[1] **Marshet Tamirat***

[2] **Anteneh Girma**

[3] **Tilahun Melak**

Enhancing Intrusion Detection Systems: A Unified Framework Leveraging User Personality Behavior Analysis to Detect Insider Threats and Social Engineering Attacks through Deep Learning

Journal of Electrical Systems

Abstract: - Insider threats and social engineering attacks (SEAs) pose significant challenges in cybersecurity (CS), often resulting in data breaches and substantial financial losses. Insider actions, whether intentional or unintentional, can lead to severe costs for organizations. Despite the implementation of multiple detection strategies, human errors continue to play a significant role in financial losses and the increased risk of data breaches. Traditional intrusion detection systems (IDS) focus primarily on network and host activities but tend to overlook the critical role of human behavior, which limits their ability to detect insider threats and SEAs effectively. This article proposes a novel and unified detection approach that integrates network detection, host-based detection, and user psychological behavior analysis to enhance IDS performance. The primary objective of this research is to improve the detection capabilities of conventional IDS by incorporating psychometric analysis of user behavior. Using psychological insights of humans and correlating them with cyber threat vulnerabilities, this approach aims to reduce false alarms and increase the accuracy of threat detection. To achieve this, we utilize deep neural networks (DNNs). Our unified detection framework integrates datasets, including threat intelligence and psychometric dataset, to enhance the identification of malicious activities and improve the overall detection performance. We evaluate the effectiveness of our model using accuracy, precision, recall, and F1-score metrics, then comparing our results to those of existing detection models. Our findings demonstrate promising results, highlighting the importance of incorporating psychological factors into threat detection systems to better protect organizational resources from evolving cyber risks. By integrating user behavior analysis with established detection methods, we strengthen the capabilities of traditional IDS. However, given the ever-growing complexity of modern cyber threats, continued innovation in threat mitigation strategies is essential.

Keywords— Intrusion Detection Systems, User Personality Behavior, Insider Threats, Social Engineering Attacks, Deep Learning.

I. INTRODUCTION

The rapid growth of digital networks and the Internet has dramatically changed how organizations function, while also increasing their susceptibility to numerous cyber threats, especially insider threats and social engineering attacks (SEAs). Insider threats are particularly concerning as they can result in significant data breaches and heavy financial losses, positioning them as a major focus in cybersecurity frameworks [1]. As companies increasingly rely on technology for their daily operations, they expose themselves to risks from insiders who may misuse their authorized access to sensitive data [2]. Research revealed that 90% of organizations utilize multiple of technology to detect and counter the various threat and attacks, yet continue to experience difficulties in effective detection [1]. Traditional detection methodologies are insufficient for managing the complex landscape of insider threats, often resulting in expensive false positives and negatives that can disrupt standard business operations [3].

Research indicates that different in personality traits, particularly those classified within the Big Five openness, conscientiousness, extraversion, agreeableness, and neuroticism have a considerable impact on individuals' behaviors related to CS [4] and [5]. For example, individuals who score high on openness are usually more inclined to interact with new and unfamiliar online content, which heightens their risk of falling victim to phishing and social engineering tactics. In contrast, individuals with greater conscientiousness typically exhibit stronger adherence to security measures, thereby making them less vulnerable to manipulation [6], [7] and [8]. To overcome these challenges, this paper suggests a unified threat detection framework that integrates user psychometric behavior analysis with existing network-based and host-based detection systems. By employing deep learning techniques, the proposed framework seeks to enhance the performance of insider threat detection. The main objective is to enhance threat detection that addresses insider threats and SEAs.

[1] Adama Science and Technology University, Marshet.Tamirat@astu.edu.et
[2] PhD,University of the District of Columbia, Anteneh.Girma@udc.edu
[3] PhD, Adama Science and Technology University, Tilahun.Melak@astu.edu.et

II. RELATED WORKS

2.1 Overview of Threat Detection approaches

Existing systems for detecting threats focus on either network or host operations, contributing to significant blind spots regarding insider threats. Studies have shown that conventional methods often result in high rates of false positives and negatives [9]. The majority of organizations use CS tools such as firewalls, intrusion detection system (IDS), and electronic access controls to safeguard data from both external threats and potentially malicious insiders [10]. However, those existing detection methods are not efficient in the insider scenario as the insiders have special characteristics and privileges, they can access both physical and logical network resources [1], [11] and [10]. Following is the main contributions of this paper and how it differs from earlier works. In order to describe the challenges that come with detecting insider threats and SEAs, we first explore and analyze a variety of threat and attacks detection methods including ML and DL approaches. Then a comprehensive behavioral analysis method will introduce. Second, as far as we know, this proposed comprehensive insider behavior analysis is the first approach that combines the network and host behavior of insiders to make a robust threat detection method.

2.2 Cybersecurity and Insiders

CS has become a global concern as it is a safeguard to organizations' networks [12]. The Internet has enforced organizations to rely on it, and as a result, most economic, commercial, social, and governmental activities and communication among organizations are handled over it. Organizations use different security countermeasures including technical, physical, and administrative controls [13]. CS provides computer systems, networks, programs, and data, from internal and external attacks [14]. It involves utilizing technological products, procedures, and practices to block unauthorized access to these assets [15]. In the context of CS, a threat is defined as a potential event, whether intentional or unintentional, that has the capacity to negatively impact the security of systems and data [15]. Threats can stem from various origins, including malicious actors, system vulnerabilities, and insider of organizations employees [11]. The move to a hybrid work environment makes the insider risk the most challenging ever before in the CS landscape [1].

2.3 Threat and Attacks

A threat in CS is any potential risk that can exploit vulnerabilities within a digital asset. It can manifest as an event, or individual capable of compromising the confidentiality, integrity, or availability of digital resources [16] and [1]. It can be deliberately or unintentionally originated from insiders or deliberately by external attackers [2], [9], and [13]. However, attack is an actual exploitation of vulnerabilities to compromise digital resources, involves the execution of a threat with the intent to gain unauthorized access, then steal data, disrupt services, or damage systems [17] and [18]. Attacks including malware infections, phishing, denial-of-service (DoS) attacks, SEA, and more [11], [19], [18] and [20]. Individuals with authorized access to an organization's network or systems, such as contractors, authorized personnel, or employees, are the source of internal threats. On the other hand, outside threats originate from outside sources and are usually initiated by hackers or attackers who aim to obtain unauthorized access or take advantage of weaknesses [17].

2.4 Internal and External Threat and Attacks

Internal threats originate from insiders within an organization who possess privileged access and have the potential to facilitate external attacks [7]. Insiders can engage in malicious activities such as stealing sensitive information, sabotaging systems, or collaborating with external attackers [1]. Insider attacks involve insiders carrying out malicious actions against their own organization, which may include exploiting vulnerabilities, leaking confidential information, or disrupting operations [21]. On the other hand, external threats arise from individuals or groups outside the organization who attempt to gain unauthorized access [22]. External attacks refer to the deliberate acts of malicious entities targeting an organization from beyond its boundaries, encompassing techniques like phishing, ransomware, or DDoS attacks [23]. In essence, a cyber-attack is a deliberate action aimed at compromising the security, integrity, or availability of digital systems and can be executed by both internal and external actors, utilizing various techniques such as SEA and phishing attacks [24]. Cybersecurity needs a continual improvement, for detecting, preventing, and mitigating these threat and attacks [8], [25], [26], [17] and [18].

2.5 Insider Threats

Insiders are individuals with authorized access to a network or system who can exploit their privileges, whether knowingly or unknowingly, to carry out malicious activities such as data theft, sabotage, fraud, and espionage [27]. Utilizing organization insiders, including current, temporary, and former employees, is a prevalent strategy to

bypass an organization's physical and logical security controls [28]. Insiders can modify or destroy sensitive organizational resources, extract money from financial institutions, and interrupt organization business processes [12] and [4]. Insiders with malicious intent may exploit their knowledge and expertise in internal systems, processes, and vulnerabilities to carry out harmful activities [20], [11] and [5]. Internal vulnerabilities can also create opportunities for external attacks

[13] and [29], insider threats create vulnerabilities to SEAs [30]. While the scope of the proposed study is focused on insider threats and SEAs, here the researchers intentions are addressing internal threats arise by insiders are very important, as insiders can facilitate external attacks by either intentionally or unintentionally enabling unauthorized bodies to gain access to sensitive information, weaken security measures, or grant unauthorized access to external entities. Therefore, tackling insider threats also mitigating external attacks as well [31].

Financial losses that cost companies due to insiders is an average of $16 million per incident, which exceeding those caused by external attacks. However, both insider threats and attacks can result in various negative consequences [1] and [32]. Therefore, it is important to acknowledge that there are associations between insider threats and attacks, as well as external threats and attacks, in terms of their objectives and collaborative efforts [33].

2.6 Social Engineering Attacks

A manipulating practice applied to individuals by attackers to get into the organizations' restricted network and systems [1]. In SEA, the human psychology is the most preferable for attackers to be trusted and then deceive the human victims into revealing confidential information like financial detail and password [24]. SEA and phishing attacks often occur simultaneously, as phishing is a prevalent technique within SEAs [34], it deceive insiders to divulging confidential data, such as login information or financial details, SEAs involve psychological manipulation to trick insiders [35], as a result, now insider threats are a significant concern, a statistics showed about 90% of data breaches happening due to insider threats [1] and [36].

Unintentional insider threats often arise due to negligence, human error, lack of awareness, or inadequate training [11]. Insiders are also attractive targets for attackers [35] and [21], for instance, an employee might unknowingly click on a phishing email's malicious link, thereby granting unauthorized access to sensitive organizational data [5]. Similarly, an employee might carelessly misconfigure a system, leading to unintended security vulnerabilities [15]. In phishing, attackers mimic authentic bodies like financial institutions to trick individuals to disclosing sensitive information or performing malicious actions. Nowadays, phishing attacks have become a common method of SEAs, involving and deceptive electronic mail, websites, or telephone calls to extract credentials information and confidential data [34] and [37]. It is crucial to be able to differentiate phishing tactics to mitigate the risk of such malicious activities [1].

2.7 Threat and Attack Vectors

Malware or malicious also known as malware, software, presents a substantial risk to digital systems such as computers and networks by aiming to exploit or harm them. It encompasses a range of harmful programs, comprising worms, Trojans, viruses, worms, spyware, adware and ransomware. It can intrude and has the ability to infiltrate computer systems in many ways, including attachments or infected software downloads [38]. Ransomware refers to malicious software that encrypts files or restricts system access, with attackers demanding payment in crypto currencies to maintain transaction anonymity. This results in the victim's files becoming inaccessible unless a ransom is paid [39] and [19].

Zero-day attacks are the exploitation of software or system vulnerabilities that are either unrecognized by the software vendor or have not yet been addressed with a patch [40]. Malicious actors take advantage of these vulnerabilities before a solution is developed; presenting challenges for organizations in their efforts to defend it. Zero-day attacks are also often directed at specific targets and can result in significant damage [41] and [40].

2.8 Network and Host based Threat Detection

The two main types of IDSs (network based IDS and host based IDS) by [39], [42], [43] and [44] are currently implementing either in signature-based or anomaly-based approaches [39]. Signature-based NIDS (SNIDS) detect threat and attacks by comparing network traffic to a database of predefined rules [45]. In contrast, anomaly-based NIDS (ANIDS) focus on identifying deviations from established normal behavior patterns in network traffic [9]. Traffic deviates from normal patterns is treated as an anomaly, that potentially indicating a cyber-attack [46]. Research by [47], [9], [45] and [48] explores several works on anomaly detection using network traffic data. Although the network provides communication, cooperation, and sharing of costly resources within organizations

[16]. However, insider threats seriously impair organization's system ever before [1]. As a result, it is essential to improve and enhance the capabilities of existing NIDS and HIDS.

Recent scholarly articles have emphasized the utilization of machine learning methods to enhance the efficiency and effectiveness of intrusion detection systems [48]. In the case of host-based intrusion detection, individual hosts are equipped with host-based IDS (HIDS) to monitor their activities and identify any indications of potential attacks or malware [49]. Research studies also have shown that integrating ML techniques into host-based intrusion detection presents a promising approach to fortifying computer systems against insider threats [50]. However, further investigation is required to address existing challenges in this domain, including improving detection capabilities and ensuring resilience against emerging threats and attacks [15].

2.9 Signature and Anomaly Based Detection

Two main approaches for threat detection are signature-based detection and anomaly-based detection [39]. Signature-based detection relies on predefined patterns or signatures of known threats to identify malicious activities [22]. It compares network traffic or system behavior against a database of signatures and raises an alert or takes action when a match is found. Anomaly-based detection focuses on identifying deviations from normal behavior and is effective against unknown or evolving threats [39] and [22] However, signature-based detection struggle with new emerging threats such as zero-day attacks, which are previously unknown threats [34]. Anomaly-based detection, establishes a baseline of expected behavior and detects activities that significantly differ from it. This approach utilizes ML algorithms to analyze network traffic, system logs, or user behavior and detect anomalies that may indicate threats [51] and [25]. Recent literature emphasizes the importance of user behavioral analytics and considering behavioral aspects in CS counter measures [15].

2.10 Deep Learning for threat Detection

The continuous progress of technology has given rise to powerful techniques like machine and DL. These advanced technologies have significantly bolstered organizations' security measures by detecting anomalies through analysis from vast amounts of data [48]. By recognizing patterns, ML algorithms enable proactive threat management. DL takes threat detection a step further ahead by excelling in processing unstructured data, identifying complex patterns, and making accurate predictions [31]. Researchers have harnessed the po- tential of these technologies to develop threat detection systems that can adapt to the ever-changing landscape of cyber risks [13] and [31].

DL methods have shown better detection accuracy, when compared to conventional ML techniques, as DL accepts large and com- plex datasets [52], [9], [13] and [45]. For instance in Fog networks, the Autoencoder (AE) with Isolation Forest (IF) technique were utilized and this method greatly classifies inbound network traffic to normal and malicious intents [48].

Furthermore, DL techniques such as Denoising AutoEncoder (DAE), Variational AutoEncoder (VAE), Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNNs) have emerged as powerful tools for anomaly detection [31], [9], [53] and [48]. The ability of DL to process large, heterogeneous datasets and learn complex patterns makes it preferable in the CS field [52]. VAEs introduce probabilistic modeling, capable for generating new data samples and estimating input likelihood [48]. Additionally, DAEs attract researchers' attention as it handles diverse noisy datasets in training of anomaly-based threat detection models [9]. Scholars often employ Mean Squared Error (MSE) and Mean Absolute Error (MAE) to compute the reconstruction error of AEs [45].

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{1}$$

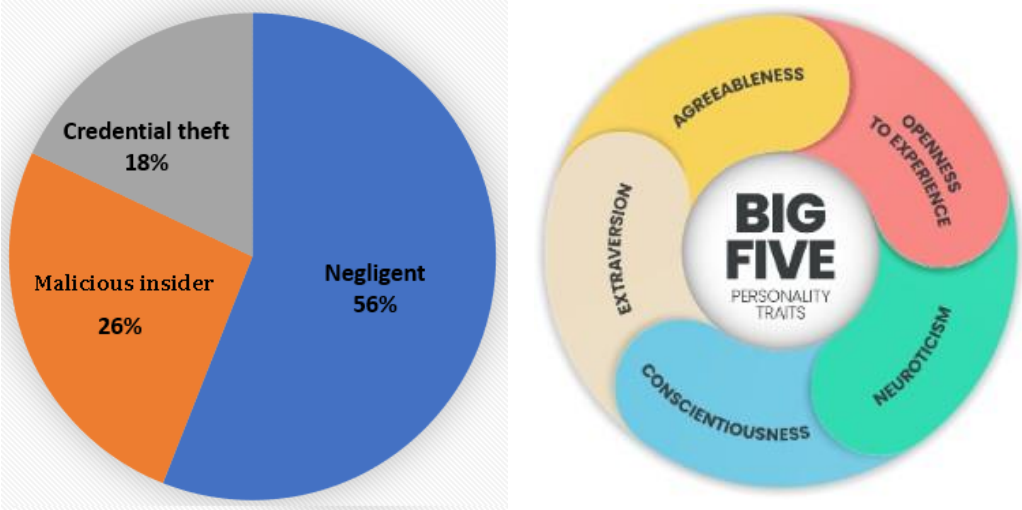
$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \tag{2}$$

However, still the conventional ML learning techniques like Random Forest (RF), Isolation Forest (IF), Principal Component Analysis (PCA) and Gaussian Mixture Models (GMM) have been utilized by various scholars, having well-structured and fewer features in the datasets demonstrating higher detection performance [48], [44], [54], and [41].

2.11 Personality Traits as a Detection Challenges

Studies suggest that variations in personality traits, especially those identified within the Big Five openness, conscientiousness, extraversion, agreeableness, and neuroticism significantly influence individuals' behaviors in the context of CS [4], [5]. Personal traits are vital in shaping CS countermeasures [55], affecting behaviors such as

caution when clicking links, sharing personal information online, and following security protocols [1], [56] and [35]. Therefore, it is crucial to examine how personality traits influence CS behavior to effectively address insider threats and SEAs including phishing [7], [5], [57] and [36]. Figure 1 illustrates the common insider threat profiles and five big personality traits classification.



(a) Insider Threat Profiles (b) Personality Traits [55]

Figure 1. Insider threat Profiles and Five Big Personality Traits

Understanding the link between personal traits and CS threat suspicion is crucial for improving the cyber intrusion detection and prevention systems [58]. Previous research has demonstrated significant connections between CS threats such as insider threats, SEAs, and phishing and the Big Five personality traits. For instance, individuals with high openness are often curious and imaginative, which may lead them to engage with unfamiliar stimuli, including risky online activities. This tendency can increase their vulnerability to social engineering and phishing attacks, as they might be more willing to click on unknown links. Table 2 illustrates the comparative analysis of the impact of the Big Five personality traits on CS vulnerabilities, specifically Insider Threats, SEA and Phishing Attacks. According to the literature, there is an association between the big personality traits and CS behavior. Individuals with high levels of openness are more suspected to SEAs and phishing attacks, as the personality willingness to engage with new experiences [55]. On the other hand, employees with high conscientiousness are less vulnerable to cyber threats [4] and [12]. Extroverted individuals, naturally more sociable, as a result susceptible to SEAs are high. Agreeable people are also exploited to threat and attacks due to their trusting nature [59]. Additionally, high neuroticism is associated with greater vulnerability to cyber threats due to emotional instability, whereas low neuroticism is better CS resilience [8]. These associations underscore the importance of considering personality traits when developing CS measures and training programs [7]. Figure 2 illustrates the association between personality traits and CS vulnerability.

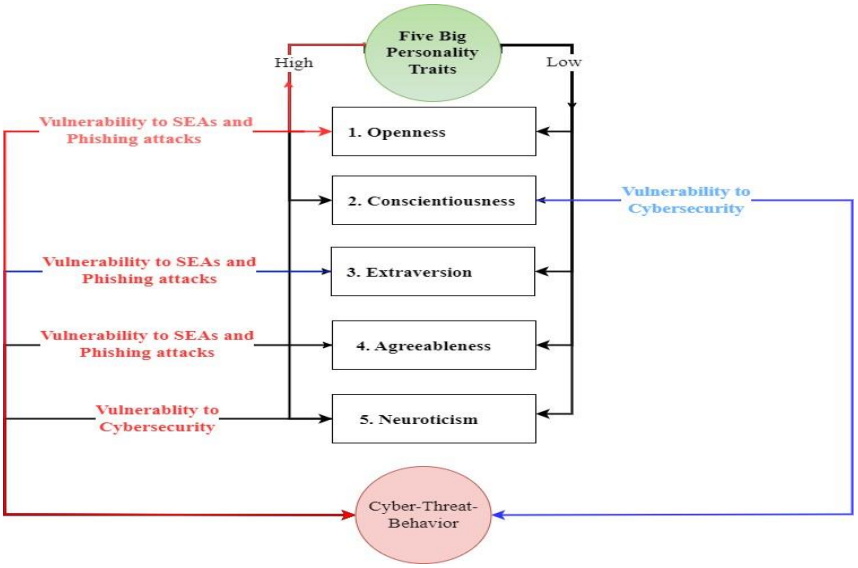


Figure 2: Personality Traits versus Cybersecurity Vulnerability

2.12 Datasets for Detection

Currently datasets utilized for intrusion detection research include DARPA, KDD cup 99, NSL-KDD and UNSW-NB15 [60], [50] and [61]. These datasets are available online and free for researchers. To evaluate the performance of anomaly based detection, these datasets have playing a crucial roles [13]. The CERT insider threat dataset includes a psychometric dataset, which had been utilized to investigate personality traits and their impact on decision-making abilities [55] and [62]. The psychometric datasets utilized in this article comprises 1,000 samples, providing a foundation for analyzing the relationship between personality traits and cyber-threat behavior. The dataset is structured with seven columns [50]. Literature findings from prior research highlights a correlations between personality traits and vulnerabilities in CS. Figure 3 presents the distribution of psychometric traits within the CERT Insider Threat dataset, specifically with a total sample size of 1,000. The distribution is as follows: Openness (21.9%), Conscientiousness (20.2%), Extraversion (19.3%), Agreeableness (19.0%), and Neuroticism (19.5%).

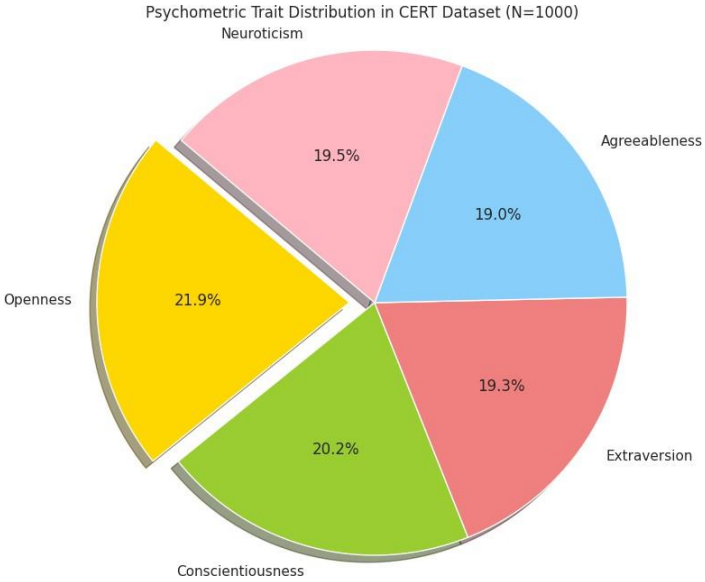


Figure 3: Personal Traits Distribution in the CERT Psychometric dataset

III. COMPARATIVE ANALYSIS

If individuals within an organization fall victim to phishing emails or websites and disclose their login credentials or other sensitive information, it can provide attackers with unauthorized access to systems and data. This unauthorized access can then be used to carry out further insider threats or facilitate more sophisticated attacks [55], [63] and [8]. If an insider threat goes undetected, it can continue to operate within an organization, potentially escalating their activities and causing more damage over time. Without effective detection and mitigation measures in place, the insider threat may go unnoticed for an extended period, allowing them to exploit their privileges and cause significant harm [7], [5] and [57]. Moreover, the undetected insider threat can also provide insider knowledge and access to external attackers, enabling them to launch more targeted and sophisticated attacks. This collaboration between insiders and external attackers can be SEAs can lead to a higher level of threat [64] and [59].

Overall, the escalation of risks occurs when insider threats are not effectively detected and mitigated. It allows the threats to persist, potentially collaborate with external attackers, and cause more significant harm to the organization's systems, data, reputation, and overall security posture. Therefore, it is crucial for organizations to implement robust detection and mitigation measures to prevent the escalation of insider threats and their potential collaboration with other threat actors [64], [59] and [57]. Insider threats, SEAs and phishing attacks are interconnected and can facilitate the emergence and escalation of each other. Organization individuals may exploit their privileges to steal sensitive information, sabotage systems, or cause other forms of harm [65]. On the other hand, SEAs involve manipulating individuals through psychological manipulation and deception to gain unauthorized access to systems or sensitive information [35]. Phishing attacks are a specific type of SEAs where attackers use fraudulent emails or websites to trick individuals into revealing sensitive information. Insider threats lead to the facilitation of SEAs and phishing attacks in several ways [1]. For example, an insider may be manipulated by external attackers to provide access credentials and enabling the attackers to carry out SEAs through phishing. Insider threats can also create vulnerabilities due to insiders having different personality [55], as

a result, making organizations' easier for external attackers, social engineering or phishing attacks [46], [57] and [66]. Table 1 presents exiting scholarly work done recently.

Table 1: Comparative Analysis of Methods, Advantages, Disadvantages, and identified Gaps

No.	Title, Ref.& Year	Methods	Advantage	Disadvantage	Gaps
1.	Anomaly Detection for Insider Threats Using Unsupervised Ensembles [31]	Unsupervised ML, Agglomerative Clustering to extract features & HMM, predicts next event	Identify normal & malicious behavior for early warning & reduce malicious activities	If datasets have outlier results in correct clusters	High accuracy is required FPRs & FNRs be achieved using strong computing capacity.
2.	Insider Threat Detection using DAE and VAE Neural Networks, [9]	DAE with labeled training data & VAE for AD & ensemble learning for probability evaluation	Detect malicious users automatically, reduce FPRs & FNRs	Computational costly	Optimize existing methods s required.
3.	Intrusion detection methods based on integrated deep learning model [45]	Explore current ID methods & proposed DL ensemble (VMs, RFs, KNNs, MLPs& CNNs)	Provides solutions to noisy datasets to be robust with high dimensionality	Require long training time and will affected by feature scaling	Require Optimal performance and inference time
4.	A Hybrid IDS Based on Scalable K-means+ Random Forest and Deep Learning, [32]	K-means+ RM, DL algorithms (CNNs, RNNs, LSTMNs, AEs)	improved accuracy, HIDS combines scalability & DL detect complex attacks as it can learn from contextual data	Accuracy can be limited when parameters are not tuned correctly	Solution limited to host machines or disjointed approaches
5.	ITD Based on User Behavior Modeling and Anomaly Detection Algorithms [16]	UBM, detection algorithms (ANN, SVM, PCA & Decision Tree)	Improving existing techniques by combining multiple methods for finding anomalies.	Need large volume of users log datasets, if not insider activities might treated incorrectly	A comprehensiveap-Proach required to reduce FPs & FPs or cost
6.	ID using CNN feature extraction with EPCA for dimentionality reduction, [67]	CNN, EPCA for dimensionality reduction	High accuracy of ID & the ability to categorize multiple attacks	Lacks real-time testing Which could in slower results	Further Optimization needs regarding potential breach responses fast
7.	Insider Threat Detection Using Machine Learning Approach, [68]	Employing datasets from the CERT (Computer Emergency Response Team), use RF & SVM	Provide real time detection	May produce malicious flags for normal user behavior	required Optimal performance and detection time

Table 2: Comparative Analysis of Insider Threat, Social Engineering Attack, and Phishing Attack along with Personality Traits

Personality Traits	Insider Threat	Social Engineering Attacks	Phishing Attacks	General Description	Reference
Openness	High susceptibility due to curiosity	High susceptibility due to imagination	High susceptibility due to engagement with novel stimuli	High openness is associated with curiosity and imagination, making individuals more susceptible to insider threats, social engineering, and phishing attacks. Conversely, low openness reduces susceptibility to cyber threats due to less engagement with novel stimuli.	[55], [63], [64], [59], [8], [7], [5], [57]
Conscientiousness	Low susceptibility due to diligence	Low susceptibility due to careful behavior	Low susceptibility due to cautious online behavior	High conscientiousness is linked to carefulness and diligence, reducing vulnerability to cyber threats by following security protocols and cautious online behavior. Low conscientiousness, however, increases susceptibility due to less careful behavior.	[55], [63], [4], [64], [59], [8], [7], [5], [57]
Extraversion	High susceptibility due to social engagement	High susceptibility due to social interaction	High susceptibility due to sociability	High extraversion is associated with social engagement, increasing vulnerability to insider threats, social engineering, and phishing attacks. In contrast, low extraversion reduces susceptibility due to less social interaction.	[55], [63], [4], [64], [59], [8], [7], [5], [57]
Agreeableness	High susceptibility due to trust	High susceptibility due to cooperation	High susceptibility due to willingness to trust	High agreeableness is associated with trust and cooperation, increasing vulnerability to insider threats, social engineering, and phishing attacks. Low agreeableness, associated with skepticism, reduces susceptibility to cyber threats.	[55], [63], [4], [64], [59], [8], [7], [5], [57]
Neuroticism	High susceptibility due to emotional instability	High susceptibility due to stress response	High susceptibility due to anxiety	High neuroticism is linked to emotional instability, increasing vulnerability to insider threats, social engineering, and phishing attacks. Low neuroticism, related to emotional stability, reduces threat susceptibility.	[55], [63], [4], [64], [59], [8], [7], [5], [57]

3.1 Baseline Research Performance comparison

Researchers have been developed a DL based detection [45], [9] and [69]. Table 3 displays a comparison of baseline researches, including their methods, accuracy, precision, recall, F1-score and gap identified. These anomaly detection techniques offer a segmented strategy that relies on network or host-based IDS [45], [9], and [69]. Moreover, it is becoming difficult to appropriately handle insider threats with the current detection methods. Table 3 shows the performance comparison of baseline articles.

Table 3: Summary of Related Works

No.	Reference	Methods	Acc	Prec	Rec	F1-S	Gaps
1.	[9]	NNs ensemble learning (DAE, VAE) for DAE	0.900	0.950	0.950	0.920	For detecting newly threats & to reduce FPRs, optimize existing models is required,
2.	[9]	NNs ensemble learning (DAE, VAE) for VAE	0.920	0.960	0.960	0.940	For detecting newly threats & to reduce FPRs, optimize existing models is required,
3.	[45]	Ensemble based IDS (SVM, KNNs, MLPs& CNNs with DL)	0.900	0.920	0.92	0.95	Noise accumulation may result in incorrect decisions.
4.	[32]	Evaluate a hybrid IDS, combines DL with (CNNs, RNNs, LSTMNs, AEs)	N/A	N/A	N/A	N/A	It seems traditional techniques like signature based

Note: Acc =Accuracy, Prec= Precision, Rec= Recall and F1-S=F1-Score

3.2 Gap Analysis

Among the several gaps identified in current threat detection methods, one common gap is the need for enhanced detection methods for insider threats and SEAs [24]. Existing detection methods had had disjointed, with a focus on either network-based intrusion detection or host-based detection methods. These distinct approaches have limitations in effectively addressing the unique challenges posed by insider threats and SEAs [1], [9] and [45]. In order to address the shortcomings of current detection method, a comprehensive analysis of insider behavior is proposed. This analysis should encompass both network and host activities to gain a comprehensive understanding of insider behaviors. Current detection, overlooks the human factors [65], [63] and [46]. The limitations on conventional IDSs in effectively identifying and mitigating various threats, highlighting the need for more advanced and efficient detection systems [1]. Existing literature, emphasizing the need for further research to optimize models. For instance, [9] proposed an ID using deep AEs and VAE DNNs. [45] used an integrated DL model for ID and [32] proposed a hybrid IDS based on scalable k-means+, RF and DL. [67] used a deep CNN feature extraction with enhanced PCA for dimensionality reduction. While [20] applied ML techniques to detect malicious network traffic in cloud computing. Finally, [16] suggested an insider threat detection based on UBM (user behavior modeling) and anomaly detection algorithms. All these studies highlighted that anomaly detection is an effective method for detecting, however, potential improvement is crucial.

IV. METHODS

The primary aim of this study was to develop a unified threat detection model that effectively identified insider threats and SEAs by integrating user psychometric behavior analysis and applying DL techniques. The approach was structured into a series of methodical steps, beginning with a thorough review of existing literature to identify gaps in current detection methods for insider threats and SEAs. Despite numerous efforts to improve intrusion detection techniques using ML and DL [9], [45], [48], and [22], these methods often failed to address the complexities inherent in detecting insider threats and SEAs, highlighting the need for ongoing advancements in detection capabilities. After reviewing the literature, we analyzed existing detection methods, focusing on both network-based and host-based approaches. This analysis emphasized the critical role of human factors, which significantly influenced the effectiveness of IDS. A detailed examination of various techniques used by researchers allowed us to better understand their adoption, effectiveness, and limitations.

Following this, we gathered heterogeneous datasets from multiple sources, including both intrusion detection and insider behavioral datasets. We specifically utilized well-established datasets such as UNSW-NB15 and NSL-KDD for intrusion detection research. Our unified detection framework, illustrated in figure 4, outlined the overall methodological approaches we followed throughout the research process. We then traine three distinct models: a

network-based detection model, a host-based detection model, and a behavioral model based on personality traits. To create our unified threat detection model, we integrated the insights and features from all three models. The performance of this integrated model was then evaluated using standard metrics. Through comparative analysis, we assessed the effectiveness of our approach relative to existing models. By combining technical analysis with behavioral insights, this study contributed to advancing insider threat detection.

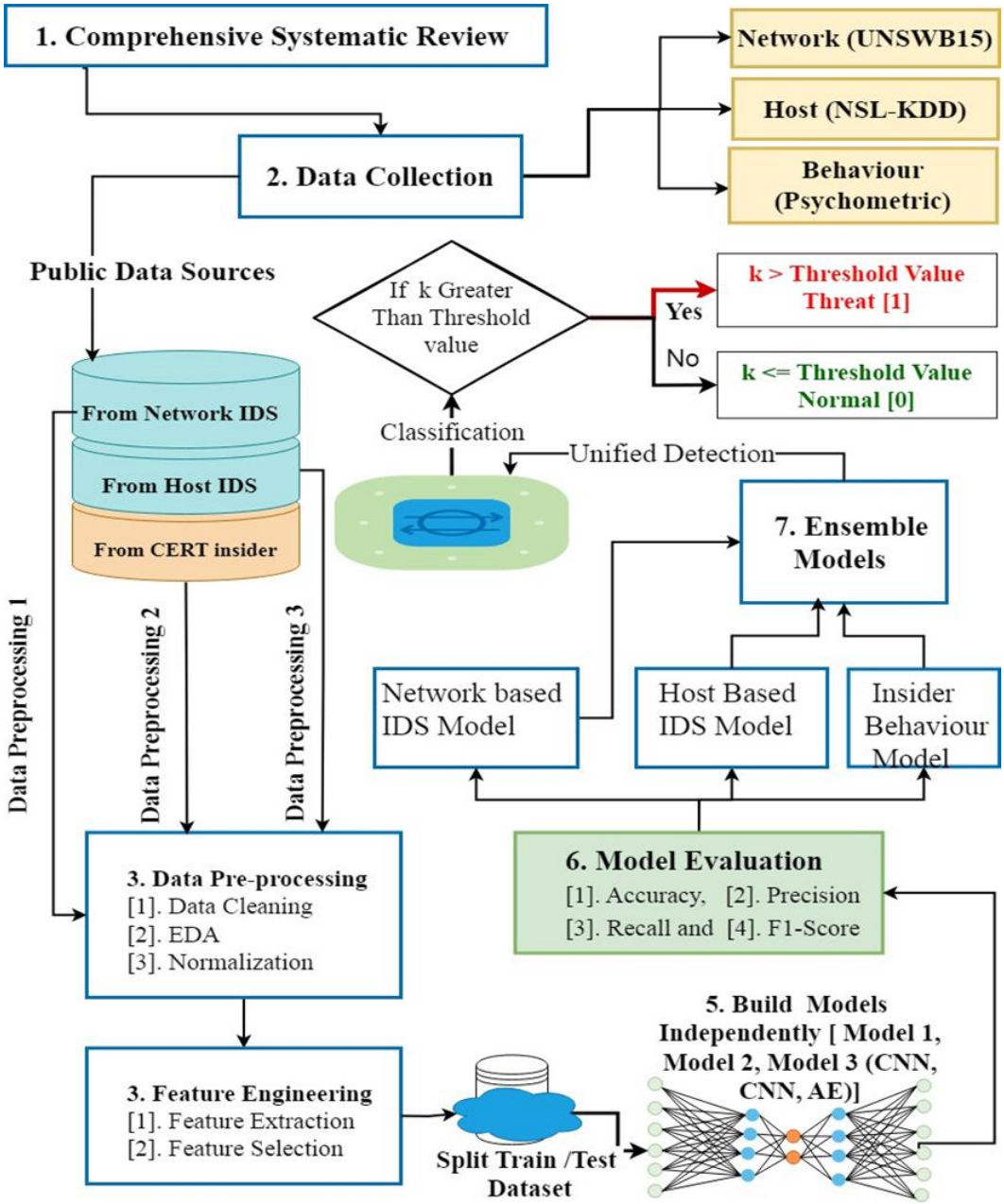


Figure 4: Proposed Conceptual System Architecture

4.1 Data Preprocessing

During this process, several tasks including cleaning the data, selecting relevant features, normalizing numerical values, and handling missing values. To clean the data, we replaced missing categorical values with the most frequent value in the respective feature. For continuous feature values, we substituted missing values with the average mean. Additionally, we converted category labels into numerical feature values to address any non-standard components in the dataset. Categorical features of the network and host datasets were converted into numeric values. To ensure fair feature contribution, numerical feature values underwent data normalization. We applied the min-max scaler technique, transformed them to a range of 0 and 1. These steps prepared our datasets for analysis and model training that we planed to improve existing NIDS and HIDS performances and for better insights into insider threats and SEAs. Figure 5 demonstrate the overall work flow underwent in the data preprocessing.

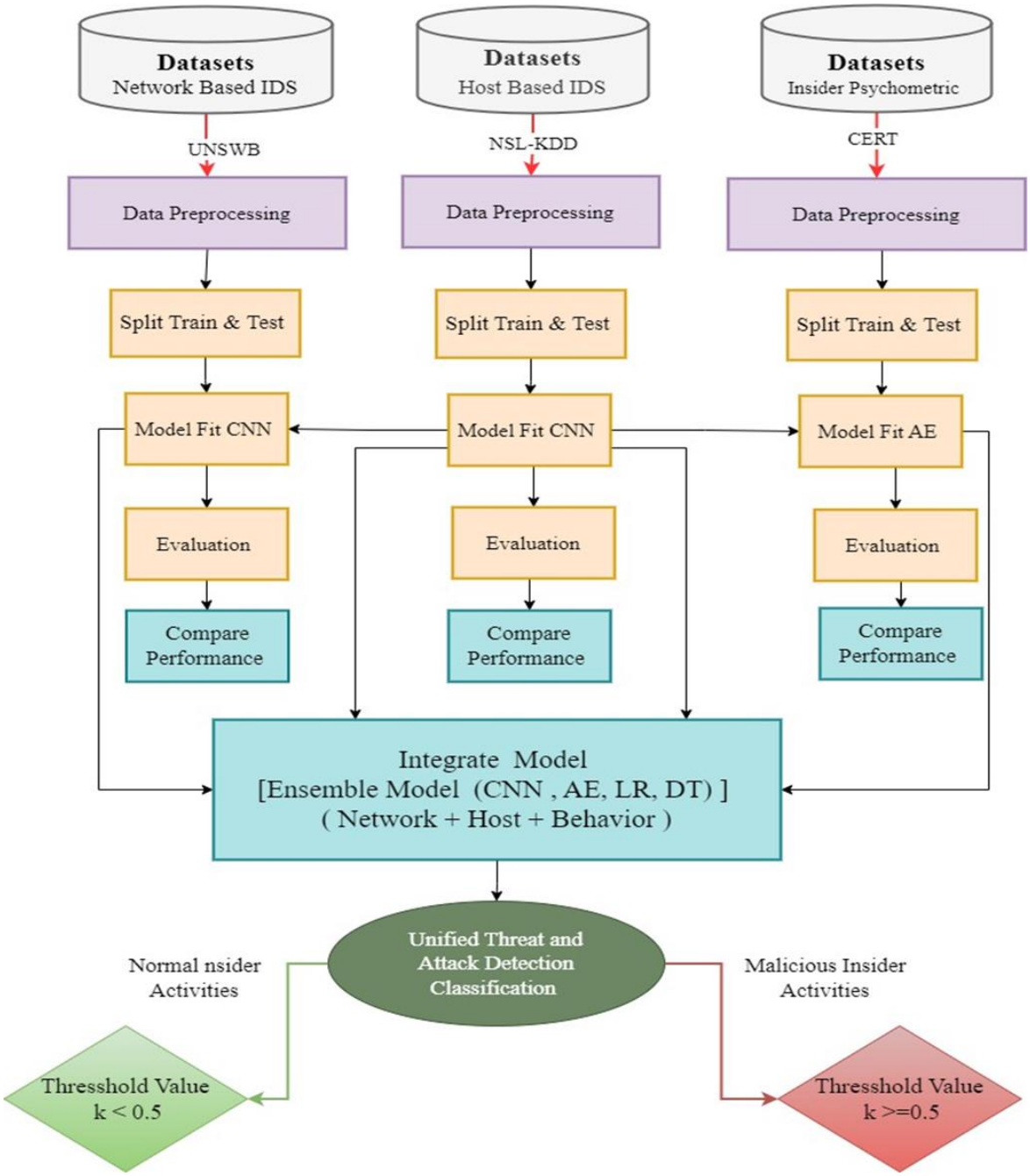


Figure 5. Integrated Model Workflow

V. EXPERIMENTAL SETUP

he primary aim of this study is to enhance the effectiveness of existing threat detection methods, with a specific focus on detecting insider threats and SEAs. Traditional IDS systems typically rely on either NIDS or HIDS methods. However, these fragmented approaches are often insufficient to address the emerging and complex nature of modern cybersecurity threats. Most existing IDS systems focus heavily on technical factors but overlook the critical role of human behavior. Given that humans are often considered the weakest link in organizational security, it is essential to incorporate their cybersecurity behavior into the detection models to improve the overall effectiveness of traditional IDS systems. This research proposes a unified detection framework that combines NIDS and HIDS with human behavioral analysis using DNNs specifically CNN and AEs. By integrating psychometric data derived from the Big Five personality traits into the detection models, we aim to improve the accuracy of detecting insider threats and SEAs. Figure 6 illustrates the framework of our experimental setup, showcasing the methodological approach we have taken to combine technical and behavioral analysis in our threat detection model.

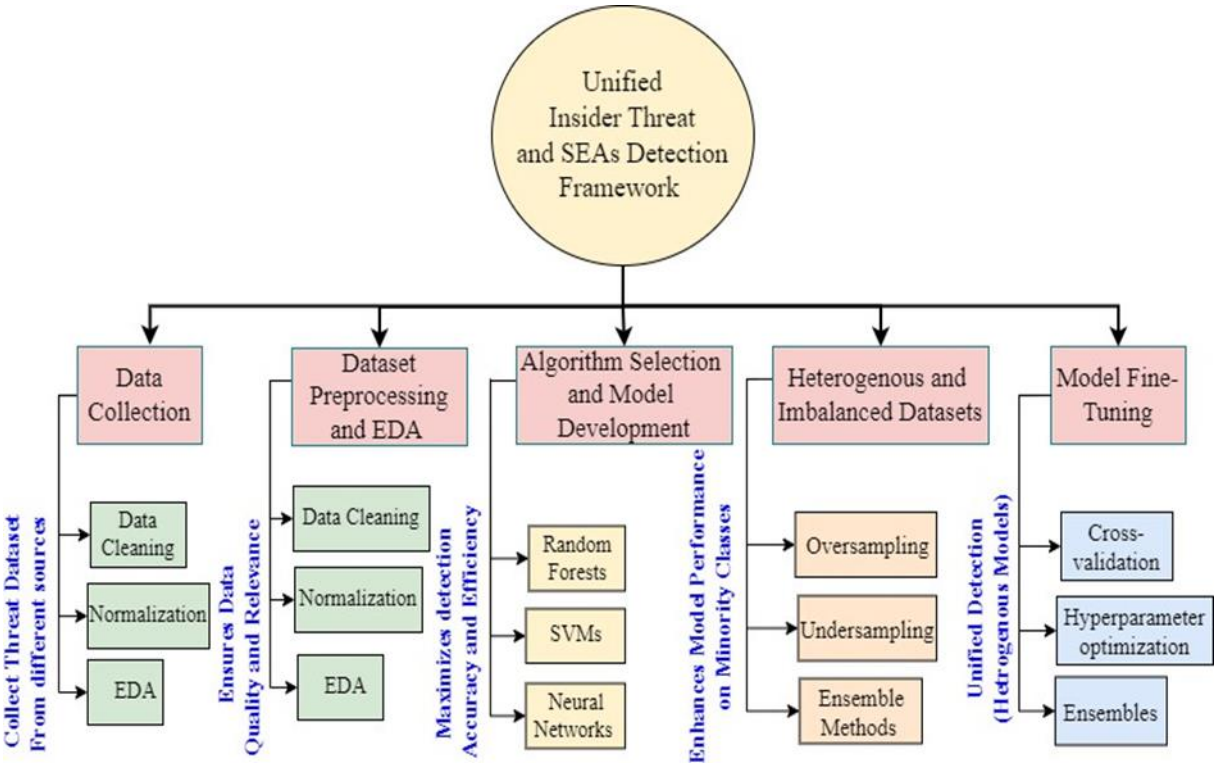


Figure 6. Overview of Experimental Setup Framework

5.1 Dataset Overview

We selected three distinct publicly available datasets from the cloud. The datasets chosen include the UNSW-NB15, which represents network intrusion, the NSL-KDD, serving as a marker for host intrusion and the CERT Insider Threat dataset, which focuses on insider psychometric behavior. The UNSW-NB15 dataset, obtained from a real-world environment, consists of a collection of features critical for network intrusion detection. The CERT Insider Threat dataset adds a unique dimension by providing insights into how personality traits correlate with insider threat behaviors, highlighting the psychological aspects underlying cyber threats. Integrating these datasets provides a comprehensive detection framework by combining CS with human behavior variables. These datasets are commonly used in various CS research [70], [71], [60], [9], [23] and [72]. Datasets employed in this study described under table ??

Table 4: Description of Detection Datasets

No.	Dataset Name	Size for Training	Size for Testing	Column	Reference
1.	UNSW-NB15	175,341 records	82,332 records	45	[26]
2.	NSL-KDD	125,973 records	22,544 records	42	[72]
3.	CERT Insider Threat	1,000 samples	N/A	7	[16]

The UNSW-NB15 dataset consists a total of 257,673 rows and 45 columns, making it important for training and testing the proposed models. It includes a dependent variable termed "label," containing binary values (1 or 0) that indicate whether an activity is categorized as a threat or normal. Other columns, such as "id," "duration," and "protocol," represent independent variables or features. These features capture various behaviors and characteristics of network traffic, facilitating the classification of activities as either threats or normal. To evaluate the effectiveness of this proposed solution, we selected the NSL-KDD dataset, widely utilized in intrusion detection research, this dataset features a comprehensive collection of network traffic data. From NSL-KDD dataset features, 14 independent variables were selected based on feature correlation, highly correlated with the target variable. The target variable values in the network dataset and the target variable name called labels from the host datasets have termed "normal," are represented by 0, and all other non-normal values, representing different threat types, are grouped and classified as threats and represented by 1. The network dataset consists of 257,673 rows and 45 columns, which will be utilized for training and testing the suggested models. This network intrusion dataset contains a dependent variable called the "label," consisting of binary values (1 or 0) to classify activities as threats or normal. The remaining columns, such as "id," "duration," and "protocol," represent independent variables that

capture different behaviors and characteristics of network traffic. The network dataset comprises 175,343 rows with 45 features are allocated for training, and 82,327 rows with 45 features are reserved for testing, with the testing data accounting for approximately 46.98% of the entire network dataset. Dataset descriptions illustrate in Table 5.

Table 5: Network Dataset

No.	Feature	No. of Records	Data Type
0	id	257,673	int64
1	dur	257,673	float64
2	proto	257,673	object
3	service	257,673	object
4	state	257,673	object
5	spkts	257,673	int64
6	dpkts	257,673	int64
7	sbytes	257,673	int64
8	dbytes	257,673	int64
9	rate	257,673	float64
10	sttl	257,673	int64
11	dttl	175,341	int64
12	sload	175,341	float64
13	dload	175,341	float64
14	sloss	175,341	int64
15	dloss	175,341	int64
16	sinpkt	175,341	float64
17	dinpkt	175,341	float64
18	sjit	175,341	float64
19	djit	175,341	float64
20	swin	175,341	int64
21	stcpb	175,341	int64
22	dtcpb	175,341	int64
23	dwin	175,341	int64
24	tcprtt	175,341	float64
25	synack	175,341	float64
26	ackdat	175,341	float64
27	smean	175,341	int64
28	dmean	175,341	int64
29	trans_depth	175,341	int64
30	response_body_len	175,341	int64
31	ct_srv_src	175,341	int64
32	ct_state_ttl	175,341	int64
33	ct_dst_ltm	175,341	int64
34	ct_src_dport_ltm	175,341	int64
35	ct_dst_sport_ltm	175,341	int64
36	ct_dst_src_ltm	175,341	int64
37	is_ftp_login	175,341	int64

No.	Feature	No. of Records	Data Type
38	ct_ftp_cmd	175,341	int64
39	ct_flw_http_mthd	175,341	int64
40	ct_src_ltm	175,341	int64
41	ct_srv_dst	257,673	int64
42	is_sm_ips_ports	257,673	int64
43	attack_cat	257,673	object
44	label	257,673	int64

The host dataset contains 148,517 rows and 42 columns, used for training and testing purposes. In the host-based intrusion dataset, the "labels" variable serves as the dependent variable. It consists of binary values indicating whether an activity is classified as a threat (1) or normal (0). On the other hand, the independent variables, or features such as "duration", "protocol_type", "dst_host_srv_rerror_rate", and so on. These independent variables represent different behaviors of the host-based logs or traffic data that can be used to classify an insider activity as a threat or normal. Table 6 presents the summary of total number of samples and number of features available in the NSK-KDD dataset.

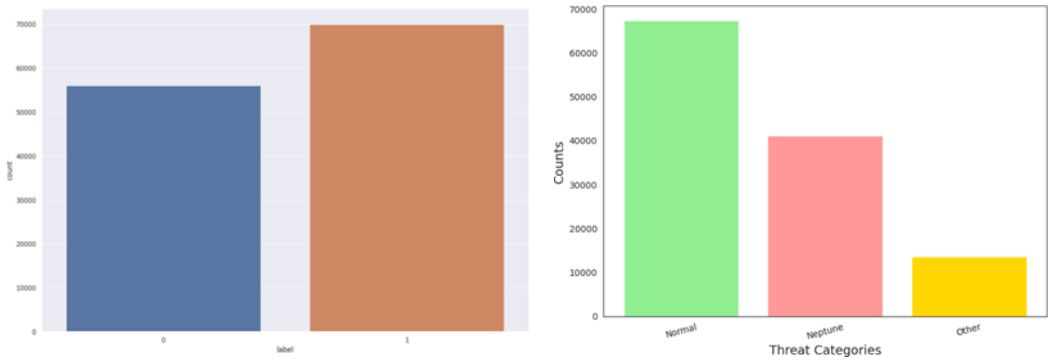
Table 6: Host Dataset

No.	Feature	No. of Records	Data Type
0	duration	148,517	int64
1	protocol_type	148,517	object
2	service	148,517	object
3	flag	148,517	object
4	src_bytes	148,517	int64
5	dst_bytes	148,517	int64
6	land	148,517	int64
7	wrong_fragment	148,517	int64
8	urgent	148,517	int64
9	hot	148,517	int64
10	num_failed_logins	148,517	int64
11	logged_in	148,517	int64
12	num_compromised	148,517	int64
13	root_shell	148,517	int64
14	su_attempted	148,517	int64
15	num_root	148,517	int64
16	num_file_creations	148,517	int64
17	num_shells	148,517	int64
18	num_access_files	148,517	int64
19	num_outbound_cmds	148,517	int64
20	is_host_login	148,517	int64
21	is_guest_login	148,517	int64
22	count	148,517	int64
23	srv_count	148,517	int64
24	serror_rate	148,517	float64
25	srv_serror_rate	148,517	float64
26	rerror_rate	148,517	float64
27	srv_rerror_rate	148,517	float64
28	same_srv_rate	148,517	float64

No.	Feature	No. of Records	Data Type
29	diff_srv_rate	148,517	float64
30	srv_diff_host_rate	148,517	float64
31	dst_host_count	148,517	int64
32	dst_host_srv_count	148,517	int64
33	dst_host_same_srv_rate	148,517	float64
34	dst_host_diff_srv_rate	148,517	float64
35	dst_host_same_src_port_rate	148,517	float64
36	dst_host_srv_diff_host_rate	148,517	float64
37	dst_host_serror_rate	148,517	float64
38	dst_host_srv_serror_rate	148,517	float64
39	dst_host_rerror_rate	148,517	float64
40	dst_host_srv_rerror_rate	148,517	float64
41	labels	148,517	object

5.2 Exploratory Data Analysis (EDA)

We employed EDA to visually explore the distribution of classes within the dataset, focusing on UNSW-NB15 datasets, the NSL-KDD and CERT psychometric dataset. EDA was also conducted to see the correlations between features. A correlation function was applied, and a correlation map diagram was generated to provide a clear visual representation of the correlation matrix. Additionally, we assessed the distribution of feature values in the dataset using kurtosis and skewness functions. Figure 7 present the value distribution of network and host datasets' target classes (namely Label and Labels).



(a) Network dataset (b) Host datasets

Figure 7. Target Class Value Distribution in Network and Host Intrusion Datasets

5.3 Model Building

Our model building process involved multiple phases. Model 1: A CNN technique was utilized for NIDS. Model trained and evaluated on the UNSW-NB15 datasets, and compared to baseline NIDS models. Model 2, a CNN technique was also employed for HIDS for threat classification, trained and evaluated on the NSL-KDD dataset. Third, Unified Model, a more comprehensive model, proposed to make unified and comprehensive detection. The psychometric data from the CERT Insider Threat dataset was incorporated to enhance the system's ability to detect insider threats, SEA and phishing threats. The proposed unified threat model was trained using a stacking ensemble for detection optimization. Since the third dataset consists of unlabeled data, Autoencoders (AE) were applied for feature learning. Additionally, the Synthetic Minority Oversampling Technique (SMOTE) was implemented to augment the psychometric data, and to increase the minority class in the network data sample. Figure 8 presents the proposed model building approaches.

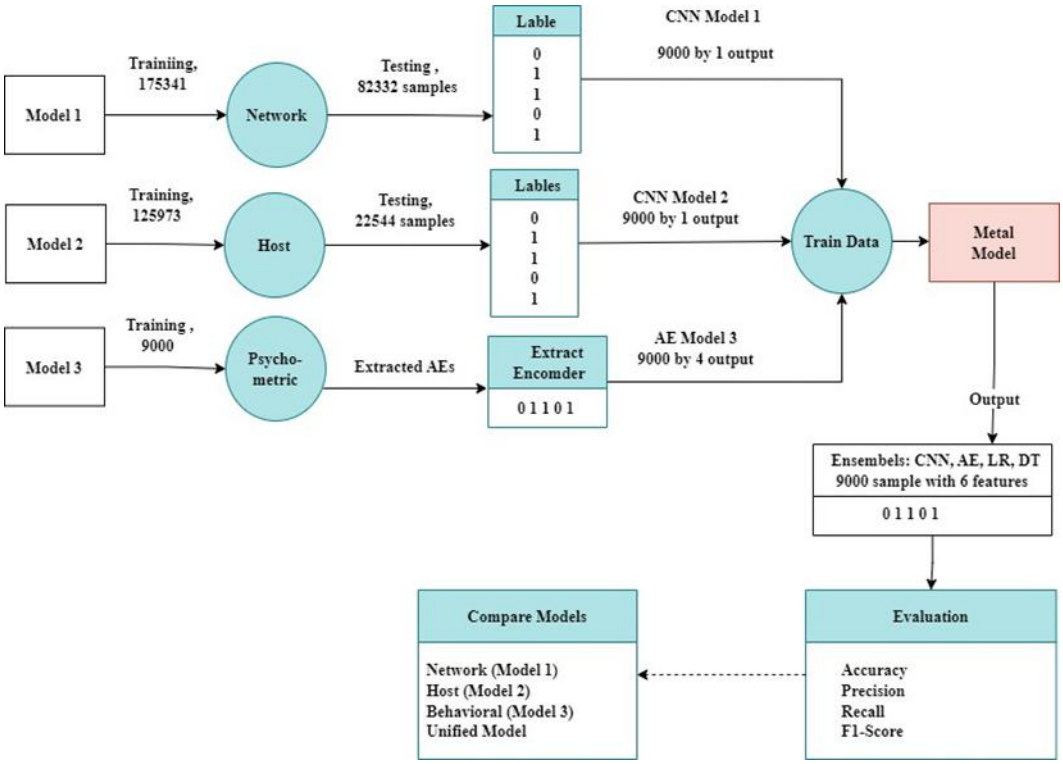


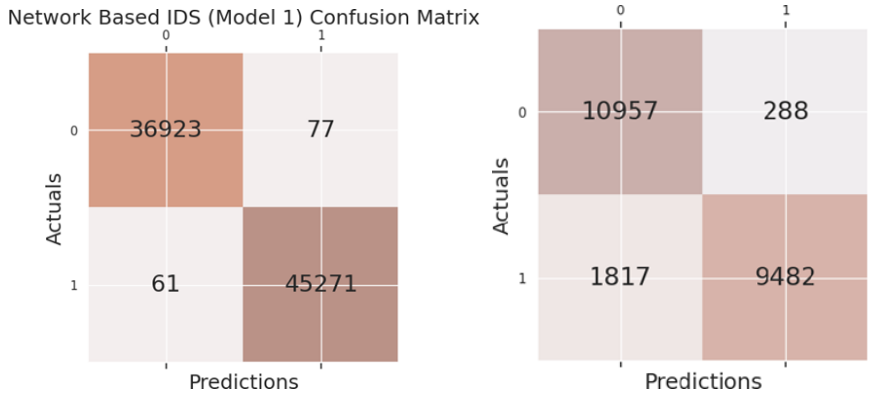
Figure 8. Holistic /Unified Threat Detection Model

5.4 Performance Metrics

We assess the effectiveness of our model by evaluating its accuracy, precision, recall, and F1-score. In our threat classification research, we used a confusion matrix to evaluate our model's performance by breaking down its predictions into four categories: True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). True Positives (TP): These are instances where the model correctly identifies malicious activities as threats. True Negatives (TN): These are instances where the model correctly identifies normal activities as non-threatening. False Positives (FP): These are instances where normal activities are mistakenly classified as threats, leading to unnecessary investigations or disruptions. False Negatives (FN): These represent the critical cases where the model fails to detect actual threats, leaving potential security risks unaddressed. The confusion matrix is a vital tool in understanding the models strengths and weaknesses, helping us refine its ability to detect real threats while minimizing false alarms. Balancing TP, TN, FP, and FN is key to optimizing the performance of our threat detection system.

VI. RESULT

The results of our research demonstrated significant improvements in the performance of our models compared to baseline systems. For Model 1 (CNN for NIDS), we achieved an impressive accuracy of 99.9%, with high precision (99.7%), recall (99.7%), and F1-score (99.7%), showcasing a substantial enhancement over existing NIDS. This indicates that our approach has significantly improved the detection capabilities of NIDS, reinforcing the need for continual advancements in detection systems to keep pace with evolving threats. For Model 2 (CNN for HIDS), we observed similar improvements, with strong performance in HIDS as well. The behavioral dataset, which included psychometric data, still requires further investigation and refinement. Due to the limited number of samples in the psychometric dataset, its performance was somewhat lower, and this will be addressed in future work. As the behavioral data grows and is better integrated into the framework, we anticipate further enhancements in its effectiveness. The confusion matrix, shown in Figure 9, clearly illustrates the performance metrics. To achieve even better results, more extensive behavioral data is required, and ongoing work will focus on expanding this dataset and refining the model.



(a) Confusion Matrix (NIDS Model 1) (b) Confusion Matrix (HIDS Model 2) (c) N/A

Figure 9. Confusion Matrix

Table 7 presents the results of our experiment conducted on three various datasets. It compares the performance metrics of different threat detection models, including NIDS, HIDS, behavior analysis models and a unified detection model that integrates all three. The network model, based on the UNSW-NB15 dataset, achieved high performance with 99.9% accuracy, 99.7% precision, 99.7% recall, and 99.7% F1-score.

Table 7: Unified Detection Model Comparisons

Model	Dataset	Algorithm	Accuracy	Precision	Recall	F1-Score
Network	UNSW-NB15	Supervised CNN, Logistic Regression, Decision Tree	99.9%	99.7%	99.7%	99.7%
Host	NSL-KDD	Supervised CNN, Logistic Regression, Decision Tree	90.5%	97.4%	85.8%	91.1%
Behavior	CERT (Psychometric)	Unsupervised Autoencoder, Mean Squared Error	N/A	N/A	N/A	N/A
Unified Model	Meta Data (Psychometric data+ NIDS data + HIDS data)	DL (CNN, AE), Stacking, Ensemble Learning (LR & DR)	93%	96%	94%	93.5%

VII. Conclusion

The research outlined in this study highlights the critical role that integrating user psychology and behavior plays in enhancing IDSs. By merging psychometric analyses with existing network-based and host-based detection methods, we have developed a novel unified framework capable of improving the detection of insider threats and SEAs. Our findings indicate that the characterization of user behavior through the lens of personality traits not only enriches the understanding of why certain individuals may become vulnerabilities but also serves to enhance the effectiveness of detection algorithms. Despite the limitations posed by a relatively small psychometric dataset, our results have depicted promising trends, demonstrating that the application of psychological factors within CS can substantially bolster traditional systems. This research advocates for a more holistic approach to CS that places emphasis on the human factor, encouraging ongoing exploration into the interplay between behavior and CS threats.

VIII. Future Works

To improve the unified detection framework further, augmenting the psychometric dataset beyond its current size of 1,000 samples, although this has been increased to 4,500 through data augmentation techniques, it remains essential. We plan to focus on acquiring larger and more diverse psychometric datasets, which would facilitate a deeper understanding of the psychological aspects underlying cyber vulnerabilities. Integrating additional behavioral data sources, such as emotional intelligence or stress levels, may enhance the model's performance by capturing more nuanced indicators of user behavior while interacting with digital systems. Exploring a wider variety of DL techniques also improve detection capabilities. This includes examining hybrid models that can combine the strengths of different DNNs, such as RNN and CNNs. Embracing these future directions promises to

make significant contributions to the field of CS, ultimately aiding organizations in better defending against increasingly complex and sophisticated threats.

REFERENCES

[1] J. Payne, "Annual data exposure report 2023." https://www.code42.com/resources/reports/2023-data-exposure, 2023. Code42.

[2] K. Fotiadou, T.-H. Velivassaki, A. Voulkidis, D. Skias, S. Tsekeridou, and T. Zahariadis, "Network traffic anomaly detection via deep learning," Information, vol. 12, no. 5, p. 215, 2021.

[3] T. Wisanwanichthan and M. Thammawichai, "A double-layered hybrid approach for network intrusion detection system using combined naive bayes and svm," IEEE Access, vol. 9, pp. 138432–138450, 2021.

[4] M. K. Alotaibi, The Influence of Personal Characteristics and Other Factors on the Susceptibility of Public Sector Employees to Cyber-Social Engineering Through LinkedIn: A Mixed-Methods Sequential Explanatory Study. PhD thesis, Trinity College Dublin, 2021.

[5] Verizon, "DBIR 2023 Data Breach Investigations Report." https://example.com/dbir2023, 2023. Accessed on June 1, 2023.

[6] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," computers & security, vol. 73, pp. 345–358, 2018.

[7] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things," IET Communications, vol. 16, no. 5, pp. 421–432, 2022.

[8] A. Fatima, T. A. Khan, T. M. Abdellatif, S. Zulfiqar, M. Asif, W. Safi, H. Al Hamadi, and A. H. Al-Kassem, "Impact and research challenges of penetrating testing and vulnerability assessment on network threat," in 2023 International Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–8, IEEE, 2023.

[9] E. Pantelidis, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Insider detection using deep autoencoder and variational autoencoder neural networks," arXiv preprint arXiv:2109.02568, 2021.

[10] M. N. Al-Mhiqani, R. Ahmad, Z. Zainal Abidin, W. Yassin, A. Hassan, K. H. Abdulkareem, N. S. Ali, and Z. Yunos, "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," Applied Sciences, vol. 10, no. 15, p. 5208, 2020.

[11] M. F. Alghenaim, N. A. A. Bakar, R. C. M. Yusoff, N. H. Hassan, and H. Sallehudin, "Employee awareness model to enhance awareness of social engineering threats in the saudi public sector," in 2021 International Congress of Advanced Technology and Engineering (ICOTEN), pp. 1–6, IEEE, 2021.

[12] S. Kemp, "Digital 2021: Global overview report," DataReportal. Recuperado de https://datareportal.com/reports/digital-2021-global-overview-report, vol. 0, no. 1, 2021.

[13] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021.

[14] M. Lehto and J. Limnéll, "Strategic leadership in cyber security, case finland," Information Security Journal: A Global Perspective, vol. 30, no. 3, pp. 139–148, 2021.

[15] M. A. Alanezi, "Vulnerabilities, threats and challenges on cyber security and the artificial intelligence based internet of things: A comprehensive study," IJCSNS, vol. 22, no. 2, p. 153, 2022.

[16] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, "Insider threat detection based on user behavior modeling and anomaly detection algorithms," Applied Sciences, vol. 9, no. 19, p. 4018, 2019.

[17] A. Masood and A. Masood, "A taxonomy of insider threat in isolated (air-gapped) computer networks," in 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST), pp. 678–685, IEEE, 2021.

[18] A. Mohan and D. G. A. Swaminathan, "Analysis of vulnerabilityassessment with penetration testing," Available at SSRN 4040684.

[19] Q. K. A. Mirza, M. Brown, O. Halling, L. Shand, and A. Alam, "Ransomware analysis using cyber kill chain," in 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 58–65, IEEE, 2021.

[20] A. Alshammari and A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing," Journal of Big Data, vol. 8, no. 1, pp. 1–24, 2021.

[21] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," Journal of Information Security and Applications, vol. 58, p. 102804, 2021.

[22] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes, and J. Gama, "Host-based ids: A review and open issues of an anomaly detection system in iot," Future Generation Computer Systems, 2022.

[23] L. Malhotra, B. Bhushan, and R. V. Singh, "Artificial intelligence and deep learning-based solutions to enhance cyber security," in Proceedings of the International Conference on Innovative Computing & Communication (ICICC), 2021.

[24] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," Computers in Human Behavior Reports, vol. 4, p. 100126, 2021.

[25] L. Wang and R. Jones, "Big data analytics in cyber security: network traffic and attacks," Journal of Computer Information Systems, vol. 61, no. 5, pp. 410–417, 2021.

[26] I. Ahmad, Q. E. Ul Haq, M. Imran, M. O. Alassafi, and R. A. AlGhamdi, "An efficient network intrusion detection and classification system," Mathematics, vol. 10, no. 3, p. 530, 2022.

[27] K. Machap and A. Muaza, "Use of network and cyber security tools to counter the security obstacles," Journal of Applied Technology and Innovation (e-ISSN: 2600-7304), vol. 6, no. 1, p. 5, 2022.

[28] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting insider threat via a cyber-security culture framework," Journal of Computer Information Systems, pp. 1–11, 2021.

[29] A. G. Akpan, J. O. Ugah, and V. N. Ezeano, "Leveraging on cyber security for digital economy: Analysis of emerging cyber security threats and attacks,"

[30] H. Alqahtani, I. H. Sarker, A. Kalim, S. M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, "Cyber intrusion detection using machine learning classification techniques," in Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1, pp. 121–131, Springer, 2020.

[31] D. C. Le and N. Zincir-Heywood, "Anomaly detection for insider threats using unsupervised ensembles," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1152–1164, 2021.

[32] C. Liu, Z. Gu, and J. Wang, "A hybrid intrusion detection system based on scalable k-means+ random forest and deep learning," IEEE Access, vol. 9, pp. 75729–75740, 2021.

[33] H. Owen, J. Zarrin, and S. M. Pour, "A survey on botnets, issues, threats, methods, detection and prevention," Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 74–88, 2022.

[34] P. Bayl-Smith, R. Taib, K. Yu, and M. Wiggins, "Response to a phishing attack: persuasion and protection motivation in an organizational context," Information & Computer Security, vol. 30, no. 1, pp. 63–78, 2022.

[35] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social engineering attacks prevention: A systematic literature review," IEEE Access, 2022.

[36] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," IEEE Access, vol. 9, pp. 11895–11910, 2021.

[37] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social engineering attacks prevention: A systematic literature review," IEEE Access, vol. 10, pp. 39325–39343, 2022.

[38] J. Singh and N. Jyoti, "A comprehensive review: Detection and mitigation solutions of ddos attacks in cps," Security and Resilience of Cyber Physical Systems, p. 61, 2022.

[39] N. Gupta, V. Jindal, and P. Bedi, "Cse-ids: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems," Computers & Security, vol. 112, p. 102499, 2022.

[40] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, "Comparative evaluation of ai-based techniques for zero-day attacks detection," Electronics, vol. 11, no. 23, p. 3934, 2022.

[41] M. Verkerken, L. Dhooge, T. Wauters, B. Volckaert, and F. De Turck, "Unsupervised machine learning techniques for network intrusion detection on modern data," in 2020 4th Cyber Security in Networking Conference (CSNet), pp. 1–8, IEEE, 2020.

[42] S. Nayyar, S. Arora, and M. Singh, "Recurrent neural network based intrusion detection system," in 2020 International Conference on Communication and Signal Processing (ICCSP), pp. 0136–0140, IEEE, 2020.

[43] M. A. Khan, "Hcrnnids: hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol. 9, no. 5, p. 834, 2021.

[44] M. D. Rokade and Y. K. Sharma, "Mlids: A machine learning approach for intrusion detection for real time network dataset," in 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), pp. 533–536, IEEE, 2021.

[45] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," Computers & Security, vol. 103, p. 102177, 2021.

[46] M. Al-Fawa'reh, M. Al-Fayoumi, S. Nashwan, and S. Fraihat, "Cyber threat intelligence using pca-dnn model to detect abnormal network behavior," Egyptian Informatics Journal, vol. 23, no. 2, pp. 173–185, 2022.

[47] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with svm for network intrusion detection," Ieee Access, vol. 6, pp. 52843–52856, 2018.

[48] K. Sadaf and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," IEEE Access, vol. 8, pp. 167059–167068, 2020.

[49] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, p. e4150, 2021.

[50] N. Bharathi, “Cert insider threat,” 2023.

[51] T. Boros, A. Cotaie, A. Stan, K. Vikramjeet, V. Malik, and J. Davidson, “Machine learning and feature engineering for detecting living off the land attacks.,” in IoTBDS, pp. 133–140, 2022.

[52] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, “Deep learning for intrusion detection and security of internet of things (iot): current analysis, challenges, and possible solutions,” Security and Communication Networks, vol. 2022, 2022.

[53] Z. Wang, Y. Ren, H. Zhu, and L. Sun, “Threat detection for general social engineering attack using machine learning techniques,” arXiv preprint arXiv:2203.07933, 2022.

[54] M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, and S. Othman, “A detailed analysis of benchmark datasets for network intrusion detection system,” Asian Journal of Research in Computer Science, vol. 7, no. 4, pp. 14–33, 2021.

[55] A. T. Shappie, C. A. Dawson, and S. M. Debb, “Personality as a predictor of cybersecurity behavior.,” Psychology of Popular Media, vol. 9, no. 4, p. 475, 2020.

[56] V. Zimmermann and K. Renaud, “Moving from a human-as-problem to a human-as-solution cybersecurity mindset,” International Journal of Human-Computer Studies, vol. 131, pp. 169–187, 2019.

[57] T. Al-Shehari and R. A. Alsowail, “An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques,” Entropy, vol. 23, no. 10, p. 1258, 2021.

[58] K. Oyibo and J. Vassileva, “The relationship between personality traits and susceptibility to social influence,” Computers in Human Behavior, vol. 98, pp. 174–188, 2019.

[59] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, “Human factor, a critical weak point in the information security of an organization’s internet of things,” Heliyon, vol. 7, no. 3, p. e06522, 2021.

[60] M. Radhi Hadi and A. Saher Mohammed, “A novel approach to network intrusion detection system using deep learning for sdn: Futuristic approach,” arXiv e-prints, pp. arXiv–2208, 2022.

[61] N. Ahmed, A. b. Ngadi, J. M. Sharif, S. Hussain, M. Uddin, M. S. Rathore, J. Iqbal, M. Abdelhaq, R. Alsaqour, S. S. Ullah, et al., “Network threat detection using machine/deep learning in sdn-based platforms: A comprehensive analysis of state-of-the-art solutions, discussion, challenges, and future research direction,” Sensors, vol. 22, no. 20, p. 7896, 2022.

[62] M. Singh, B. Mehtre, S. Sangeetha, and V. Govindaraju, “User behaviour based insider threat detection using a hybrid learning approach,” Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 4, pp. 4573–4593, 2023.

[63] P. López-Aguilar and A. Solanas, “Human susceptibility to phishing attacks based on personality traits: The role of neuroticism,” in 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1363–1368, IEEE, 2021.

[64] K. F. Steinmetz, A. Pimentel, and W. R. Goe, “Performing social engineering: A qualitative study of information security deceptions,” Computers in Human Behavior, vol. 124, p. 106930, 2021.

[65] D. C. Le, N. Zincir-Heywood, and M. I. Heywood, “Analyzing data granularity levels for insider threat detection using machine learning,” IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 30–44, 2020.

[66] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, “Phishing attacks and defenses,” International journal of security and its applications, vol. 10, no. 1, pp. 247–256, 2016.

[67] A. Kayyidavazhiyil and M. Silic, “Intrusion detection using deep (cnn) convolutional neural network feature extraction with (epca) enhanced principal component analysis for dimensionality reduction,” Global journal of Business and Integral Security, 2022.

[68] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, “Insider threat detection with deep neural network,” in International Conference on Computational Science, pp. 43–54, Springer, 2018.

[69] S. Venkatesha, K. R. Reddy, and B. Chandavarkar, “Social engineering attacks during the covid-19 pandemic,” SN computer science, vol. 2, pp. 1–9, 2021.

[70] A. S. Dina and D. Manivannan, “Intrusion detection based on machine learning techniques in computer networks,” Internet of Things, vol. 16, p. 100462, 2021.

[71] M. Nunes, P. Burnap, P. Reinecke, and K. Lloyd, “Bane or boon: Measuring the effect of evasive malware on system call classifiers,” Journal of Information Security and Applications, vol. 67, p. 103202, 2022.

[72] A. Aribisala, M. S. Khan, and G. Husari, “Feed-forward intrusion detection and classification on a smart grid network,” in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0099–0105, IEEE, 2022.