**MASTER OF SCIENCE DISSERTATION**

|  |  |  |
| --- | --- | --- |
|  | Dissertation Title: | An Integrated Approach to Detecting and Mitigating Internal Misuse |
|  | Surname: | Jadhav |
|  | First Name: | Sagar |
|  | Student Number: | 19276146 |
|  | Supervisor: | Muhammad Hilmi Kamarudin |
|  | Dissertation Module: | TECH7009 |
|  | Course Title: | MSc Dissertation in Computing Subjects |
|  | Date Submitted: | 27/09/2024 |

**Statement of Originality**

Except for those parts in which it is explicitly stated to the contrary, this project is my own work. It has not been submitted for any degree at this or any other academic or professional institution.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature of Author | Sagar Ramesh Jadhav | Date | 27/09/2024 |

Regulations Governing the Deposit and Use of Master of Science Dissertations in the School of Engineering, Computing and Mathematics, Oxford Brookes

University.

1. A copy of dissertation final reports submitted in fulfilment of Master of Science course requirements shall normally be kept by the School.
2. The author shall sign a declaration agreeing that, at the supervisor’s discretion, the dissertation will be submitted in electronic form to any plagiarism checking service or tool.
3. The author shall sign a declaration agreeing that the dissertation be available for reading and copying in any form at the discretion of either the dissertation supervisor or in their absence the Programme Lead of Postgraduate Programmes, in accordance with 5 below.
4. The project supervisor shall safeguard the interests of the author by requiring persons who consult the dissertation to sign a declaration acknowledging the author's copyright.
5. Permission for anyone other than the author to reproduce in any form or photocopy any part of the dissertation must be obtained from the project supervisor, or in their absence the Programme Lead of Postgraduate Programmes, who will give his/her permission for such reproduction only to the extent to which he/she considers to be fair and reasonable.

I agree that this dissertation may be submitted in electronic form to any plagiarism checking service or tool at the discretion of my project supervisor in accordance with regulation 2 above.

I agree that this dissertation may be available for reading and photocopying at the discretion of my project supervisor or the Programme Lead of Postgraduate Programmes in accordance with regulation 5 above.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature of Author | Sagar Ramesh Jadhav | Date | 27/09/2024 |

An Integrated Approach to Detecting and Mitigating Internal Misuse

**Contents**

[Abstract 5](#_Toc178342957)

[Glossary 5](#_Toc178342958)

[1. Introduction 6](#_Toc178342959)

[1.1 Background 6](#_Toc178342960)

[1.2 Aim 6](#_Toc178342961)

[1.3 Objectives 6](#_Toc178342962)

[1.4.1 Scope 7](#_Toc178342963)

[1.4.2 Audience 7](#_Toc178342964)

[2. Literature Review 7](#_Toc178342965)

[2.1 Internal Fraud 7](#_Toc178342966)

[2.2 The Sources of Internal Security Threats 8](#_Toc178342967)

[2.2.1 Human Error and Negligence 8](#_Toc178342968)

[2.2.2 Deliberate Insider Attacks 9](#_Toc178342969)

[2.2.3 Organizational and Cultural Factors 9](#_Toc178342970)

[2.2.4 Insider Threat Detection Approaches 10](#_Toc178342971)

[2.2.5 Recent Developments in Intrusion Detection System 10](#_Toc178342972)

[2.3 Types of an Insider Threat 11](#_Toc178342973)

[2.3.1 Espionage 11](#_Toc178342974)

[2.3.2 Terrorism 11](#_Toc178342975)

[2.3.3 Unauthorized Disclosure of Information 12](#_Toc178342976)

[2.3.4 Corruption and Transnational Organized Crime 12](#_Toc178342977)

[2.3.5 Sabotage 12](#_Toc178342978)

[2.3.6 Workplace Violence 13](#_Toc178342979)

[2.3.7 Loss or Degradation of Resources or Capabilities 13](#_Toc178342980)

[2.3.8 Routine Drills 13](#_Toc178342981)

[2.4 Existing Security Measures and Their Limitations 14](#_Toc178342982)

[2.5 Identifying Attack Vectors 15](#_Toc178342983)

[2.6 User Behaviour Analysis 15](#_Toc178342984)

[2.7 Misuse Strategic Solutions 16](#_Toc178342985)

[2.8 Integrated Solutions Increase the Level of Protection 16](#_Toc178342986)

[2.9 Integrated Misuse Intrusion Architecture 17](#_Toc178342987)

[3. Methodology 17](#_Toc178342988)

[3.1 The Realities of Internal Fraud 17](#_Toc178342989)

[3.1.1 Statistical Overview of Internal Fraud 17](#_Toc178342990)

[3.1.2 Case Studies and Examples 17](#_Toc178342991)

[3.1.3 Economic Impact of Internal Fraud 18](#_Toc178342992)

[3.2 Approach 18](#_Toc178342993)

[3.3 Technology 18](#_Toc178342994)

[3.4 Version Management 19](#_Toc178342995)

[3.5 Test and Evaluation 19](#_Toc178342996)

[3.6 Implementation & Discussion 19](#_Toc178342997)

[3.6.1 Dataset Overview 20](#_Toc178342998)

[3.6.2 Supervised Learning Models for Misuse Detection 20](#_Toc178342999)

[3.6.3 Unsupervised Learning for Anomaly Detection 20](#_Toc178343000)

[3.6.4 Feature Importance Analysis 21](#_Toc178343001)

[3.6.5 User Activity and Service Analysis 21](#_Toc178343002)

[3.6.6 Network Traffic Analysis 21](#_Toc178343003)

[3.6.7 Comparison of Models 21](#_Toc178343004)

[3.6.8 IP Address Description and Network Setup 21](#_Toc178343005)

[3.6 Risk Management 22](#_Toc178343006)

[3.7 Professional, Legal, Ethical & Sustainability Issues 22](#_Toc178343007)

[3.7.1 Professional Standards 22](#_Toc178343008)

[3.7.2 Legal Compliance 22](#_Toc178343009)

[3.7.3 Ethical Considerations 23](#_Toc178343010)

[3.7.4 Sustainability 23](#_Toc178343011)

[3.7.5 Social Responsibility 24](#_Toc178343012)

[4. Project Plan 24](#_Toc178343013)

[4.1 Activities 24](#_Toc178343014)

[4.2 Schedule 24](#_Toc178343015)

[4.3 Data Management Plan 25](#_Toc178343016)

[4.4 Deliverables 25](#_Toc178343017)

[5. Discussion and Evaluation 26](#_Toc178343018)

[6. Recommendations 26](#_Toc178343019)

[7. Conclusion 26](#_Toc178343020)

[8. Bibliography/References 27](#_Toc178343021)

# **Abstract**

In the modern, digitally-driven business landscape, internal misuse and fraud by employees pose significant security threats. Unlike external cyber-attacks, insider threats leverage legitimate access, making them more difficult to detect and prevent. This research addresses the critical need for robust solutions by proposing an integrated misuse intrusion detection architecture. Leveraging advanced technologies such as user behaviour analytics, machine learning algorithms (Random Forest, Decision Trees, Isolation Forest), and centralized security systems, the architecture aims to prevent, detect, monitor, and recover from insider threats. By analysing anomalies in user behaviour, network traffic, and system activities, the solution enhances organizational capacity to identify and mitigate internal misuse. The study follows an agile development methodology to ensure flexibility and responsiveness to evolving threats. The integration of managerial, operational, and technical controls within the proposed system ensures a comprehensive defense against internal threats, addressing the limitations of traditional external-focused security measures. This multifaceted approach incorporates continuous monitoring, statistical analysis, and real-time evaluation, allowing for early detection and prevention of insider fraud. Ultimately, this research provides a scalable, adaptable framework that strengthens organizational security, protecting data, financial assets, and reputation from the damaging effects of internal fraud, while advocating for a culture of ethical behaviour within organizations.

# **Glossary**

1. AI - Artificial Intelligence
2. API - Application Programming Interface
3. CCPA - California Consumer Privacy Act
4. CI/CD - Continuous Integration/Continuous Deployment
5. DEMIDS - Database Misuse Detection System
6. DIDAFIT - Database Intrusion Detection and Forensic Information Tool
7. GDPR - General Data Protection Regulation
8. HIPAA - Health Insurance Portability and Accountability Act
9. IDS - Intrusion Detection System
10. IP - Internet Protocol
11. IT - Information Technology
12. KDD - Knowledge Discovery in Databases (refers to KDD Cup 99 dataset)
13. ML - Machine Learning
14. NDA - Non-Disclosure Agreement
15. NIST - National Institute of Standards and Technology
16. PT - Packet Tracer
17. RNN - Recurrent Neural Networks
18. SIEM - Security Information and Event Management
19. TCP - Transmission Control Protocol
20. UDP - User Datagram Protocol

# **1. Introduction**

In today's digital-first business environment, the threat of computer crimes looms large, posing increasingly significant challenges. While popular narratives tend to highlight external hackers as the main perpetrators of cyber-attacks, a closer examination of the data reveals a more complex and troubling reality. A substantial number of computer intrusions are carried out by insiders’ employees who exploit their trusted positions. With legitimate access and intimate knowledge of an organization's systems and processes, these insiders can easily bypass traditional security measures. The concept of "insider threat" encompasses a broad spectrum of malicious activities, including data theft, financial fraud, sabotage, and intellectual property leaks. Whether motivated by personal gain, revenge, coercion, or even unintentional negligence, the consequences for the organization's financial health, reputation, and operational integrity are invariably severe. These insiders often know how to circumvent security mechanisms to avoid detection, making the challenge of protecting against such threats formidable. This dissertation addresses the pressing issue of insider threats by proposing an integrated misuse intrusion architecture, aiming to enhance information system security. This architecture is designed to cover the full spectrum of security measures: prevention, detection, monitoring, and recovery from incidents of employee fraud. By focusing on internal threats, my research aims to address a crucial gap in current security practices, which often prioritize external threats over internal vulnerabilities.

## **Background**

When trusted workers or insiders abuse their access to data, systems, or networks often for their own benefit or to harm the company internal misuse is a developing concern in organisations. Although there is a lot of focus on external cybersecurity threats, inside threats are frequently more damaging because they take use of lawful access, which makes identification and prevention more difficult.

## **Aim**

The aim of this research is to design a system that would focus on internal misuse identification and prevention within networked organizations. Moreover, the system will perform the deep analysis of users’ behaviour, the anomalies detection, and feature importance by applying natural machine learning algorithms like Random Forests, Decision Trees, and Isolation Forests.

## **1.3 Objectives**

* To develop and implement machine learning models, including Random Forests, Decision Trees, and Isolation Forests, to detect anomalies and suspicious activities within organizational networks.
* To analyse user behaviour and network traffic patterns to identify potential internal misuse by insiders, such as employees or trusted actors.
* To assess the performance of proposed models by comparing accuracy, feature importance, and effectiveness in preventing malicious actions.
  1. **Product Overview**

### **1.4.1 Scope**

The concern of this research is to design an integrated system that can be used for internal misuse detection within the organizational networks. The study will adopt Random Forests, Decision Trees, and Isolation Forests to analyse the user activity, network traffic, and system activities for identifying any malicious activity from insider staff. The project will mainly focus on detecting abnormality, evaluating performance of the models and evaluating importance of features for better security measures (Taherdoost, 2021). This research will focus on insider threats including employees with malicious intents for using their privileged access and offer implementable solutions that will be scalable for organizations across different industries and network architectures.

### **1.4.2 Audience**

The audience that is being targeted for this research will include cybersecurity experts, IT security directors and managers, data analysts, and organizational executives and administrators who are instructed to protect organizational sensitive information and networks. They have been facing a growing threat of internal misuse, most of which are initiated by insiders like the employees or contractors (Al-Mhiqani et al., 2021). For cybersecurity professionals, this research offers an understanding of how machine learning algorithms work when detecting threats in real time. For data scientists, this research provides insights regarding analysis of users’ behaviour and modelling to find anomalies. Decision makers and IT managers will consider the practical implications of the system and analyse how it would help to improve security measures inside an organization, compliance with the strict requirements of specific industry sectors, and combat the threats associated with the insider menace (Ahsan et al., 2022). This study is also useful for theorists and scientists who are working in the cybersecurity, machine learning, and organizational security field as this study provides them concrete literature on which they can build further studies to avoid internal malpractice and improving the efficiency of detection mechanisms.

# **2. Literature Review**

## **2.1 Internal Fraud**

Internal fraud, also known as insider fraud, refers to a broad spectrum of malicious activities carried out by employees or individuals who have authorized access to an organization’s systems and resources. These deceptive practices can take various forms, such as theft of sensitive data, embezzlement of funds, unauthorized system access, or deliberate sabotage of hardware and data. The consequences of internal fraud are far-reaching, resulting in severe financial losses, tarnishing the organization’s reputation, and eroding the trust within the workplace (Zaid et al., 2023; Zimon et al., 2022). Given that insiders have legitimate access to sensitive information, detecting their misuse is particularly challenging. Traditional security measures, such as firewalls and access controls, are often insufficient to address these sophisticated threats (Liang & Kim, 2022). As a result, organizations must implement layered defense mechanisms that combine conventional security tools with advanced analytical models, such as machine learning and behavioural analytics, to effectively identify and mitigate insider threats (Moneva & Leukfeldt, 2023; Akinbowale et al., 2023). The growing prevalence of internal misuse underscores its position as a significant concern for organizations, as it leverages the trust and access granted to insiders’ employees who have legitimate rights to handle organizational assets. Identifying these threats is especially difficult because traditional security systems primarily focus on external attacks. The use of sophisticated analytical tools and multi-layered security strategies is essential in addressing these threats, ensuring that any suspicious patterns in employee behaviour are flagged before they lead to significant damage. Integrating such complex models with existing security frameworks allows organizations to better detect anomalies in real-time, enhancing their capacity to prevent insider fraud effectively (Khan et al., 2024; Schultz, 2002). The layered approach is crucial because insider threats exploit loopholes that conventional defenses, designed primarily for external threats, cannot always detect. By utilizing machine learning, behaviour analytics, and anomaly detection tools, organizations can continuously monitor patterns of access, data manipulation, and user behaviour to flag any deviations that may indicate fraudulent activity. This proactive strategy not only helps in identifying potential threats but also mitigates the significant risks posed by trusted insiders.

## **2.2 The Sources of Internal Security Threats**

In the realm of information security, understanding the sources of internal threats is paramount. Internal security threats are primarily driven by human factors, whether through inadvertent errors or deliberate malicious actions. Organizational culture also plays a significant role in influencing employee behaviour and mitigating or exacerbating these threats. This chapter delves into the complexities of human error, deliberate insider attacks, and the impact of organizational culture on internal security.

### **2.2.1 Human Error and Negligence**

Human error and negligence are pervasive and often underestimated contributors to internal security threats. Employees, irrespective of their intentions, can inadvertently cause security breaches through several common actions:

- Failure to Follow Protocols: Even with established security protocols in place, employees may neglect to adhere to them due to a lack of understanding, oversight, or perceived inconvenience. For instance, an employee might disable security software to speed up their computer's performance, inadvertently leaving the system vulnerable to attacks.

- Leaving Systems Unattended: In many cases, employees might leave their workstations unattended without locking their screens, allowing unauthorized individuals to access sensitive information. This is particularly risky in environments where multiple individuals share access to computers.

- Mishandling Sensitive Information: Employees might inadvertently send sensitive information to the wrong recipients, store passwords in easily accessible locations, or use unsecured devices for work purposes. Such actions can lead to data breaches and unauthorized access.

The root causes of these behaviours often stem from a lack of awareness and inadequate training. Many employees are not fully aware of the potential security risks associated with their actions or the importance of following security protocols. Training programs that emphasize the significance of security measures and demonstrate their impact can help mitigate these risks. For example, regular security awareness training, phishing simulations, and clear communication of security policies can foster a more security-conscious workforce (Leach, 2003).

### **2.2.2 Deliberate Insider Attacks**

Deliberate insider attacks are among the most challenging security threats to detect and prevent. These attacks involve malicious actions by employees who exploit their access privileges for personal gain or to harm the organization. Common motivations for such attacks include financial gain, revenge, and espionage. Key characteristics of deliberate insider attacks include:

- Data Theft: Insiders may steal sensitive data, such as customer information, intellectual property, or financial records, to sell to competitors or use for personal gain. For example, an employee with access to confidential customer data might download and sell this information on the dark web.

- System Sabotage: Some insiders may deliberately sabotage systems by introducing malware, deleting critical files, or disrupting operations. This could be motivated by a desire to cause harm to the organization, such as in cases of disgruntled employees seeking revenge.

- Unauthorized Access and Information Leakage: Insiders may misuse their access privileges to gain unauthorized access to systems and information. This could involve bypassing security controls, exploiting vulnerabilities, or sharing confidential information with unauthorized parties.

Detecting and preventing these attacks is challenging due to the insider's familiarity with the organization's systems and processes. Traditional security measures, such as firewalls and intrusion detection systems, are often insufficient to identify insider threats. Advanced techniques, such as user behaviour analytics (UBA), machine learning, and anomaly detection, are increasingly being employed to identify unusual patterns of behaviour that may indicate malicious intent (Casey, 2003).

### **2.2.3 Organizational and Cultural Factors**

Organizational culture significantly influences the likelihood of internal security threats. A positive organizational culture can act as a deterrent to insider threats, while a toxic culture can create an environment conducive to fraud and misuse. Several cultural factors play a role in shaping employee behaviour:

- Mistrust and Resentment: Organizations characterized by mistrust, poor communication, and lack of employee engagement are more likely to experience insider threats. Employees who feel undervalued, unappreciated, or resentful may be more inclined to commit fraud or sabotage systems. For example, an employee who perceives unfair treatment or lack of career progression might be motivated to harm the organization as a form of retribution.

- Respect, Loyalty, and Responsibility: Conversely, organizations that foster a culture of respect, loyalty, and responsibility can significantly reduce the likelihood of insider attacks. When employees feel valued and integral to the organization's success, they are less likely to engage in malicious activities. Initiatives such as employee recognition programs, transparent communication, and opportunities for professional development can strengthen organizational loyalty and commitment (Sekar et al., 1999).

- Ethical Leadership and Role Models: Ethical leadership and the presence of positive role models within the organization are crucial in promoting a culture of integrity and security. Leaders who demonstrate ethical behaviour, transparency, and accountability set the tone for the entire organization, encouraging employees to follow suit.

- Clear Policies and Consequences: Having clear, well-communicated policies regarding acceptable behaviour and the consequences of security breaches is essential. Employees should be aware of what constitutes a security violation and the potential repercussions of such actions. Regularly reviewing and updating these policies ensures they remain relevant and effective.

### **2.2.4 Insider Threat Detection** **Approaches**

Several studies have highlighted the limitations of traditional security solutions when it comes to addressing insider threats, most current security frameworks predominantly concentrate on external threats, leaving internal misuse largely unprotected (Jang-Jaccard & Nepal, S. 2014). The researchers advocate for a shift in focus toward behavioural analysis, utilizing machine learning models capable of assessing the specific actions and behaviours of users. This change in approach is necessary to effectively counter the growing threat of insider attacks. This perspective is reinforced by highlighting the critical role anomaly detection methods play in uncovering deviations from normal user behaviour (Kim et al., 2019). These deviations often signal potential insider misuse, making anomaly detection a vital tool in addressing this issue. As insider threats are inherently unpredictable and difficult to predefine, anomaly detection provides a way to spot unusual behaviours that could otherwise go unnoticed. In recent years, the application of machine learning techniques has garnered significant attention due to their proven effectiveness in predicting outcomes based on historical data and adapting to ever-evolving threat landscapes. Ensemble techniques such as Random Forest and Gradient Boosting are more effective in identifying insider threats than traditional methods (Khan, Chaudhari & Chandra, 2024). One of the key improvements brought by these machine learning techniques is the substantial reduction in false positive rates, which is a common drawback in conventional security approaches. This finding suggests that the integration of more sophisticated machine learning algorithms into existing security systems can greatly enhance their ability to detect insider threats effectively.

### **2.2.5 Recent Developments in Intrusion Detection System**

To tackle the specific challenges posed by internal threats, recent advances in intrusion detection systems (IDS) have increasingly focused on more sophisticated methods for identifying and mitigating insider fraud. These approaches rely heavily on techniques such as anomaly detection, behaviour analysis, and machine learning, which have become central to modern insider threat detection strategies.

Anomaly detection works by continuously monitoring user activities and identifying deviations from established behavioural patterns, flagging these anomalies as potential indicators of fraudulent behaviour. Behaviours analysis further refines this by considering the context and frequency of user actions, allowing for the detection of malicious activities that may not be immediately obvious. Machine learning amplifies the effectiveness of these methods by enabling continuous learning and adaptation, ensuring that the system evolves with emerging threats, including previously unknown patterns of insider fraud.

Examples of cutting-edge systems leveraging these advancements include the Database Misuse Detection System (DEMIDS) and the Database Intrusion Detection And Forensic Information Tool (DIDAFIT). DEMIDS focuses on profiling user access behaviours, identifying anomalies in database usage that may indicate misuse, while DIDAFIT is designed to monitor SQL queries for suspicious activity (Chung et al., 1999; Low et al., 2002). These systems represent significant progress in the ability to detect and mitigate insider threats, demonstrating the power of machine learning and behaviour-based detection strategies in this critical area of cybersecurity.

## **2.3 Types of an Insider Threat**

### **2.3.1 Espionage**

Insider threats related to espionage pose a significant risk to organizations by involving the theft of sensitive information by employees who may be collaborating with competitors, foreign governments, or criminal entities (Hegazy et al., 2022). Detecting these threats requires vigilance for unusual behavioural patterns, such as excessive interest in confidential data, unauthorized access attempts, irregular financial activities, or sudden changes in behaviour (Moritz et al., 2023). Technical indicators might include unauthorized data transfers, unexplained communication channels, or repeated login failures (Haryono et al., 2023). Anomalies in background checks, such as inconsistent work histories or affiliations with suspicious groups, may also signal potential threats (Rovira et al, 2023). Once identified, addressing espionage threats involves monitoring user activity, network traffic, and implementing an insider threat program that integrates both technological and human intelligence (Silowash et al., 2016). This program should feature a specialized team dedicated to analysing technical and behavioural data, working closely with HR, legal, and security departments (Villarreal-Vasquez et al., 2023). Handling these threats discreetly is vital to avoid alerting the suspected insider. Investigations should be conducted under legal guidance, using methods like access log reviews and discreet interviews with colleagues, adhering to ethical standards (Blank & Osofsky, 2020). Fostering an environment where employees can report suspicious activities without fear is equally crucial. Organizations should employ a multi-layered approach, combining technological measures such as data encryption and access controls with procedural and cultural strategies, including regular security audits, staff training on espionage threats, and a robust incident response plan (Chimbutane & Gonçalves, 2023).

### **2.3.2 Terrorism**

To effectively manage insider threats associated with terrorism, organizations must adopt a comprehensive approach that includes early detection, continuous monitoring, and robust mitigation strategies (Villarreal-Vasquez, Modelo-Howard, Dube, & Bhargava, 2023). This involves identifying signs of radicalization or extremist views among employees, such as sudden behavioural changes, unexplained absences, dissemination of extreme ideologies, or unauthorized access to sensitive data. Regular background checks are essential, especially for those in sensitive positions (Zeoli, McCourt, & Paruk, 2022). Systems should be implemented to detect abnormal activity and access patterns, and a culture that encourages reporting suspicious activities without fear of retaliation must be maintained. Continuous monitoring of both offline and online behaviours using advanced techniques like User and Entity Behaviours Analytics (UEBA) is also critical. Mitigating these threats requires proactive measures, including stringent hiring practices and regular security training, as well as reactive measures like a well-defined incident response strategy. By integrating these tactics, organizations can create a robust defense against internal terrorist threats, ensuring the safety of both personnel and assets.

### **2.3.3 Unauthorized Disclosure of Information**

Preventing unauthorized disclosure of information in the context of insider threats involves several key actions. Organizations should deploy robust monitoring systems to detect abnormal activity or access patterns that may indicate potential security breaches (Kaur, Kumar, & Kaushik, 2023). This includes monitoring access logs, data transfers, and the use of unauthorized communication channels. Regular audits and anomaly detection tools can help identify unusual behaviour indicative of unauthorized disclosures. Once suspicious activity is detected, it should be promptly investigated to determine the source and scope of the breach. Mitigation measures include a combination of technical controls, such as enhanced data encryption and access management (Ramachandra et al., 2022), and procedural controls, like targeted employee training (Brunello et al., 2023) and strict information handling policies (Tolba et al., 2018). Cultivating a culture of vigilance and encouraging staff to report suspicious activities are vital steps in reducing the risk of insider threats (Mishler & Chen, 2023).

### **2.3.4 Corruption and Transnational Organized Crime**

Addressing insider threats related to corruption, including involvement in transnational organized crime, requires a comprehensive approach. Organizations should conduct thorough background checks and continuous monitoring for individuals in sensitive roles to identify potential red flags associated with corruption or criminal connections (Rovira, 2023). Regular financial audits and monitoring can help detect suspicious transactions or discrepancies. Strong reporting systems that allow anonymous reporting of suspicious activities are crucial for early detection. Training programs should emphasize ethical behaviour and highlight warning signs of corruption (Pan et al., 2023). Additionally, investigation procedures should be established to thoroughly examine allegations and verify employee integrity (Ghurairi & Al-Hamdani, 2019). Collaboration with law enforcement and external entities can be beneficial in addressing aspects of transnational organized crime. Strict compliance standards and penalties for unethical conduct can further deter potential insiders from engaging in corrupt activities, thus safeguarding organizational integrity (Ivanov, 2021).

### **2.3.5 Sabotage**

Dealing with sabotage as an insider threat requires a comprehensive approach. Organizations must establish effective monitoring systems to detect any irregularities in employee activities or access patterns, such as unauthorized changes or disruptions in data (Gómez-Cabrera & Escamilla-Ambrosio, 2022). Keeping detailed logs of system access, modifications to critical files, and communications is crucial, as these records can reveal suspicious actions and serve as early indicators of possible sabotage (Zhan et al., 2016; Cui et al., 2023). Preventing sabotage also involves conducting regular security training and defining clear protocols for reporting suspicious activities (Brady & M'manga, 2022). Developing a thorough response plan to address and mitigate sabotage-related incidents is essential (Li et al., 2022). A strong security culture, maintained through regular audits and open communication about the importance of security practices, further reduces the risk of sabotage by ensuring that employees understand the consequences of malicious behaviour (Olaniyi et al., 2023).

### **2.3.6 Workplace Violence**

Addressing workplace violence as an insider threat requires a multifaceted approach. Organizations should establish robust reporting mechanisms that allow employees to discreetly report concerning behaviours. Utilizing data analytics and anomaly detection techniques can help identify patterns that suggest potential threats (Aldayri & Albattah, 2022). Regular risk and threat assessments are critical to identifying new threats and vulnerabilities (Yin et al., 2023). Clear guidelines and training programs should be in place to educate employees on recognizing and responding to signs of workplace violence (Howard et al., 2021). Creating comprehensive response plans, conducting frequent drills, and ensuring effective collaboration between security, HR, and legal departments are necessary to minimize risks (Asi et al., 2022). Constant monitoring, timely intervention, and providing support services are essential to maintaining a safe workplace and proactively addressing insider threats (Hoffmann et al., 2014; Boerner et al., 2023).

### **2.3.7 Loss or Degradation of Resources or Capabilities**

Managing insider threats related to the intentional or unintentional loss or degradation of departmental resources or capabilities requires an organized strategy (Rauf, Mohsen, & Wei, 2023). Organizations should establish reliable monitoring systems to detect anomalies, such as unauthorized access or suspected data manipulation (Hahn et al., 2022). Regularly reviewing and auditing resource utilization, system performance metrics, and access logs can help identify any unusual patterns (Stepanova et al., 2022; Li et al., 2021). Clearly defining reporting and investigation procedures ensures that both intentional and unintentional risks are adequately addressed (Ghurairi & Al-Hamdani, 2019). Employee training on security awareness and best practices is essential to prevent inadvertent breaches and foster a vigilant work environment (Quality - Access to Success, 2023). Developing and maintaining incident response plans, which outline actions for containment, remediation, and recovery, can be refined by learning from past incidents (Teichmann & Boticiu, 2023). By combining proactive monitoring, effective incident reporting, and comprehensive training, organizations can enhance their ability to manage and mitigate insider threat risks.

### **2.3.8 Routine Drills**

Implementing regular drills and exercises can significantly strengthen an organization's security posture concerning insider threats, particularly those involving terrorism and espionage (Rauf, Mohsen, & Wei, 2023). Simulated espionage exercises, where employees with access to sensitive information act as potential attackers, help in identifying vulnerabilities and evaluating defenses. Insider threat detection drills leverage anomaly detection tools to enhance monitoring systems and identify suspicious behaviour (Deng & Li, 2022). Red Team versus Blue Team exercises test the organization's ability to detect and neutralize internal threats in a controlled environment (Puschner et al., 2023). Background verification drills regularly reassess the security clearances and histories of employees (Mahajan et al., 2022). Additionally, legal and ethical compliance simulations ensure investigations adhere to privacy and organizational policies, while communication and response protocol drills enhance internal coordination. Encouraging proactive reporting through employee reporting drills and practicing containment and recovery techniques via incident response tabletop exercises are essential for cultivating a strong security culture and preparedness (Ban et al., 2023).

## **2.4 Existing Security Measures and Their Limitations**

Traditionally, organizations have relied on foundational security measures like firewalls, antivirus software, and access control mechanisms to protect their information systems. These security tools are primarily designed to counteract external threats, such as cyberattacks originating from outside the organization’s network. However, internal threats pose a unique and more intricate challenge that these conventional security mechanisms often struggle to address effectively. For instance, while firewalls serve as a strong defense against unauthorized external access, they are not as effective at dealing with internal threats, where malicious activity comes from within the organization itself. Similarly, antivirus software is effective in detecting and removing known malware but may fall short when dealing with custom malware specifically developed by an insider with knowledge of the system. Access controls, while successful at limiting entry to specific parts of a system, do not monitor the behaviour of authorized users once they have gained access. As a result, insiders who already have legitimate access to critical systems can exploit these privileges without triggering any alarms, posing significant security risks (Schultz et al., 2002). Previous research aimed at identifying and preventing internal misuse in organizational networks has mainly focused on security tools such as firewalls, intrusion detection systems (IDS), and authentication methods. While these approaches are adept at detecting external threats, they tend to overlook the risks posed by insiders who already have legitimate access to the system. Rule-based systems and signature-based IDS, for example, are effective at recognizing known malicious behaviours but often fail to detect more sophisticated insider threats, especially when these threats involve subtle deviations from normal user activities (Ambalavanan & Bala, 2020). To address these limitations, advanced behavioural analysis techniques have been developed. These techniques monitor and analyse user activities to identify abnormal behaviours that may indicate illegitimate use of organizational resources. For example, threshold-based systems, which set predetermined limits for normal activity, are often prone to generating false positives, or they may fail to identify genuine threats when the deviations from normal behaviour are small but significant (Mehmood et al., 2023). This challenge has led to the exploration of machine learning approaches that offer more intelligent, adaptive algorithms capable of detecting insider threats with greater precision. Recent developments in machine learning, such as Random Forest models, have enhanced the ability to distinguish between normal and anomalous behaviours. These models utilize data mining techniques like Decision Trees and Isolation Forests to analyse multiple aspects of user activity, such as login times, data access patterns, and network usage, enabling organizations to better detect and prevent insider threats (Sakthivelu & Kumar, 2023). Despite these advancements, there remains a need for a more integrated solution that combines these various models into a cohesive, multifaceted security system capable of addressing the full spectrum of insider threats efficiently and effectively.

## **2.5 Identifying Attack Vectors**

Identifying attack vectors within an organization involves understanding the various ways insiders can exploit their access to harm the company. One common method is the misuse of documents and data. Insiders with authorized access may alter, steal, or delete sensitive information. Keeping track of document interactions—such as when and how long they are accessed, and whether they are copied to external devices—can help detect suspicious behaviour (Casey, 2003). Another threat comes from system and network exploits, where insiders gain unauthorized access to critical systems, disable security measures, install malicious software, or create backdoors for future use. Protecting these assets requires strong access controls and constant monitoring of network activities (Thompson et al., 2004). Additionally, certain behavioural changes, like unusual work habits, accessing systems at odd times, or deviating from normal patterns, can indicate potential fraud. User behaviour analytics (UBA), which uses machine learning to spot these anomalies, can help security teams identify and mitigate insider threats (Schultz, 2002).

## **2.6 User Behaviour Analysis**

The significance of human factors in information security is a vital area of research, as it explores the psychological and social elements that contribute to insider fraud. The psychological profile of employees, the organizational culture they operate within, and their behavioural patterns all influence the probability of engaging in fraudulent activities. According to multiple studies, employees who feel appreciated and motivated are far less likely to commit fraud. A positive work environment, where employees feel respected and recognized for their contributions, acts as a deterrent to internal fraud. This approach is often referred to as creating a "human firewall," highlighting the notion that a content and motivated workforce is one of the strongest barriers against fraudulent behaviour (Sekar et al., 1999). In addition, organizational culture plays a critical role in preventing fraud. A culture that fosters ethical behaviour, promotes transparency, and holds individuals accountable can effectively dissuade employees from engaging in dishonest actions. On the other hand, a toxic organizational environment, marked by high stress levels, ineffective management, and ambiguous or absent ethical standards, tends to increase the risk of insider fraud. Thus, cultivating a healthy organizational culture is just as crucial as deploying technical security systems. The analysis of user behaviour is another key component in identifying insider threats. Although deriving solid conclusions from behavioural analytics can be challenging, combining traditional data sources with behavioural insights has proven to be effective in estimating typical user behaviour. These estimates, when compared against real-time analytics, can significantly enhance the detection of unusual activity, thereby improving the signal-to-noise ratio. Emphasizing the importance of monitoring users' behaviour within systems, identifying patterns such as login times, access frequency, and data manipulation activities (Khraisat et al. 2019). These metrics can establish baseline behaviours such as mean values and standard deviations that, when deviated from, serve as indicators of potential insider threats. Furthermore, recent research has expanded the use of deep learning techniques in user behaviour analysis (Nepal and Joshi, 2022). They found that Recurrent Neural Networks (RNNs) are particularly effective at capturing the temporal features of user activities, offering significant improvements over previous methods. This innovative approach suggests the potential for even more advanced techniques in the future, particularly for real-time detection of insider threats. With further refinement and application, these evolving methods are expected to enhance the analysis of user behaviour, making insider threat detection more accurate and timelier.

## **2.7 Misuse Strategic Solutions**

Prevention strategies aim to minimize the risk of internal fraud by combining strong security measures with fostering a positive organizational culture. These measures typically include perimeter protections like firewalls, identity card access systems, thorough recruitment screening, and regular security awareness training (Furnell, 2004). On the detection side, mechanisms are put in place to identify fraudulent activity in real time, utilizing tools like intrusion detection systems (IDS), real-time monitoring, and user behaviour analysis. Systems such as DEMIDS and DIDAFIT offer valuable insights by tracking access patterns and spotting irregularities (Chung et al., 1999). Monitoring, on the other hand, focuses on the continuous observation of user activity to catch suspicious actions early. Techniques such as anomaly detection, behaviour analysis, and even using honeypots to attract potential malicious insiders are effective methods (Low et al., 2002). In the event of fraud, recovery procedures play a critical role in minimizing damage and resuming operations. These include conducting forensic investigations to assess the breach, taking corrective actions, and enhancing security measures to prevent future incidents (Sekar et al., 1999).

## **2.8 Integrated Solutions Increase the Level of Protection**

One of the latest trends has been to develop a unified system incorporating the use of multiple detection methodologies. The integration of complex systems that combine machine learning, user behavioural patterns, and security measures is necessary (Asmar and Tuqan, 2024). Therefore, integrated solutions can help organizations have a stronger protection against insiders threatening and enable early identification of the malicious actions. A systematic review of integrated cybersecurity approaches suggests that both risk assessment and anomaly detection can function as equally important and complementary tools (Erbas, Khalil and Tsiopoulos, 2024). According to their research, integrated systems can improve the detection of threats in organisations while at the same time preventing disruptions of operation. Accordingly, it highlights the significance of the security culture as the main reason why insiders pose threats: Technology and users are always insufficient for detecting insider threats. One of the key elements of the study is that in the issue of an insider threat, it is necessary to focus on organizational culture and security practices among users. In conclusion, while traditional security measures are crucial, they are not sufficient to address the complex nature of internal fraud. A multi-faceted approach that includes advanced IDS technologies and a strong emphasis on human factors and organizational culture is essential for effectively mitigating the risk of insider threats. The integration of these elements forms the basis for the comprehensive security architecture proposed in this dissertation, aimed at enhancing the overall effectiveness of information system security against internal fraud.

## **2.9 Integrated Misuse Intrusion Architecture**

Integrated misuse intrusion architecture aims to safeguard organizations from internal threats through a blend of managerial, operational, technical, and additional protective measures. On the managerial side, the focus is on creating clear policies and procedures, ensuring employees understand security expectations, and conducting regular audits. This includes educating staff on acceptable use of IT resources. Operationally, security is maintained through daily tasks like monitoring system logs, managing access controls, and performing routine security checks to ensure compliance with the established policies. Technologically, advanced tools such as firewalls, encryption, and multi-factor authentication offer multiple layers of protection against potential insider threats. Additionally, physical security measures and legal safeguards, like restricted access to sensitive areas and NDAs, help deter malicious activity. Integrating these controls into a cohesive framework involves a phased approach, beginning with policy development and awareness training, followed by deploying technical defenses and maintaining ongoing monitoring efforts to ensure a secure environment.

# **3. Methodology**

## **3.1 The Realities of Internal Fraud**

### **3.1.1 Statistical Overview of Internal Fraud**

In Europe, the financial ramifications of internal fraud are profoundly alarming. In 2000 alone, losses soared beyond $2.16 billion, a stark testament to the pervasive nature of this threat. Even more concerning is that insiders were implicated in 52% of all large-scale fraud incidents during this period. Delving deeper into the demographics, management grades accounted for 40% of these fraudulent activities, while junior employees were responsible for 12% (Thomson, 2002). These figures highlight the breadth of the issue, affecting all levels of an organization and underscoring the critical need for comprehensive internal security protocols.

### **3.1.2 Case Studies and Examples**

High-profile cases bring the abstract statistics of internal fraud into stark reality, emphasizing the severe consequences for organizations and their customers (Rohemah, Prasetyono, & Yuliana, 2023). For instance, an incident reported by Computer Fraud & Security in September 2002 detailed how three insiders exploited their positions to reveal customers' online bank account details for personal financial gain. This breach not only resulted in significant financial losses for the affected individuals and the bank but also severely tarnished the institution's reputation.  
Another illustrative case involved a major multinational corporation where an employee manipulated the financial reporting system to embezzle millions of dollars over several years. This case only came to light after an internal audit revealed inconsistencies, leading to a prolonged and costly investigation. The fallout included a substantial drop in the company's stock price, legal battles, and a loss of stakeholder trust. Such cases starkly illustrate the necessity for robust internal security measures. These measures must be designed to detect and deter fraud early, minimizing the damage and preserving the integrity of the organization.

### **3.1.3 Economic Impact of Internal Fraud**

The economic impact of internal fraud extends far beyond the immediate financial losses. The ripple effects can be devastating, encompassing diminished customer confidence, severe reputational damage, and increased operational costs associated with investigating and mitigating fraud incidents. According to the FBI, the average cost of an insider attack is nearly 50 times greater than that of an external attack, underscoring the heightened risk and severe repercussions of internal breaches (Thompson et al., 2004). Diminished customer confidence is perhaps one of the most significant and intangible costs. When customers learn of an internal fraud incident, particularly one involving their personal or financial data, their trust in the organization is severely eroded. This loss of confidence can lead to customer attrition, reduced sales, and long-term damage to the brand's reputation. Restoring trust often requires substantial investment in public relations, customer compensation, and enhanced security measures, further straining the organization's resources. Reputational damage can also have far-reaching consequences, affecting relationships with partners, investors, and regulatory bodies. Companies with a history of internal fraud may face increased scrutiny from regulators and may find it more challenging to secure investment or form strategic partnerships. This scrutiny can lead to increased compliance costs and a more conservative operational approach, potentially stifling innovation and growth (Perera et al., 2022). Operational costs rise significantly as organizations respond to and recover from internal fraud incidents. These costs include forensic investigations, legal fees, and the implementation of additional security measures. For example, after an internal fraud incident, a company might need to overhaul its IT systems, conduct extensive employee training programs, and engage external auditors to restore confidence in its financial reporting and security practices (Wang et al., 2022). In summary, the economic impact of internal fraud is multifaceted and far-reaching. Beyond the immediate financial losses, organizations must contend with long-term consequences that can affect their market position, operational efficiency, and overall sustainability. The high cost of internal fraud reinforces the critical need for effective internal security measures that can prevent, detect, and respond to insider threats promptly and efficiently.

## **3.2 Approach**

The detection and prevention of internal misuse within an organization involve a structured, multi-step process. Initially, data is collected from the organization’s networks, with a particular focus on user activity logs, access patterns, and their overall interactions with the system. This data forms the foundation for further analysis. In the next phase, advanced machine learning models namely Random Forests, Decision Trees, and Isolation Forests are applied to the data to identify any anomalies that deviate from typical user behaviour (Al-Mhiqani et al., 2020). The goal is to establish behavioural baselines by analysing users' normal activities and interactions. By continuously monitoring the flow of information through the network, the system aims to detect unusual patterns that could signal insider threats. The system’s performance and its accuracy in detecting potential threats are evaluated based on these behavioural baselines and deviation patterns.

## **3.3 Technology**

To effectively combat internal misuse, several technologies and tools are deployed. Central to this process are machine learning algorithms, behavioural analytics, and real-time monitoring systems. Machine learning techniques, such as Random Forests and Decision Trees, are particularly effective in managing large-scale datasets generated from user activity. These algorithms help identify deviations from normal behaviour that could indicate malicious activity (Vaddadi, Vallabhaneni, and Whig, 2023). Behavioural analytics are crucial for creating models of standard user behaviour, making it easier to detect any anomalous activities that deviate from these patterns. In addition to these, integrated security systems that employ real-time monitoring and alert mechanisms allow organizations to quickly respond to potential threats as they occur. The combination of these technologies significantly enhances an organization's ability to proactively detect, prevent, and address insider threats.

## **3.4 Version Management**

Version management is a critical component of developing and maintaining insider threat detection systems, as it tracks the evolution of software, data sets, and computational models. This process involves recording every iteration of the codebase, documenting changes, and tracking updates and bug fixes. Git, a widely used version control system, facilitates collaboration by allowing team members to work on different parts of the project simultaneously, roll back to previous versions when needed, and manage feature branches efficiently (Al-Mhiqani et al., 2020). The documentation of these changes not only ensures transparency but also enhances the testing process and ensures compliance with security standards. By systematically managing versions, the reliability and integrity of the detection system are greatly improved, allowing the team to trace the development process and maintain a stable system throughout the project lifecycle. Here’s the link to GitHub: <https://github.com/sagar0135/Dissertation>

## **3.5 Test and Evaluation**

The testing and evaluation of the insider threat detection system are essential to measure its performance and accuracy. A variety of tests are conducted, starting with unit tests for individual components and progressing to composite tests that assess the interaction between different system modules. To evaluate the effectiveness of the machine learning models used, key performance metrics such as precision, recall, and F1 scores are calculated using a pre-labelled dataset (Vaddadi, Vallabhaneni, and Whig, 2023). This dataset helps establish a benchmark for evaluating the models' ability to correctly identify insider threats while minimizing false positives and negatives. Additionally, case studies of real insider threat scenarios are used to test the system’s capability in handling real-world situations. Throughout the testing process, feedback loops are implemented to refine and improve the algorithms, ensuring that the system is continuously optimized for better performance and sustainability.

## **3.6 Implementation & Discussion**

Network internal misuse is a strong threat for organizations, particularly if they are dealing with huge amounts of data, having a number of entrances, and using various kinds of devices. In order for such abuse to be noted, presumed necessary to use such advanced technologies as machine learning models that can detect trends and suspicion in relation to user activity, utilization of the service and the network. This discourse presents the core-strategies and method of an integrated approach using supervised learning techniques like; Random novelties, decision trees classifiers, and unsupervised by Isolation Forest.

### **3.6.1 Dataset Overview**

The KDD Cup 99 dataset, a benchmark resource in intrusion detection research, was used to implement the suggested algorithms. It contains several attributes, including protocol type, service, connection duration, and traffic statistics, that make it easier to analyse network activity and traffic. This dataset classifies network activity including misuse and intrusion as normal or abnormal. Before utilising machine learning models, data preprocessing was necessary. This involved handling categorical data, using LabelEncoder to encode features to numerical values, and making sure the data was full. The loading of the dataset into a pandas DataFrame, basic statistical analysis to ensure data integrity, and exploratory data analysis using programs like Seaborn and Matplotlib were important preparation procedures. To improve model efficacy and decision-making processes, additional procedures included feature selection and correlation analysis to find and remove redundant features and encode categorical variables like protocol type and service into numerical representations appropriate for machine learning analysis.

### **3.6.2 Supervised Learning Models for Misuse Detection**

The Random Forest Classifier effectively handles complicated, high-dimensional data and captures the interactions between attributes by combining findings for more impartial and accurate outputs through the use of decision trees. Following preprocessing, the data was divided into 70% for training and 30% for testing. By utilising 100 trees to balance speed and performance, an astounding 99.95% accuracy was attained. Its ability to discern between typical and suspicious activity is demonstrated by its strong precision, recall, and F1-scores in the confusion matrix and classification reports. The Decision Tree Classifier, on the other hand, is marginally less accurate at 99.89%. It does this by using rules that are developed from data attributes to identify internal misuse. The Random Forest Classifier effectively handles complicated, high-dimensional data and captures the interactions between attributes by combining findings for more impartial and accurate outputs through the use of decision trees. Following preprocessing, the data was divided into 70% for training and 30% for testing. By utilising 100 trees to balance speed and performance, an astounding 99.95% accuracy was attained. Its ability to discern between typical and suspicious activity is demonstrated by its strong precision, recall, and F1-scores in the confusion matrix and classification reports. The Decision Tree Classifier, on the other hand, is marginally less accurate at 99.89%. It does this by using rules that are developed from data attributes to identify internal misuse.

### **3.6.3 Unsupervised Learning for Anomaly Detection**

Unsupervised methods such as the Isolation Forest Algorithm were used to identify abnormalities and peculiar behaviours in user activities and network traffic without requiring labelled data. By detecting departures from the norm, this algorithm is able to locate outlier data points that may indicate potential abuse or security breaches. By examining these anomalies according to protocol and service type, the algorithm was able to identify network segments where risks were most common, giving important information about the precise locations of any security

### **3.6.4 Feature Importance Analysis**

In the feature importance analysis, both Random Forest and Decision Tree classifiers emphasise the importance of specific features in detecting misuse. The Random Forest's most important attributes are src\_bytes, dst\_bytes, and duration, which measure the amount of data delivered and received during a connection, indicating that they are crucial indicators of overuse. Similarly, the Decision Tree classifier prioritises the same attributes but places a high value on the serror\_rate, or source error rate, emphasising its importance in spotting potential risks. This research assists in determining which properties are most important for detecting misuse within network systems.

### **3.6.5 User Activity and Service Analysis**

In this study, extensive evaluations of user and service behaviours were carried out alongside the usage of machine learning algorithms. By categorising user data, we were able to see how frequently various activities both normal and suspicious occurred, which is critical for determining which people may be engaging in potentially hazardous behaviours. Similarly, by analysing the distribution of service linkages, we were able to identify the most commonly utilised services, allowing us to determine which ones were more prone to misuse. This dual analysis helps us better identify where security emphasis is most needed.

### **3.6.6 Network Traffic Analysis**

Analysing network traffic by protocol type is important when it comes to analysis of misuse. Various protocols of internet connections including TCP, UDP and ICMP were also inspected to determine unusually high or highly intense traffic. This analysis demonstrates that it best illustrates that protocols that require misuse, as in the case of TCP, are more vulnerable because many client server applications use it.

### **3.6.7 Comparison of Models**

This paper aimed at comparing the efficiency of the Random Forest and Decision Tree classifiers, for distinguishing between misuse and non-misuse instances. Generally, both models were accurate and reliable, but the Random Forest model had proved itself to be slightly more efficient than the Decision Tree model. The Random Forest is an ensemble mode of operation which ensures that it performs better in this case and does not tend to over-fit its ability to handle data.

### **3.6.8 IP Address Description and Network Setup**

As a practical implementation they have created a scenario with Packet Tracers that looks into misuses within the network inside segments. This network includes different devices like PC, Laptops, and servers in different departments which have their own & internal or private IP address.

**Routers:** Routers in the IT and HR departments work as relay between internal subnets, such as 192.168.20.x for IT and 192.168.11.x for HR, with other the global IP address rage such as 10.1.1.x.

**Cloud-PT:** The cloud component is a public network that helps with the traffic flow between departments while also bearing traffic analysis responsibilities.

## **3.6 Risk Management**

Effective risk management is fundamental in mitigating the potential impact of insider threats. This process begins with a thorough risk analysis to identify the organization’s key assets and evaluate the likelihood of insider threats. Once these risks are identified, appropriate measures are put in place to reduce the organization’s exposure. These measures include enhanced access control systems, improved training programs for employees to raise awareness of security best practices, and advanced monitoring tools to detect unusual activities (Al-Mhiqani et al., 2020). Moreover, the risk management framework is dynamic, meaning it can be adjusted based on ongoing audits and reviews. Regular security awareness training and fostering a culture of continuous improvement are essential components of this strategy, helping to ensure that the organization remains vigilant against insider threats and that its security posture evolves with emerging risks.

## **3.7 Professional, Legal, Ethical & Sustainability Issues**

The development and implementation of an integrated approach to detecting and mitigating internal misuse must consider a wide array of professional, legal, ethical, and sustainability issues. Addressing these concerns is crucial to ensure the solution is not only effective but also responsible and aligned with broader societal values and regulations.

### **3.7.1 Professional Standards**

Adhering to professional standards is crucial for ensuring the quality, reliability, and security of any cybersecurity solution. This requires the implementation of recognized industry frameworks and guidelines, such as those from the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), which set best practices for cybersecurity (Majid et al., 2022). Maintaining high code quality through rigorous code reviews, automated testing, and continuous integration/deployment (CI/CD) pipelines is equally important for ensuring ongoing reliability and maintainability (Yetistiren et al., 2023). Moreover, continuous professional development is essential, as it ensures that team members remain knowledgeable about the latest advancements in cybersecurity (Nazaretsky et al., 2022). Insider threat identification specifically focuses on ethical considerations, legislative compliance, and the incorporation of industry standards (Bishop et al., 2014). Security personnel must regularly participate in refresher courses and obtain certifications to stay informed about emerging threats and trends. Transparency in data management and user protection is also key to building organizational trust (Wilkinson et al., 2016). Regular reviews and updates of security policies ensure they remain relevant and aligned with dynamic industry standards, supporting both ethical conduct and the continuous improvement of security strategies (Alfawzan et al., 2021).

### **3.7.2 Legal Compliance**

Legal compliance is a fundamental component of any cybersecurity initiative, especially when handling sensitive data. Organizations must adhere to a range of data protection laws, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, along with other relevant local and international regulations (Cervi, 2022). A key legal concern is balancing the need to monitor user activities with safeguarding employee privacy, which requires transparent communication about monitoring practices and obtaining necessary consent where appropriate (Teebken & Hess, 2021). Additionally, respecting intellectual property rights is crucial, particularly in ensuring that any third-party tools or software libraries used are properly licensed. In the context of insider threat management, legal requirements also encompass compliance with regulations like the Health Insurance Portability and Accountability Act (HIPAA), especially when dealing with large or raw datasets. To address potential legal issues, organizations must implement regular audits and timely updates to their platforms, ensuring ongoing alignment with the latest regulatory standards.

### **3.7.3 Ethical Considerations**

Ethical considerations are crucial when developing and deploying surveillance and monitoring systems, particularly in the context of internal threat detection. Key issues include transparency, fairness, and the minimization of intrusiveness. Transparency requires that employees are fully informed about monitoring practices, including what data is being collected, how it will be used, and the safeguards in place to protect their privacy (Bommasani et al., 2023). This open communication fosters trust and ensures that the monitoring process is aligned with privacy rights. Fairness is also essential, especially in the use of machine learning algorithms, which must be regularly audited to identify and mitigate any biases that could result in unfair treatment (Gallegos et al., 2023). Furthermore, minimizing intrusiveness is critical to respecting user privacy; this means collecting only the data necessary to detect and mitigate threats, thus reducing unnecessary surveillance. Ethical concerns in insider threat detection particularly revolve around safeguarding personal data and maintaining organizational trust. Employees should have access to policies regarding how their data is handled, ensuring that privacy rights are upheld while supporting a culture of accountability and responsible cybersecurity practices (Khatun et al., 2023).

### **3.7.4 Sustainability**

Sustainability is increasingly critical in technology development, including cybersecurity, where energy efficiency, resource optimization, and lifecycle management play key roles (Ali et al., 2023). Energy-efficient solutions help minimize environmental impacts by optimizing algorithms, using sustainable hardware, and leveraging cloud services with eco-friendly practices. Resource optimization ensures efficient use of both computational and human resources, reducing waste and enhancing project sustainability (Aithal & Aithal, 2023). Lifecycle management involves planning for the entire solution lifecycle, from development to decommissioning, ensuring that hardware is properly disposed of and data is securely erased to prevent long-term environmental damage (Adu-Amankwa et al., 2023). In the context of insider threat detection and prevention, sustainability also includes adopting energy-efficient technologies, reducing electronic waste, and integrating cloud-based solutions, which collectively reduce the carbon footprint (Xiao et al., 2023; Ali & Shirazi, 2023). Furthermore, raising awareness among employees about sustainable practices and responsible behaviour is essential to reinforcing these efforts (Li et al., 2023).

### **3.7.5 Social Responsibility**

The project holds a significant social responsibility, ensuring its outcomes not only meet technical objectives but also contribute positively to society. By enhancing internal security within organizations, it strengthens overall societal security by safeguarding individual data and minimizing the risk of widespread data breaches (Mayer et al., 2023). Furthermore, the project must uphold fair and ethical employment practices, promoting diversity, inclusion, and professional development within its team (Valentine et al., 2023). It also involves engaging with the broader cybersecurity community to share insights, best practices, and contribute to the collective knowledge, thus enhancing the industry's resilience (Kaur et al., 2023). This focus on social responsibility extends to insider threat management, where organizations are accountable for protecting sensitive data while also serving as valuable societal assets. Organizations should actively raise security awareness and educate stakeholders on potential threats, which helps improve the general understanding of cybersecurity (Bulgurcu et al., 2010). Fair monitoring policies and creating secure work environments not only protect employees but also the wider community from cyber risks (Cho et al., 2022). Ultimately, addressing professional, legal, ethical, and sustainability issues is essential for the project's success, contributing to the larger goal of fostering a secure, ethical, and sustainable digital environment (Momand, Jan, & Ramzan, 2023).

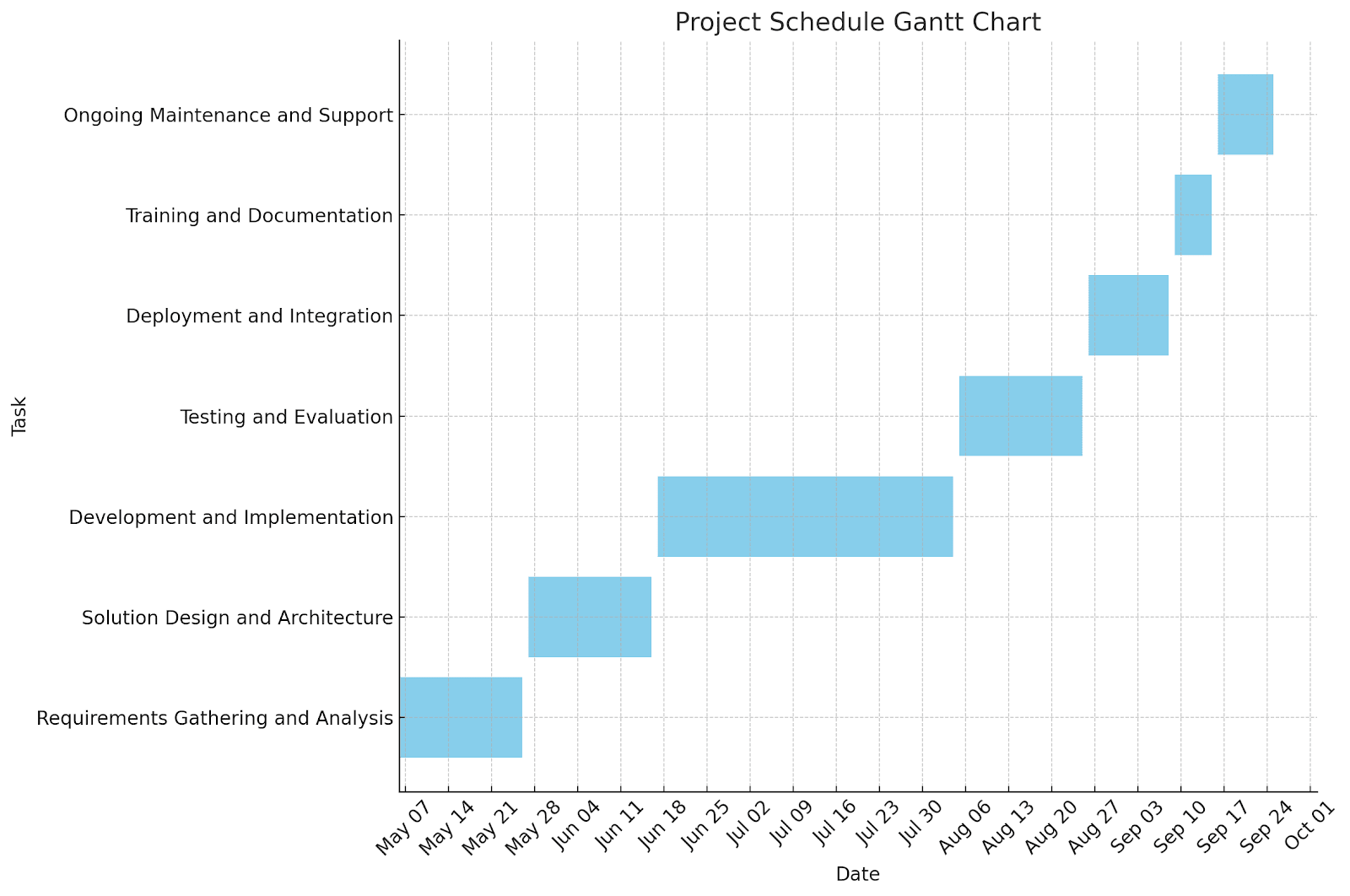
# **4. Project Plan**

## **4.1 Activities**

The project will be organised into many important phases:

1. Requirements Gathering and Analysis: This entails determining the organization's unique needs and limits.
2. Solution Design and Architecture: This phase focusses on developing the overall structure and design of the solution.
3. Development and Implementation: At this stage, the solution is built and put into action.
4. Testing and Evaluation: This step entails extensive testing to ensure the solution's functioning and security.
5. Deployment and Integration: The solution is implemented and integrated into existing systems.
6. Training and documents: Training and essential documents are supplied to ensure that the solution is used effectively.
7. Ongoing Maintenance and Support: This guarantees that the solution continues to perform properly and remains up to date.

## **4.2 Schedule**



## **4.3 Data Management Plan**

This plan involves sharing, storage, and organization of data during the project. Data will be gathered from the dataset which ensures cleaning and preprocessing data. The entire data will be stored securely on a platform based on cloud which has limited accessibility to authorized members of the team (Ashfaq Khan and Kim, 2021). Daily backups will be performed for preventing loss of data. On the completion of project, datasets will be shared in adherence to the ethical guidelines for ensuring anonymization of sensitive data, and it will be made accessible through a repository.

## **4.4 Deliverables**

The tangible deliverables in the project entitled, ‘An Integrated Approach to Detecting and Mitigating Internal Misuse’ consist of the following key artefacts that provide for complete evaluation and use of detection tools. The key outputs of the integrative study project entitled an integrated approach to detecting and mitigating internal misuse involves that the data exploratory tool set has an investigation of the categorical and numerical data preprocessing, analysing features and variables. It gives initial understanding of the misuse behaviour that takes place and the type of misuse (Momand, Jan and Ramzan, 2023). The project also provides output in form of models which is developed using Random Forest and Decision Tree classifier along with accuracy, confusion matrix and classification report. It is possible to find out possible misuse within the network through these models. Moreover, for the purpose of improving security, the anomaly detection function is included in the Isolation Forest model for detecting abnormal usage. Such important values like model evaluation, features’ contribution, and anomalies’ occurrence are represented visually not only for better understanding but also for making important decisions. In addition, simulations of the network architecture based on the IP address and routing with configuration tables are added with regard to practical training and testing of the detection system. It provides a comprehensive solution including the high-quality data analysis, the reliable machine learning algorithms and a practical network topology needed to recognize and prevent internal misuse accurately and thus help improve the organisational cybersecurity.

# **5. Discussion and Evaluation**

In evaluating the proposed architecture's effectiveness in combating employee fraud, it has proven successful in preventing, detecting, monitoring, and recovering from various types of internal threats. Case studies and simulations underscore its reliability, showing a significant reduction in the risk of insider fraud (Schultz, 2002). When compared to existing solutions, the integrated approach stands out for its enhanced detection capabilities, faster response times, and greater resilience against insider attacks. Traditional methods often fall short in these areas, making the new architecture a more comprehensive solution to internal fraud (Furnell, 2004). However, there are some challenges to consider, such as the possibility of false positives and the need for regular updates to address emerging threats. Implementing this system may also require considerable investment and changes within the organization (Sekar et al., 1999).

# **6. Recommendations**

To strengthen the proposed architecture, it’s essential to enhance both policies and technical systems. Regularly updating security policies, prioritizing employee training, and setting clear protocols for responding to incidents are key steps for ensuring success. On the technical side, incorporating advanced security tools like AI-powered intrusion detection systems and stronger encryption will help defend against evolving threats. Ongoing research and development are critical to maintaining these protections. Future research should continue to explore innovative approaches, such as machine learning and behavioural analytics, for identifying insider threats. Additionally, understanding the psychological and organizational factors behind internal fraud could lead to more effective prevention strategies.

# **7. Conclusion**

The proposed research underscores the growing importance of adopting an integrated approach to detecting and mitigating internal misuse within organizations, a critical issue in today's cybersecurity landscape. Utilizing cutting-edge technologies such as user behaviour analytics, machine learning algorithms, and centralized security management systems, the solution aims to deliver comprehensive protection against insider threats. The use of machine learning models like Decision Trees and Random Forests helps identify key anomalies and patterns in user behaviour, network traffic, and system usage. These models enhance the understanding of potential threats by analysing data to detect and predict harmful activities, offering organizations a robust framework for improving their cybersecurity measures. The project's methodology is designed around an agile development process, ensuring that the system remains adaptable to evolving threats and organizational needs. Continuous evaluation and refinement are central to the project, with rigorous testing of the machine learning models to ensure effectiveness, scalability, and seamless integration with existing systems. The adaptability of this approach allows for ongoing improvement and enables the detection framework to evolve in response to new and emerging threats, thereby maintaining a high level of security within the organization. A key contribution of this research is the integration of managerial, operational, and technical controls within the proposed architecture. These controls work together to prevent, detect, monitor, and recover from internal misuse, providing a holistic solution to insider threats. The architecture not only addresses the technical aspects of security but also incorporates the significance of fostering a positive organizational culture that encourages ethical behaviour and reduces the likelihood of internal fraud. As identified in the research, existing security measures often fall short in detecting insider threats, as they primarily focus on external threats or utilize rule-based detection methods that fail to capture the complexity of internal misuse. The proposed architecture bridges this gap by incorporating both behavioural analysis and proactive monitoring strategies, ensuring a comprehensive defense against internal threats. The insights gained from this research extend beyond technical solutions, highlighting the importance of continuous monitoring, statistical analysis, and real-time data evaluation to stay ahead of potential insider attacks. By refining machine learning models and improving feature extraction, organizations can significantly enhance their ability to detect internal misuse early on, thereby safeguarding their data, financial assets, and reputation from the damaging effects of employee fraud. In conclusion, the research emphasizes that effectively addressing internal fraud and misuse requires a multifaceted approach that integrates robust security measures with continuous evaluation and a strong organizational culture. The proposed architecture offers a forward-thinking solution that enhances information system security and equips organizations with the tools to prevent, detect, and respond to insider threats more effectively. Future work should focus on refining these models further, expanding the feature sets, and implementing real-time monitoring systems to maintain a secure digital environment. This approach represents a significant step forward in the ongoing effort to protect organizations from the potentially devastating impact of insider threats.

# **Bibliography/References**

1. Alloulbi, A., Öz, T. and Alzubi, A., 2022. The use of artificial intelligence for smart decision-making in smart cities: A moderated mediated model of technology anxiety and internal threats of IoT. *Mathematical Problems in Engineering*, *2022*.
2. Ni, S., Zou, S. and Chen, J., 2022. Evolutionary game model of Internal threats to nuclear security in spent fuel reprocessing plants based on RDEU Theory. *Sustainability*, *14*(4), p.2163.
3. Çevik, S.B. and Friedman, R., 2024. Turkey’s soldier’s matrix: Fighting against internal threats and external enemies. *Politics, Groups, and Identities*, *12*(1), pp.66-84.
4. Kang, H.J. and Lo, D., 2021. Active learning of discriminative subgraph patterns for api misuse detection. *IEEE Transactions on Software Engineering*, *48*(8), pp.2761-2783.
5. Sever, Y. and Dogan, A.H., 2023. A Kubernetes dataset for misuse detection.
6. Ban, T., Takahashi, T., Ndichu, S. and Inoue, D., 2023. Breaking alert fatigue: Ai-assisted siem framework for effective incident response. *Applied Sciences*, *13*(11), p.6610.
7. Bolek, V., Romanová, A. and Korček, F., 2023. The information security management systems in E-business. *Journal of Global Information Management*, *31*(1), pp.1-29.
8. Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., Corrado, G.S., Davis, A., Dean, J., Devin, M. and Ghemawat, S., 2016. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. *arXiv preprint arXiv:1603.04467*.
9. Zhao, X., Jin, Z., Liu, Y. and Hu, Y., 2022. Heterogeneous information network embedding for user behaviour analysis on social media. *Neural Computing and Applications*, pp.1-17.
10. Edison, H., Wang, X. and Conboy, K., 2021. Comparing methods for large-scale agile software development: A systematic literature review. *IEEE Transactions on Software Engineering*, *48*(8), pp.2709-2731.
11. Brauneck, A., Schmalhorst, L., Kazemi Majdabadi, M.M., Bakhtiari, M., Völker, U., Baumbach, J., Baumbach, L. and Buchholtz, G., 2023. Federated machine learning, privacy-enhancing technologies, and data protection laws in medical research: scoping review. *Journal of Medical Internet Research*, *25*, p.e41588.
12. Cervi, G.V., 2022. Why and how does the EU rule global digital policy: an empirical analysis of EU regulatory influence in data protection laws. *Digital Society*, *1*(2), p.18.
13. Ahsan, M., Nygard, K.E., Gomes, R., Chowdhury, M.M., Rifat, N. and Connolly, J.F., 2022. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), pp.527-555.
14. Al-Mhiqani, M.N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K.H., Ali, N.S. and Yunos, Z., 2020. A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), p.5208.
15. Al-Mhiqani, M.N., Ahmed, R., Zainal, Z. and Isnin, S.N. (2021). An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection. International Journal of Advanced Computer Science and Applications, [online] 12(1). doi: <https://doi.org/10.14569/ijacsa.2021.0120166>.
16. Ambalavanan, V. and Bala, S. (2020). Cyber Threats Detection and Mitigation Using Machine Learning. Advances in information security, privacy, and ethics book series, [online] pp.132–149. doi: https://doi.org/10.4018/978-1-5225-9611-0.ch007.‌Ashfaq Khan, M. and Kim, Y. (2021). Deep Learning-Based Hybrid Intelligent Intrusion Detection System. *Computers, Materials & Continua*, 68(1), pp.671–687. doi: https://doi.org/10.32604/cmc.2021.015647.
17. Asmar, M. and Tuqan, A., 2024. Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon*.
18. Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S. and Pitner, T., 2023. Addressing insider attacks via forensic-ready risk management. Journal of Information Security and Applications, 73, p.103433.
19. Erbas, M., Khalil, S.M. and Tsiopoulos, L., 2024. Systematic literature review of threat modeling and risk assessment in ship cybersecurity. Ocean Engineering, 306, p.118059.
20. Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, [online] 80(5), pp.973–993. doi: <https://doi.org/10.1016/j.jcss.2014.02.005>.
21. Ibrahim, H., 2022. A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. Wasit Journal of Computer and Mathematics Science, 1(3), pp.50-68.
22. ‌Khan, A.A., Chaudhari, O. and Chandra, R. (2024). A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation. *Expert Systems with Applications*, [online] 244, pp.122778–122778. doi: https://doi.org/10.1016/j.eswa.2023.122778.
23. Khatun, M.A., Memon, S.F., Eising, C. and Dhirani, L.L., 2023. Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation. *IEEE Access*.
24. Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), pp.1-22.
25. Kim, J., Park, M., Kim, H., Cho, S. and Kang, P., 2019. Insider threat detection based on user behavior modeling and anomaly detection algorithms. Applied Sciences, 9(19), p.4018.
26. Mehmood, M., Amin, R., Muslam, M.M.A., Xie, J. and Aldabbas, H., 2023. Privilege escalation attack detection and mitigation in cloud using machine learning. *IEEE Access*, *11*, pp.46561-46576.
27. Momand, A., Jan, S.U. and Ramzan, N., 2023. A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy. *Journal of Sensors*, *2023*(1), p.6048087.
28. Nepal, S. and Joshi, B., 2021. User Behavior Analytics for Insider Threat Detection using Deep Learning.
29. Sakthivelu, U. and Vinoth Kumar, C.N.S., 2023. Advanced Persistent Threat Detection and Mitigation Using Machine Learning Model. Intelligent Automation & Soft Computing, 36(3).
30. Taherdoost, H., 2021. A review on risk management in information systems: Risk policy, control and fraud detection. *Electronics*, *10*(24), p.3065.
31. Vaddadi, S.A., Vallabhaneni, R. and Whig, P., 2023. Utilizing AI and Machine Learning in Cybersecurity for Sustainable Development through Enhanced Threat Detection and Mitigation. *International Journal of Sustainable Development Through AI, ML and IoT*, *2*(2), pp.1-8.
32. Liang, J. and Kim, Y., 2022, January. Evolution of firewalls: Toward securer network using next generation firewall. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0752-0759). IEEE.
33. Moneva, A. and Leukfeldt, R., 2023. Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology*, *56*(4), pp.416-440.
34. Akinbowale, O.E., Mashigo, P. and Zerihun, M.F., 2023. The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, *10*(1), p.2163560.
35. Majid, M., Habib, S., Javed, A.R., Rizwan, M., Srivastava, G., Gadekallu, T.R. and Lin, J.C.W., 2022. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6), p.2087.
36. Yetiştiren, B., Özsoy, I., Ayerdem, M. and Tüzün, E., 2023. Evaluating the code quality of ai-assisted code generation tools: An empirical study on github copilot, amazon codewhisperer, and chatgpt. arXiv preprint arXiv:2304.10778.
37. Nazaretsky, T., Ariely, M., Cukurova, M. and Alexandron, G., 2022. Teachers' trust in AI‐powered educational technology and a professional development program to improve it. *British journal of educational technology*, *53*(4), pp.914-931.
38. Bishop, M., Conboy, H.M., Phan, H., Simidchieva, B.I., Avrunin, G.S., Clarke, L.A., Osterweil, L.J. and Peisert, S., 2014, May. Insider threat identification by process analysis. In *2014 IEEE Security and Privacy Workshops* (pp. 251-264). IEEE.
39. Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.W., da Silva Santos, L.B., Bourne, P.E. and Bouwman, J., 2016. The FAIR Guiding Principles for scientific data management and stewardship. *Scientific data*, *3*(1), pp.1-9.
40. Alfawzan, N., Christen, M., Spitale, G. and Biller-Andorno, N., 2022. Privacy, data sharing, and data security policies of women’s mhealth apps: scoping review and content analysis. *JMIR mHealth and uHealth*, *10*(5), p.e33735.
41. Teebken, M. and Hess, T., 2021. Privacy in a digitized workplace: Towards an understanding of employee privacy concerns.
42. Bommasani, R., Klyman, K., Longpre, S., Kapoor, S., Maslej, N., Xiong, B., Zhang, D. and Liang, P., 2023. The foundation model transparency index. *arXiv preprint arXiv:2310.12941*.
43. Gallegos, I.O., Rossi, R.A., Barrow, J., Tanjim, M.M., Kim, S., Dernoncourt, F., Yu, T., Zhang, R. and Ahmed, N.K., 2024. Bias and fairness in large language models: A survey. *Computational Linguistics*, pp.1-79.
44. Ali, S.M., Appolloni, A., Cavallaro, F., D’Adamo, I., Di Vaio, A., Ferella, F., Gastaldi, M., Ikram, M., Kumar, N.M. and Martin, M.A., 2023. Development Goals towards Sustainability. Sustainability 2023, 15, 9443.
45. Aithal, S. and Aithal, P.S., 2023. Importance of circular economy for resource optimization in various industry sectors–a review-based opportunity analysis. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *7*(2), pp.191-215.
46. Adu-Amankwa, N.A.N., Rahimian, F.P., Dawood, N. and Park, C., 2023. Digital Twins and Blockchain technologies for building lifecycle management. *Automation in Construction*, *155*, p.105064.
47. Xiao, J., Yang, L., Zhong, F., Wang, X., Chen, H. and Li, D., 2022. Robust anomaly-based insider threat detection using graph neural network. *IEEE Transactions on Network and Service Management*, *20*(3), pp.3717-3733.
48. Ali, S. and Shirazi, F., 2023. The paradigm of circular economy and an effective electronic waste management. *Sustainability*, *15*(3), p.1998.
49. Li, T., Liao, C., Law, R. and Zhang, M., 2023. An integrated model of destination attractiveness and tourists’ environmentally responsible behavior: the mediating effect of place attachment. Behavioral Sciences, 13(3), p.264.
50. Mayer, P., Zou, Y., Lowens, B.M., Dyer, H.A., Le, K., Schaub, F. and Aviv, A.J., 2023. Awareness, Intention,(In) Action: Individuals’ Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction*, *30*(5), pp.1-53.
51. Valentine, S.R., Godkin, L. and Fleischman, G., 2024. The Impact of Ethical Forms of Organizational Leadership and Ethical Employment Contexts on Employee Job Satisfaction in Nigerian Hospitality and Recreation Firms. *Employee Responsibilities and Rights Journal*, *36*(1), pp.41-62.
52. Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, p.101804.
53. Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, pp.523-548.
54. Cho, Y., Oh, J., Kwon, D., Son, S., Lee, J. and Park, Y., 2022. A secure and anonymous user authentication scheme for IoT-enabled smart home environments using PUF. *IEEE Access*, *10*, pp.101330-101346.
55. Momand, A., Jan, S.U. and Ramzan, N., 2023. A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy. *Journal of Sensors*, *2023*(1), p.6048087.Hegazy, W., Salem, I., Alotaibi, H. F., Khafagy, E.-S., & Ibrahim, D. (2022). Terazosin Interferes with Quorum Sensing and Type Three Secretion System and Diminishes the Bacterial Espionage to Mitigate the Salmonella Typhimurium Pathogenesis. Antibiotics, 11.
56. Moritz, S., Nguyen, C., Jelinek, L., Borsutzky, S., Scheunemann, J., Hegerl, U., Püschel, K. and Gallinat, J., 2023. Behavioral and location‐related antecedents of train suicides. *Suicide and Life‐Threatening Behavior*, *53*(2), pp.303-311.Haryono, A. T., Sarno, R., & Sungkono, K. R. (2023). Transformer-Gated Recurrent Unit Method for Predicting Stock Price Based on News Sentiments and Technical Indicators. IEEE Access, 11.
57. Rovira, M., 2023. The global rise of criminal background checks. *International Criminology*, *3*(1), pp.1-11.
58. Silowash, G.J., Spooner, D.L., Costa, D.L. and Albrethsen, M.J., 2016. Low-Cost Technical Solutions to Jump Start an Insider Threat Program. *The CERT Division of Carnegie Mellon University*.
59. Villarreal-Vasquez, M., Modelo-Howard, G., Dube, S. and Bhargava, B., 2021. Hunting for insider threats using LSTM-based anomaly detection. *IEEE Transactions on Dependable and Secure Computing*, *20*(1), pp.451-462.
60. Blank, J.D. and Osofsky, L., 2020. Automated legal guidance. *Cornell L. Rev.*, *106*, p.179.
61. Chimbutane, F. and Gonçalves, P., 2023. Family language policy and language shift in postcolonial Mozambique: a critical, multi-layered approach. *Language Policy*, *22*(3), pp.267-287.
62. Zeoli, A.M., Mccourt, A.D. and Paruk, J.K., 2022. Effectiveness of firearm restriction, background checks, and licensing laws in reducing gun violence. *The ANNALS of the American Academy of Political and Social Science*, *704*(1), pp.118-136.
63. Kaur, B., Kumar, S. and Kaushik, B.K., 2023. Novel wearable optical sensors for vital health monitoring systems—A review. *Biosensors*, *13*(2), p.181.
64. Ramachandra, M.N., Srinivasa Rao, M., Lai, W.C., Parameshachari, B.D., Ananda Babu, J. and Hemalatha, K.L., 2022. An efficient and secure big data storage in cloud environment by using triple data encryption standard. *Big Data and Cognitive Computing*, *6*(4), p.101.
65. Brunello, G., Rückert, D., Weiss, C. and Wruuck, P., 2023. Advanced digital technologies and investment in employee training: Complements or substitutes?.
66. Tolba, M., Benferhat, S., Tabia, K. and Belkhir, A., 2018, August. Handling capabilities in security policies. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1922-1927). IEEE.
67. Mishler, S. and Chen, J., 2024. Boring but demanding: Using secondary tasks to counter the driver vigilance decrement for partially automated driving. *Human factors*, *66*(6), pp.1798-1811.
68. Pan, A., Chan, J.S., Zou, A., Li, N., Basart, S., Woodside, T., Zhang, H., Emmons, S. and Hendrycks, D., 2023, July. Do the rewards justify the means? measuring trade-offs between rewards and ethical behavior in the machiavelli benchmark. In *International Conference on Machine Learning* (pp. 26837-26867). PMLR.
69. Al-Ghurairi, A.S.T. and Al-Hamdani, N.M., 2019. The power of the judge in criminal investigation procedures. *TIKRIT UNIVERSITY JOURNAL FOR RIGHTS*, *3*(3/2).
70. Ivanov, E., 2021. In the ocean of anti-corruption compliance standards and guidelines: Time for codification?. In *The Transnationalization of Anti-Corruption Law* (pp. 243-262). Routledge.
71. Gomez-Cabrera, A. and Escamilla-Ambrosio, P.J., 2022. Review of machine-learning techniques applied to structural health monitoring systems for building and bridge structures. *Applied Sciences*, *12*(21), p.10754.
72. Zhan, D., Ye, L., Fang, B., Du, X. and Su, S., 2016, May. Cfwatcher: A novel target-based real-time approach to monitor critical files using vmi. In *2016 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
73. Cui, M., Wu, Z., Lu, Y., Wei, X. and Dai, L., 2022. Near-field MIMO communications for 6G: Fundamentals, challenges, potentials, and future directions. *IEEE Communications Magazine*, *61*(1), pp.40-46.
74. Brady, C. and M'manga, A., 2022, October. Gamification of Cyber Security Training-EnsureSecure. In *2022 IEEE international conference on e-business engineering (ICEBE)* (pp. 7-12). IEEE.
75. Li, G., Kou, G. and Peng, Y., 2021. Heterogeneous large-scale group decision making using fuzzy cluster analysis and its application to emergency response plan selection. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(6), pp.3391-3403.
76. Olaniyi, O.O., Asonze, C.U., Olabanji, S.O. and Adigwe, C.S., 2023. A regressional study on the impact of organizational security culture and transformational leadership on social engineering awareness among bank employees: The interplay of security education and behavioral change. *Asian Journal of Economics, Business and Accounting*, *23*(23), pp.128-143.
77. Aldayri, A. and Albattah, W., 2022. Taxonomy of anomaly detection techniques in crowd scenes. *Sensors*, *22*(16), p.6080.
78. Yin, Y., Zhang, R. and Su, Q., 2023. Threat assessment of aerial targets based on improved GRA-TOPSIS method and three-way decisions. *Math. Biosci. Eng*, *20*(7), pp.13250-13266.
79. Howard, M.C., Gutworth, M.B. and Jacobs, R.R., 2021. A meta-analysis of virtual reality training programs. *Computers in Human Behavior*, *121*, p.106808.
80. Asi, Y.M., Bebasari, P., Hardy, E., Lokot, M., Meagher, K., Ogbe, E., Parray, A.A., Sharma, V., Standley, C.J. and Vahedi, L., 2022. Assessing gender responsiveness of COVID-19 response plans for populations in conflict-affected humanitarian emergencies. *Conflict and health*, *16*(1), p.4.
81. Hoffmann, T.C., Glasziou, P.P., Boutron, I., Milne, R., Perera, R., Moher, D., Altman, D.G., Barbour, V., Macdonald, H., Johnston, M. and Lamb, S.E., 2014. Better reporting of interventions: template for intervention description and replication (TIDieR) checklist and guide. *Bmj*, *348*.
82. Boerner, T.J., Deems, S., Furlani, T.R., Knuth, S.L. and Towns, J., 2023. Access: Advancing innovation: Nsf’s advanced cyberinfrastructure coordination ecosystem: Services & support. In *Practice and Experience in Advanced Research Computing* (pp. 173-176).
83. Hahn, C., Kim, J., Kwon, H. and Hur, J., 2020. Efficient IoT management with resilience to unauthorized access to cloud storage. *IEEE transactions on cloud computing*, *10*(2), pp.1008-1020.
84. Rauf, U., Mohsen, F., & Wei, Z. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. Journal of Cyber Security and Mobility, 12, 221-252.
85. Quality - Access to Success. (2023). Employee Performance: Education, Training, Experience and Work Discipline.
86. Teichmann, F., & Boticiu, S. R. (2023). The Importance of Cybersecurity Incident Response Plans for Law Firms. Jusletter.
87. Li, W., Leung, A., & Yue, W. (2023). Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches. MIS Q.
88. Deng, H. and Li, X., 2022. Anomaly detection via reverse distillation from one-class embedding. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 9737-9746).
89. Puschner, E., Moos, T., Becker, S., Kison, C., Moradi, A. and Paar, C., 2023, May. Red team vs. blue team: a real-world hardware Trojan detection case study across four modern CMOS technology generations. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 56-74). IEEE.
90. Mahajan, K., Pathak, S., Take, S. and Pawar, C., 2022. Employee Background Verification on Blockchain.
91. Rohemah, R. and Yuliana, R., 2023. Peran Mediasi Internal Fraud Terhadap Kinerja Perbankan. *Jurnal Reviu Akuntansi Dan Keuangan*, *13*(1), pp.70-82.