ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Insider Threat Detection and Mitigation

Anvesh Gunuganti

USA

ABSTRACT

Insider threats have been discussed in this review based on two selected articles adopting the SWOT analysis. It outlines the advantages and disadvantages of the existing approaches and technologies used in the detection, gaps in resources, funding, and organization, opportunities to advance cooperation and development of new methods and strategies, and risks in the extrapolation of tactics and compliance issues. The information presented focuses on the prevention and control of insiders and the major strategies proposed, stressing the use of technological, behavioral, and organizational measures. Further studies should focus on the use of analytics, communication with stakeholders, and adjustments in security management to improve an organization's protection against insider threats.

***Corresponding author**

Anvesh Gunuganti, USA.

Received: July 16, 2024; **Accepted:** July 22, 2024, **Published:** July 29, 2024

Keywords: Insider Threats, SWOT Analysis, Cybersecurity, Detection Technologies, Mitigation Strategies

Abbreviations

1. ICT - Information and Communications Technology
2. USB - Universal Serial Bus
3. SWOT - Strengths, Weaknesses, Opportunities, Threats

Introduction

Insider risks are among the most significant threats to organizations' cybersecurity due to the personnel with legitimate access to critical systems, documents, or networks. These threats range from purposeful negative actions, which this paper will classify as attacks, accidents, or oversights, as they also have the potential to threaten the confidentiality, integrity, and availability of organizational assets [1]. It is therefore important to have an elaborate understanding of the different motives and actions that cause insider activities, accompanied by good means of identifying and responding to the same.

Overview

An insider threat is a major challenge to organizations' cybersecurity strategy, whereby risks are embodied in people with legitimate access to systems, data, or networks. Such threats can be in the form of malicious attacks and/or accidental or intentionally negligent acts that undermine the organization's assets' confidentiality, integrity, and availability. Insider threats are a complex issue that cannot be dealt with unless organizations acquire significant knowledge about the categories, reasons, and powerful approaches to handling insider threats [2].

Insider threats are security risks that are posed by individuals who are allowed full access to the systems and networks of an organization and, after that, use this privilege to indulge in malicious activities, incompetence, or unlawful conduct [3]. This category can range from a level of motivation that results in security incidences, data breaches, or any pertinent negative impact on organizational security.

Types of Insider Threats

- Malicious Insiders: These insiders may operate intentionally, taking advantage of their facility's privileges to harm the organization. The possible incentives might be financial rewards, a desire to harm the organization/colleagues, or political/philosophical beliefs [4].
- Negligent Insiders: Employees who contribute to security breaches by their negligence or ignorance of security measures and policies.
- Compromised Insiders: Such insiders have their credentials or access rights misused by other people on the outside. Subconsciously, they enable launches caused by phishing, social engineering, or any other kind of compromise. Fig.1 explains the categorize of insiders

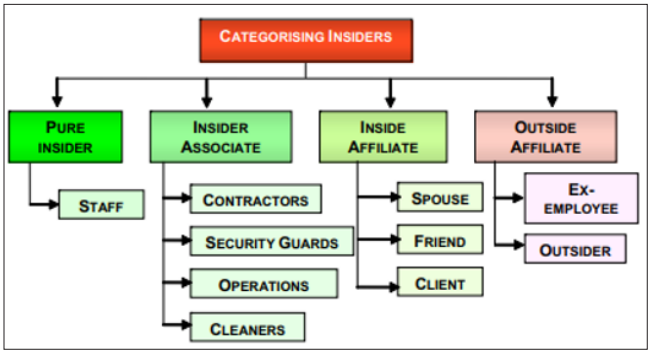

Figure 1: Categorizing insiders [2]

Importance of Effective Detection and Mitigation Strategies

The prevalence of insider threats underscores the critical need for organizations to implement robust detection and mitigation strategies:

- **Prevention of Data Breaches:** An informal user poses various risks that escalate into massive leakage and information exposure, which cost money, attract fines, and erode reputation.
- **Protection of Intellectual Property:** Trade secrets often serve as the foundation for competitive advantage and are widely used by organizations. When insiders attack the organizations' intellectual property, the risks are financial and strategic.
- **Compliance Requirements:** Certain regulatory requirements, such as the GDPR, HIPAA, and the PCI-DSS, dictate that organizations must put in place adequate measures to protect data that is deemed sensitive [5]. Proper insider threat programs assist in the compliance processes.
- **Enhanced Cybersecurity Posture:** To address insider threats, organizations should utilize technologies that monitor potential abusers; conduct security reviews periodically, employ access restrictions, and develop a security-aware culture.
- **Behavioral Analysis and Training:** By explaining cybersecurity protocols to the employees and doing routine security sensitization, possible insider threats can be identified and addressed before they occur.

Insider threat risks can only be addressed by defending them through diverse methods that combine engineering, administrative measures, and surveillance of employee behavior. Insider threats pose a great risk to the organizations' strategic assets, business continuity, and stakeholder confidence, thus requiring organizations to build robust defense-in-depth strategies [6]. Therefore, the important identification of insider threats and their possible consequences indicates how organizational security risks can be prevented and managed as a significant internal security problem in today's complex cybersecurity environment. Fig 2 characterizes insider attacks.

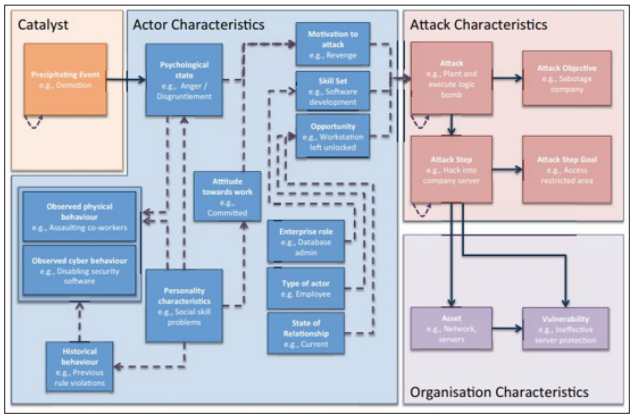

Figure 2: A framework for characterizing insider attacks [5]

Research Aims and Objectives

Aims and Objectives to be Addressed

The purpose of this research will be to identify and cover all the aspects of insider threats in cybersecurity and provide current knowledge regarding their types, motivations, ways of detection, and possible ways of prevention to improve an organization's preparedness to handle such threats.

Objectives

- **Identify Types of Insider Threats:** Analyze and differentiate different categories of threats posed by insiders; these are the malevolent insiders, those who act inadvertently, and impersonators.
- **Examine Motivations and Risk Factors:** Examine the various possible reasons for insider threat, which may include financial motives, vindictiveness, accidental acts, and carelessness.)
- **Evaluate Detection Techniques:** Examine current approaches and tools for identifying insider threats and evaluating their real-life advantages and disadvantages.
- **Explore Mitigation Strategies:** Evaluate the methods of managing insider threats, such as policies, controls, and behavior-based observations. Fig 3 shows the behavior element.

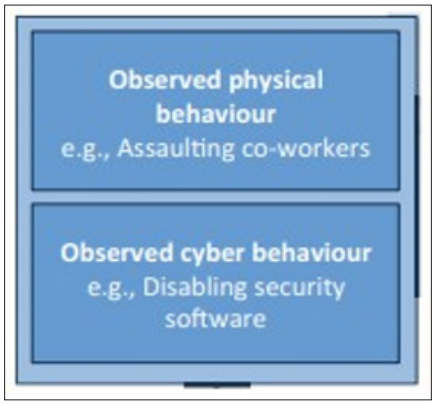

Figure 3: Behavior element [5]

- **Assess Organizational Preparedness:** Assess the level of organization preparedness for insider threats, such as training, incident response measures, and adherence to prescribed legislations.
- **Propose Recommendations:** Outlining clear suggestions for organizations to enhance their security against insiders, considering the established risks and lessons learned in cybersecurity.

Research Questions

How can data analytics and real-world case studies be integrated to enhance the detection and mitigation of insider threats in ICT systems?

Literature Review

Insider threats remain one of the significant cybersecurity threats coming from individuals within an organization or with authorized access to an organization's resources. These threats can be further divided based on motivation, such as motivated insiders, the ones who have a pound of motive, such as financial gains, and accidental insiders who threaten security without intention. Insider threat identification and prevention entails using traditional approaches, such as audit logs, among others, and new strategies like behavioral analysis and machine learning [7]. The proposed means of minimization would include but not be limited to the following: strict control of access, strong security policies and procedures, frequent training, and an organization's security-conscious culture. Preparedness appears to be the common thread in much of the literature, as it is used in incident response plans, security audits, and general adherence to regulatory requirements for managing risks properly and preventing peer attacks on the organization's cybersecurity. Fig. 4 explains the insider threat assessment cycle.

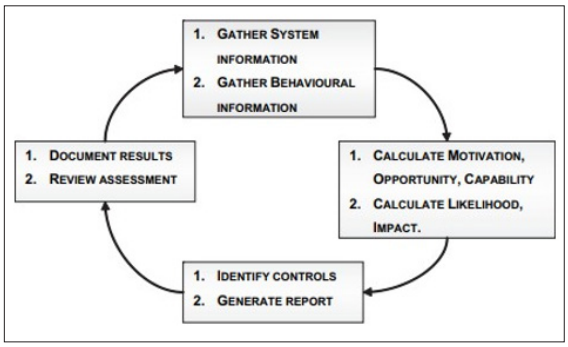

Figure 4: Insider threat assessment cycle [2]

This paper explores the increasing cases of cybercrimes that target ICT systems, emphasizing insiders as the source of attacks [1]. It also points to the significant difficulties of identifying and preventing insider threats due to the insiders' authorized access and bypassing standard protection mechanisms. The survey conducted within the article categorizes various schemes and systems designed to tackle insider threats, focusing specifically on three prevalent types: few actions are carried out by authentic witting enemies but rather by traitors, masqueraders, and innocent parties.

This paper follows a data analytical approach in categorizing existing studies based on their effectiveness against insider threats. It states the importance of recognizing and controlling risks that may develop into malicious insider actions at the initial stage. In this regard, the article presents ideas of host-based, network-based, and contextual data- based countermeasures, comparing different types of insider threats, direct and indirect ones, based on the audit data sources. Each reviewed work is then assessed according to its likelihood of handling insider threats, the methods used to acquire knowledge from data sources, and the decision-making processes in use.

Key Points Highlighted Include

- **Types of Insider Threats:** The article classifies the insider threat actors into the traitors or malicious insiders, the masqueraders or terrorists or strangers who cloak themselves as insiders and the unintentional offenders or insiders who do not mean harm but cause one anyhow.
- **Approach and Methodology:** The work ad liberal reliance on data classifies countermeasures according to audit data sources, presenting a holistic major on the strategies to address insider threats.
- **Challenges and Recommendations:** The article stresses the fact that it is quite challenging to protect an organization against insider threats at an initial stage, which asks for the applications of technologies, behavior assessments, and organizational paradigms to enhance the internal security of an organization.

The article provides practical experiences showing how insider threats can significantly harm organizations and public confidence [2]. This article is based on an unfortunate and rather pathetic scenario of a contractor working for the Home Office who lost a USB stick containing the personal details of 84,000 prisoners as it was not encrypted. These actions resulted in a severance, which saw a £1. Later, in 1996, Nike signed a $5 million contract for another segment and faced massive criticism from the public. The article also describes one failed attempt at what could have been the biggest bank robbery because of the inside job at one of the branches in London of a Japanese bank.

It emphasizes the exposure of organizations and corporations to insider activities, whether due to recklessness, intentionally, or by accident. It paints insiders as dangerous people who can cause large financial losses, harm an organization's reputation, and steal valuable information. Through the use of motives outlined in the article, such as theft or money-making, vindictive attitudes, or mistakes, insider risk is complex, therefore agreeing with the given statement.

Key Points Highlighted Include

- **Examples of Insider Threats:** The Home Office data breach is a vivid example of how negligence on the part of an employee can lead to contract cancellation and negative publicity. The failed bank heist also demystifies the monetary fraud that insiders planned in executing their plots.
- **Impact and Consequences:** Inadvertent actions by insiders also lead to severe business implications, such as significant financial costs and loss of brand image, highlighting the necessity for adequate security controls and monitoring.
- **Insider Types and Motivations:** The article categorizes insider threats as being the malicious insiders; these are those who are motivated to breach the security of the organizations with the sole intention of embezzling money and seeking revenge, among other motives, and the unintentional insiders, these are those who are constrained by ignorance, lack of knowledge and experience or Training and may consequently breach the security of the organization.
- **Response and Recommendations:** It promotes a multilayered approach comprising technological solutions, behavioral monitoring, and bureaucratic measures as the best proactive strategy to prevent insider threats and build organizational resistance to insider risks.

Methodology: Swot Analysis

Utilizing a SWOT analysis that has been conducted based on research on insider threats means that the current situation can be assessed within a structured framework to ensure that all possible aspects are considered. This means that strengths like having specialized detection technologies and awareness of an organization's strengths help those involved in this project gauge the capacities already in place. Identifying deficiencies in the implementation and resources devoted to it is critical because it enables specific adjustments to enhance security systems. Strategic innovation and preventative action are facilitated concerning future opportunities like growth, new technologies, and collaboration opportunities [8]. Measuring risk situations derived from changes in insider tactics and regulations helps organizations be ready to successfully shift their defenses and compliance approach to regulations. Finally, a SWOT analysis based on the study's findings is as follows, which would be vital to enhance the investigator-developed insider threat frameworks, enhance the resilience levels among the organizations, and prevent threats effectively.

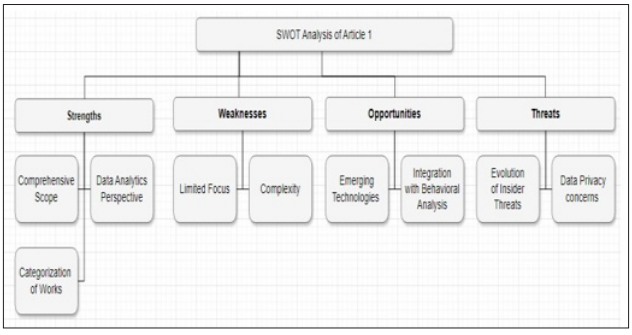

Figure 5: SWOT Analysis of Article 1

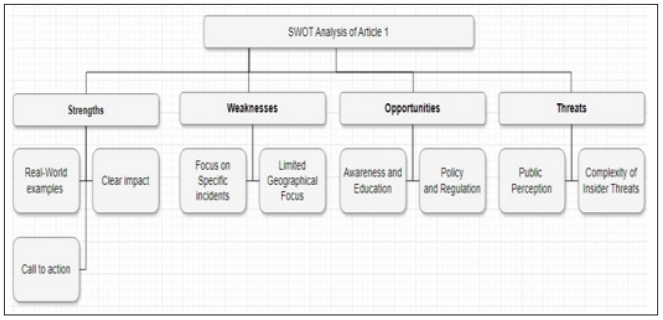

Figure 6: SWOT Analysis of Article 2

Analysis and Synthesis

Compilation of Findings

The literature review on insider threat and possible solutions highlighted the following SWOT analysis: Opportunities exist for sophisticated technology solutions like analytics and machine learning algorithms that improve the company's ability to identify and prevent IT insider threats. The last one refers to coping assets found to be common with behavioral analysis methodologies capable of hinting at possible insider threats due to their unusual behavioral patterns. Furthermore, many organizations have improved their understanding and recognition of insider threats and compliance needs, promoting preparedness and effectiveness in organizations today.

The strengths relating to this research are that it has combined theoretical research with case studies and practitioners' insights. In contrast, the weaknesses focused mostly on the human aspect and the misconceptions about effectively identifying insider threats. The insiders acting out their human frailties present a huge challenge beyond technology. Moreover, issues arising from analyzing different data types and privacy issues with monitoring people were mentioned as problems. Such factors cause challenges in effective insider threat detection and make implementing comprehensive insider threat solutions difficult.

In particular, developments in big data and data analysis, as well as in AI and machine learning, present definite opportunities. These technologies appear to offer opportunities for automating threat detection, increasing the efficiency of threat detection, and mitigating cases of false alarms that may slow down responses to insider threats. There is also an opportunity for improved insider threat information–sharing systems between industry players, academics, and government agencies, thus enabling the development of new, improved insider threat detection methodologies. Moreover, getting committed to training and awareness could help to build the workforce capacity needed to identify and report illicit actions, thus enhancing the organization's protection.

Group Findings into Actionable Insights

This synthesis of the findings makes it possible to identify practical recommendations to improve biological and physical control of insider threats. Best practices for organizations should include the improvement of technological competence, which may be achieved by allocating resources to the development and implementation of analytics and machine learning devices. The current consolidation of BAM and UBA enhances the constant tracking and identification of IT insiders' threats. Launching awareness training programs for the organization's staff is crucial as it helps to establish and implement a cybersecurity culture and enforce reporting of suspicious activities.

It is recommended that people in the industry and governments promote the sharing of information and practices to identify insider threats. The conflict of interest between security and privacy is key; organizations must employ security monitoring that is not invasive of the workforce's privacy while at the same time preventing insider threats. This could entail having a regular appraisal of the strategies due to the potential changes in the inside threats' modus operandi as well as the ever-shifting paradigm in the regulation of the inside threats.

By executing these recommendations, an organization increases its protection against insiders and substantially reduces risks linked to the leakage of important data and infrastructure resources.

Strategic Recommendations

Based on SWOT Analysis

One critical risk factor is insider threats, which remain an active challenge in organizations calling for effective tactics that build on the cardinal rule of management: strengths, weaknesses, opportunities, and threats analyzed in the SWOT business model.

Enhancing Current Detection Technologies and Methodologies

To build upon existing advantages in sophisticated detection methodologies such as AI, machine learning, and behavioral analysis, cybersecurity leaders must constantly look for opportunities to enhance their capabilities [9]. The anomalous data analysis system that should be obtained is the one that offers real-time analysis and the ability to identify patterns. These technologies can filter the data to look for odd user behavior or access patterns betraying Heisenberg attacks. Researchers can always improve the technologies used to have better detection, which can help organizations be one step ahead of any tactic’s insiders use.

Addressing Weaknesses in Implementation and Resource Allocation

These are some of the areas of weakness that we have identified that need more attention, including human elements and resource limitations. It is recommended that organizations supervise and implement extensive awareness campaigns that focus on raising awareness of the existing threats, the code of ethics, and the necessity to report any abnormalities. It is also necessary to assign sufficient funds for investment in cybersecurity and the right people to perform cybersecurity activities. This is done by ensuring the availability of skilled personnel, especially within the cybersecurity department, and proper integration of various data feeds to get a more comprehensive threat picture. Reducing steps and implementing AI-driven solutions where effective would make an enterprise's utilization of resources efficient to counter insider threats.

Capitalizing on Opportunities for Innovation and Collaboration

Challenges are also present in areas of innovation where collaboration among parties in the cybersecurity environment can be encouraged. Organizations should establish cooperative and collaborative relationships with academe, senior peers, technology suppliers, and vendors. Joint research projects can spur the improvement of modern detection methods that are more focused on emerging insider threats. Adapting to the integration of new technologies like blockchain and secure computation denotes the chance of promoting the security of data, which, in turn, prevents insider risks. Through knowledge exchange and pooling, manufacturers can drive new technologies' implementation faster and adapt more quickly to threats when they arise.

Mitigating Threats and Risks Associated with Evolving Insider Tactics and Regulatory Challenges

The threats of new tendencies in insider activity and supervisory issues suggest that organizations must take measures to prevent these. A particular focus of monitoring should be shifted from activity-based pattern detection. Implementing methods for identifying insider threats requires increasing attentiveness toward slight deviations in the employees' behavior and peculiar actions. This encompasses using intelligence techniques to observe users' real-time actions within the network, systems, and applications. It is also important to know how cybersecurity policies and procedures are occasionally updated based on the regulatory bodies' ever-changing requirements and other standards.

Effective compliance measures and auditing another set is the legal standards to monitor compliance with data protection laws while building up defenses against insider threats [10]. Risk management plans and contingency tactics such as simulating and creating plans in the event of an insider threat help organizations prevent or lessen the consequences of such threats on business continuity.

Therefore, this paper recommends the following strategies based on the SWOT analysis to improve the insider threat detection and prevention of organizations: To mitigate insider threats and potential regulatory policies, the overall cybersecurity maturity level needs to be improved through the constant enhancement of innovative practices, cooperation, and key risk management initiatives that will protect the organizational resources, reputation, and stakeholders' confidence.

Evaluation and Validation

Validation of Findings

The evaluation of SWOT analysis findings and the proposed strategies include comparing the results received and the current trends within the companies' industries and experts' opinions while keeping in view the stakeholders and the strict, critical analysis of the conducted studies.

Compare Findings with Current Industry Practices and Expert Opinions

The strategic recommendations from the SWOT analysis and the actions identified to achieve the competitive advantage are further supported and aligned with benchmarking to industry best practices and cybersecurity professionals' advice. Recent technological advancements characterize today's industries as adopting innovative methods such as artificial intelligence, anomaly detection, machine learning, and behavioral analytics as critical components of insider threat solutions. It is evident from the personnel experts that the consideration of ensuring organizational protection should be grounded on the technical aspect of protection, as well as the human aspect. Thus, following the results of investigations, bringing them into different categories of the recognized standards and professional opinions, the recommendations get the background of validity and applicability to the issues and challenges of the present day.

Validate Recommendations through Stakeholder Feedback and Study Analysis

The stakeholders' opinions are vital in confirming the effectiveness and implementing ability of the proposed strategies in implementing insider threat threats. Interacting with a diverse population consisting of cybersecurity professionals, management, and clients yields first-hand information regarding the likely ramifications of the proposed suggestions and the peculiarities of instilling change. As a result of feedback sessions and structured questionnaires, it is possible not only to determine the weaknesses and strengths of the current business environment but also to assess the effectiveness of the measures suggested by the author in addressing the existing challenges and utilizing the opportunities. In addition, such activities as a case study and empirical research strengthen the theoretical coverage of the recommendations by contrasting the theoretical framework with actual settings and activities.

With findings compared to enshrine industry best practices, authorities' opinions, stakeholder inputs, and conclusions in a plethora of, and a systematic investigation of the study, various organizations can improve the authority and efficacy of strategies that aim to mitigate insider threats. This validation initiates an important verification process that allows conceptual, practical, and accurate approaches to be offered, noting the dynamicity of risks, especially from insider threats in organizations.

Limitations and Biases

Recognize Biases or Limitations Inherent in the Reviewed Literature

The literature overview on insider threats and cybersecurity measures might contain some biases typical for works originating from Western countries. Thus, investigations from other areas, such as Asia, Africa, or Latin America, could be overlooked. Such geographic bias may pose a threat to the external validity of the research and the recommendations they make, as cybersecurity measures and threats differ from one location to another. However, emphasizing cases and conducting research confined to established organizations could bring drawbacks. Such studies may not provide an adequate variety of sizes of organizations across the world, types of IT structures, and demographics of the workforce, thus limiting the ability to extrapolate findings at a wider level.

Geographic or Industry-Specific Focuses that May Impact Generalizability

The choice of geographic locations and industry segments in the literature affects the applicability or transferability of conclusions and suggestions. Due to the differences in resource limitation in low- and middle-income countries and the distinct regulatory settings for cybersecurity in these countries, insights from research studies most often carried out in high-income countries may not fully represent the problem to be solved. Likewise, conclusions that can be obtained from one industry may not be valid for another; for example, the finance or healthcare industry is likely to vary from a manufacturing or retail industry, which has unique ways via which IT systems may be invaded. It is important to understand these differences when it comes to applying and interpreting the literature findings; it guarantees the comprehensiveness of the review and recognition of the necessity of using different approaches to developing inclusive studies.

Conclusion

Summary of Insights

The literature review on insider threat detection and prevention resolved by this study provides a clear understanding of the insights where integration of technology, behavioral analysis, and prevention measures is essential to reduce insider threat. This approach is critical to improving the detection of threats and minimizing the threats posed by insiders to the organization. Insider threats can be managed intentionally with the help of many applications of advanced analytics, machine learning, and artificial intelligence solutions.

Implications for Improving Insider Threat Detection and Mitigation Strategies

Analyzing the consequences of enhancing the work on detecting and neutralizing insiders, the current shortcomings in their implementation, including the distribution of funds and the coordination of actions, are highlighted. There should be more investment in strong training models, the response to incidents, and monitoring cycles without interruption. Moreover, apart from having a security- awareness culture and multiple layers of access controls, organizations must adequately address other forms of insider threats.

Future Research

The future work will identify novel paradigms for timely anomaly detection, data mining for insider threat prediction, and knowledge sharing among the domains. Learning about how risky insider threats are, how regulation affects them, and geopolitics will be important in creating proper prevention techniques. It will be useful to concentrate on these aspects to increase the preparedness against insider threats and improve the safeguarding of valuable assets in today's evolving threat landscape. Here is a question that sets the stage for exploring innovative approaches to enhancing insider threat detection and prevention strategies through technological and collaborative means.

- **Research Question:** How can novel paradigms in anomaly detection, data mining for prediction, and cross-domain knowledge sharing enhance the prevention of insider threats in diverse organizational environments?
- **Hypothesis:** Implementing advanced anomaly detection algorithms integrated with machine learning and AI techniques will improve the accuracy and timeliness of insider threat prediction. Enhanced data mining capabilities coupled with effective knowledge sharing mechanisms across different domains will significantly bolster organizations' preparedness against insider threats, thereby safeguarding valuable assets in an increasingly complex threat landscape.

References

1. M Bishop, Sophie Engle, Deborah A Frincke, Carrie Gates, Frank L Greitzer, et al. (2010) A Risk Management Approach to the 'Insider Threat,'" Insider Threats in Cyber Security 49: 115-137.
2. K Roy Sarkar (2010) Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report 15: 112-133.
3. J Glasser, B Lindauer (2013) Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data. IEEE Xplore https://ieeexplore.ieee.org/document/6565236+measure%20s&ots=N6sTXJpV4J&sig=hxCiXofE8BIp8CtFZmrjtuR%208RvM.
4. DP Brown, D Buede, SD Vermillion (2019) Improving Insider Threat Detection Through Multi- Modelling/Data Fusion. Procedia Computer Science 153: 100-107.
5. J Nurse, Oliver Buckley, Philip A Legg, Michael Goldsmith, Sadie Creese, et al. (2014) Understanding Insider Threat: A Framework for Characterising Attacks. 2014 IEEE Security and Privacy Workshops https://ieeexplore.ieee.org/document/6957307/authors#authors.
6. I Homoliak, F Toffalini, J Guarnizo, Y Elovici, M Ochoa (2019) Insight into Insiders and IT. ACM Computing Surveys 52: 1-40.
7. G Gavai, K Sricharan, D Gunning, R Rolleston, J Hanley, et al. (2015) Detecting Insider Threat from Enterprise Social and Online Activity Data. Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats 13-20.
8. FL Greitzer, JD Lee, J Purl, AK Zaidi (2019) Design and Implementation of a Comprehensive Insider Threat Ontology. Procedia Computer Science 153: 361-369.
9. F Whitelaw, J Riley, N Elmrabit (2024) A Review of the Insider Threat, a Practitioner Perspective Within the U.K. Financial Services. IEEE Access 12: 34752-34768.
10. FR Alzaabi, A Mehmood (2024) A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. IEEE Access 12: 30907-30927.