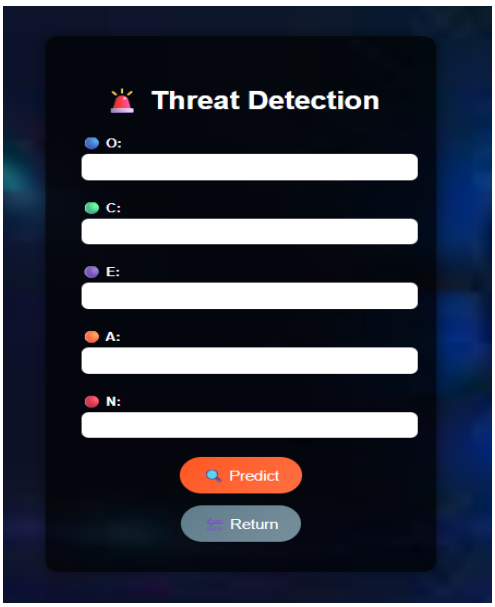

Fig 4: Threat Detection

Threat Detection input interface of the system. The page allows the user to enter behavioural parameter values labeled as O, C, E, A, and N, which represent monitored user behaviour attributes. These inputs are used by the machine learning model to analyze activity patterns. After entering the required values, the user clicks the Predict button to submit the data for analysis. The system then processes the inputs and determines whether the behavior indicates a potential insider threat. The Return button allows the user to navigate back to the previous page.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X
www.ijdim.com
Original Research Paper

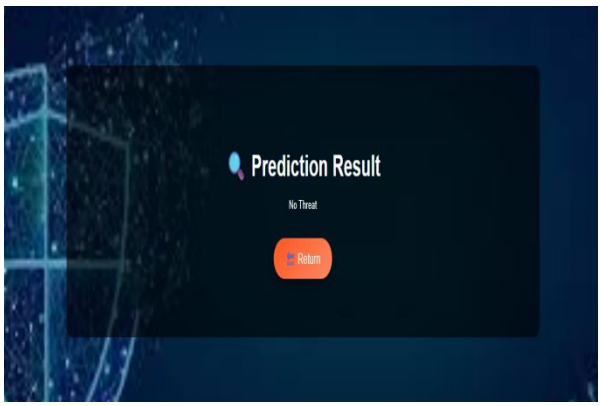

Fig 5: Prediction Result Page

Based on the machine learning model's evaluation, the system displays the result as "Threat Detected" or "No Threat Detected". This output enables security administrators to take immediate preventive actions. The experimental results demonstrate that the proposed system accurately detects insider threats and improves organizational security by reducing response time and enhancing situational awareness

CONCLUSION

This paper presented a Machine Learning-Powered Insider Threat Detection System designed to enhance organizational security. By analyzing user behavior through machine learning techniques, the system effectively identifies potential insider threats that traditional methods fail to detect. The web-based interface ensures ease of use and real-time threat prediction. The proposed approach improves detection accuracy, reduces manual intervention, and supports proactive risk mitigation strategies.

FUTURE SCOPE

Future enhancements may include integrating deep learning models for improved accuracy, incorporating real-time log streaming, and deploying the system on cloud platforms for scalability. Additional features such as role-based access control, alert notifications, and integration with Security Information and Event Management (SIEM) systems can further strengthen the system's effectiveness.

REFERENCES

1. Harini, D. P. (2013). Two Level Intrusion Detection For Detecting Intruders in Multitier Web Applications. *International Journal of Engineering & Science Research*, *3*, 472-478.
2. D. Arp et al., "Dos and Don'ts of Applying Machine Learning to Cyber Security," *arXiv preprint*, 2020.
3. S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson Education, 2021.
4. J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed., Morgan Kaufmann, 2012.

5. M. Song, H. Song, and L. Zhou, "Applications of Machine Learning in Cyber Security," *Information Processing & Management*, vol. 59, no. 2, 2022.

6. A. Alwarafy et al., "Security and Privacy Challenges in Cloud and IoT Environments," *Electronics*, vol. 9, no. 9, 2020.

7. S. Yadav, K. Kalaskar, and P. Dhumane, "A Comprehensive Survey on Cloud Computing Security," *Oriental Journal of Computer Science and Technology*, vol. 15, pp. 27–52, 2023.

8. T. Huong et al., "Low-Complexity Cyber Attack Detection Using Machine Learning," *arXiv preprint*, 2020.

9. M. S. Mahdavinejad et al., "Machine Learning Techniques for Cyber Security Applications," *Tikrit Journal of Pure Science*, 2022.

10. C. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.

11. A. Patcha and J. Park, "An Overview of Anomaly Detection Techniques," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 2, pp. 1–15, 2007.

12. E. Cole, Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft, Syngress, 2016.

13. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, 2010.

14. A. K. Rana, S. Gupta, and S. Arora, "A Survey of Machine Learning Methods for Security Applications," *Amity Journal of Computational Sciences*, vol. 2, no. 2, 2018.