ISSN: 3107-6513

HIDR-Insider: Cross-Artifact Insider Threat Detection System

Janaganish B , Ms. V.Yogashri M.Sc,

Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamilnadu, India.

Abstract *- Insider threats have become a serious cybersecurity challenge, as malicious or negligent activities are performed by trusted users within an organization. These threats often involve unauthorized data access, misuse of privileges, and covert data exfiltration, making them difficult to detect using traditional security systems. Early detection is essential to protect sensitive data and maintain system integrity, but conventional rule-based and signature-based methods often fail to identify complex behavioral patterns associated with insider misuse. This project proposes an intelligent system for detecting insider threats using cross-artifact digital forensics correlation. The system analyzes multiple sources of system activity such as login records, file access logs, and external device usage to identify suspicious behavior. By correlating these artifacts and evaluating user actions over time, the system assigns a risk score and classifies activities based on severity. Compared to traditional approaches, this method provides improved detection capability, better adaptability to unknown threats, and efficient identification of multi-step insider attacks. Therefore, it serves as a reliable and scalable solution for host-based security monitoring and forensic analysis.*

Keywords *– Insider Threat Detection, Digital Forensics, Behavioral Analysis, Log Correlation, USB Forensics, Risk Scoring, Cybersecurity, Event Analysis, Host Security, Incident Response.*

Introduction

Insider threats have emerged as a critical concern in modern cybersecurity, as they involve individuals within an organization who have legitimate access to systems and data. These threats may arise from malicious intent, negligence, or compromised accounts, leading to unauthorized data access, data leakage, or system misuse. Unlike external attacks, insider threats are difficult to detect because they often involve valid user credentials and normal system access patterns. With the increasing dependence on digital systems, the risk of insider misuse has grown significantly, posing serious threats to organizations and individuals.

Detecting insider threats requires analyzing user behavior and system activity to identify abnormal patterns. Activities such as unusual login times, excessive file access, and unauthorized use of external storage devices can indicate potential misuse. Additionally, system logs, event records, and device usage history provide valuable information for identifying suspicious actions. By analyzing and correlating these artifacts, it is possible to detect complex insider attack patterns.

Several approaches have been proposed for insider threat detection using behavior analysis and log monitoring techniques. Some methods focus on analyzing individual logs, while others use statistical and machine learning techniques to identify anomalies. However, many existing systems fail to correlate multiple activities, making it difficult to detect multi-step insider attacks. These systems may also generate false positives or lack real-time detection capabilities.

To address these challenges, this project proposes a cross-artifact correlation-based insider threat detection system. The system integrates multiple sources of forensic data and analyzes them collectively to identify suspicious behavior. By combining timeline analysis with risk scoring mechanisms, the proposed approach improves detection accuracy and provides meaningful insights into insider activities.

2.Related Works

Several approaches have been developed to detect insider threats using different cybersecurity techniques. Early methods relied on log monitoring and rule-based detection, which identify predefined suspicious activities but fail to detect new and evolving threats. To overcome this limitation, behavior-based techniques were introduced to analyze user activity patterns and detect anomalies.

Machine learning approaches such as clustering, classification, and anomaly detection have been widely used to identify unusual user behavior. These methods analyze system logs, user actions, and access patterns to distinguish between normal and suspicious activities. While these techniques provide improved accuracy, they often require large datasets and may produce false positives.

Digital forensics techniques have also been applied to insider threat detection by analyzing artifacts such as system logs, file access records, and device usage history. These approaches focus on identifying evidence of suspicious activity through detailed analysis of system data. However, many systems analyze artifacts independently without correlating them across multiple sources.

Recent research emphasizes the importance of correlation-based approaches, where multiple events are analyzed together to detect complex attack patterns. By combining behavioral analysis with forensic data correlation, these systems can identify multi-step insider threats more effectively. Despite these advancements, challenges such as real-time detection, scalability, and accuracy still remain, highlighting the need for more efficient and integrated solutions.

3.System Design

The system design focuses on developing an efficient insider threat detection system using cross-artifact correlation. The proposed system analyzes multiple sources of user activity data to identify suspicious behavior and assign risk levels. The architecture is designed to ensure modularity, scalability, and ease of analysis.

The primary contributions of this system are as follows:

(i) Collecting and processing user activity data from multiple sources such as login logs, file access records, and device usage.

(ii) Implementing timeline analysis to organize events in chronological order for better understanding.

(iii) Applying correlation techniques to identify relationships between multiple events.

(iv) Developing a risk scoring mechanism to classify user behavior based on severity.

3.1 Data Collection:

This process involves collecting system-level data such as login records, file access logs, and USB device usage history. The collected data serves as input for further analysis.

3.2 Event Processing:

In this stage, raw data is processed and structured into meaningful event records. Each event is categorized based on its type, such as login, file access, or device usage.

3.3 Correlation Analysis:

This process identifies relationships between multiple events to detect suspicious behavior patterns. For example, accessing sensitive files after inserting a USB device may indicate potential data exfiltration.

3.4 Risk Evaluation:

The system assigns a risk score based on detected patterns and anomalies. The score is used to classify user behavior into different risk

levels such as LOW, MEDIUM, and HIGH.

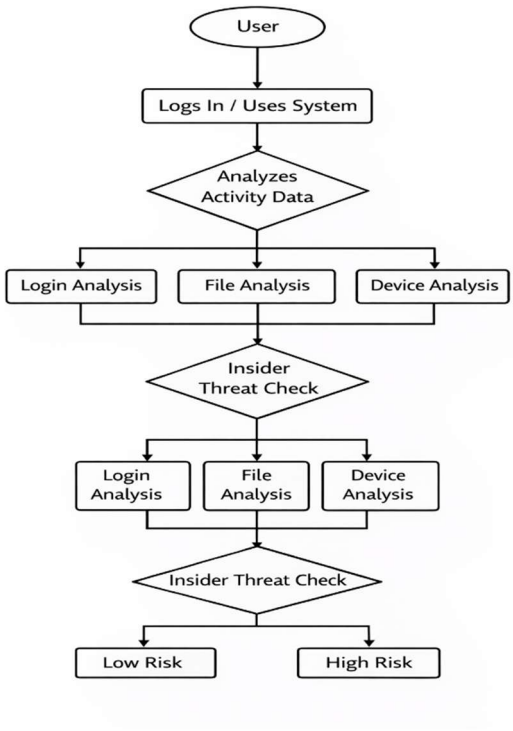


Fig 1. Dataflow Diagram

4. Object and Scope

The objective of this project is to develop an intelligent system for detecting insider threats using behavioral analysis and forensic data correlation. The system aims to identify suspicious user activities and prevent potential security breaches by analyzing system logs and user behavior patterns.

The scope of this project includes analyzing multiple types of system data, including login activity, file access records, and device usage history. The system focuses on detecting abnormal patterns and correlating multiple events to identify insider threats. It is designed to operate on a single host system and provide structured outputs for analysis and reporting.

5.Literature Review

Insider threat detection has gained increasing attention due to the growing number of internal security breaches. Traditional security systems are primarily designed to detect external threats, making them less effective in identifying insider misuse. As a result, recent research has focused on behavioral analysis and forensic techniques to improve detection accuracy.

Behavior-based approaches analyze user activity patterns to identify anomalies. Techniques such as user behavior analytics (UBA) and anomaly detection have been widely used to detect suspicious actions. These methods rely on statistical analysis and machine learning to identify deviations from normal behavior.

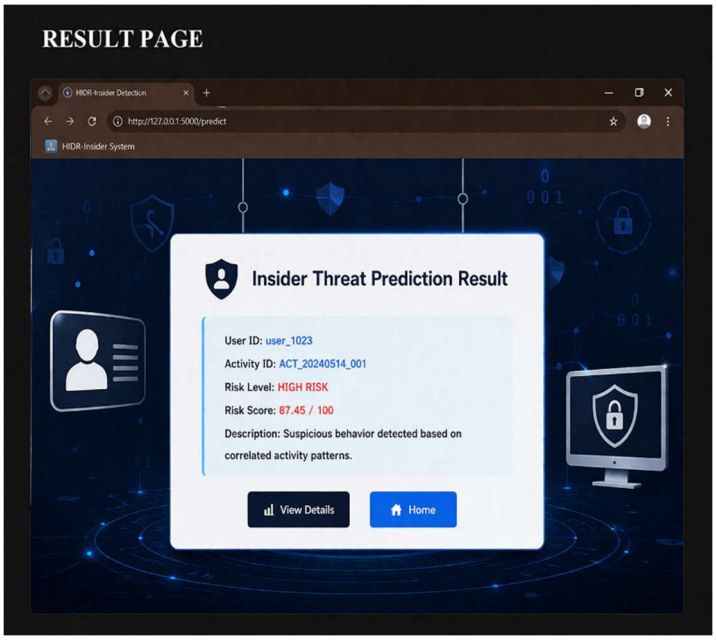
Digital forensics approaches focus on analyzing system artifacts such as logs, files, and device usage data. These methods provide detailed insights into user activities and help identify evidence of suspicious behavior. However, analyzing artifacts independently may not provide a complete picture of insider threats.

Correlation-based techniques combine multiple sources of data to identify complex attack patterns. By analyzing relationships between events, these approaches can detect multi-step insider attacks more effectively. Overall, combining behavioral analysis with forensic data correlation provides a more reliable solution for insider threat detection.

Insider threat detection has become an important area of research in cybersecurity due to the increasing number of internal security breaches and data misuse incidents. Traditional security systems are primarily designed to detect external attacks and often fail to identify threats originating from legitimate users. Recent studies have focused on behavior-based and anomaly detection techniques, where user activities such as login patterns, file access, and system usage are analyzed to identify deviations from normal behavior. Machine learning approaches, including classification and clustering methods, have been widely used to improve detection accuracy; however, they often require large

ISSN: 3107-6513

datasets and may produce false positives. Digital forensics techniques have also been applied to analyze system artifacts such as logs and device usage history, providing detailed insights into user actions. More advanced approaches emphasize the use of correlation-based analysis, where multiple events are examined together to detect complex and multi-step insider threats. Despite these advancements, challenges such as real-time detection, scalability, and accuracy remain, highlighting the need for efficient and integrated solutions like HIDR-Insider.



6. Output

The output of the system is presented in a structured format that includes a timeline of events, risk assessment, and identified findings. The results clearly show user activities, detected anomalies, and corresponding risk levels. This structured output helps administrators understand system behavior and take appropriate actions.

The output of the HIDR-Insider system is presented in a structured and user-friendly format that provides a clear overview of detected activities and potential security risks. It includes a chronological timeline of user actions such as login events, file accesses, and external device usage, along with a calculated risk score and corresponding threat level. The system highlights key findings such as abnormal behavior patterns and suspicious activities, enabling quick identification of potential insider threats. Additionally, real-time alerts are generated for high-risk activities, ensuring immediate attention from administrators. The output may also be exported in formats such as CSV for documentation and further analysis. Overall, the system provides clear, actionable insights that support effective monitoring, investigation, and response to insider security incidents.

7. Results

The results obtained from the proposed system demonstrate its effectiveness in detecting insider threats using behavioral analysis and event correlation. The system successfully identifies suspicious patterns such as abnormal login times, excessive file access, and unauthorized device usage. The results are presented in a clear and organized format, enabling easy interpretation.
By correlating multiple events, the system provides deeper insights into user behavior and improves detection accuracy. The risk scoring mechanism
effectively classifies activities based on severity, helping administrators prioritize responses. Overall, the system shows reliable performance in identifying potential insider threats.

8.Conclusion

The proposed HIDR-Insider system provides an effective solution for detecting insider threats using cross-artifact correlation and behavioral analysis. By analyzing multiple sources of system data, the system can accurately identify suspicious activities and classify them based on risk levels.

The system improves detection accuracy by correlating events and identifying complex patterns that are not detectable using traditional methods. It provides structured outputs and actionable insights, enabling administrators to take timely and effective measures. Overall, the proposed approach offers a scalable and efficient solution for insider threat detection and contributes to improving system security.

9. References

[1] Cappelli, D., Moore, A., and Trzeciak, R., “The CERT Guide to Insider Threats,” Addison-Wesley Professional, 2012.

[2] Greitzer, F.L. and Frincke, D.A., “Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation,” Insider Threats in Cyber Security, Springer, 2010.

[3] Eberle, W. and Holder, L., “Insider threat detection using graph-based approaches,” Cybersecurity Applications & Technology Conference for Homeland Security, IEEE, 2009.

[4] Salem, M.B., Hershkop, S., and Stolfo, S.J., “A survey of insider attack detection research,” Insider Attack and Cyber Security, Springer, 2008.

[5] Liu, A., Wang, W., and Wang, M., “Detecting insider threats using behavior-based anomaly detection,” IEEE Security and Privacy Workshops, 2018.

[6] Legg, P.A., Buckley, O., Goldsmith, M., and Creese, S., “Automated insider threat detection system using user and role-based profile assessment,” IEEE Systems Journal, 2017.

[7] Rashid, A., Danezis, G., and Chivers, H., “Using digital forensics for insider threat detection,” Digital Investigation Journal, 2016.

[8] Ahmed, M., Mahmood, A.N., and Hu, J., “A survey of network anomaly detection techniques,” Journal of Network and Computer Applications, 2016.

[9] Chandola, V., Banerjee, A., and Kumar, V., “Anomaly detection: A survey,” ACM Computing Surveys, 2009.

[10] Axelsson, S., "The base-rate fallacy and the difficulty of intrusion detection," ACM Transactions on Information and System Security, 2000.

[11] Behl, A. and Behl, K., "Cybersecurity and cyberwar: What everyone needs to know," Oxford University Press, 2017.

[12] Casey, E., "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet," Academic Press, 2011.

[13] Kent, K. and Souppaya, M., "Guide to Computer Security Log Management," NIST Special Publication 800-92, 2006.

[14] Scarfone, K. and Mell, P., "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2007.

[15] Tankard, C., "Advanced persistent threats and how to monitor and deter them," Network Security Journal, 2011.

10. Acknowledgment

This article is the outcome of the research work carried out in the **Department of Computer Science.** The authors would like to express their sincere gratitude to the Department for providing the necessary support and resources to successfully complete this work. We also extend our thanks to the faculty members and mentors for their valuable guidance and encouragement throughout the research. Their continuous support has greatly contributed to the successful development of this project.