National College of Ireland

A Novel Approach for Detecting Insider Threats by Combining Behavioural Analytics and Threat Intelligence

Industry Internship
MSc Cyber Security

Fumnanya Umunna
Student ID: X22133071

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:……. Fumnanya Omoniyi Umunna……..

Student ID: …… X22133071 ….……..……

Programme: …… MSc Cybersecurity …… **Year:** …… 1 ….

Module: …… Industry Internship ……..……

Supervisor: ……Vikas Sahni ……..……..……

Submission Due Date: ……5/01/2024……..….

Project Title: …A Novel Approach for Detecting Insider Threats by Combining Behavioural Analytics and Threat Intelligence ……..……

Word Count: ……3828…… **Page Count**……22……...

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: …… Fumnanya Omoniyi Umunna ……

Date: ……4/01/2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Novel Approach for Detecting Insider Threats by Combining Behavioural Analytics and Threat Intelligence

Fumnanya Umunna
X22133071

Abstract

With insider threats posing a formidable risk due to the privileged access and knowledge of organizational infrastructure, traditional security measures often fail to detect such anomalies. The research objectives focus on applying the Isolation Forest Model for anomaly detection, assessing system logs to uncover insider threats, and detecting inconsistencies in user activities. The primary research question investigates the integration of behavioural analytics with threat intelligence to improve insider threat detection within corporate environments. The methodologies adopted address the dynamic nature of these threats by utilizing machine learning and behavioural analytics to discern anomalies in user behaviour. The application of deep learning approaches, specifically the Deep Isolation Forest methodology, demonstrates significant advancements in this field. The solution entailed a systematic approach, utilizing anomaly scores to flag potential insider threats. Visualizations of user-PC interactions, file transfer frequencies, and logon/logoff activities were generated, highlighting users with irregular behaviours. An integrated threat assessment combined these varied data points to provide a comprehensive risk analysis.

1 Introduction

In the contemporary era of technological advancements, securing organizational data has become paramount. This research delves into the complex field of cybersecurity, particularly focusing on the detection of insider threats. The primary aim is to enhance the detection of insider threats by amalgamating behavioural analytics with threat intelligence. The objectives target anomaly detection, analysis of system logs, and inconsistencies in different user behaviours. This chapter sequentially covers the background of the issue, defines the research problem, states the research aims and objectives, and then concludes with a brief chapter summary.

1.1 Background

While digitisation has been quite fast in the last years information systems have been exposed to multiple cyber related threatens shown by Alsowail and Al-Shehari (2021). Insider attacks are one among many other concerns regarding this vulnerability that cuts through the public and private sector. There is what one can call internal threats that come from legitimate individuals that are in an organizational frame work hence they can cause extensive damages that affect the infrastructure of that organization as well as the reputation. According to Glasser and Lindauer (2013), the difficulties involved in obtaining original material

necessary for forward movement on the subject call for the use of fabricated information as an appropriate substitute.

In particular, the two instances of 2018 and 2019 constitute real-world implications of an insider's threat. For instance, recently, a security engineer of Facebook lost his job because of the accusation that he used authorised access to obtain confidential data which were not approved by him.[1] As a result, this engineer used those private details for stalking women in social media. Concurrently, another event involving a Tesla employee occurred that made him guilty of tampering with the organization's security network as well as passing classified details onto unauthorized third parties.[2]

In addition, 2019 was marked by another major cyber-attack at Capital one whose AWS cloud services were accessed by a former amazon worker who used his knowledge of amazon ec2 to devise a way to penetrate through capital one's cloud services weakly secured.[3] Therefore, this malefactor managed to retrieve over 100 million customer record, leading to a massive breach.

In 2020, a former Google official involved in the company's self-driving car branch was sentenced to 18 months in prison for stealing trade secrets (Statt, 2020). It became worse when the stolen trade secrets were conveyed to his new employer, which is none other than Uber. Hence, such empirical situations prove the significance of detection instruments that Legg et al. (2015) point out for minimizing great consequences from insiders.

1.2 Problem definition

Despite robust defences against external attacks, insider threats pose a formidable challenge. This is due to their ability to operate within the organization and their intimate knowledge of the infrastructure (Bhavsar & Trivedi, 2018). Traditional security measures like firewalls often prove ineffective against insider threats. Anju et al. (2023) underscore the complexities of detecting insider threats, citing uneven data, evolving user behaviour, and limited ground truth as significant hurdles.

This research primarily builds upon the CERT Division's synthetic insider threat test dataset specifically Version 3.2, as developed by Glasser and Lindauer.[4] This dataset provides insights into user activity, device connections, and psychological traits. Our research leverages the Isolation Forest Model to detect anomalous behaviors and identify potential insider threats. Liu et al. (2018) delivered a comprehensive examination of insider threats, focusing on the challenges posed by privileged network users. They categorized these threats into traitors, masqueraders, and unintentional perpetrators, providing valuable data analytics-based countermeasures. Detecting insider threats efficiently and promptly remains a crucial

[1] https://www.nbcnews.com/tech/social-media/facebook-investigating-claim-engineer-used-access-stalk-women-n870526
[2] https://www.forbes.com/sites/forbestechcouncil/2018/07/19/what-teslas-spygate-teaches-us-about-insider-threats/
[3] https://www.cnbc.com/2019/07/30/capital-one-hack-allegations-describe-a-rare-insider-threat-case.html
[4] https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247?file=24856979

challenge. Our research aims to fill existing knowledge gaps and augment current countermeasures by utilizing the CERT dataset and the Isolation Forest Model.

1.3 Research Question

The main question driving this research is:
To what extent can behavioural analytics be amalgamated with threat intelligence to bolster the identification of insider threats within corporate settings?

The primary aim of this research is to augment the detection of insider threats by singling out potential insiders infringing on confidential data access protocols and bypassing the least privilege principle. The objectives focus on three areas:

1. Application of the Isolation Forest Model for detecting anomalies.
2. Assessment of system logs as a technique for uncovering insider threats.
3. Detection of inconsistencies in logon patterns, device use, and file transfer activities.

1.4 Rationale of Research

Insider threats remain a substantial worry for many businesses, organisations, and governmental entities (Nurse et al., 2014). Despite its significance, the cyber sector lacks a unified framework for understanding this threat in depth. Addressing this gap, our study combines behavioural analytics with threat intelligence, aiming to provide a holistic framework, informed by empirical evidence, to characterise and combat these threats. Raval et al. (2018) showcased how machine learning methods, specifically in analysing USB device events and user login patterns, yielded promising results in anomaly detection.

1.5 Significance of Study

The significance of this research is multi-fold. As highlighted by empirical studies demonstrating the increasing prevalence of insider threats, such as the work of (Liu et al., 2018), the need for robust detection mechanisms becomes even more critical. Similarly, the extended Isolation Forest algorithm has proven to be highly efficient in identifying abnormal user behaviours, even without the need for prior examples of anomalies (Sun et al., 2016). Moreover, Xu et al. (2023) unveiled the potential of a deep isolation forest, revealing its superiority over standard isolation-based methods across diverse datasets.

The subsequent chapters delve into the research conducted on insider threat detection using behavioral analytics and threat intelligence. The research methodology employed is explored, followed by the design specifications for the proposed solution. Subsequently, the implementation process is delved into, and the results obtained are evaluated. Finally, the findings are concluded, and future research directions are discussed.

2 Related Work

The magnitude of insider threats has been underscored with the increasing frequency and magnitude of cybersecurity breaches. Recognising these threats and their potential repercussions is pivotal, as (Liu et al., 2018) highlighted, showing cyber insider threats affecting 20% of organisations. This paper aims to thoroughly investigate the ways in which

threat intelligence and behavioural analytics, particularly the Isolation Forest Model (Sun et al., 2016), can work together to enhance the efficacy of insider threat detection. (Aldairi, Karimi, and Joshi, 2019) provide a compelling example of unsupervised learning, which detected 91% of internal threats, underscoring the promise and pertinence of this research's objectives. By amalgamating behavioural data with threat intelligence, this study endeavours to address the existing research vacuum in detecting potential insiders accessing confidential data, ensuring the safeguarding of organisational assets.

2.1 Historical Context of Insider Threats

The concept of insider threats is not novel, yet its interpretation has evolved substantially, especially since the digital age began. In the past, insiders were thought to be those with authorised access to the system who would abuse their position (Sun, Y., Xu, H., Bertino, E., & Sun, C., 2016). Modern computational strategies, such as context-aware computing, attempt to detect these threats by analysing user behaviour across different modalities like device usage, resource access, and communication patterns (Memory, A., Goldberg, H. G., & Senator, T. E., 2013). As technologies advanced, so did the complexities of these threats, requiring more nuanced detection methodologies. For instance, in the digital age, not all malicious behaviours breach security rules, making predefined regulations insufficient. Instead, a data-driven approach, considering both group patterns and individual routine patterns, is now essential for robust insider threat detection (Sun et al., 2016). This evolution highlights how important it is to update threat detection techniques on a regular basis in order to handle the difficulties brought about by technological advancements.

2.2 Characteristics and Nature of Insider Threats

Insider threats remain a daunting challenge for businesses and governmental organisations, evident in both empirical surveys and academic discourse (Nurse et al., 2014). Despite the vast knowledge, a unifying framework to decipher the complexity of insider attacks remains elusive. Nurse et al. (2014) proposed a framework underpinned by real-world cases, existing literature, and pertinent psychological theories, emphasising not only the technical and behavioural indicators of attacks but also delving into the attackers' motivations. These reasons could be anything from malevolent intent to unintended human error that unintentionally jeopardises security. Moreover, the dynamic nature of insider threats is emphasized in a research paper by Greitzer and Purl (2022). They discovered that indicator values change over time, and the threat level from multiple indicators doesn't always increase when the number of indicators rises. As a result, this complexity emphasizes the significance of a multifaceted strategy to insider threat detection and mitigation.

2.3 The Role of Machine Learning in Insider Threat Detection

As the vast amount of data shared across interconnected systems raises concerns about trustworthiness, Behavior-Based Access Control (BBAC) emerges as a prominent approach. Mayhew et al. (2015) advocated for this method, emphasizing the need to assess the integrity of documents and actors. BBAC strategically combines batch processing with real-time stream processing, effectively analyzing various factors to identify malicious activities. This

harmonized approach optimizes detection capabilities, effectively addressing misconduct stemming from network connections and HTTP requests.

Raval et al. (2018) delved into the application of machine learning in identifying insider threats. They examined the launch mechanisms and consequences of insider attacks, showcasing advanced methodologies that integrate psychology, criminology, and game theory. Their research highlighted the ability of machine learning to detect anomalies, particularly in real-world settings where malicious events are infrequent. By applying linear regression, Cook's and Mahalanobis distance to USB device events, and neural networks and support vector machines to login activities, they achieved precise anomaly detection. This precision, combined with future approaches merging natural language processing and behavioural analysis, demonstrates the transformative potential of machine learning in tackling insider threats.

2.4 Behavioural Analytics and Anomalous User Behaviour Detection

Behavioural analytics is a pivotal tool in the field of information security, primarily for its ability to identify deviations in routine user patterns, thus signalling potential insider threats. The identification of abnormal user behaviour is a crucial part of many security systems, including intrusion detection and authentication systems (Sun, L., Versteeg, S., Boztas, S., & Rao, A., 2016). Sun et al. (2016) presented an extended version of the Isolation Forest algorithm, highlighting its efficiency in detecting anomalies without needing example anomalies during training. Their enterprise-focused research substantiates that anomalous instances can be isolated effectively using singular or combined features.

Prarthana and Gangadhar (2017) highlighted the limitations of traditional security mechanisms in detecting anomalies, emphasizing the role of User Behaviour Anomaly Detection (UBAD). By utilizing a multidimensional statistical test and an OLAP Cube data model, they demonstrated enhanced statistical accuracy in detection as the dimensionality increases, backed by significant improvements in true negative and positive rates with real-life log data. Savenkov and Ivutin (2020) recommended the implementation of machine learning in UEBA/DSS systems to overcome the challenges of handling large, unstructured datasets and enhance data analysis quality. By highlighting behavioral biometric traits, this study promotes data-driven, informed decision-making in the cybersecurity domain.

2.5 Deep Learning Approaches and Their Advancements

Deep learning has proven instrumental in enhancing cybersecurity, particularly in detecting insider threats. Deep isolation forest, a notable evolution from the traditional iForest, facilitates high freedom of partition in the original data space, leading to improved anomaly detection (Xu et al., 2023). Notably, deep isolation forest addresses the linear axis-parallel isolation challenges inherent in the traditional iForest, which sometimes resulted in high false negative errors. The methodology employs casually initialised neural networks, mapping original data into random representation ensembles, offering a unique synergy between random representations and partition-based isolation.

Anju et al. (2023) showcased the effectiveness of deep learning in insider threat detection using an anomaly-based approach with the Computer Emergency Response Team (CERT) dataset. Their model highlighted how thefts, web application attacks, and other malicious actions, when perpetrated by authorised users, could result in devastating impacts. Through unsupervised learning and deep learning techniques, their study was able to extract behavioural traits from historical data, substantially enhancing the detection of insider threats.

Yet, for all its merits, the application of unsupervised learning for insider threat detection is not without challenges. Aldairi et al. (2019) examined the CERT insider threat dataset and presented an unsupervised anomaly detection model. Their study underscored the importance of trust scores derived from previous anomaly cycles, showcasing a novel introduction of considering users' psychometric scores in the insider threat detection paradigm. Results confirmed the proposed approach's superiority over traditional methods, with significant improvements in accuracy and actionable intelligence (Aldairi et al., 2019).

2.6 Challenges in Detecting and Preventing Insider Threats

Detecting and countering insider threats are multifaceted challenges, considering the privileged access these individuals possess (Liu et al., 2018). Liu et al. (2018) categorised insiders into three distinct types: traitor, masquerader, and unintentional perpetrator. Addressing these threats requires a robust understanding of each category's behavioural nuances. From a data analytics perspective, countermeasures range from host, network, to contextual data-based approaches, with unique strengths and weaknesses inherent in each.

Yuan and Wu (2021) further outlined the complications of detecting insider threats, citing issues like high-dimensionality, heterogeneity, sparsity, and the innate adaptive nature of insider threats. While deep learning models exhibit enhanced performance in insider threat detection over traditional machine learning models, they identified challenges like lack of labelled data and adaptive attacks that still remain. The subtle behaviour differences between insiders and typical users can make detection particularly challenging, emphasising the need for future research directions that can surmount these obstacles (Yuan & Wu, 2021).

2.7 Conclusion of the Literature Review

The literature review highlights the growing potential of deep learning to enhance insider threat detection, with deep isolation forests showing promise over traditional iForest. Yet, detecting and preventing insider threats remains a complex task, compounded by the diverse nature of insider categories and their subtle behaviours. This multifaceted challenge underscores the need for further research to address the challenges of high-dimensional data and the nuances of insider threats. Future studies must strategically bridge these gaps, improving the accuracy, efficiency, and reliability of insider threat detection mechanisms.

Table 1: Summaries of Studies Included in the Review

Paper	Strengths	Limitations
Aldairi et al. (2019)	- Investigates unsupervised anomaly detection algorithms - Introduces trust and	- Comparison limited to CERT dataset

	psychometric scores	
Anju et al. (2023)	- Uses unsupervised deep learning - Focuses on historical data for behavior trait extraction	- May not address real-time threat detection
Greitzer and Purl (2022)	- Studies dynamic nature of insider threat indicators - Uses expert knowledge elicitation	- Temporal effects and interactions may not cover all threat scenarios
Liu et al. (2018)	- Categorizes insider types - Reviews countermeasures from data analytics perspective	- Early-stage threats may not be well represented
Mayhew et al. (2015)	- Combines big data processing for trustworthiness measurement	- Focuses primarily on mal-behavior detection, which may not cover all insider threat activities
Memory et al. (2013)	- Focuses on context-aware detection across multiple modalities	- Challenges in achieving identity-aware and privacy-preserving methods
Nurse et al. (2014)	- Proposes a framework grounded in real-world cases and psychological theories	- Framework may not be easily adaptable to all organizational environments
Prarthana and Gangadhar (2017)	- Develops multidimensional anomaly detection - Improved statistical efficiency with dimensionality	- Higher computational cost for increased dimensionality
Raval et al. (2018)	- Showcases anomaly detection with advanced statistical and machine learning techniques	- Future directions needed for integrating natural language processing and behavioral analysis
Savenkov and Ivutin (2020)	- Proposes methods for navigating large, unstructured datasets	- Focuses on behavioral biometrics, which may not capture all types of insider threats
Sun et al. (2019)	- Presents an efficient extended Isolation Forest algorithm	- Efficiency tested primarily in enterprise datasets
Sun et al. (2016)	- Introduces a data-driven evaluation model - Uses probabilistic methods for anomaly detection	- Grouping and routine patterns may not account for sophisticated threat actors
Xu et al. (2023)	- Utilizes neural networks for improved anomaly detection	- Improvements demonstrated over state-of-the-art methods may not translate to all use cases
Yuan and Wu (2021)	- Surveys deep learning for insider threat detection - Identifies enhancements over traditional methods	- Lacks discussion on implementation in varied and complex real-world scenarios outside of common datasets

Based on the above review of different papers, it was concluded that the isolated forest technique is the best for this work.

3 Research Methodology

This chapter outlines the methodology employed to address the primary research question and the aim is to detect insider threats by identifying potential insiders accessing confidential information without adhering to the least privilege principle. Specifically, the objectives stated in first chapter.

3.1 Research Design

Given the research's positivist paradigm (Park et al., 2020), the nature of this study is quantitative. The positivist paradigm aligns with the study as it seeks objective and empirical evidence, viewing reality as objective and unchanging (Bryman, 2017). This paradigm's choice is justified, considering the research aims to quantify irregularities in log files and detect anomalies, best approached through quantitative methods.

3.2 Dataset

The dataset comes from the CERT Division, produced in partnership with ExactData, LLC, and sponsored by DARPA I2O. The synthetic insider threat test dataset was chosen because of its comprehensive representation of user activities (Lindauer, 2020).[5]

3.3 Data Processing

Prior to analysis, it was essential to clean the data by identifying missing values, outliers, and inconsistencies. Outliers and missing values can distort results, compromising the validity of the findings (Kwak & Kim, 2017). The process ensures a higher degree of accuracy in the results.

For the model to process the data, transformation techniques, such as normalization, encoding, and scaling, was employed (Potdar et al., 2017). This step ensures that data was in a format suitable for the Isolation Forest Model, enhancing the model's accuracy and efficiency. Feature engineering further enhances this process, focusing on factors like user logon patterns, device usage, file transfers, and the five-factor model of personality dimensions (Zheng & Casari, 2018).

3.4 Feature Engineering

3.4.1 Log_on_off_stats

After-hour logins can act as potential red flags signalling potential unauthorized access (Glasser & Lindauer, 2013). Monitoring user logon and logoff activities using the data from the Logon.csv file offers critical insights into user behaviour (Liu et al., 2018). By tracking these statistics, researchers can detect deviations from normative patterns, strengthening the efficacy of insider threat detection (Alsowail & Al-Shehari, 2022).

[5] https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247?file=24856979

3.4.2 Device_disconn_stats & Device_conn_stats

The connection and disconnection patterns of devices, as captured in the Device.csv file, can reveal potential threats (Greitzer & Purl, 2022). Analyzing such patterns can unmask anomalies, like frequent connections of unauthorised thumb drives which may be indicative of data exfiltration attempts (Zheng & Casari, 2018).

3.4.3 File_stats_new

File transfers to removable devices, as represented in File.csv, are pivotal in understanding potential unauthorized data exfiltration (Sun et al., 2016). Identifying large or frequent transfers can act as strong indicators of insider threats, especially if they do not align with an employee's regular duties (Anju et al., 2023).

3.4.4 Psychometric_users_tidy

The five-factor model is a widely recognized psychological metric offering insights into an individual's behaviour and tendencies (Kwak & Kim, 2017). By using Big 5 psychometric scores from the Psychometric.csv file, this research integrates human behavioural analytics into the threat detection process, adding an additional layer of analysis that goes beyond mere system logs (Nurse et al., 2014).

3.4.5 User_pc relationship

Through the introduction of graph analysis, the dynamic relationship between users and PCs can be comprehended (Park et al., 2020). Understanding these relationships is paramount, as irregularities can signal malicious intent or compromised accounts (Raval, et al., 2018).

3.5 Model Selection and Application

The Isolation Forest Model is renowned for its proficiency in detecting anomalies (Xu et al., 2023). Its suitability for this research derives from its ability to isolate outliers, making it apt for identifying insider threats (Aldairi et al., 2019). However, like all models, it comes with its advantages, such as its efficiency in high-dimensional datasets, and limitations, which was critically assessed in the context of insider threat detection (Zhou et al., 2017).

The CERT-generated synthetic dataset divides the input data file into training (80%) and testing (20%) datasets, respectively (Bryman, 2017), in order to make the model more robust during classification. Furthermore, parameter tuning and optimization techniques applied during the training enhance the model to have greater predictive capability (Bolón-Canedo et al., 2013).

Validating the model's accuracy and relevance, a thorough evaluation process was undertaken. This involved employing cross-validation, visual analytics, and an integrated threat assessment to assess the models' robustness, identify patterns, and pinpoint potential threats effectively. These methods were combined to provide a thorough understanding of the model's capabilities and the nuances of insider threats.

3.6 Limitations and Assumptions

The study utilizes a synthetic dataset (r3.2) from CERT, which can introduce biases. Zheng and Casari (2018) recommend understanding dataset characteristics before using them for machine learning. Dataset biases may result from the creation process (Bolón-Canedo et al., 2013). While processing log files, certain assumptions were made to extract features. Khalid et al. (2014) and Potdar et al. (2017) supported these processes; however, they might limit the analysis' robustness. The study's applicability is limited to scenarios similar to those shown in the dataset (Bryman, 2017). Real-world datasets may differ from synthetic ones.

3.7 Ethical Considerations

Ethical concerns arise in managing vast amounts of data. Synthetic datasets mirror real-world scenarios, so user privacy and potential misuse of data are pivotal. This research strictly adheres to ethical guidelines and removes personally identifiable information (Park et al., 2020; Glasser & Lindauer, 2013). However, the potential for misuse of research findings exists, so users and practitioners must employ them ethically (Alsowail & Al-Shehari, 2022).

3.8 Summary of the Chapter

The methodology adopted in this research, seeks to answer the primary research question regarding the enhancement of insider threat detection within organisations. It uses version 3.2 of the CERT synthetic dataset to identify anomalies in behavioural patterns (Glasser & Lindauer, 2013; Zhou et al., 2017). These anomalies are then passed through the Isolation Forest Model, a machine learning algorithm that can detect potential insider threats (Xu et al., 2023).

The methodology's relevance stems from its alignment with the overarching aim and objectives. By focusing on anomalies in logon, device usage, and file transfer activities, the study aligns closely with current academic dialogues on the subject (Memory et al., 2013; Yuan & Wu, 2021).

4 Design Specification

This chapter explores the meticulous design specifications instrumental in detecting potential insider threats. The architecture presented underpins the complex methodology employed in threat identification through the lens of data acquisition, preprocessing, and advanced analytics.

4.1 Data Acquisition and Preprocessing

The research utilises the CERT synthetic dataset, which exceeds 20GB and comprises various system log files. These logs detail user interactions, such as logons and devices, accompanied by timestamps. The raw data undergo preprocessing to distil essential attributes for feature construction, pivotal for isolating behavioural anomalies (Deokar & Hazarnis, 2012).

4.2 Anomaly Detection Model

The Isolated Forest Algorithm operates on custom settings, with user-PC interaction thresholds fixed at 40, marking a critical point for anomaly identification (Lesouple et al.,

2021). An anomaly score below zero pinpoints potential threats, as delineated in the model's results.

4.3 Flowchart

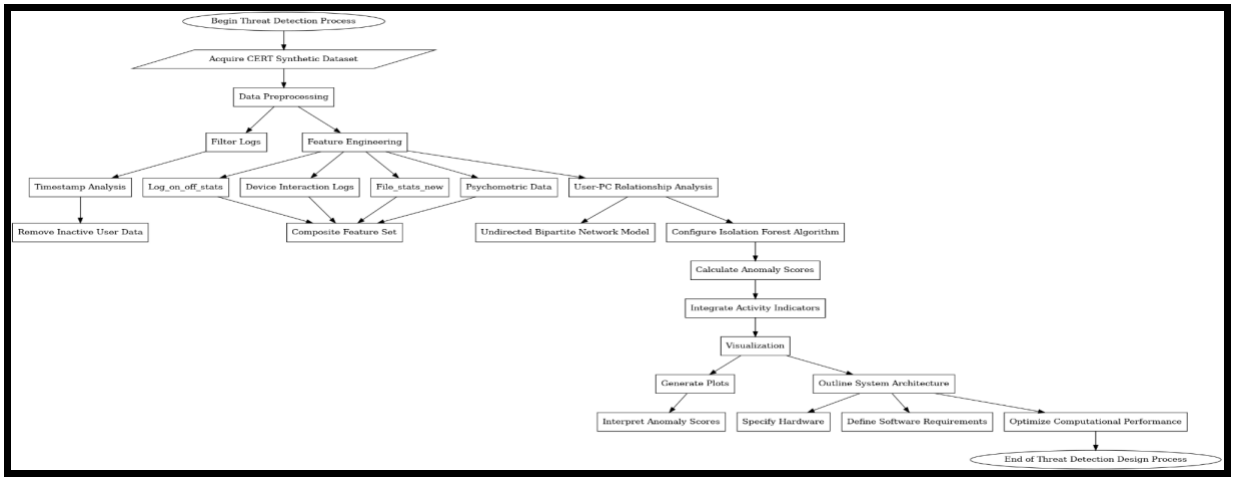

Figure 1: Flowchart

4.4 System Architecture

The architecture encompasses all system components and delineates the data flow, specifying both hardware and software requirements, ensuring the system is equipped to handle large datasets and complex analytical processes efficiently (Bitincka et al., 2010).

4.5 Performance Considerations

Efficiency in managing large data volumes is paramount, with strategies employed to enhance computational performance in feature extraction and modelling, crucial for real-time threat detection.

5 Implementation

In the final stage of the implementation of the insider threat detection system, it focused on the aspects of data processing, model development, and result visualisation. This was achieved by utilising Python and Google Colab, tools known for their efficiency in handling and analysing large datasets (Saxena et al., 2020; Sav and Magar, 2021). The detailed findings and results of this phase will be presented and thoroughly discussed in the subsequent chapter on evaluation and discussion of results.

The journey commenced with the acquisition of the CERT synthetic dataset, symbolized by a parallelogram denoting data input/output. This step, labelled "Acquire CERT Synthetic Dataset," set the foundation for subsequent processes. The seamless arrow from the start of the flowchart to this data acquisition step highlighted the initiation of the threat detection process. The subsequent rectangular block, labelled "Data Preprocessing," represented a pivotal process step. Sub-processes, namely "Filter Logs," "Timestamp Analysis," and "Remove Inactive User Data," unfolded sequentially, emphasizing the meticulous cleaning and transformation of data. This phase adhered to established techniques, including normalization and encoding, to ensure the dataset's readiness for model application (Liu et

al., 2018). A crucial facet of the implementation phase was feature engineering, visualized by another rectangular block labelled "Feature Engineering." The subsequent branches for distinct feature types, such as "Log_on_off_stats," "Device Interaction Logs," "File_stats_new," and "Psychometric Data," illustrated the diverse dimensions considered in the model. These features were strategically engineered in alignment with recommended approaches, enhancing the system's ability to detect insider threats (Alsowail and Al-Shehari, 2022; Nurse et al., 2014). The subsequent process, represented by the block "User-PC Relationship Analysis," underscored the exploration of user-PC dynamics. This step, connecting to a symbol representing an "Undirected Bipartite Network Model," showcased a sophisticated analysis of relationships within the dataset. The implementation then delved into configuring the Isolation Forest Algorithm, illustrated by a rectangle labelled "Configure Isolation Forest Algorithm." The flowchart seamlessly transitioned to the subsequent step, "Calculate Anomaly Scores," highlighting the critical nature of anomaly detection in identifying potential insider threats (Aldairi, Karimi, and Joshi, 2019). The process seamlessly continued with the "Integration of Activity Indicators," a rectangular block emphasizing the amalgamation of insights from "Log_on_off_stats," "Device Interaction Logs," and "Psychometric Data." The arrows symbolizing data flow underscored the interconnectedness of these indicators in bolstering threat detection. Visualizing anomaly scores emerged as a key aspect, depicted by a rectangular block labelled "Visualization." Sub-processes like "Generate Plots" and "Interpret Anomaly Scores" exemplified the role of visual representation in understanding and interpreting the model results. This step, executed using Python's matplotlib and seaborn libraries, enriched the interpretation process (Legg et al., 2015; Mayhew et al., 2015). The flowchart then transitioned to the "System Architecture" phase, represented by a rectangle labelled "Outline System Architecture." Sub-processes such as "Specify Hardware" and "Define Software Requirements" highlighted the comprehensive planning involved in establishing a robust system architecture. Efficiency considerations were addressed in the subsequent step, depicted by a rectangle labelled "Optimize Computational Performance." Connections to steps like "Feature Extraction" and "Modelling" underscored the importance of optimization in handling large datasets efficiently (Luengo et al., 2020). The flowchart concluded with an oval shape labelled "End of Threat Detection Design Process," signifying the completion of the intricate process designed to enhance insider threat detection.

A flowchart was used to organise the insider threat detection system development process, encompassing data processing, feature engineering, model development, and results visualization. The flowchart clearly depicted the workflow and relationships between the various components, facilitating a seamless execution.

6 Evaluation

This research combines behavioural analytics and threat intelligence to develop a more effective method for detecting insider threats within corporate environments. The isolation forest model was specifically chosen for this task and evaluated using the CERT dataset. The results show the model is accurate in detecting anomalies in system logs, logon patterns, and file transfer activities, which suggests that it can be used to detect and prevent insider threats.

6.1 Model Results

This section presents the critical analysis of anomaly scores produced by Isolation Forest Algorithm useful to identify potential insider threats within a corporate domain. The aforementioned threat refers to those users that their interactions with the PCs are anomalous.

6.1.1 User-PC Relationship Analysis

The User-PC Relationship Analysis is illustrated in Figure 2, where a threshold of interactions is set at 40, based on a research rate by Greitzer and Purl (2022). Users with 55 interactions or higher, such as LWB0078, are flagged as anomalies. Table 2 depicts negative anomaly scores (ascores) for users whose behaviour deviates from the established norms. AJR0231, with an ascore of -0.227213, stands out as the most anomalous, indicating a higher probability of malice. This aligns with the findings of Aldairi et al. (2019), who confirmed the effectiveness of unsupervised anomaly detection in such investigative settings.

Table 2: Anomaly Score for User-PC Relationship

User	ascore
AJR0231	-0.227213
ALC0100	-0.153243
BGZ0902	-0.242321
CGH0088	-0.144462
LWB0078	-0.342761

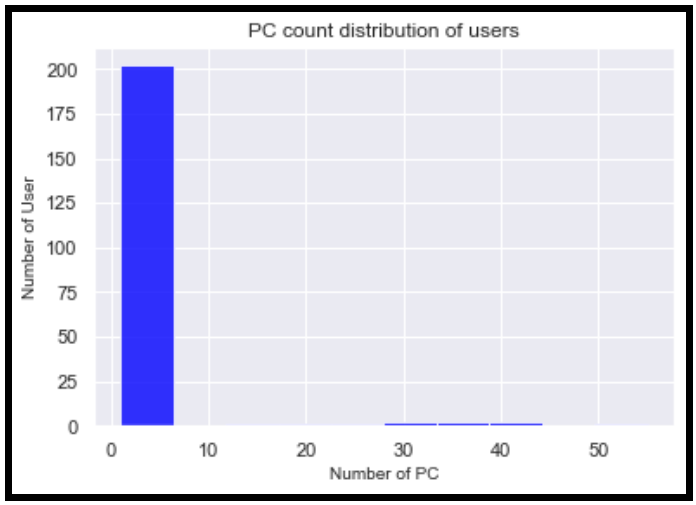

Figure 2: PC Count Distribution of Users

6.1.2 Device/File Transfer Analysis

In the evaluation of device and file transfer activities, Table 3 provide a dual perspective on user behaviour. The outlier suggests behaviour that may be inconsistent with expected use, potentially indicative of malicious intent or a breach in protocol.

Table 3: Anomaly Score for Device/File Transfer Analysis

User	ascore
AJQ0376	-0.027424
BCP0247	-0.010455

BMS0057	-0.084555
...	...
SBM0063	-0.094124
WXW0044	-0.014448
ZBL0379	-0.115604

Table 2 complements these findings by providing anomaly scores for device and file transfer interactions. Users such as "AJQ0376" and "WXW0044" present negative ascores, albeit relatively minor deviations, while "ZBL0379" stands out with a score of -0.115604, which could point to substantial irregularities in device use or file transfer patterns. This user's ascore, when juxtaposed with the maximum file transfers, reinforces the anomaly detected and underscores the necessity for further examination.

The combination of file transfer frequency and the time frame for device connectivity provides a comprehensive view of user conduct, resonating with Anju et al.'s (2023) strategy to utilise historical data for behavioural analysis. The integration of these methods presents a robust approach to insider threat detection, ensuring that potential risks are not merely identified but also evaluated within the broader context of user activity patterns.

6.1.3 Logon/Logoff Activity Analysis

The analysis of logon and logoff activities, as presented in Table 4, has identified a series of users exhibiting anomalous patterns in their usage of system resources. This scrutiny, focusing on the maximum, minimum, mode, and average timeframes for user logon and logoff activities, has revealed significant deviations from normal behaviour, indicative of potential insider threats.

Table 4: Anomaly Score for Logon/Logoff

User	ascore
AJR0231	-0.010307
BCP0247	-0.007238
BMS0057	-0.103316
CAE0080	-0.013561
CQS0899	-0.115045
QKA0388	-0.020668
RAC0058	-0.001421
RAW0533	-0.072573
SBM0063	-0.61513
VLB0069	-0.052415

A detailed examination of individual users shows varied degrees of anomaly scores (ascores), which are crucial in determining the level of suspicion associated with each user:

- AJR0231, with an ascore of -0.010307, displays slightly longer than average logon durations. Although not a significant outlier, this user's activities merit continued observation for any further deviations.

- BCP0247's ascore of -0.007238 similarly suggests marginally extended logon periods. This pattern, while not immediately alarming, could become significant if correlated with other abnormal activities.
- BMS0057 stands out with the highest negative ascore of -0.103316, indicating substantially shorter logon durations. This anomaly is a red flag for potential unauthorized access or deliberate evasion attempts and warrants immediate and thorough investigation.
- Users like CAE0080 and QKA0388, with ascores of -0.013561 and -0.020668 respectively, also show slightly longer logon durations. These users should be monitored for any further unusual activities.
- CQS0899, with an ascore of -0.115045, exhibits one of the most concerning patterns, mirroring the concerns raised for BMS0057. This user's behaviour suggests significantly brief logon durations, necessitating urgent investigation.
- RAW0533 and SBM0063, with ascores of -0.072573 and -0.061513, respectively, present alarming patterns. RAW0533's significantly longer logon durations and SBM0063's extremely short durations are indicative of potential misuse or compromised credentials.
- VLB0069, with an ascore of -0.052415, mirrors the patterns observed in AJR0231, BCP0247, CAE0080, and QKA0388, requiring monitoring in conjunction with other suspicious activities.

To summarize, the analysis of logon/logoff activity successfully identified several users with anomalous data access patterns. Further investigations are crucial, particularly for users with the most pronounced anomalies, such as BMS0057, CQS0899, RAW0533, and SBM0063. This aligns with the recommendations of Mayhew et al. (2015), who emphasize the importance of logon/logoff patterns in assessing user trustworthiness and detecting potential insider threats. These findings are instrumental in strengthening security measures and safeguarding system integrity.

6.1.4 Psychometric Evaluation

The psychometric evaluation in Table 3 provides valuable insights into user behaviours that may pose security risks. The Big Five personality traits, also known as OCEAN, are used to assess these behaviours. An anomaly score of -0.057603 for user GGK0375 suggests behavioural tendencies that may not align with the organization's security standards. This could indicate lower conscientiousness or agreeableness, which could contribute to insider threats, according to Nurse et al. (2014).

Table 5: Anomaly Score for Psychometric Evaluation

User	ascore
BZK0095	-0.070558
JAB0249	-0.050925
JTB0079	-0.026172
...	...
ACL0394	-0.018298

YSB0779	-0.008631
GGK0375	-0.057603

Other users, like JAB0249 with an ascore of -0.050925 and BZK0095 with -0.070558, also demonstrate significant deviations from the norm. These scores potentially reveal personality aspects that, when combined with other factors, could signal a propensity for actions that pose security threats. For example, a low score in conscientiousness paired with high neuroticism might result in impulsive and risky behaviour, warranting closer monitoring and intervention.

Conversely, users with less negative scores, such as ACL0394 and YSB0779, may still require attention but do not immediately stand out as high-risk based solely on their psychometric evaluation. However, it is crucial to consider these scores in the context of other behavioural data and not in isolation. Collectively, these psychometric assessments contribute to a multi-faceted approach to insider threat detection. They allow for a more nuanced understanding of user behaviour that extends beyond mere system interactions, highlighting the importance of psychological profiling in comprehensive security strategies.

6.2 Integrated Threat Assessment

In this integrated threat assessment illustrated on Table 6 are detailed datapoints including a visual line plot representation in Figure 4 present an insightful perspective of organizational potential threats. This approach conforms to Sun et al.'s (2016) emphasis on the strong model of anomaly detection that needs a combination of individual together with joint parameters.

Table 6: Integrated Threat Assessment

User	ascore
ACL0394	-0.017909
AJR0231	-0.074172
ALC0100	-0.072796
...	...
BCP0247	-0.045768
BGZ0902	-0.035601
ZBL0379	-0.025502

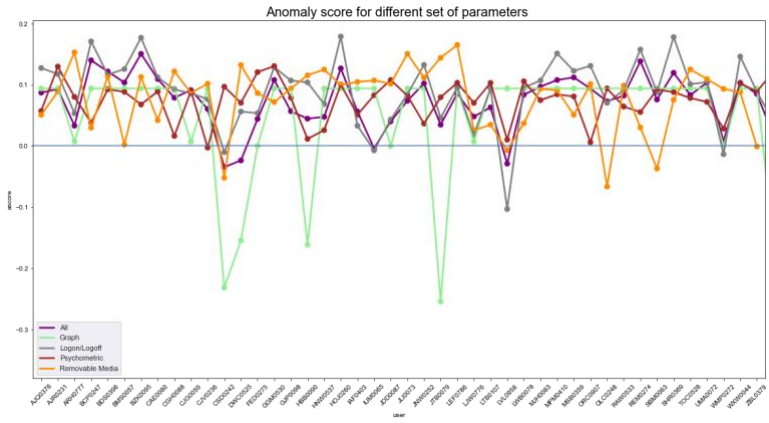

Figure 4: Anomaly Score for Different Set of Parameters

The line graph in Figure 4 reveals how different models contribute to the overall anomaly scores (ascore) of users, with notable deviations indicating potential insider threats. Users such as ACL0394, AJR0231, and ALC0100, for instance, have scores that fall well below the threshold, suggesting significant anomalous activity. The graph and logon/logoff models register sharp variances in scores, reflecting irregular user-PC interactions and concerning logon/logoff behaviours that may point to unauthorized access attempts or misuse of privileges.

The psychometric data, while showing fewer negative scores, still contributes to the integrated assessment, underscoring the importance of psychological factors in predicting potential threat behaviours. Users with consistently low scores across multiple models, such as BCP0247 and BGZ0902, are highlighted as high-risk, corroborating the integrated model's ability to pinpoint individuals who exhibit a pattern of concerning behaviour across various measures.

This integrated analysis is crucial in identifying users who may pose a security risk, and it necessitates further scrutiny. The anomaly scores serve as a quantifiable metric for risk assessment, guiding the focus towards users who consistently display outlier behaviours across all monitored dimensions. The nuanced understanding of these patterns, as provided by the integrated model, is imperative for the proactive management of insider threats. It underscores the need for a vigilant and dynamic approach to security, as advocated by contemporary cybersecurity research.

7 Conclusion and Future Work

This research explored the challenges of identifying insider threats amidst evolving corporate environments. By combining behavioural analytics with threat intelligence, the study sought to uncover potential threats lurking within organizations. The Isolation Forest Model proved effective in identifying anomalous behaviours, raising alarms for potential insider actions. This was achieved by meticulously analysing system logs, logon patterns, device usage, and file transfer activities, successfully fulfilling the research objectives.

Further research should refine this detection method. Implementation of deep learning techniques, as recommended by Yuan and Wu (2021), would further provide an enhancement on user behaviour. Moreover, increasing the basic scrap code used in this study with complex algorithms would give more accurate results.

The research has achieved its objectives and has affirmed an answer to the central question. Although the code used is foundational, it is a stepping stone to new improvements. Just as there are changes in the digital landscape, there should be new ways of securing the environment. his study contributes a vital piece to the complex puzzle of insider threat detection, offering a stepping stone for subsequent endeavours in this critical field of cybersecurity.

References

Aldairi, M., Karimi, L., & Joshi, J. (2019). A Trust Aware Unsupervised Learning Approach for Insider Threat Detection. 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), 89–98.

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. PeerJ Computer Science, 8, e938.

Anju, A., Shalini, K., Ravikumar, H., Saranya, P., & Krishnamurthy, M. (2023). Detection of Insider Threats Using Deep Learning. In 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN) (pp. 264-269). IEEE.

Bhavsar, K., & Trivedi, B. (2018). Predicting Insider Threats by Behavioural Analysis using Deep Learning. International Conference on SAM.

Bin Hamid Ali, F. A. & Yee Yong Len. (2011). Development of host based intrusion detection system for log files. 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), 281–285.

Bitincka, L., Ganapathi, A., Sorkin, S., & Zhang, S. (2010). Optimizing Data Analysis with a Semi-structured Time Series Database.

Bolón-Canedo, V., Sánchez-Maroño, N. & Alonso-Betanzos, A. (2013). A review of feature selection methods on synthetic data. Knowl Inf Syst 34, 483–519.

Bryman, A. (2017). Quantitative and qualitative research: further reflections on their integration. In Mixing methods: Qualitative and quantitative research (pp. 57-78). Routledge.

Deokar, B., & Hazarnis, A. (2012). Intrusion Detection System using Log Files and Reinforcement Learning. International Journal of Computer Applications, 45.

Fagade, T., & Tryfonas, T. (2017). Malicious Insider Threat Detection: A Conceptual Model.

Glasser, J., & Lindauer, B. (2013). Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data. 2013 IEEE Security and Privacy Workshops, 98–104.

Greitzer, F. L., & Purl, J. (2022). The Dynamic Nature of Insider Threat Indicators. SN COMPUT. SN COMPUT. SCI, 3.

Jérôme Kunegis (2015). Exploiting The Structure of Bipartite Graphs for Algebraic and Spectral Graph Theory Applications, Internet Mathematics, 11:3, 201-321.

Khalid, S., Khalil, T., & Nasreen, S. (2014). A survey of feature selection and feature extraction techniques in machine learning. 2014 Science and Information Conference, 372–378.

Kwak, S. K., & Kim, J. H. (2017). Statistical data preparation: Management of missing values and outliers. Korean Journal of Anesthesiology, 70(4), 407–411.

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Caught in the act of an insider attack: detection and assessment of insider threat. In 2015 IEEE International Symposium on Technologies for Homeland Security (HST) (pp. 1-6). IEEE.

Lesouple, J., Baudoin, C., Spigai, M., & Tourneret, J.-Y. (2021). Generalized isolation forest for anomaly detection. Pattern Recognition Letters, 149, 109–119.

Lindauer, Brian (2020). Insider Threat Test Dataset. Carnegie Mellon University. Dataset.

Liu, L., De Vel, O., Han, Q. -L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials, 20(2), 1397–1417.

Luengo, J., García-Gil, D., Ramírez-Gallego, S., García, S., & Herrera, F. (2020). Big data preprocessing. Cham: Springer.

Mayhew, M., Atighetchi, M., Adler, A., & Greenstadt, R. (2015). Use of machine learning in big data analytics for insider threat detection. MILCOM 2015-2015 IEEE Military Communications Conference (pp. 915-922). IEEE.

Memory, A., Goldberg, H. G., & Senator, T. E. (2013). Context-Aware Insider Threat Detection. Workshops at the Twenty-Seventh AAAI Conference on Artificial Intelligence.

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterising Attacks. 2014 IEEE Security and Privacy Workshops, 214–228.

Park, Y. S., Konge, L., & Artino, A. R. J. (2020). The Positivism Paradigm of Research. Academic Medicine, 95(5), 690.

Potdar, K., Pardawala, T., & Pai, C. (2017). A Comparative Study of Categorical Variable Encoding Techniques for Neural Network Classifiers. International Journal of Computer Applications, 175, 7–9.

Prarthana, T. S., & Gangadhar, N. D. (2017). User Behaviour Anomaly Detection in Multidimensional Data. 2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 3–10.

Raval, M. S., Gandhi, R., Chaudhary, S. (2018). Insider Threat Detection: Machine Learning Way. In: Conti, M., Somani, G., Poovendran, R. (eds) Versatile Cybersecurity. Advances in Information Security, vol 72. Springer, Cham.

Sav, U., and Magar, G. (2021). Insider Threat Detection Based on Anomalous Behavior of User for Cybersecurity. Data Science and Security: Proceedings of IDSCS 2020 (pp. 17-28). Springer Singapore.

Savenkov, P. A., Ivutin, A. N. (2020). Methods of Machine Learning in System Abnormal Behavior Detection. In: Tan, Y., Shi, Y., Tuba, M. (eds) Advances in Swarm Intelligence. ICSI 2020. Lecture Notes in Computer Science(), vol 12145. Springer, Cham.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., and Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.

Sun, L., Versteeg, S., Boztas, S., & Rao, A. (2016). Detecting anomalous user behavior using an extended isolation forest algorithm: an enterprise case study. arXiv preprint arXiv:1609.06676.

Sun, Y., Xu, H., Bertino, E., & Sun, C. (2016). A Data-Driven Evaluation for Insider Threats. Data Science and Engineering, 1(2), 73–85.

Xu, H., Pang, G., Wang, Y., & Wang, Y. (2023). Deep Isolation Forest for Anomaly Detection. IEEE Transactions on Knowledge and Data Engineering, 1–14.

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. Computers & Security, 104, 102221.

Zhao, & E. Hovy (Eds.), Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems (pp. 79–91). Association for Computational Linguistics.

Zheng, A. & Casari, A., (2018). Feature engineering for machine learning: principles and techniques for data scientists. " O'Reilly Media, Inc.".

Zhou, L., Pan, S., Wang, J., & Vasilakos, A. V. (2017). Machine learning on big data: Opportunities and challenges. Neurocomputing, 237, 350-361.