A PROJECT REPORT

on

"Human Factor in Network Security: Understanding and Mitigating Insider Threat"

Submitted to

KIIT Deemed to be University

In Partial Fulfillment of the Requirement for the Award of

BACHELOR'S DEGREE IN INFORMATION TECHNOLOGY

BY

Arnav Subudhi	2105529
Bikramaditya Munshi	2105538
Jatin Nayak	21052669

UNDER THE GUIDANCE OF

Dr. Ajit Kumar Pasayat

SCHOOL OF COMPUTER ENGINEERING

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY

BHUBANESWAR, ODISHA -751024

April 2024

KIIT Deemed to be University

School of Computer Engineering
Bhubaneswar, ODISHA 751024

CERTIFICATE

This is certify that the project entitled

"Human Factor in Network Security: Understanding and Mitigating Insider Threat"

submitted by

Arnav Subudhi	2105529
Bikramaditya Munshi	2105538
Jatin Nayak	21052669

is a record of bonafide work carried out by them, in the partial fulfilment of the requirement for the award of Degree of Bachelor of Engineering Computer Science & Engineering at KIIT Deemed to be university, Bhubaneswar. This work is done during year 2024-2025, under our guidance.

Date: / /

(Guide Name)
Dr. Ajit Kumar Pasaya

Acknowledgements

We are profoundly grateful to **Dr. Ajit Kumar Pasayat** of **Affiliation** for his expert guidance and continuous encouragement throughout to see that this project meets its target since its commencement to its completion.

Arnav Subudhi
Bikramaditya Munshi
Jatin Nayak

ABSTRACT

The escalating dependence on interconnected networks in the modern digital era necessitates a robust cybersecurity strategy. Network security forms the foundation of this defense mechanism, safeguarding sensitive information. However, human factors can significantly influence the effectiveness of these measures. Inadvertent user actions or lack of awareness can create exploitable gaps in an organization's security posture. Consequently, mitigating human factors has become an essential component of a comprehensive cybersecurity strategy.

This paper explores the significant role human factors play in network security. It highlights the impact of human errors, emphasizes the importance of security awareness training, and acknowledges the crucial role of human judgment in threat detection and response. The paper then delves into the challenge of insider threats, malicious activity by authorized users. It reveals limitations in current practices for addressing insider threats and emphasizes the need for organizations to prioritize mitigation strategies.

The paper proposes a framework and mitigation techniques to identify and mitigate insider threats. The remainder of the paper outlines the research methodology, findings, and analysis, culminating in a discussion on the proposed framework and its implications for future research.

Keywords: Insider threat, insider threat detection, insider threat mitigation, insider threat framework, insider threat security.

Contents

List of Figures

Chapter 1

Introduction

In the digital era of the 21st century, the network is the basis of every mode of communication. The escalating dependence on interconnected networks in the modern digital era mandates a rigorous approach to cybersecurity. Network security serves as the foundation of this strategy, functioning as a sophisticated barrier against unauthorized access, data breaches, and malicious attacks. Firewalls, encryption protocols, and intrusion detection systems form the core of this defense mechanism, safeguarding the integrity and confidentiality of sensitive information and it should also ensure that the information is always available when required so that the CIA triad is maintained at all times. However, a critical vulnerability can often reside within the system, as well as, the human element. Human factors can have a wide range of user behavior, decision-making processes, and inherent cognitive biases and can significantly influence the effectiveness of network security measures. Inadvertently clicking on a malicious link within a phishing email, neglecting to implement strong password practices, or failing to report suspicious activity – these seemingly harmless actions can create exploitable gaps in an organization's security posture. The consequences of such lapses can be severe, potentially resulting in substantial financial losses, reputational damage, and the degradation of public trust in digital infrastructure. Consequently, acknowledging and mitigating human factors has become an essential component of establishing a truly comprehensive cybersecurity strategy. By proactively addressing these vulnerabilities, organizations can fortify their digital defenses and create a more secure environment for all stakeholders.

In the current scenario, human factors play a significant role in network security, affecting organizations in various ways. Here are some current scenarios and their impact on network security:

- **Errors caused by humans**: Errors caused by humans can lead to security breaches, such as victims falling to phishing attacks, clicking on malicious links, or inadvertently sharing sensitive information. This can result in data breaches, financial losses, and reputational damage to the organization.

- **Awareness and Training:** Cultivating a security-conscious culture through comprehensive training and awareness programs is crucial for mitigating the human factor's impact. Regular training and simulated phishing campaigns can help employees recognize and avoid phishing threats. This also includes providing training related to detection of manipulative attempts to all customer facing staff members to reduce the probability of disclosure of sensitive information.
- **Human-led Security Measures:** The judgment, expertise, and intuition of humans play a crucial role in interpreting security alerts, identifying anomalies, and responding to cyber incidents. Human analysis and decision-making are essential for effective threat detection and response. The error caused by human beings can only be solved by another human being.
- **Insider Threats:** Human actors within an organization can intentionally or unintentionally compromise security, leading to unauthorized access to sensitive data, misuse of privileges, or unintentional data leaks due to circumstances like financial problems or the global recession. Managing insider threats requires a combination of technical controls and human awareness.

With the advancement of technology, security is improving, but relying on technology has its own limitations. Technology will only focus on outside actors and provide security in the form of firewalls, intrusion detection, and other common tools that are great for providing security from external threats. When it comes to dealing with internal actors, these same technologies become less effective. Employees in an organization need information on a daily basis to work, and applying the same technology, same restrictions internally can be an impractical and expensive approach to provide security from internal threats. A recent UK government survey [1] highlights improvements in overall organizational security controls. These advancements primarily focus on deterring external threats. Some are:

- **Documented policies:** 55% of organizations have a documented security policy that outlines security protocols.

- **Staff training:** 40% of organizations provide ongoing security awareness training to educate employees on recognizing and mitigating cyber threats.
- **Authentication:** 14% of organizations have utilized string, multi-factor authentication for added access security.
- **Standardization:** 11% of organizations have implemented security management standards.
- **Backups:** 99% have backed up critical software and data for disaster recovery.
- **Anti-Malware:** 98% have employed software to scan for spyware and filter out spam emails.
- **Network Protection:** 97% of organizations utilize firewalls to safeguard their websites and scan incoming emails for viruses.
- **Wireless Security:** 94% encrypt their wireless network transmissions to prevent events like unauthorized access.

The insider threat, which is a malicious activity by someone with authorized access, poses a persistent challenge to security. However, data regarding internal threats based on which analysis can be done and conclusions can be drawn is far less as compared to external threats.
In a report, the National Infrastructure Advisory Council highlights a concerning lack of consistency in how several businesses address insider threats. Awareness and mitigation strategies vary across organizations and often fall short of best practices. Similarly, a UK government survey [1] reveals potential vulnerabilities like:

- **Risk assessment:** Over half of the organizations do not conduct any kind of formal security risk assessment, which leaves them unprepared for various threats, including insider activity.
- **Data loss prevention:** The majority of the organizations lack safeguards to prevent confidential data from being transferred via portable storage devices.
- **Data Encryption:** The majority of the organizations reported stolen computers with unencrypted hard drives, potentially exposing sensitive data.

These findings from the survey indicate that organizations should move beyond pure external focus and should also prioritize measures to address insider threats.

Another survey by RSA/IDC reveals that:

- **Misplaced Focus:** Organizations and security leaders are overwhelmingly concerned with external threats, with 82% of them being unsure of the source of the insider threats of the respective organizations. This lack of awareness leaves the organization vulnerable.
- **Contractors and Temporary Workers:** This study has identified contractors and temporary workers as a major source of insider threats. These costs outsourcing companies nearly $800,000 due to insider breaches.
- **Internal Attacks Prevalent:** The data from the survey highlights a significant number of internal attacks. Over 11,600 of such incidents involved malware/spyware, privilege abuse, and access control violations. Nearly 19% of these attacks were believed to be deliberate attacks.

The findings of various studies underscore the urgency of addressing the insider threat. Organizations must move their attention beyond external threats and implement strategies to mitigate the risks posed by those with authorized access. The main objective will be to develop an incident response plan to quickly respond to and mitigate the impact of insider threats.

In this paper, we will propose a framework and mitigation techniques to identify and mitigate insider threats, and we will also discuss how the system can act as an insider threat to an organization.

Chapter 2
Basic Concepts

2.1 Insider Threats
An insider threat arises when an individual with authorized access to an organization's network, systems, or data misuses those privileges. This misuse can be intentional (malicious insider) or unintentional (careless or negligent user) and can have severe consequences for the confidentiality, integrity, and accessibility of the organization's information assets [2].

2.1.1 Malicious Insiders
Malicious insiders deliberately exploit their authorized access to harm the organization. Their motivations can vary, including financial gain, revenge, or espionage. Malicious insiders can steal sensitive data, disrupt operations, or sabotage systems.

2.1.2 Careless and Negligent Users
Careless and negligent users lack malicious intent but introduce vulnerabilities through actions like clicking phishing links, using weak passwords, or mishandling sensitive data. These actions can create entry points for attackers or lead to accidental data breaches.

2.2 Contributing Factors to Insider Threats
Several factors can contribute to insider threats, including:

- **Lack of training or unclear policies**: Inadequate training or poorly defined security policies can leave employees unaware of cyber threats and unsure of how to handle sensitive information.
- **Financial problems**: Employees experiencing financial hardship may be more susceptible to bribery or other financial incentives offered by attackers.
- **Excessive privileges**: Granting excessive access to a single individual creates a vulnerability, as those privileges can be abused to compromise sensitive data or systems.
- **Global recession**: Economic downturns can increase the risk of insider threats as employees facing financial insecurity may be more likely to engage in malicious activity.

2.3 Mitigation Strategies

Organizations can implement various strategies to mitigate insider threats:

- **Two-person integrity**: This control mandates the presence of two authorized individuals for tasks involving sensitive data, making it more difficult for a single insider to act maliciously.
- **Mandatory access control (MAC)**: MAC classifies both information and users based on a security hierarchy, ensuring users can only access information at their designated security level or below.
- **Role-based access control (RBAC)**: RBAC assigns access based on job duties, limiting access to data only necessary for specific roles and preventing unauthorized use of information.
- **Layered security approach**: This approach combines traditional access controls with additional measures like network segmentation, data encryption, and continuous monitoring to create a multi-layered defense against insider threats and social engineering tactics.
- **Penetration testing**: Regularly simulating cyberattacks with ethical hackers helps identify vulnerabilities in systems that could be exploited by insiders.
- **Patch management**: Timely deployment of security updates addresses vulnerabilities in software that could be exploited by malicious actors.
- **Vulnerability assessments**: Regularly identifying and remediating system weaknesses reduces the risk of insider exploitation.
- **Security awareness training**: Training employees to recognize and respond to manipulation attempts and suspicious activity is crucial for mitigating insider threats.
- **Simplified misconduct reporting**: An easy and anonymous reporting system encourages employees to report suspicious behavior without fear of reprisal.
- **Data backups and offsite replication**: Regularly backing up data and storing copies offsite ensures data recovery in case of insider attacks.

- **Access termination upon employment exit**: Immediately revoking access to all systems, sites, and information upon employee termination minimizes the risk of unauthorized access by former employees.

Chapter 3
Problem Statement / Requirement Specifications

3.1 Problem Statement

Organizations increasingly rely on interconnected networks, making them vulnerable to insider threats. These threats arise when individuals with authorized access to an organization's network, systems, or data misuse those privileges. Malicious insiders can steal sensitive data, disrupt operations, or sabotage systems. Careless or negligent users can also introduce vulnerabilities through actions like clicking phishing links or using weak passwords. These insider threats can have severe consequences for the confidentiality, integrity, and accessibility of an organization's information assets.

Existing mitigation strategies often focus on training and awareness programs. While these are important, a more comprehensive approach is necessary to address the evolving nature of insider threats.

3.2 Project Requirements

This project aims to develop a framework that effectively mitigates insider threats. The framework should address the limitations of traditional methods by:

- **Encompassing both technical and procedural controls:** The framework should incorporate technical safeguards like access controls and data encryption alongside clear security policies and employee training.
- **Addressing human vulnerabilities:** The framework should recognize the human element in insider threats and include strategies to address factors like financial problems and lack of awareness.
- **Providing a layered defense:** The framework should employ a multi-layered approach, combining access controls with measures like network segmentation and continuous monitoring to create robust defenses against various insider tactics.

3.3 Project Planning

The project will follow these key stages:

- **Literature Review:** Conduct a thorough review of existing research on insider threats, mitigation strategies, and best practices.
- **Framework Development:** Design a comprehensive framework incorporating technical controls, procedural measures, and user education components.
- **Evaluation and Refinement:** Evaluate the proposed framework through expert review or simulation exercises. Refine the framework based on the evaluation results.
- **Implementation Guidelines:** Develop guidelines for implementing the framework within an organization, including recommendations for policy development, training programs, and technical controls.

3.4 Project Analysis

Following framework development, a thorough analysis will be conducted to ensure:

- **Clarity and Conciseness:** The framework should be clearly defined and easy to understand for both technical and non-technical audiences.
- **Completeness:** The framework should address all aspects of insider threat mitigation, including technical controls, procedural measures, and user awareness.
- **Feasibility:** The framework should be practical and implementable within different organizational contexts and resource constraints.

3.5 System Design

3.5.1 Design Constraints

The proposed framework is designed to be adaptable and implementable across various organizational structures and technical environments. The specific implementation details will depend on the unique needs and resources of each organization.

3.5.2 System Architecture

The framework will not require a dedicated software system. Instead, it will function as a comprehensive strategy that integrates existing security tools and procedures with additional measures for a layered defense. A high-level

block diagram can be created to illustrate the interaction between the framework components, such as:

- Access controls (MAC, RBAC)
- Data encryption
- Network segmentation
- Security awareness training
- Misconduct reporting system
- Data backup and offsite replication
- This block diagram will be included in the final report.

By following these steps and addressing the outlined requirements, this project aims to develop a robust insider threat mitigation framework that surpasses traditional methods and empowers organizations to safeguard their critical information assets.

DIAGRAM:

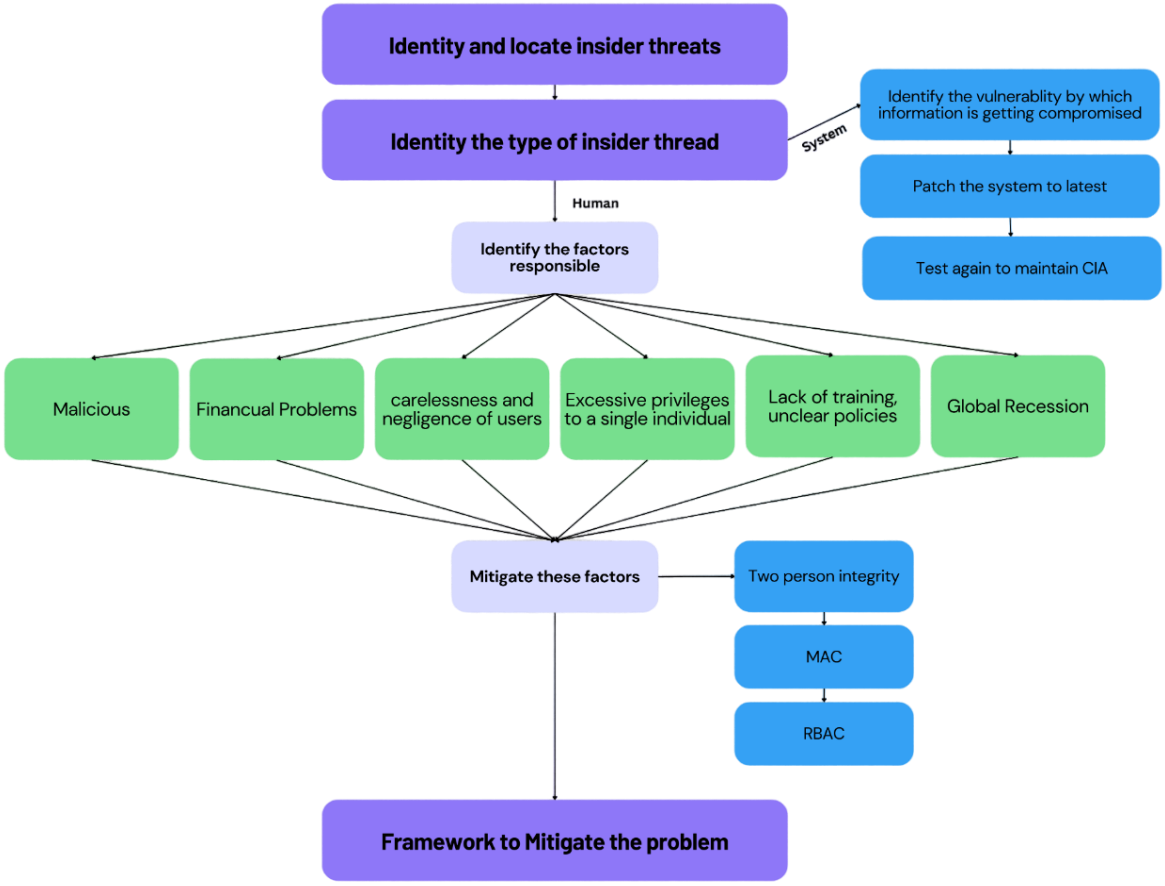

Fig. 1

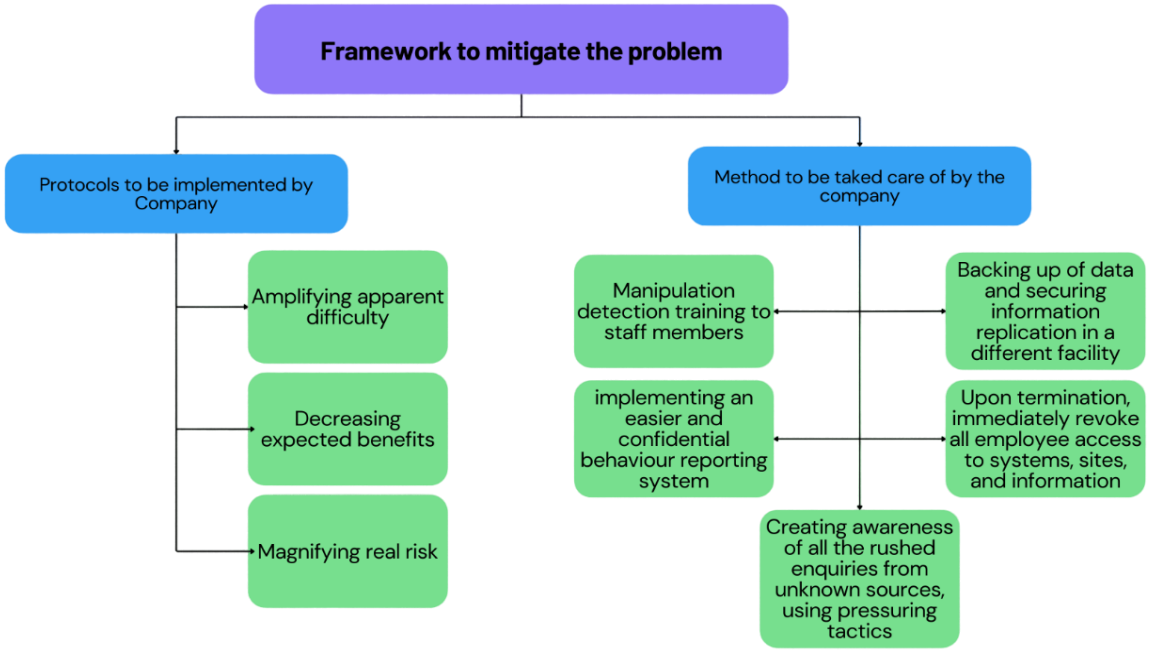

Fig. 2

Chapter 4
Implementation

4.1 Methodology

This proposal outlines a comprehensive framework to mitigate insider threats, encompassing preventative measures, access controls, and user awareness initiatives.

4.1.1 Addressing System Vulnerabilities

- **Regular Patching and Updates:** Implement automated patching processes to ensure timely deployment of security updates and address software vulnerabilities. Conduct regular vulnerability assessments to identify and remediate weaknesses before exploitation.
- **Penetration Testing:** Simulate real-world cyberattacks through ethical hacking to identify vulnerabilities within systems. Proactively address these vulnerabilities to reduce the risk of financial losses.
- **Network Segmentation:** Divide the network into smaller segments to limit the blast radius of a potential breach and prevent attackers from gaining access to critical systems.
- **Data Encryption:** Encrypt sensitive data at rest and in transit to render it unreadable in case of a breach.

4.1.2 Strengthening Access Controls

- **Two-Person Integrity:** Mandate the presence of two authorized individuals for tasks involving sensitive data or critical system controls. This deters potential insider threats by introducing an extra hurdle for compromising information or systems.
- **Mandatory Access Control (MAC):** Classify both information and users based on a security hierarchy. Users can only access information at their security level or below, limiting the potential damage an insider could cause.
- **Role-Based Access Control (RBAC):** Assign access to information and systems based on an employee's job duties. This prevents both accidental and intentional misuse of information by insiders.

- **Access Review:** Regularly review user access privileges to ensure they remain aligned with current job roles and responsibilities. Revoke access for terminated employees immediately.

4.1.3 User Awareness and Training

- **Manipulation Detection Training:** Train staff members to identify and respond to social engineering tactics used by malicious actors.
- **Confidential Behavior Reporting System:** Establish a simplified and anonymous system for employees to report suspicious activity or security concerns.
- **Security Awareness Campaigns:** Regularly educate staff about cybersecurity best practices, including password hygiene, phishing email identification, and the importance of reporting suspicious activity.

4.1.4 Framework Effectiveness

This framework surpasses traditional methods by focusing on:

- **Identification and Mitigation:** Proactive identification and remediation of both system and human vulnerabilities.
- **Shared Responsibility:** Shared responsibility between the organization and its users for enhanced security.
- **Layered Approach:** A layered security approach combining traditional controls with modern strategies for comprehensive protection.

4.2 Testing And Verification

Following implementation, a comprehensive testing plan is crucial to verify the system's functionality and identify any potential shortcomings. Here's a sample test case table:

TEST ID	TEST CASE TITLE	TEST CONDITION	SYSTEM BEHAVIOUR	EXPECTED RESULT
1	Knowledge Retention	Trainees take a pre-training assessment on cybersecurity awareness.	Scores are recorded.	Trainees demonstrate a baseline understanding of cybersecurity concepts.
2	Knowledge Acquisition	Trainees complete the cybersecurity awareness training program.	Training is delivered as designed.	Trainees pass a post-training assessment with a score exceeding a predefined threshold.
3	Behavioral Change	Trainees are presented with simulated phishing attempts after training completion.	Trainees attempt to access simulated phishing emails.	Trainees identify and avoid phishing attempts at a rate exceeding a predefined threshold.
4	Reporting	Trainees are presented with a scenario involving suspicious activity.	Trainees are given the opportunity to report the activity.	Trainees report the suspicious activity through designated channels.
5	Password Hygiene	Trainees are prompted to create a new password.	Trainees follow password creation best practices.	Trainees create passwords that meet complexity requirements and avoid using easily guessable information.
6	Social Engineering Awareness	Trainees are presented with scenarios involving social engineering tactics.	Trainees identify and respond appropriately to social engineering attempts.	Trainees resist social engineering attempts and avoid disclosing sensitive information.
7	Secure Data Handling	Trainees are presented with scenarios involving data transfer.	Trainees follow secure data handling procedures.	Trainees utilize approved methods for data transfer and avoid transferring sensitive information through insecure channels.
8	Patch Management Awareness	Trainees are presented with information on software updates.	Trainees demonstrate understanding of the importance of timely patching.	Trainees prioritize installing software updates and avoid delaying critical security patches.
9	Physical Security Awareness	Trainees are presented with scenarios involving physical access to devices.	Trainees demonstrate awareness of physical security measures.	Trainees secure devices when unattended and avoid leaving them accessible to unauthorized individuals.
10	Incident Response Training	Trainees participate in a simulated security incident.	Trainees follow established incident response procedures.	Trainees effectively identify, report, and respond to the simulated security incident.

4.3 Result Analysis

By analyzing the results of these test cases, we can gain valuable insights into the effectiveness of our cybersecurity awareness training program in mitigating human factors that influence network security.

In accordance with the findings of the testing plan analysis:

- **Pre-training assessment scores:** Summarize the baseline knowledge level of trainees.
- **Post-training assessment scores:** Compare these scores to pre-training results to measure knowledge acquisition.
- **Phishing simulation results:** Analyze the success rate of trainees in identifying and avoiding phishing attempts. This can be presented as a percentage or success rate graph.
- **Suspicious activity reporting results:** Report the percentage of trainees who reported the suspicious activity.

Chapter 5
Standards Adopted

5.1 Insider Threat Mitigation Standards

Similar to the well-defined design standards (e.g., IEEE, ISO) in various engineering disciplines, specific best practices can be implemented to bolster an organization's insider threat mitigation efforts. These standards serve as a foundation for establishing a secure environment:

- **Two-Person Integrity:** This principle mandates the requirement for two authorized individuals to be present during actions involving sensitive data or critical system controls. This approach functions as a system of checks and balances, deterring potential insider threats by introducing an additional hurdle for unauthorized activity.

- **Mandatory Access Control (MAC):** MAC differs from traditional access controls by classifying both information and users based on a security hierarchy. This stratified system ensures that users can only access information at their designated security level or below. By limiting access based on a user's security clearance, MAC minimizes the potential damage an insider could inflict.

- **Role-Based Access Control (RBAC):** RBAC assigns access privileges based on an employee's job function. Similar to granting specific keys to different areas within a building, RBAC restricts access to information based on job roles. This approach helps prevent both accidental and intentional misuse of data by insiders.

These core principles, along with a layered security approach, establish a robust defense mechanism.

5.2 Layered Security Approach

Beyond the aforementioned standards, a layered security approach is crucial in today's evolving threat landscape. This approach integrates traditional controls with modern strategies to fortify an organization's security posture:

- **Network Segmentation:** Network segmentation partitions a network into smaller segments, limiting the potential blast radius of a security breach. By compartmentalizing the network, a compromise in one segment can be contained before impacting the entire system

- **Data Encryption:** Data encryption safeguards sensitive information by rendering it unreadable without a decryption key. This adds an extra layer of protection for confidential data, even in the event of a breach.

- **Continuous Monitoring:** Constant monitoring of systems and user activity is essential for detecting suspicious behavior. Security Information and Event Management (SIEM) systems can be employed to aggregate and analyze log data from various sources, enabling the identification of potential insider threats.

This layered approach, coupled with the core mitigation standards, creates a comprehensive security architecture that adapts to emerging threats.

5.3 Maintaining System Integrity

While the aforementioned standards and approaches provide a strong foundation, additional measures are necessary to address system vulnerabilities that could be exploited by malicious actors:

- **Patch Management:** Regular system updates and software patches are critical to address vulnerabilities in software. Patching eliminates security holes that attackers could exploit, significantly reducing the risk of compromise. Organizations are encouraged to implement automated patching processes to ensure timely deployment of security updates.

- **Vulnerability Assessments:** Regular vulnerability assessments are essential for proactively identifying and remediating weaknesses within systems before they can be targeted. Penetration testing, which involves simulating real-world cyberattacks by ethical hackers, can be a valuable tool in uncovering vulnerabilities.

Chapter 6
Conclusion and Future Scope

6.1 Conclusion

In the digital age, where networks serve as the lifeline of communication and information exchange, ensuring robust cybersecurity is paramount. While technological advancements fortify defences against external threats, the human element introduces persistent vulnerabilities. Human errors, inadequate awareness, and insider threats pose significant risks to network security, necessitating a comprehensive approach.

Studies reveal a lack of consistency in addressing insider threats, with many organizations prioritizing external threats. However, internal breaches remain prevalent, highlighting the need for a shift in focus.

Moving forward, organizations must adopt a proactive stance in mitigating insider threats. This entails implementing robust security policies, conducting regular risk assessments, and fostering a culture of security awareness. Furthermore, investing in technologies that augment human capabilities in threat detection and response is essential.

In conclusion, addressing human factors in network security is imperative for creating a resilient digital infrastructure. By acknowledging the human element and implementing a comprehensive security strategy that encompasses both technological solutions and human-centric measures, organizations can mitigate risks effectively and foster trust in the digital ecosystem.

Expanding on the discussion, organizations should also prioritize continuous monitoring and adaptation of security measures to stay ahead of evolving threats. Additionally, collaboration with industry peers and sharing best practices can enhance collective resilience against cyber threats. This proactive approach fosters a culture of continuous improvement and resilience in the face of an ever-changing threat landscape, ultimately safeguarding critical assets and ensuring the integrity of digital infrastructure.

In the digital age, where networks serve as the lifeline of communication and information exchange, ensuring robust cybersecurity is paramount. While

technological advancements fortify defenses against external threats, the human element introduces persistent vulnerabilities. Human errors, inadequate awareness, and insider threats pose significant risks to network security, necessitating a comprehensive approach.

This paper has underscored the multifaceted impact of human behavior on network security, emphasizing the critical role of awareness training and the need to address both internal and external threats. Despite advancements, organizations still face challenges in mitigating insider threats, which require a nuanced understanding and tailored strategies.

Studies reveal a lack of consistency in addressing insider threats, with many organizations prioritizing external threats. However, internal breaches remain prevalent, highlighting the need for a shift in focus.

Moving forward, organizations must adopt a proactive stance in mitigating insider threats. This entails implementing robust security policies, conducting regular risk assessments, and fostering a culture of security awareness. Furthermore, investing in technologies that augment human capabilities in threat detection and response is essential.

In conclusion, addressing human factors in network security is imperative for creating a resilient digital infrastructure. By acknowledging the human element and implementing a comprehensive security strategy that encompasses both technological solutions and human-centric measures, organizations can mitigate risks effectively and foster trust in the digital ecosystem.

6.2 Future Scope

As technology continues to evolve and organizations face increasingly sophisticated cybersecurity challenges, the scope for insider threat mitigation is poised for significant expansion. By anticipating future trends and adopting proactive strategies, organizations can stay ahead of emerging threats and fortify their security postures.

- **Advanced Behavioural Analytics:**
  The future of insider threat mitigation lies in leveraging advanced behavioural analytics to detect anomalous user behaviour's indicative of potential insider threats. By analyzing patterns of user activity, organizations can identify deviations from normal behaviour and proactively intervene before malicious actions occur. Machine learning algorithms can be trained to recognize subtle indicators of insider threats, enhancing detection capabilities and reducing false positives.

- **Context-Aware Access Controls:**
  Traditional access control mechanisms rely on static permissions assigned to users based on their roles. However, the future of insider threat mitigation involves implementing context-aware access controls that dynamically adjust permissions based on the user's behaviour, location, and other contextual factors. By contextualizing access decisions in real-time, organizations can prevent unauthorized access and limit the impact of insider threats.

- **Integration of Threat Intelligence:**
  To stay abreast of evolving threats, organizations must integrate threat intelligence feeds into their insider threat mitigation strategies. By monitoring external sources for indicators of potential insider threats, such as compromised credentials or malicious insider activity in similar industries, organizations can proactively adapt their security measures to mitigate emerging risks. Collaborating with industry peers and sharing threat intelligence can also enhance collective defence against insider threats.

- **Continuous Monitoring and Response:**
  The future of insider threat mitigation emphasizes the importance of continuous monitoring and rapid response capabilities. By implementing real-time monitoring solutions that capture and analyze user activities across the network, organizations can detect suspicious behaviour as it occurs and respond swiftly to mitigate potential damage. Automated response mechanisms, such as user account suspension or data quarantine, can help contain insider threats before they escalate.

- **Enhanced User Awareness and Training:**
  While technological solutions play a crucial role in insider threat mitigation, the human element remains paramount. Future initiatives should prioritize enhancing user awareness and providing comprehensive training on cybersecurity best practices. Interactive training modules, simulated phishing exercises, and personalized feedback can empower employees to recognize and report potential insider threats, fostering a culture of security awareness throughout the organization.

- **Collaboration and Information Sharing:**
  In an increasingly interconnected digital ecosystem, collaboration and information sharing are essential for effective insider threat mitigation. Future efforts should focus on facilitating collaboration between different stakeholders, including security teams, HR departments, legal counsel, and external partners. By sharing insights, best practices, and threat intelligence, organizations can collectively strengthen their defences against insider threats and mitigate risks more effectively.

- **Regulatory Compliance and Governance:**
  With the proliferation of data privacy regulations and industry standards, future insider threat mitigation strategies must prioritize regulatory compliance and governance. Organizations should conduct regular audits and assessments to ensure adherence to relevant regulations, such as GDPR, HIPAA, or PCI DSS. By aligning insider threat mitigation efforts with regulatory requirements, organizations can mitigate legal and financial risks associated with non-compliance.

- **Adoption of Zero Trust Architecture:**
  Zero Trust Architecture (ZTA) represents the future paradigm for insider threat mitigation, emphasizing the principle of "never trust, always verify." By implementing granular access controls, continuous authentication, and micro-segmentation, organizations can minimize the attack surface and prevent lateral movement by insider threats. ZTA ensures that every user and device undergo rigorous verification before accessing sensitive resources, reducing the risk of insider threats infiltrating the network undetected.

In conclusion, the future scope of insider threat mitigation is characterized by a holistic approach that integrates advanced technologies, user awareness initiatives, collaborative frameworks, and regulatory compliance measures. By embracing innovation and proactive strategies, organizations can effectively mitigate insider threats and safeguard their assets, reputation, and stakeholders' trust in an evolving cybersecurity landscape.

References

1. Colwill, Carl. (2009). Human factors in information security: The insider threat-who can you trust these days?. Information Security Technical Report. 14. 10.1016/j.istr.2010.04.004.

2. Yusop, Zulkefli & Abawajy, Jemal. (2014). Analysis of Insiders Attack Mitigation Strategies. Procedia – Social and Behavioural Sciences. 129. 581-591. 10.1016/j.sbspro.2014.03.716.

3. Puthiyavan Udayakumar. "Design and Deploy a Secure Azure Environment", Springer Science and Business Media LLC, 2023

4. Amit Kumar Tyagi, V. Hemamalini, Gulshan Soni. "chapter 9 Digital Health Communication With Artificial Intelligence Based Cyber Security", IGI Global, 2023

INDIVIDUAL CONTRIBUTION REPORT:

Human Factor in Network Security: Understanding and Mitigating Insider Threat

ARNAV SUBUDHI **2105529**
BIKRAMADITYA MUNSHI **2105538**
JATIN NAYAK **21052669**

Abstract: Strong network security is crucial in today's interconnected world, but human factors can weaken it. User errors and lack of awareness can be exploited. This paper explores how human actions impact network security. It covers human error, security awareness training, and the importance of human judgment in detecting threats. Insider threats, malicious actions by authorized users, are a growing challenge. The paper proposes a framework to identify and mitigate insider threats.

Individual contribution to project report preparation: Arnav Subudhi and Bikramaditya Mushi collaborated on the initial sections of the group project report. Arnav Subudhi primarily contributed to Chapter 1 - "Introduction", providing a comprehensive overview of the project's background, objectives, and scope. Bikramaditya Mushi focused on Chapter 2 - "Basic Concepts", where he elucidated fundamental principles and theoretical frameworks relevant to the project.

In Chapter 3 - "Problem Statements and Requirement Specification", both Arnav Subudhi and Bikramaditya Mushi played significant roles in identifying and articulating the project's challenges, as well as outlining specific requirements for addressing them. Their combined efforts ensured clarity and coherence in presenting the project's problem statements and the corresponding specifications.

Furthermore, in Chapter 4 - "Implementation", Arnav Subudhi and Bikramaditya Mushi collaborated to detail the practical implementation aspects of the project. They outlined the methodologies, technologies, and strategies employed in executing the project, providing a comprehensive understanding of its operationalization.

Jatin Nayak took charge of Chapter 5 - "Standards Adopted", where he meticulously researched and documented the standards relevant to the project. He ensured that all necessary standards were adequately addressed and explained, providing a solid foundation for the project's implementation.

In Chapter 6 - "Conclusion and Future Scope", Jatin Nayak synthesized the project's findings and discussions, providing a well-rounded conclusion. He also explored potential future directions and areas for further research, offering valuable insights for stakeholders to consider moving forward.

Individual contribution for project presentation and demonstration: Arnav Subudhi and Bikramaditya Mushi have both worked on creating the entire project presentation and all parts of the proposed model. Our roles encompassed conceptualization, design, and development of the project components showcased in the presentation. In the presentation, We effectively demonstrated the proposed model's various aspects, including its architecture, functionalities, and potential applications. We meticulously crafted slides and visuals to elucidate key concepts and highlight the project's significance and innovation.

Full Signature of Supervisor:
…….

Full signature of the student:
……..

Introduction

ORIGINALITY REPORT

8%	4%	4%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	docplayer.net Internet Source	1%
2	Puthiyavan Udayakumar. "Design and Deploy a Secure Azure Environment", Springer Science and Business Media LLC, 2023 Publication	1%
3	Submitted to American Public University System Student Paper	1%
4	Submitted to Manipal University Student Paper	1%
5	fastercapital.com Internet Source	1%
6	sciendo.com Internet Source	<1%
7	Submitted to Indiana University Student Paper	<1%
8	Submitted to University of Central Florida Student Paper	<1%