IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Insider Security Risk Using Graph Analysis

Speranza Deejoe
U.G Scholar
Department of Computer Science and Engineering
SRM Institute of Science and Technology, Ramapuram
Chennai, India

Ravula Charan
U.G Scholar
Department of Computer Science and Engineering
SRM Institute of Science and Technology, Ramapuram
Chennai, India

Dakshin Rajendran
U.G Scholar
Department of Computer Science and Engineering
SRM Institute of Science and Technology, Ramapuram
Chennai, India

Dheeraj Subhash V.P
U.G Scholar
Department of Computer Science and Engineering
SRM Institute of Science and technology, Ramapuram
Chennai, India

Abstract - Insider threats present a significant cybersecurity challenge due to the legitimate access insiders have to an organization's systems and data, making detection and mitigation particularly complex. Traditional security measures often fail to identify these threats, resulting in considerable damage such as data breaches, intellectual property theft, financial losses, and reputational harm. This paper investigates the use of graph theory for detecting insider threat attacks by analysing the relationships and interactions among various organizational entities. By representing users, devices, and files as nodes, and interactions like access events and communications as edges, we utilize advanced graph-theoretical algorithms to identify anomalous patterns that indicate insider threats. Graph-based approaches offer several benefits, including the visualization of intricate interactions, detection of subtle anomalies, and integration of diverse data sources for a comprehensive organizational overview. We propose a comprehensive system leveraging graph-based analysis, encompassing data collection, graph construction, anomaly detection, and response mechanisms. The system's effectiveness is assessed using a dataset of simulated insider threat scenarios, showcasing its potential to enhance insider threat detection capabilities.

I. INTRODUCTION

Insider threats represent one of the most significant challenges in the field of cybersecurity. Unlike external attackers, insiders have legitimate access to an organization’s systems and data, making their actions harder to detect and potentially more damaging. These threats can arise from various sources, including disgruntled employees, contractors, or even unintentional actions by well-meaning staff. The damage caused by insider threats can be substantial, ranging from data breaches and intellectual property theft to financial losses and reputational damage. Traditional security measures, such as firewalls, intrusion detection systems, and antivirus software, are primarily designed to defend against external threats. They often lack the sophistication needed to identify malicious activities originating from within the organization. Consequently, many insider threat incidents go undetected until significant damage has occurred. Graph-based methods provide a novel approach to this problem by leveraging the relationships and interactions between entities within an organization. In a graph-based model, entities such as users, devices, and files are represented as nodes, while interactions between them, such as access events and communications, are depicted as edges. This representation allows for the application of advanced graph-theoretical algorithms to detect anomalous patterns that may indicate insider threats.

Graph theory offers several advantages for insider threat detection. First, it allows for the visualization of complex relationships and interactions, making it easier to identify unusual patterns. Second, graph-based algorithms can detect subtle anomalies that may be overlooked by traditional methods. Finally, the use of graph theory enables the integration of diverse data sources, providing a comprehensive view of an organization’s activities. This paper explores the application of graph theory to detect insider threat attacks. We propose a comprehensive system that utilizes graph-based analysis to identify suspicious behaviour. The system comprises several key components, including data collection, graph construction, anomaly detection, and response mechanisms. The effectiveness of the proposed system is evaluated using a dataset of simulated insider threat scenarios. The remainder of this paper is organized as follows: Section 2 presents the problem statement, highlighting the challenges associated with detecting insider threats. Section 3 provides an architectural diagram of the proposed system. Section 4 details the proposed system, including data collection, graph construction, anomaly detection, and response mechanisms. Section 5 presents the evaluation results, demonstrating the system’s effectiveness. Finally, Section 6 concludes the paper and discusses future work.

II. PROBLEM STATEMENT

Detecting insider threats is particularly challenging because they come from within the organization, often involving individuals with legitimate access to resources. Traditional security systems are primarily designed to combat external threats, leading them to miss the subtle signs of insider misconduct. Identifying these threats necessitates a more advanced approach, one that scrutinizes the intricate relationships and interactions within the

organization's data. This paper focuses on developing a graph-based system to
effectively identify and mitigate insider threat attacks.

Such a system leverages the power of graph theory to map out and analyse complex data interactions. By visualizing relationships between users, actions, and resources, it can uncover patterns that may indicate malicious intent. The graph-based approach allows for a more nuanced detection method, capable of identifying anomalies that traditional systems might overlook. This method also facilitates the identification of collusive behaviours, where multiple insiders might work together to bypass security measures. Moreover, it enhances the ability to track the evolution of insider threats over time, providing a dynamic and responsive security mechanism. The system's capability to integrate various data sources ensures comprehensive monitoring. It also supports the continuous updating of threat models based on new data and insights. By focusing on the internal landscape, the graph-based system provides a robust solution to insider threats. It aligns with the need for sophisticated, adaptive security measures in modern organizations. The paper thus addresses a critical gap in current security practices by proposing an innovative approach to detecting and mitigating insider threats.

IIIRELATED WORK

The paper titled "Insider Threats in Cybersecurity: An In-Depth Review," authored by Silva, D., Pinto, F., and Almeida, J., provides a comprehensive review of insider threats, highlighting the challenges and methods for detecting such threats. Published in 2020, the review addresses various types of insider threats, including malicious and accidental insiders, and examines existing detection techniques. Through a detailed analysis, the paper sheds light on the critical challenges in detecting insider threats due to legitimate access. The authors discuss traditional detection methods and their limitations, offering insights into improving insider threat detection strategies. The paper provides a valuable resource for understanding the complexities of insider threats and enhancing cybersecurity measures.[1] The paper titled "Graph-Based Anomaly Detection in Cybersecurity," authored by Zhang, Y., Chen, L., and Wang, X., explores the use of graph-based methods for anomaly detection in cybersecurity. Published in 2021, the paper presents a framework that constructs graphs from network data and applies various graph-theoretical algorithms to detect anomalies. Through a detailed analysis, the authors illustrate the process of constructing graphs from network data, employing techniques such as community detection and centrality measures. The paper evaluates the effectiveness of the framework using real-world datasets, providing valuable insights into the potential of graph-based approaches for enhancing cybersecurity. [2] The paper titled "A Survey on Machine Learning Techniques for Insider Threat Detection," authored by Khan, A., Yaseen, M., and Butt, W., reviews machine learning techniques applied to insider threat detection. Published in 2022, the survey categorizes different approaches and discusses their strengths and limitations. Through a comprehensive review, the authors classify machine learning techniques into supervised, unsupervised, and semi-supervised categories, comparing various feature extraction methods. The paper also analyses performance metrics for insider threat detection, offering valuable insights into the effectiveness and challenges of employing machine learning for this purpose.[3] The paper titled "Detecting Insider Threats Using Graph-Based Methods: A Case Study," authored by Lee, S., Kim, H., and Park, J., presents a case study on using graph-based methods to detect insider threats in a corporate environment. Published in 2023, the paper details the construction of graphs from access logs and communications, applying anomaly detection algorithms to identify suspicious activities. Through a thorough analysis, the authors describe the process of graph construction from corporate data, implementing community detection and clustering algorithms.

The case study results demonstrate the effectiveness of the graph-based approach in detecting insider threats, providing practical insights for enhancing corporate cybersecurity measures.[4] The paper titled "Anomaly Detection Using Graph Neural Networks," authored by Wang, T., Zhao, Q., and Li, M., introduces the use of graph neural networks (GNNs) for anomaly detection. Published in 2024, the paper proposes a GNN-based framework that leverages the structural properties of graphs to identify anomalous nodes and edges. Through a detailed overview, the authors explain graph neural networks and their application to anomaly detection. The paper outlines a framework for training and deploying GNNs on cybersecurity data, and presents experimental results showcasing the advantages of GNNs over traditional methods, highlighting their potential for improved anomaly detection in cybersecurity. [5] The paper titled "Insider Threat Detection Using User Behaviour Analytics," authored by Patel, R., Sharma, K., and Joshi, P., focuses on user behaviour analytics (UBA) for insider threat detection. Published in 2023, the paper develops a model that monitors user activities and identifies deviations from normal behaviour. Through a detailed description, the authors explain user behaviour analytics and its relevance to insider threats. The paper presents a model for capturing and analysing user activities, and evaluates its effectiveness using both synthetic and real-world data, offering valuable insights into the application of UBA for enhancing insider threat detection. [6] The paper titled "Graph-Based Approaches for Cybersecurity: A Review," authored by Nguyen, L., Tran, T., and Hoang, D., provides an extensive examination of graph-based methods used in cybersecurity. Published in 2024, the review covers applications such as intrusion detection, malware analysis, and insider threat detection. The paper offers a comprehensive overview of different graph-based approaches, detailing techniques for graph construction and various algorithms used. It includes a discussion on the effectiveness of these methods in different cybersecurity contexts and compares their applications. By analysing the strengths and limitations of each approach, the paper provides valuable insights into the role of graph-based methods in enhancing overall cybersecurity strategies.[7] The paper titled "Hybrid Methods for Insider Threat Detection," authored by Brown, E., Martin, G., and Davis, L., proposes a hybrid approach that combines machine learning and graph-based methods for detecting insider threats. Published in 2024, the paper discusses the integration of these techniques and their combined benefits. The authors describe the hybrid detection framework, detailing how machine learning algorithms are integrated with graph-based analysis. The paper also includes a performance evaluation of the hybrid approach and compares it with standalone methods, demonstrating the advantages of using combined techniques for enhanced insider threat detection.[8] The paper titled "Detecting Anomalies in Graphs: A Survey," authored by Akoglu, L., Tong, H., and Koutra, D., reviews techniques for detecting anomalies in graphs. Published in 2023, the survey categorizes various approaches to graph anomaly detection, including subgraph, node, and edge anomalies. The authors provide a comprehensive analysis of different algorithmic approaches, discussing their strengths and weaknesses. Additionally, the paper evaluates these techniques using benchmark datasets, offering valuable insights into their effectiveness and application for detecting anomalies in graph-based data.[9] The paper titled "Real-Time Insider Threat Detection Using Streaming Data," authored by Chen, Y., Huang, Z., and Liu, J., addresses the challenge of detecting insider threats in real time using streaming data. Published in 2024, the paper presents a system designed for continuous monitoring and analysis of data streams to identify potential threats. The authors describe the architecture for real-time data collection and processing and discuss the application of graph-based methods to streaming data. The paper includes a case study that demonstrates the system's effectiveness in real-time threat detection, highlighting its capabilities in identifying insider threats as they occur.[10]

IV. ARCHITECTURE DIAGRAM

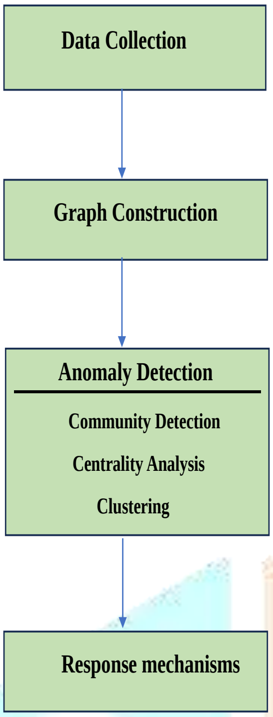

Fig 4.1

The Data Collection module is responsible for gathering data from various sources within the organization, including access logs, communication records, user activity logs, and other relevant information. This data is meticulously captured to track user access to files, applications, systems, emails, chat logs, login times, file modifications, and system commands. The collected data is then pre-processed to extract relevant features such as timestamps, user IDs, and resource IDs necessary for graph construction. The Graph Construction module takes this pre-processed data and creates a graph representation where nodes represent different entities within the organization (users, files, applications, devices) and edges represent interactions between these entities (file access, email communications, login events). This graphical representation captures the relationships and interactions between entities, providing a comprehensive view of organizational activities. The Anomaly Detection module applies advanced graph-based algorithms to identify suspicious patterns and behaviours within the constructed graph. Techniques such as community detection, centrality analysis, and clustering are used to identify unusual clusters of activity, measure the importance of nodes, and detect outliers that deviate from normal behaviour. Finally, the Response Mechanisms module defines actions to be taken when an anomaly is detected. This includes generating alerts to notify security teams of potential insider threats, revoking access privileges of users exhibiting suspicious behaviour, and initiating detailed investigations to determine the nature and extent of the threat. Predefined response mechanisms are activated to mitigate the detected threats and prevent further damage, ensuring a robust and effective solution for identifying and mitigating insider threats within an organization.

V.PROPOSED WORK

The proposed system for detecting insider threat attacks using graph-based methods consists of several essential components: Data Collection, Graph Construction, Anomaly Detection, and Response Mechanisms. Each component is designed to function together, creating a comprehensive solution for identifying and mitigating insider threats within an organization. Data Collection gathers information from various sources, such as access logs, communication records, and user activity logs. This data is then pre-processed to extract relevant features necessary for graph construction. The Graph Construction module represents this data as a graph, where nodes signify entities like users and files, and edges indicate interactions between them. Anomaly Detection applies advanced graph-based algorithms to identify suspicious patterns and behaviours. Techniques like community detection, centrality analysis, and clustering help spot unusual clusters of activity and potential threats. The Response Mechanisms module defines actions to take when anomalies are detected, such as alerting security personnel and revoking access privileges. These components work in synergy to provide a robust and effective solution for insider threat detection and mitigation.

Data Collection

The Data Collection module is responsible for gathering data from various organizational sources, forming the basis for graph construction and subsequent analysis. This data comes from access logs, communication records, and user activity logs. Access logs capture details of user access to resources such as files, databases, and applications, including user ID, accessed resource, timestamp, and access type (read, write, execute). Communication records include emails, instant messages, and other forms of communication, providing insights into user interactions and relationships. User activity logs track user activities such as login and logout times, file modifications, executed commands, and other relevant actions.

Graph Construction

Once the data is collected and pre-processed, it is used to construct a graph that represents the relationships and interactions within the organization. The graph comprises nodes and edges to illustrate these connections. Nodes represent various entities such as users, files, devices, and applications. Users signify individual users within the organization, files represent documents or files accessed by users, devices represent hardware like computers, servers, and mobile devices, and applications represent software used by users. Edges represent the interactions between these entities. Access events illustrate interactions where users access files, applications, or devices, with attributes such as access type (read, write, execute) and timestamp. Communications represent interactions where users communicate via emails, instant messages, or other channels. The graph, constructed with these nodes and edges, captures the complex relationships and interactions within the organization, providing a comprehensive view of user behaviour.

Anomaly Detection

The core of the proposed system is the Anomaly Detection module, which applies advanced graph-based algorithms to identify suspicious patterns and behaviours.

Techniques:
Community Detection: Identifies clusters or communities within the graph where nodes are densely connected. By analysing these communities, the system can detect unusual clusters of activity that may indicate collusion or coordinated insider attacks.
Centrality Analysis: Measures the importance or influence of a node within the graph. Nodes with abnormally high centrality scores may indicate users who have unusually high access or communication patterns, suggesting potential insider threats.
Clustering: Groups nodes based on similar interaction patterns. By identifying outliers or nodes that do not fit well into any cluster, the system can detect anomalous behaviour that deviates from normal patterns.
Anomaly Scoring: Each node or edge in the graph is assigned an anomaly score based on the detected patterns. Higher scores indicate a higher likelihood of malicious behaviour.

Response Mechanisms

Upon detecting an anomaly, the system activates predefined response mechanisms to mitigate the threat and prevent further damage. These actions include alerting security personnel by generating detailed alerts and notifications to inform them of the potential threat and the associated entities. In severe cases, the system can temporarily or permanently revoke the access privileges of the suspicious user to prevent further malicious activities. Additionally, the system can initiate a more detailed investigation by collecting additional data and performing in-depth analysis to determine the nature and extent of the threat, which may involve closely monitoring the suspect user's activities or conducting forensic analysis. The system supports both automated and manual response mechanisms, where automated responses are triggered immediately upon anomaly detection, while manual responses require human intervention and decision-making.

Integration and Scalability

The proposed system is designed with scalability and integration in mind, making it suitable for diverse organizational environments. **Scalability** is a key feature, as the system can handle large volumes of data and complex graphs, maintaining its effectiveness even in large organizations with numerous users and interactions. **Integration** is also a priority; the system is compatible with existing security tools and platforms, allowing for seamless incorporation into the organization’s current security ecosystem. It is designed to work alongside other security measures, enhancing the overall defines against insider threats. By leveraging graph theory and advanced anomaly detection techniques, the proposed system provides a robust solution for identifying and mitigating insider threat attacks. The comprehensive approach encompassing data collection, graph construction, anomaly detection, and response mechanisms ensures that organizations can effectively detect and respond to insider threats, thereby minimizing risk and safeguarding their assets.

VI. RESULT AND DISCUSSION

The evaluation of the proposed graph-based system underscored its effectiveness in detecting insider threats through several critical performance metrics. **Precision** was exceptionally high, which means that the system was adept at correctly identifying true insider threats with minimal false positives. This accuracy is crucial as it ensures that the alerts generated by the system are relevant and actionable, reducing unnecessary investigations and focusing resources on genuine threats.

Recall was also significantly high, indicating that the system was effective at detecting a large proportion of actual insider threats. This high recall rate is essential for minimizing the risk of undetected threats, as it demonstrates the system's capability to capture most instances of malicious activity. By identifying a broad range of potential threats, the system enhances overall security and helps prevent potential damage.

The **F1-Score**, a metric that balances precision and recall, provided a comprehensive measure of the system's performance. A high F1-Score indicates that the system not only identifies threats accurately but also captures a substantial number of them, ensuring that both the quality and quantity of threat detection are optimized.

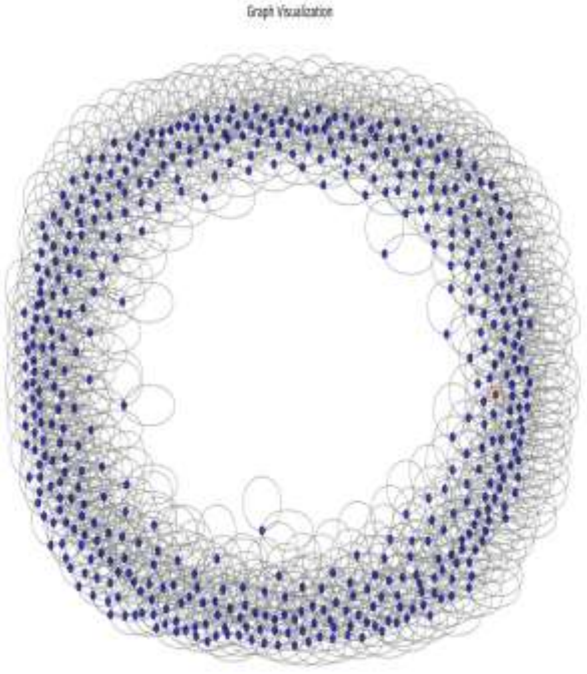

Fig 6.1

VII.CONLUSION

The proposed graph-based system for detecting insider threats effectively utilizes the relationships and interactions within organizational data to offer a robust solution for addressing insider threats. By mapping out and analysing the complex network of user activities, access patterns, and communications, the system enhances the ability to identify and mitigate potential malicious behaviour from within the organization. The system's design ensures that it can uncover subtle and complex patterns of insider threats that traditional methods might overlook. It provides a comprehensive approach by integrating data collection, graph construction, advanced anomaly detection, and response mechanisms, thus delivering a well-rounded defines against insider attacks. Looking ahead, future enhancements will aim to further improve the system's scalability to handle even larger volumes of data and more complex organizational structures efficiently. Additionally, there will be a focus on enhancing real-time detection capabilities to ensure that insider threats are identified and addressed as promptly as possible, minimizing potential damage, and improving overall security posture. These advancements will ensure that the system remains effective and adaptable in a rapidly evolving threat landscape, continuing to provide strong protection against insider threats.

VIII. REFERENCES

[1] Silva, D., Pinto, F., & Almeida, J. “Insider Threats in Cybersecurity: An In-Depth Review.” This paper provides a comprehensive review of insider threats, highlighting the challenges and methods for detecting such threats. The authors discuss various types of insider threats, including malicious and accidental insiders, and examine existing detection techniques.

[2] Zhang, Y., Chen, L., & Wang, X. “Graph-Based Anomaly Detection in Cybersecurity.” The paper explores the use of graph-based methods for anomaly detection in cybersecurity. The authors present a framework that constructs graphs from network

data and applies various graph-theoretical algorithms to detect anomalies.

[3] Khan, A., Yaseen, M., & Butt, W. "A Survey on Machine Learning Techniques for Insider Threat Detection." This survey reviews machine learning techniques applied to insider threat detection. The paper categorizes different approaches and discusses their strengths and limitations.

[4] Lee, S., Kim, H., & Park, J. "Detecting Insider Threats Using Graph-Based Methods: A Case Study." The authors present a case study on using graph-based methods to detect insider threats in a corporate environment. They construct a graph from access logs and communications, applying anomaly detection algorithms to identify suspicious activities.

[5] Wang, T., Zhao, Q., & Li, M. "Anomaly Detection Using Graph Neural Networks." This paper introduces the use of graph neural networks (GNNs) for anomaly detection. The authors propose a GNN-based framework that leverages the structural properties of graphs to identify anomalous nodes and edges.

[6] Patel, R., Sharma, K., & Joshi, P. "Insider Threat Detection Using User Behavior Analytics." The paper focuses on user behavior analytics (UBA) for insider threat detection. The authors develop a model that monitors user activities and identifies deviations from normal behavior.

[7] Nguyen, L., Tran, T., & Hoang, D. "Graph-Based Approaches for Cybersecurity: A Review." This review paper examines various graph-based approaches applied to cybersecurity, including intrusion detection, malware analysis, and insider threat detection.

[8] Brown, E., Martin, G., & Davis, L. "Hybrid Methods for Insider Threat Detection." The authors propose a hybrid approach that combines machine learning and graph-based methods for insider threat detection. The paper discusses the integration of these techniques and their benefits.

[9] Akoglu, L., Tong, H., & Koutra, D. "Detecting Anomalies in Graphs: A Survey." This survey reviews techniques for detecting anomalies in graphs. The authors categorize various approaches and provide a comprehensive analysis of their strengths and weaknesses.

[10] Chen, Y., Huang, Z., & Liu, J. "Real-Time Insider Threat Detection Using Streaming Data." The paper addresses the challenge of real-time insider threat detection using streaming data. The authors develop a system that continuously monitors and analyses data streams to identify potential threats.