Detection of Insider Threat Behavior Patterns: A Data Driven Approach Using Power BI

A Project Work Synopsis

Submitted in the partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE WITH SPECIALIZATION IN INFORMATION SECURITY

Submitted by:

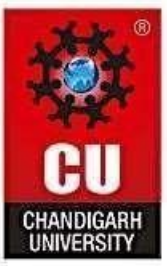
22BIS50002 Shubham Patel

22BIS50004 Lalit

22BIS50005 Shashwat

Under the Supervision of:

SHEETAL LAROIYA



CHANDIGARH UNIVERSITY
Discover. Learn. Empower.

CHANDIGARH UNIVERSITY, GHARUAN, MOHALI - 140413, PUNJAB

Aug 2025

Abstract

Insider threats, caused by individuals with legitimate access, are difficult to detect due to their subtle and normal- appearing actions. This study introduces a data-driven method to identify such threats using Microsoft Power BI. By integrating user activity logs, network data, and HR records, the approach establishes behavioral baselines and detects anomalies. Power BI's dashboards, heatmaps, and role-based access comparisons enable real-time monitoring and quick investigation. Consolidating multi-source data into interactive visualizations helps security teams detect suspicious activity, prioritize risks, and improve security posture. The method offers a scalable, cost-effective, and easy-to-use solution for insider threat detection in organizations.

Keywords:

- Insider Threat
- Behavior Patterns
- Cybersecurity
- Power BI
- Anomaly Detection
- User Activity Monitoring
- Data Visualization
- Threat Intelligence
- Security Analytics

Table of Contents

Title Page

Abstract

1. Introduction 1-4

   1.1 Problem Definition

   1.2 Project Overview

   1.3 Hardware Specification

   1.4 Software Specification

2. Literature Survey 5-8

   2.1 Existing System

   2.2 Proposed System

   2.3 Literature Review Summary

3. Problem Formulation 9

4. Research Objective 10

5. Methodologies 11

6. Experimental Setup 12-14

7. Conclusion 15

9. Reference 16

1. INTRODUCTION

Insider threats represent a significant and evolving challenge in the field of cybersecurity. Unlike external attacks, these threats originate from trusted individuals within an organization—such as employees, contractors, or partners—who have authorized access to critical systems and sensitive information. Their actions may be malicious, involving deliberate data theft or system sabotage, or unintentional, resulting from negligence, policy violations, or compromised accounts. The complexity of detecting insider threats lies in the fact that their activities often resemble legitimate user behavior, making them difficult to distinguish using traditional security tools.

With organizations increasingly relying on digital infrastructure, vast amounts of user activity logs, system access records, and network traffic data are generated daily. However, without effective analysis, this data remains underutilized, leaving potential security gaps. A data-driven approach to analyzing behavioral patterns can help identify anomalies that indicate possible insider threats. By integrating multi-source datasets and applying visual analytics, organizations can proactively detect risks, reduce incident response times, and strengthen their overall security posture.

1.1 Problem Definition

Insider threats are among the most difficult security challenges for organizations because they originate from individuals with legitimate access to systems and sensitive data. Such threats may be intentional, involving deliberate misuse of privileges, or unintentional, resulting from negligence or compromised accounts. The primary challenge lies in detecting these activities, as they often mimic normal user behavior and bypass conventional security controls.

Organizations collect large volumes of logs from network devices, applications, and HR systems; however, these datasets are often stored in silos and remain underutilized. Manual log analysis is time-consuming, prone to human error, and ineffective for identifying subtle or long-term behavioral changes. Advanced detection tools exist, but they are often expensive and require specialized expertise. Therefore, there is a clear need for a scalable, cost-effective, and accessible solution that can analyze multi-source data, detect anomalies, and present actionable insights for timely intervention against insider threats.

1.2 Problem Overview

This project proposes a data driven approach to detecting insider threat behavior patterns using Microsoft Power BI as the core analysis and visualization tool. The system integrates multiple data sources, including user activity logs, network traffic records, system access logs, and HR datasets, to build a unified view of user behavior. Data is processed through an ETL workflow, ensuring it is cleaned, standardized, and prepared for analysis.

Behavioral baselines are established for each user, enabling the detection of deviations that may indicate malicious or negligent activity. Power BI dashboards, featuring heatmaps, time-series trends, and role-based access comparisons, provide security analysts with clear and actionable insights. The interactive interface supports drill-down investigations and prioritization of high-risk alerts. By leveraging Power BI's capabilities, organizations can adopt a scalable, cost-effective, and user-friendly solution that strengthens their ability to detect insider threats and respond proactively.

1.3 Hardware Specification

- Processor
- RAM
- Storage
- Graphics
- Network
- Display

1.4 Software Specification

- Operating System
- Data Visualization Tool
- Database
- ETL Tools
- Programming Support
- Log Sources

2. LITERATURE SURVEY

- **Insider Threat Detection Challenges:**

  Insider threats are difficult to detect because malicious activities often resemble normal user behavior. Traditional security systems struggle to identify these subtle deviations, leading to delayed response and increased risk of data breaches.

- **Data-Driven Behavioral Analysis:**

  By consolidating multi-source logs, data-driven methods can establish user behavior baselines. Any significant deviation triggers alerts, enabling early detection of potentially harmful insider actions.

- **Visualization in Cybersecurity:**

  Power BI dashboards translate complex datasets into clear visual insights. Heatmaps, time-series charts, and anomaly highlights make it easier for security teams to monitor and investigate unusual activities in real time.

- **Multi-Source Data Integration:**

  Combining logs from HR systems, network monitoring tools, and application access records provides a comprehensive view of user activities. This integration strengthens anomaly detection accuracy and reduces false positives.

2.1 Existing System

Existing insider threat detection systems primarily rely on SIEM tools, DLP solutions, and predefined rule-based monitoring. These platforms collect logs from various endpoints, servers, and applications, flagging suspicious activity based on fixed thresholds. While effective for known attack patterns, they struggle with evolving behaviors and subtle insider threats. High operational costs, complexity, and limited visualization capabilities often hinder adoption, especially in mid-sized organizations, and lead to slower response times and higher false-positive rates in threat investigations.

2.2 Proposed System

The proposed system aims to enhance cybersecurity by automating vulnerability detection and enumeration processes. It integrates advanced scanning tools with an intelligent reporting mechanism to identify users, services, and system details efficiently. The system reduces manual effort by consolidating results from multiple enumeration methods, ensuring comprehensive data collection. By providing detailed, real-time insights, it supports penetration testers in identifying potential attack vectors early. This approach improves accuracy, saves time, and strengthens overall security posture against evolving threats.

2.3 Literature Review Summary **(Minimum 7 articles should refer)**

Year and Citation	Article/ Author	Tools/ Software	Technique	Source	Evaluation Parameter
2018	A Framework for Data-Driven Physical Security and Insider Threat Detection	PS0 framework (ontological, rule-based)	Anomaly detection via provenance graphs	2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)	Visualize rule-based alerts, show deviations over time
2018 – Gamachchi & Boztas	Insider Threat Detection Through Attributed Graph Clustering	Graph clustering tools	Attributed graph clustering, outlier ranking	16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2017	Display clustering results and anomaly scores
2019 – Hall et al	Predicting Malicious Insider Threat Scenarios Using Organizational Data and a Heterogeneous Stack-Classifier	Machine-learning classifiers ensemble	Ensemble ML on CERT dataset r4.2	http://arxiv.org/pdf/1907.10272	Dashboard ROC, confusion matrix, prediction trends
2024 – Velush	Protecting Against Oversharing Power BI Reports with Microsoft Sentinel	Power BI + Sentinel + Purview DLP	Audit log monitoring for oversharing	https://www.microsoft.com/insidetrack/blog/protecting-against-oversharing-power-bi-reports-with-microsoft-sentinel/	Use Power BI for real-time oversharing alerts, thresholds

2021 – Pantelidis et al.	Insider Detection using Deep Autoencoder and Variational Autoencoder NN	Autoencoder, VAE deep learning	Deep learning anomaly detection	https://arxiv.org/abs/2109.02568	Show anomaly scores, model comparison, detection accuracy
202X – TechRepublic	Custom Security & Threat Dashboard in Power BI	Power BI dashboards, Defender APIs	Aggregated security visualization, AI anomaly detection	https://www.techrepublic.com/article/how-to-visualise-security-and-threat-information-in-power-bi	Visualize detection, anomaly, access control patterns
2025 – Ajagun	Cybersecurity-Intelligence Visualization using Power BI	Power BI dashboards	User behavior analytics, anomaly visualization	https://medium.com/%40ajagunalliyu/cybersecurity-intelligence-visualization-using-power-bi-b4efdb6f04e5	Interactive analytics of insider behaviors, drill-downs

.

3. PROBLEM FORMULATION

Insider threats pose a significant risk to organizational security as they originate from trusted individuals with authorized access. Traditional monitoring systems often fail to detect subtle behavioral anomalies that precede malicious actions. The challenge lies in identifying patterns within large datasets, correlating user activities, and presenting actionable insights in real time. A data-driven approach using Power BI can enable effective visualization and detection of such patterns.

Key Challenges:

a) Data Collection & Integration:

Collecting accurate and comprehensive insider activity logs from multiple sources (e.g., HR data, access logs, system usage patterns) can be challenging due to data silos, inconsistent formats, and integration complexities. Ensuring seamless data ingestion into Power BI for real-time monitoring is crucial yet technically demanding.

b) Privacy, Compliance & Ethical Issues:

Monitoring employee activities raises privacy concerns and must comply with legal regulations like GDPR or internal corporate policies. Implementing transparent, lawful data handling practices while maintaining trust between employees and the organization is a constant challenge.

4. OBJECTIVES

The main objective of this research is to detect and analyze insider threat behavior patterns using Power BI, focusing on data-driven analysis to identify anomalies, visualize patterns, and provide actionable insights for strengthening cybersecurity posture.

- **Identify suspicious patterns in employee activities:**
  This objective involves analyzing user logins, file access, data transfers, and unusual working hours to spot potential indicators of malicious intent. The focus is on recognizing deviations from normal behavior that may signify security risks.
- **Create interactive Power BI dashboards for monitoring:**
  Developing intuitive, real-time dashboards that consolidate diverse security data into a single interface. These dashboards will help security teams quickly identify anomalies, track activities over time, and assess the severity of potential threats effectively.
- **Provide actionable insights to improve security decisions:**
  This objective aims to generate reports and alerts based on analyzed data, offering security teams concrete recommendations. These insights will assist in proactive threat mitigation, policy refinement, and informed decision-making to enhance organizational resilience against insider threats.

5. METHODOLOGY

The proposed methodology combines data collection, preprocessing, analysis, and visualization to detect insider threat behavior patterns. Using Power BI for interactive dashboards and real-time monitoring, anomalies are quickly identified. The process is divided into key stages for systematic detection.

a. **Data Collection and Integration-**

   Data is gathered from multiple organizational sources, including access logs, HR records, and network activity. These datasets are cleaned and integrated into a unified database, ensuring completeness and consistency for accurate insider threat detection.

b. **Data Preprocessing and Feature Engineering-**

   Irrelevant and noisy data are removed, missing values are handled, and essential features—such as abnormal access times, excessive file downloads, and unusual login patterns—are engineered to improve model performance and analytical accuracy.

c. **Visualization and Threat Analysis using Power BI-**

   Interactive dashboards are created in Power BI to visualize employee activity trends, detect anomalies, and provide real-time alerts. Advanced filters and drill-down options enable deeper investigation into suspicious behavioral patterns.

6.EXPERIMENTAL SETUP

The experimental setup uses Power BI for visualization, integrated with processed insider threat datasets. Data undergoes cleaning, modeling, and analysis to generate interactive dashboards, enabling anomaly detection and real-time monitoring for proactive threat identification.

- **Data Collection-**

  Data was gathered from publicly available insider threat datasets and simulated organizational logs, including user activity records, system access logs, file transfers, and email communications to ensure a comprehensive representation of potential malicious and benign behaviors.

  Multiple data sources were integrated, cleaned, and standardized to create a unified dataset. This process ensured consistency, removed redundant entries, and enhanced the reliability of subsequent feature extraction and anomaly detection processes for insider threat analysis.

- **Feature Extraction-**

  Feature extraction transforms raw security data into meaningful attributes for detecting insider threats. It selects relevant factors like login frequency, file access patterns, and abnormal data transfers from logs and monitoring tools. By cleaning, normalizing, and

structuring data, it ensures accuracy, reduces noise, and enhances machine learning models to effectively differentiate normal user behavior from potential malicious activities.

- **Evaluation-**

  Evaluation assesses the performance of the insider threat detection model using metrics like accuracy, precision, recall, and F1-score. This process ensures the model's predictions are reliable and balanced, avoiding false positives that may disrupt normal operations or overlook genuine threats.

  It involves testing the model on unseen data to validate its generalization ability. Comparing different algorithms or configurations helps identify the most effective approach, ensuring robust detection capabilities in real-world environments while maintaining efficiency and minimizing computational overhead.

- **Deployment-**

  Deployment of the insider threat detection system involves integrating the data-driven model into the organization's existing security infrastructure. Power BI dashboards provide real-time visualization of user behavior patterns, enabling security teams to monitor anomalies, receive alerts, and respond promptly to potential insider threats.

  The deployment also includes continuous data updating and model retraining to adapt to evolving insider threat tactics. By leveraging

Power BI's interactive reports, stakeholders can gain insights from complex data, improving decision-making and strengthening the overall security posture against insider threats effectively.

7.CONCLUSION

The detection of insider threat behavior patterns using a data-driven approach with Power BI significantly enhances an organization's ability to identify and mitigate risks from within. By leveraging real-time data visualization, pattern recognition, and anomaly detection, security teams can proactively monitor user activities, reducing the chances of damage caused by malicious insiders or accidental breaches. This approach not only improves situational awareness but also supports informed decision-making, enabling faster responses to suspicious behaviors before they escalate into serious threats.

Furthermore, integrating Power BI into insider threat detection workflows provides a scalable and flexible platform that adapts to changing organizational needs. Continuous data updates and advanced analytics ensure that evolving threat patterns are promptly captured and analyzed. Overall, this methodology strengthens an organization's security posture by combining powerful visualization tools with robust data analysis techniques, fostering a proactive culture of security awareness and resilience against insider threats.

REFERENCES

[1] P. Langlois, A. Pinto, D. Hylender, and S. Widup, “DBIR 2023 data breach investigations report 10K 20K 30K about the cover,” Tech. Rep., Jun. 2023.
[2] X. Kan, Y. Fan, J. Zheng, C.-H. Chi, W. Song, and A. Kudreyko, “Data adjusting strategy and optimized XGBoost algorithm for novel insider threat detection model,” *J. Franklin Inst.*, vol. 360, no. 16, pp. 11414–11443, Nov. 2023.
[3] S. Asha, D. Shanmugapriya, and G. Padmavathi, “Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment,” *Comput. Electr. Eng.*, vol. 105, Jan. 2023, Art. no. 108519.
[4] M. AlSlaiman, M. I. Salman, M. M. Saleh, and B. Wang, “Enhancing false negative and positive rates for efficient insider threat detection,” *Comput. Secur.*, vol. 126, Mar. 2023, Art. no. 103066.
[5] B. Bin Sarhan and N. Altwaijry, “Insider threat detection using machine learning approach,” *Appl. Sci.*, vol. 13, no. 1, p. 259, Dec. 2022.