Human-centric Computing and Information Sciences

May 2026 | Volume 16



KCIA
Korea Computer Industry Association

www.hcisjournai.com

HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2026) 16:29
DOI: https://doi.org/10.22967/HCIS.2026.16.029
Received: March 5, 2025; Accepted: May 4, 2025; Published: May 30, 2026

A Meta-Analysis on Insider Threat Detection Using Non-invasive Methods: Analyzing Stress-Inducing Factors and Behavioral Patterns

Jihye Park[1], Sangtae Lee[1], Yelim Jeon[1], and Hangbae Chang[2,*]

Abstract

Detecting Insider threats poses a major challenge due to the limitations of traditional security systems in identifying behavioral anomalies. This study investigated how stress-inducing factors—such as time pressure, workload, and task complexity—affected insider behavior and evaluated the effectiveness of non-invasive detection techniques. A meta-analysis of 30 empirical studies focused on behavioral changes under stress and on the performance of various detection methods including keystroke dynamics, heart rate variability, eye tracking, and electroencephalogram. The findings indicate that keystroke dynamics and heart rate variability are among the most accurate techniques, with highly stressed individuals being up to three times more likely to commit security violations. These results support the integration of stress-aware, non-invasive monitoring into organizational security systems. The study enhances human-centered cybersecurity by validating behavioral monitoring under stress and advocating multimodal approaches to real-time insider threat detection.

Keywords

Insider Threat Detection, Psychological Stress, Non-invasive Monitoring, Meta-Analysis

1. Introduction

1.1 Research Background

With digital infrastructures continuing to expand and organizations increasingly depending on data-driven operations, the assurance of information security has emerged as a critical concern [1–3]. While conventional security systems are primarily designed to mitigate external cyber threats, insider threats pose a multifaceted challenge due to their nuanced, human-centric characteristics. These threats arise from individuals who have legitimate access—such as employees or contractors—and encompass both deliberate breaches and unintentional violations stemming from human error [4, 5].

Despite considerable advancements in cybersecurity tools, traditional detection mechanisms frequently prove to be inadequate in identifying insider threats. Such inadequacy underscores the need for alternative

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
***Corresponding Author:** Hangbae Chang (hbchang@cau.ac.kr)
[1]Department of Security Convergence, Chung-Ang University, Seoul, Republic of Korea
[2]Department of Industrial Security, Chung-Ang University, Seoul, Republic of Korea

methodologies that can effectively capture the underlying psychological and behavioral indicators associated with such threats.

A substantial body of research indicates that deviations in insider behavior are closely associated with psychological conditions particularly stress. Elevated levels of stress are said to impair attention, increase cognitive load, and diminish decision-making accuracy, consequently heightening the probability of both inadvertent errors and violations of policy. In high-pressure environments, stress may lead to alterations in decision-making patterns, whereas excessive workloads can adversely affect compliance with security protocols [6–10]. Nevertheless, most of the previous research studies have been confined to isolated experimental environments, concentrating on individual variables or technologies and lacking comprehensive synthesis across studies [11, 12]. Such fragmented methodology limits the generalizability and practical applicability of the existing findings, especially concerning the comparative effects of various stressors or behavioral signals.

Despite the increasing interest in non-invasive monitoring technologies including keystroke dynamics and physiological sensing, very few studies have undertaken comprehensive evaluations across various organizational contexts. Furthermore, discrepancies in experimental designs, sample populations, and measurement methodologies exacerbate the challenges associated with deriving consistent conclusions. To address the identified gaps in the literature, this study employed a meta-analytic approach to investigate the relationship between stress-inducing factors and insider behavioral patterns. Additionally, it assessed the detection performance of various non-invasive techniques including keystroke dynamics, mouse movement, eye tracking, and physiological metrics such as heart rate variability (HRV) and electroencephalogram (EEG) signals [13–20].

This research highlighted the significance of creating real-time, proactive monitoring systems that could identify anomalies in stress-induced user behavior. By utilizing non-invasive techniques that prioritize scalability and privacy, organizations can effectively detect insider threats without the need for intrusive surveillance or retrospective analysis of system logs [10, 21, 22]. In addition to developing a theoretical framework for the detection of insider threats, this study provided practical insights for the implementation of real-time behavioral monitoring within operational environments. Unlike traditional methods that predominantly depended on system logs or network activity [11, 23], this research highlighted the significance of utilizing real-time behavioral and physiological data to facilitate the early identification of security risks associated with insider threats [24].

The major contributions of this study are summarized as follows:

- Conducted a meta-analysis of 30 empirical studies to quantify the impact of psychological stress on insider behavior.
- Identified and ranked key stress-inducing factors such as time pressure, task complexity, and workload in relation to security risk.
- Evaluated the effectiveness of various non-invasive behavioral monitoring techniques across diverse organizational settings.
- Proposed a task-specific framework for selecting appropriate detection methods based on job characteristics.
- Provided practical insights for real-time, stress-aware monitoring systems balancing privacy and security.

This research enhanced the reliability and applicability of the findings by considering heterogeneity across studies, including variations in sample characteristics, experimental protocols, and measurement tools. Through rigorous quantitative synthesis, it sought to establish a robust, generalizable framework for identifying insider threats based on behavioral signals related to stress.

The rest of this paper is organized as follows: Section 2 provides the theoretical background on insider threats and stress factors. Section 3 outlines the research methodology and meta-analytic procedures. Section 4 presents the results and associated statistical analysis. Finally, Section 5 discusses the findings, limitations, implications for real-world applications, and presents the conclusion together with future research directions.

1.2 Research Questions (RQs)

Insider threats represent a persistent, complex challenge in cybersecurity, largely due to their context-specific characteristics and the limitations of traditional detection mechanisms. Conventional systems that depend on network logs or access histories often fail to capture the underlying psychological or behavioral indicators that precede insider incidents. Although emerging research indicates that psychological stress is a significant precursor to insider misconduct, no previous study has systematically quantified its influence across empirical findings. Similarly, while various non-invasive monitoring techniques—such as keystroke dynamics and HRV—have been proposed, their comparative effectiveness remains uncertain.

To address these critical gaps, this study presented the following central research problem:

How significantly do psychological stressors influence insider behavioral patterns, and how effective are non-invasive behavioral monitoring methods in identifying stress-related insider threats within organizational settings?

From this, three research questions were derived:

RQ1: To what extent do stress-related factors significantly influence changes in insider behavioral patterns?

RQ2: How do the effect sizes of specific stress-inducing conditions—such as time pressure, task complexity, external distractions, and competitive work environments—differ in their impact on insider behavior?

RQ3: How effective are non-invasive monitoring techniques (e.g., keystroke dynamics, mouse movement, eye tracking, and physiological metrics) in identifying insider threats associated with psychological stress?

To answer these questions, this study utilized meta-analysis as a methodological framework for synthesizing effect sizes from a wide range of empirical studies. By examining patterns and variability across previous research, the study aimed to evaluate both the impact of psychological stressors and the effectiveness of non-invasive detection methods in organizational contexts

2. Theoretical Background

2.1 Concept of Insider Data Leak

Insider data leak refers to the act of deliberately or accidentally disclosing confidential information or violating security policies by individuals with legitimate access to an organization, such as full-time employees, contractors, or business partners. These insider-related breaches represent some of the most significant cybersecurity threats today, as they can lead to substantial financial losses, reputational damage, and legal repercussions [5–7].

Unlike external cyberattacks that typically originate from unauthorized actors, insider threats arise from individuals who already have valid access to systems and data [1, 4]. This complicates the task of distinguishing their behavior from normal activities. Traditional detection methods such as firewalls and log analysis tools often fall short in identifying these threats, as they are not specifically designed to recognize misuse by authorized users.

Table 1 illustrates the key differences in detection difficulty between external and internal data leaks. External attacks are generally easier to detect due to their unauthorized nature and the triggering of established security protocols. In contrast, internal threats often circumvent these defenses by operating within permitted boundaries, making them more challenging to identify. For example, subtle behavioral deviations—such as sudden increase in file access or unusual working hours—may go unnoticed without behavior-focused monitoring systems [25]. Such gap in detection underscores the need for more advanced systems that analyze human behavior patterns, stress levels, and contextual clues. These systems can help proactively identify potential insider threats before any actual data leak occurs.

Table 1. Comparative analysis of external and internal data leaks based on detection difficulty

Criteria	External attacks	Internal attacks
Detection difficulty	Easy (Network logs and firewall monitoring)	Difficult (Normal access masks malicious behavior)
Visibility	Easily flagged by IDS/IPS	Blended within legitimate activity
Required tools	Signature-based tools	Behavior-based or context-aware systems
Response time	Often immediate	Often delayed; requires post-incident investigation

2.2 Types of Insider Data Leak

Insider data leak is generally categorized into intentional and unintentional [6, 8]. These two types differ in terms of their causes and detection mechanisms, necessitating distinct security measures and counter strategies.

2.2.1 Intentional leak

Intentional leak refers to the deliberate act of leaking sensitive information by an individual who has authorized access within an organization. This may occur for various reasons, including personal gain, revenge, or political beliefs. Unlike accidental data breaches, intentional data leak is meticulously planned. Insiders often alter their methods of accessing data or exploit vulnerabilities in the security system to evade detection [6].

Detecting this type of threat with traditional security systems poses a challenge, as the individual is utilizing his/her standard access rights. Consequently, it is essential to implement behavior monitoring systems that can identify unusual patterns in a person's work habits [12, 13, 26]. Based on previous research [1–6, 8, 12, 13, 26], intentional insider data leak can be categorized into three primary types (Table 2). These categories reflect distinct motivations and behaviors. For example, an individual seeking to harm his/her organization might share engineering files with competitors. Others may steal and sell data on the dark web. Additionally, some individuals may disclose confidential information as a political act or to expose misconduct.

Table 2. Major types and cases of intentional data leak

Type	Description
Exfiltration of competitive information	Employees leak critical technical information of the organization to competitors
Data sale for financial gain	Insiders sell customer data or sensitive information on the Dark Web
Political or ideological motives	Insiders disclose confidential information externally as an act of opposition to organizational policies or for the purpose of whistleblowing

Table 2 presents typical cases for each category. Notable real-world examples include the Edward Snowden case wherein sensitive information was leaked to reveal government activities (political motivation), and the Capital One insider incident where data was stolen and sold (financial motivation). Research indicates that approximately 75% of insider breaches are intentional, with over 60% involving employees who have special access. These statistics underscore the need for advanced security systems that can detect behavioral changes, instead of relying solely on static security protocols.

2.2.2 Unintentional leak

Unintentional data leak occurs when an employee inadvertently exposes sensitive information. These incidents are not intentional; rather, they result from simple mistakes, carelessness, or lack of understanding of security protocols [5, 9, 19]. Such accidents are more likely to occur when employees are under stress or overwhelmed with work [9, 11]. Stress negatively affects attention and memory,

thereby increasing the likelihood of errors [12]. To mitigate these unintentional threats, organizations can implement non-invasive monitoring methods that detect signs of stress or changes in user behavior. These systems can alert managers when an individual may be at risk of making a mistake. Table 3 presents common examples of unintentional information leak, such as sending an email to the wrong recipient or falling victim to a phishing scam.

Table 3. Major types and cases of unintentional data leak

Type	Description
Misaddressed email transmission	An insider inadvertently transmits a confidential document to an unintended recipient
Security configuration error	Information is exposed externally due to incorrect access permissions configured in cloud storage
Phishing attack response error	An insider erroneously recognizes a phishing email as legitimate communication and provides authentication information

According to recent studies, approximately 60% of data leaks are attributed to insiders, with the remaining 40% originating from external sources (Fig. 1). At least 75% of insider-related leaks are intentional—indicating that these breaches are executed deliberately—whereas 25% are accidental. This data suggests that insiders are the primary source of data loss, with majority of their actions being intentional rather than inadvertent [13, 26].

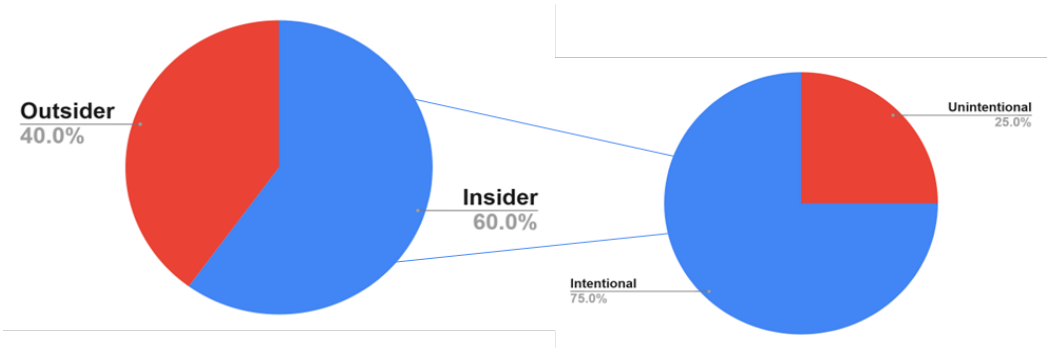


Fig. 1. Proportion of data leak by insider and outsider and distribution of insider threats [1, 3].

Fig. 1 clearly illustrates that insiders are responsible for majority of data breaches and further delineates the division of these insider threats into intentional and unintentional causes. This underscores the need for advanced systems capable of detecting not only rule violations but also behavioral indicators of risk—such as frustration, stress, or other emotional triggers—before any damage occurs.

2.3 Insider Threats and Stress Factors

Traditional security systems such as firewalls and intrusion detection systems have limitations in their ability to mitigate both intentional and unintentional insider threats effectively [27]. Unlike external threats, insiders have legitimate access privileges, and this complicates the detection of malicious activities using conventional security mechanisms. Insider threats include both intentional data exfiltration and unintentional exposure due to negligence, posing a complex security challenge. Recent studies have highlighted stress factors' significant impact on insider behavioral patterns, which subsequently increases the risk of data leak [12, 13, 26]. Insiders are more prone to making errors under conditions of heightened stress, experiencing cognitive overload, or intentionally bypassing security policies due to psychological strain [23, 28].

2.3.1 Key stress-inducing factors

Stress is widely recognized to impact individuals' thoughts, emotions, and behaviors. In the workplace, it can diminish focus, impair cognitive processing, and lead to impulsive decision making—all of which heighten the risk of security errors or intentional violations [23, 29]. Therefore, it is crucial to incorporate stress considerations into security planning and to develop monitoring systems that track user behavior based on stress indicators [8].

Studies have identified four major stress factors that influence insider behavior: time pressure, complex tasks, external distractions, and competitive environments. These stressors are prevalent in today's digital workplaces. For instance, time pressure can lead employees to make hasty decisions without sufficient consideration, whereas task complexity may result in mental fatigue and increase the likelihood of errors.

Recent studies indicate that various stress factors are closely linked to insider threats. Time pressure and challenging tasks can lead to frustration, which may compel insiders to violate rules intentionally [14, 28]. Distractions in the workplace—such as noise or interruptions—often result in careless mistakes or overlooked procedures [15]. In highly competitive environments, employees may choose to disregard policies in order to meet goals or deadlines; thus increasing the risk of deliberate data breaches [16]. The nature of the task being performed can also influence how stress impacts an individual. Simple, repetitive tasks (such as data entry or document review) may appear straightforward; under time constraints or high workloads, however, they can lead to mental fatigue and higher likelihood of unintentional errors. Conversely, complex tasks (such as security audits or code reviews) require deep concentration and attention. Individuals engaged in these tasks may resort to shortcuts or intentionally overlook rules when under stress to expedite their work [30]. These variations demonstrate that stress does not affect all jobs uniformly. Therefore, monitoring systems should not only focus on general stress indicators but should also be tailored to accommodate different job types [8, 13, 28].

Table 4 summarizes how each stress factor influences insider behavior and identifies which types of tasks are most vulnerable. To detect and respond to these risks, organizations should employ non-invasive detection techniques that monitor stress and behavior without the need to attach sensors to employees physically [24]. In addition to behavioral monitoring approaches based on psychological stress indicators, recent studies have investigated insider threat detection methods that leverage machine learning techniques optimized through metaheuristic algorithms [31, 32]. These approaches primarily aim to enhance detection accuracy by applying advanced strategies such as optimized Adaptive Boosting (AdaBoost) classifiers, sentiment analysis, and natural language processing (NLP). Although distinct from stress-based monitoring, this line of research underscores the complementary role that intelligent, optimization-driven systems can play in identifying subtle behavioral anomalies associated with insider threats [33, 34].

Table 4. Stress factors and task-specific vulnerabilities in insider threat contexts

Stress factors	Description	Vulnerable task types
Time pressure	The pressure to increase task execution speed increases the likelihood of insider errors	Repetitive tasks, time-bound decision-making
Task complexity	High complexity increases cognitive fatigue, leading to higher risk of mistakes and violations	Problem solving, risk analysis, code review
External distraction	Environmental noise reduces focus and compliance with security rules	Long-form writing, auditing, system operations
Competitive environment	High-pressure competition may encourage insiders to bypass policies for gain	Performance-driven tasks, sales quotas, high-incentive roles

2.4 Non-invasive Monitoring Techniques

Traditional methods of detecting insider threats have often relied on invasive sensors, such as wearable devices that require direct contact with the body. These devices can be costly and uncomfortable, and they also raise significant privacy concerns [8, 28]. In response to these challenges, researchers have developed non-invasive techniques that identify stress and behavioral patterns without the need for physical contact. These alternative methods are more practical and respectful of individual privacy, making them more appropriate for workplace environments.

Table 5 outlines four common non-invasive techniques used to identify stress that may contribute to insider threats: keystroke dynamics [11, 14, 15], mouse movement tracking [16, 17, 29], eye tracking [7, 18, 19], and HRV monitoring [8, 15, 24]. Each of these methodologies examines the subtle behavioral or physiological alterations typically exhibited by individuals when under stress.

Keystroke dynamics: This method analyzes an individual's typing behavior. Individuals under stress may type more quickly, make a greater number of errors, or strike the keys with increased force. For example, a person rushing to meet a deadline may press the keys more forcefully or take longer pauses between words.

Mouse movement tracking: This method monitors patterns of mouse use. Stressed users may exhibit erratic mouse movements, click excessively, or shake the mouse. A confused user might move the mouse back and forth without completing a task.

Eye tracking: This technique monitors where and how long an individual gazes at a particular object. Individuals under stress may glance around rapidly or avoid making eye contact with the screen. This information is valuable in tasks such as system monitoring where maintaining focus is essential.

Heart rate variability: HRV measures the time interval between heartbeats. A healthy heart typically exhibits small variations between beats, but this variability diminishes during periods of stress. Smartwatches and fitness bands can monitor HRV to identify when an individual may be experiencing mental fatigue.

By utilizing these tools in conjunction, organizations can monitor stress levels while respecting privacy. This proactive approach facilitates the early detection of warning signs, enhances security, and promotes employee mental health by identifying indicators of overload before errors occur.

Table 5. Non-invasive techniques for detecting stress in insider threat contexts

Technique	Description
Keystroke dynamics	Observes typing speed and rhythm; users under stress type faster with more errors
Mouse movement	Tracks cursor patterns; erratic or repetitive movements may indicate stress
Eye tracking	Analyzes gaze and fixations; stressed users show scattered or shortened eye focus
Heart rate variability (HRV)	Measures beat-to-beat heart rhythm changes; lower HRV is a marker of stress

2.5 Definition and Characteristics of Meta-Analysis

Meta-analysis is a statistical technique that allows researchers to combine and compare results from multiple studies on the same topic. Instead of examining each study in isolation, meta-analysis aggregates the findings to identify overarching patterns and trends. This approach facilitates attaining of more reliable and generalizable conclusions than any single study can provide [35]. The process involves gathering data from numerous previous studies, calculating the average (which indicates the strength of the results), assessing the variability among the studies, and searching for potential biases—such as the exclusion of studies with negative results. Depending on the degree of similarity among the studies, researchers select either a fixed-effects model (when the studies are highly similar) or a random-effects model (when there is considerable variation) to ensure accurate results [36–49]. In this research, meta-analysis proved to be valuable as it synthesized a variety of studies concerning stress and insider threats

[37, 48]. Each study employed distinct methodologies, sample sizes, and tools. Attempting to summarize these studies without statistical analysis could result in overlooking significant differences. Meta-analysis addresses this issue by transforming complex data into clear and reliable results [50–57].

To ensure that the results were both accurate and fair, this study employed several established techniques:

Effect size calculations: This section illustrates the impact of stress on behavior. We utilized Cohen's d when comparing two groups, such as individuals experiencing stress versus those who were not. Additionally, we employed Hedges' g, which adjusted for bias in studies with small sample sizes. For binary outcomes such as whether an individual adhered to security protocols, we used odds ratios (OR) to assess relative risks [38, 39, 45].

Heterogeneity assessment: Studies are rarely identical. To quantify the degree of variability among the studies, we utilized I^2 and Q-statistics. If significant differences were observed, we employed a random-effects model, which accounted for variations in study methodologies [45, 47, 58].

Sensitivity analysis: To assess whether a single study significantly impacted the overall results, we utilized a leave-one-out method, which involved removing one study at a time to observe any changes in the outcomes. This approach ensures that our conclusions are not solely reliant on any particularly influential or atypical study [58].

Publication bias check: Occasionally, studies with negative results are not published. To identify this issue, we examined a Funnel plot (a type of graph) and utilized Egger's test for determining whether bias existed in the collected studies.

In sum, meta-analysis was not only appropriate but also essential for this research. It allowed us to synthesize findings from various studies and draw clear, data-driven conclusions about how stress influenced insider behavior, including how we could detect it using non-invasive techniques [48, 50, 51].

3. Research Methodology

3.1 Research Design and Procedure

This study employed a meta-analytic approach to investigate systematically how stress-inducing factors influenced behavioral changes associated with insider threats. Meta-analysis is a statistical technique that synthesizes the results of multiple prior studies to identify patterns, calculate average effects (known as effect sizes), and examine variations among studies (heterogeneity). This method facilitates the drawing of reliable and generalized conclusions by integrating diverse research findings into a cohesive analysis. Specifically, this study focused on previous research that utilized non-invasive monitoring methods—such as keystroke dynamics and physiological sensors—to detect behavioral changes under stress. These methods do not require direct physical contact, and they are considered more practical for implementation in organizational settings. The research followed a six-step procedure:

Step 1 (Literature search and data collection): Relevant academic studies were identified through database searches and use of specific keywords. Studies that examined stress, insider behavior, and detection technologies were selected for review.

Step 2 (Establishment of inclusion and exclusion criteria): Only peer-reviewed empirical studies that reported measurable results such as effect sizes and employed non-invasive methods were included. Studies that lacked clear data or utilized invasive biometric tools were excluded.

Step 3 (Meta-analysis implementation): The selected studies were analyzed using statistical formulas.

- Cohen's d and Hedges' g were employed to compare the behaviors of stressed versus non-stressed individuals.
- OR were calculated for categorical outcomes, such as whether an individual violated a security policy.

Step 4 (Assessment of heterogeneity): The consistency of the included studies was evaluated using statistical tests, specifically the I^2 statistic and the Q test. If significant variation was identified among the studies, a random-effects model was employed to account for these differences in the analysis.

Step 5 (Examination of publication bias): To determine whether studies with negative or non-significant results were absent—a common issue in research—the study employed a Funnel plot (a type of visual chart) and Egger's regression test for statistical validation.

Step 6 (Interpretation and discussion of findings): This study interpreted the extent to which stress factors influenced insider behavior and evaluated the effectiveness of various monitoring methods in detecting these changes.

Through this comprehensive and structured approach, this research aimed to determine whether behavior-based detection models could be effectively employed to identify potential insider threats early—particularly those triggered by stress—before they resulted in actual data breaches.

3.2 Data Collection and Selection Criteria

To ensure the accuracy and comprehensiveness of the research, this study conducted a systematic literature review in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. These guidelines assist researchers in collecting and screening scientific studies in a transparent, replicable manner. Literature searches were performed using four major academic databases—IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink, encompassing studies published from January 2010 to December 2024.

The following Boolean search string was utilized to identify the relevant studies: ("Insider Threat" OR "Insider Attack") AND ("Stress" OR "Stress Factors") AND ("Behavioral Patterns" OR "Non-invasive Monitoring").

Studies that met all of the following criteria were included: (1) empirical studies analyzing the relationship between stress factors and insider threat behavior; (2) research presenting quantitative results such as effect sizes (e.g., Cohen's d, Hedges' g, or OR) or providing sufficient statistical information for such calculations; (3) studies involving non-invasive monitoring methods such as keystroke analysis, mouse movement tracking, eye tracking, or HRV, which are receiving increasing attention in research; and (4) peer-reviewed journal articles or conference papers published in English.

Studies that met any of the following criteria were excluded: (1) theoretical or conceptual papers that do not include data analysis; (2) research lacking sufficient statistical data to calculate effect sizes; (3) duplicated studies or publications utilizing overlapping datasets; and (4) studies focusing exclusively on external cybersecurity threats rather than on insider behavior

After removing duplicates and screening titles and abstracts, 30 empirical studies were selected for full-text review and inclusion in the final meta-analysis. These studies specifically examined how stress factors influenced insider behavior, employing non-invasive methods such as keystroke dynamics, mouse tracking, eye movement patterns, and HRV [14–20, 25, 28, 59–76].

To evaluate the impact of stress on insider threats, this study employed Cohen's d, Hedges' g, and OR, which facilitated comparisons across various data types [50–52]. To assess variability among studies, Higgins' I^2 test and the random-effects model were utilized. Additionally, publication bias was examined using Egger's test and Funnel Plot analysis, ensuring that the results remained robust even if some studies with non-significant findings were not published [54–58, 77–79].

3.3 Data Analysis Methods

This study employed meta-analysis—a statistical technique aggregating results from multiple independent studies—to determine the overall strength (effect size) of relationships and to assess the degree of variability in results across these studies [38, 48, 58].

To conduct the analysis, two tools were used simultaneously: (1) Python, utilizing Jupyter Notebook, was employed for data cleaning, graph generation, and automation; (2) IBM SPSS Statistics, a user-friendly statistical software package, was utilized to calculate effect sizes and assess differences between studies.

To assess the degree of variation among the study results—a concept known as heterogeneity—two common statistical measures were employed [37, 47, 49]: (1) Higgins' I^2 statistic quantifies the percentage of total variation across studies that can be attributed to heterogeneity rather than chance; (2) Q-statistic tests whether the observed variability exceeds what would be expected due to random error.

When substantial heterogeneity was detected, a random-effects model was applied, assuming that each study estimated a different effect size. This approach is suitable when studies vary in sample size, design, or population characteristics. To evaluate potential publication bias, two techniques were utilized: (1) Funnel Plot, which visually detects asymmetry in the distribution of studies; (2) Egger's Regression Test, which statistically assesses small-study effects that may indicate bias.

Finally, a leave-one-out (LOO) sensitivity analysis was conducted to confirm the robustness of the results. In this method, each study is sequentially excluded, and the overall effect is recalculated. Consistent results across iterations suggest that the findings are not unduly influenced by any single study.

3.3.1 Calculation of effect size

Effect size plays a crucial role in meta-analysis by providing a standardized statistical measure that quantifies the strength of the influence of one variable on another [38, 39, 45]. In this study, effect size was employed to evaluate the impact of stress-inducing factors on insider behavioral patterns. By converting findings from multiple studies into a common metric, effect size facilitates consistent comparison and interpretation [40].

To assess these relationships, three primary effect size metrics were employed: Cohen's d, Hedges' g, and OR. Cohen's d measures the standardized mean difference between two groups—for example, individuals experiencing high stress compared to those in low-stress conditions. This metric helps determine the extent to which stress influences user behavior. According to established benchmarks, a d value between 0.2 and 0.5 indicates a small effect, 0.5 to 0.8 signifies a moderate effect, and any value above 0.8 represents a large effect. Since stress often leads to significant cognitive and behavioral changes, large d values are anticipated in the context of insider threat behavior [37, 40, 41]. When sample sizes are small, however, Cohen's d can overestimate the true effect size. To address this issue, Hedges' g is employed as a more accurate alternative. Hedges' g is calculated in a similar manner but incorporates a correction factor that reduces bias, particularly in studies with fewer participants or unequal group sizes. This adjustment ensures that the estimated effect size remains statistically valid across various studies. In cases involving binary outcomes—such as whether a user violated a security policy—the OR is utilized. OR represents the likelihood of an event occurring in one group compared to another. For instance, an OR of 2.0 indicates that users under stress are twice as likely to engage in risky behavior as those who are not under stress. In this study, OR was used to analyze the extent to which specific stressors—such as time pressure, task complexity, and external distractions—increased the probability of security violations [29, 42].

By utilizing Cohen's d, Hedges' g, and OR in conjunction, this research achieved comprehensive, statistically robust understanding of how stress influenced insider behavior. These metrics not only provide insights into individual study findings but also establish a meaningful foundation for drawing generalizable conclusions across the field.

3.3.2 Interpretation of effect size

Accurately interpreting effect size is crucial for understanding the practical implications of the numerical findings in a meta-analysis. This study employed standardized measures—Cohen's d, Hedges' g, and OR—to guarantee that the results of various studies were directly comparable [40, 43, 44]. Cohen's d and Hedges' g are based on a common interpretative framework, where values ranging from 0.2 to 0.5 suggest a small behavioral effect, values between 0.5 and 0.8 indicate a moderate effect, and values exceeding 0.8 signify a strong influence. For instance, if a study shows that stress significantly increases typing errors compared to a low-stress condition and the Cohen's d value is 1.2, this indicates a substantial behavioral shift attributable to stress. However, it is important to note that this effect may be exaggerated

if the study's sample size is small. In such cases, applying Hedges' g can adjust the value to 1.1, for example, thereby providing a more accurate estimate by correcting for sample size bias [39, 40, 44]. The OR serves as an additional interpretive tool for analyzing categorical behaviors. For example, if employees under time pressure commit login errors 30% more frequently than those in normal conditions, OR may be calculated as 3.0. This suggests that stress triples the likelihood of that specific error occurring. OR values greater than 1 indicate an increased probability of behavioral change under stress, whereas values approaching 1 imply a negligible impact [43, 44]. The combination of these effect size indicators provides both statistical precision and practical significance. They facilitate the identification of the stress factors that most significantly predict insider threats, thereby prompting the development of more targeted detection and prevention strategies within organizations.

3.3.3 Analysis of heterogeneity

In the context of conducting a meta-analysis, it is essential to consider the degree of similarity or divergence among the studies being combined. This variability is referred to as heterogeneity. When studies exhibit significant differences, relying on a single average result may lead to misleading conclusions. To quantify this variability, we utilized Higgins' I^2 statistic, which measured the extent to which the observed variation could be attributed to genuine differences between studies rather than random chance [45, 47]. The I^2 statistic ranges from 0% to 100%. A value below 25% suggests that the studies exhibit considerable similarity, indicating low heterogeneity. Conversely, a value between 25% and 50% implies the presence of moderate differences among the studies. A value exceeding 50% indicates substantial differences, reflecting high heterogeneity. High heterogeneity may arise from variations in study methodologies, participant characteristics, or measurement techniques [46, 47].

Previous research examining the relationship between stress and job performance indicated that the I^2 statistic exceeded 60%. Consequently, researchers opted to implement a random-effects model—which accounted for variability among studies—in contrast to a fixed-effects model that assumed that all studies estimated the same parameter. Furthermore, studies employing non-invasive stress detection methods—such as keystroke patterns, mouse use, or heart rate data—also reported high I^2 values surpassing 70%; thus reinforcing the need for a random-effects model [8, 76]. The selection of an appropriate model based on the degree of heterogeneity is crucial. A fixed-effects model is most suitable when studies are comparable, but a random-effects model is preferred when there are significant differences among studies. This methodological approach enhances the overall accuracy and applicability of the findings [47]. In conclusion, evaluating heterogeneity is not merely a technical procedure but is crucial for preserving the integrity of the research. By identifying and accounting for variations across studies, we enhanced the reliability and applicability of our final results in real-world contexts [57, 58].

3.3.4 Publication bias analysis

To ensure the reliability of the results of meta-analysis, it is essential to assess publication bias. This type of bias occurs when studies with significant results are more likely to be published than those with non-significant or negative outcomes. Consequently, the overall findings may appear more robust than they truly are, as missing or unpublished studies are excluded from the analysis [48, 49].

One method of detecting publication bias is the use of Funnel Plot, a graphical representation that compares the effect size of each study (indicating the strength of the results) with the degree of uncertainty or error associated with that study. Typically, studies should create a balanced, funnel-shaped pattern. An uneven or a lopsided pattern suggests that some studies—particularly those with small or non-significant results—may be absent from the literature [48, 50, 51]. To assess this more accurately, researchers employ Egger's regression test. A p-value below 0.05 from this test indicates that the asymmetry observed in the Funnel Plot is unlikely to be due to chance, suggesting the presence of publication bias [52]. In the fields of psychology and behavioral sciences, it is recognized that over 30% of meta-analyses may be influenced by this type of bias, potentially leading to an overestimation of true effects [53].

If bias is detected, researchers can utilize a technique known as the Trim-and-Fill method to address it. This method estimates the number of potentially missing studies and incorporates the estimated studies into the analysis. This approach helps balance the Funnel plot and yields a more accurate overall effect size [54, 55]. In addition, a practice known as selective reporting—where only statistically significant results are published while other outcomes are concealed—can exacerbate the publication bias. This issue is particularly prevalent in fields such as psychology where researchers may face pressure to publish noteworthy findings [56]. By utilizing tools such as Funnel plots, Egger's test, and Trim-and-Fill, researchers can identify and address publication bias. This is crucial for ensuring that the results of the meta-analysis are reliable, accurate, and applicable to real-world scenarios.

3.3.5 Sensitivity analysis

As a crucial procedure in meta-analysis, sensitivity analysis assesses the robustness of the results. It evaluates whether the overall conclusions would change significantly when individual studies are systematically excluded, thereby identifying whether any single study wields a disproportionate influence on the combined effect size [57].

A widely used approach is the LOO method, wherein one study is excluded at a time and the effect size is recalculated. Stable results across all iterations indicate that no individual study unduly influences the findings. Conversely, if the removal of a particular study significantly alters the outcome, this suggests that the study may introduce bias or represent an outlier [38, 48].

Previous research underscores the importance of this process. For instance, Garcia-Leon et al. [77] discovered that excluding specific studies from their meta-analysis on stress and performance resulted in significant variations in effect sizes, necessitating the use of a random-effects model to address study heterogeneity. Comparable trends have been noted in medical and psychological meta-analyses, where sensitivity analyses have proven to be effective in identifying unstable conclusions [58].

Combining sensitivity analysis with techniques such as the Trim-and-Fill method enables researchers to identify missing or biased data, thereby enhancing the credibility of the results. If the findings remain consistent after these adjustments, they can be deemed statistically robust. Conversely, significant fluctuations in the results indicate the need for more thorough examination and careful interpretation [54]. In conclusion, sensitivity analysis enhances confidence in meta-analytic results by ensuring that they are not overly dependent on a small subset of studies. This process improves the validity, generalizability, and scientific rigor of the conclusions drawn.

4. Results

This study employed meta-analysis to evaluate the effectiveness of non-invasive methods in detecting insider threats. Meta-analysis is a statistical technique that synthesizes results from multiple existing studies to identify general patterns and conclusions. In this research, the relationship between stress-related factors and changes in insider behavior was examined. To achieve this, the study calculated effect sizes—a metric used to quantify the strength of the relationship—and applied a random effects model to account for variations among the studies. To ensure that the results were accurate and reliable, the study also assessed publication bias (the tendency to report only positive results) and conducted a sensitivity analysis to evaluate the stability of the findings.

4.1 Validity Verification

4.1.1 Sensitivity analysis

To assess the stability of the findings and ensure that they were not unduly influenced by one or two studies, a sensitivity analysis was conducted. This analysis employed the LOO method, which involved removing one study at a time and recalculating the overall results. This approach enables evaluating whether any single study wields excessive influence on the final outcome [38].

The analysis found that the primary trend of the results remained relatively stable, even when individual studies were excluded. For instance, a metric known as Cohen's d consistently fell within a narrow range of 1.75 to 1.98, and the OR also exhibited stability ranging from 2.35 to 3.10. This suggested that no single study significantly influenced the overall outcome, thereby reinforcing the reliability of the findings. In addition, a tool known as the Baujat plot was utilized to evaluate visually whether certain studies contributed more significantly than others to the observed differences in results. Although a few studies accounted for a larger portion of the variation (heterogeneity), they did not alter the overall conclusion. This indicated that the results were balanced and not unduly influenced by any single dataset [57] (Fig. 2).

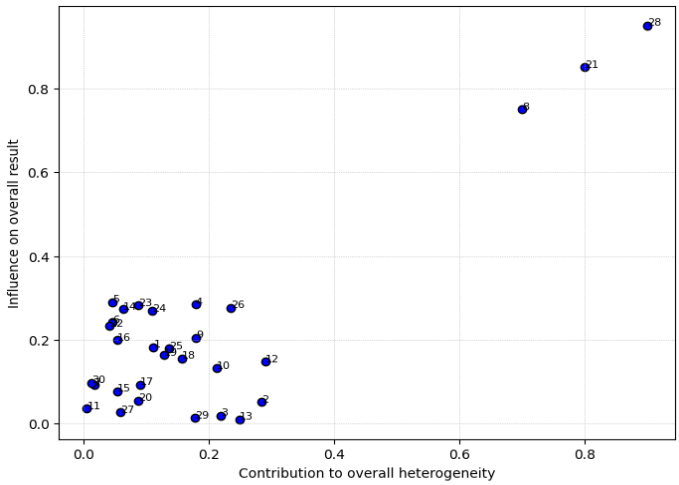


Fig. 2. Baujat plot for sensitivity analysis.

4.1.2 Publication bias analysis

To assess whether the study results may have been affected by publication bias [44, 49]—defined as the tendency to publish only studies with statistically significant outcomes—this research utilized two widely recognized methods: Funnel plot and Egger's regression test [50]. The Funnel plot is a graphical representation that helps detect bias by plotting each study's effect size (the strength of the result) on the horizontal axis and the study's standard error (a measure of uncertainty) on the vertical axis. In theory, if there is no bias, the plot should resemble a symmetrical funnel shape. Conversely, if the shape appears uneven or lopsided, it suggests that only certain types of results—typically significant ones—are more likely to be published [44, 49, 50].

In this study, the Funnel plot displayed pronounced asymmetry, particularly characterized by a lack of studies in the upper right quadrant of the graph (Fig. 3). This pattern suggests the increased likelihood of research yielding significant results being published and studies with non-significant findings being excluded [48]. Furthermore, some studies displayed standard errors that were higher than anticipated, further contributing to the observed irregularity [78]. Collectively, these findings indicate a potential presence of publication bias and warrant further investigation.

To investigate this further, Egger's regression test was conducted (Table 6). The results revealed a *t*-value of -2.08 and a *p*-value of 0.038. Since the *p*-value is less than 0.05, this indicates that the likelihood of publication bias is statistically significant [52]. Consequently, the published results may not accurately represent the full spectrum of findings in the field, particularly those with null or less pronounced outcomes. To address this potential bias, the Trim-and-Fill method was employed (Table 7). This method estimates the number of missing studies needed to achieve symmetry in the Funnel plot and subsequently recalculates the overall effect size. Following the adjustment, the number of studies increased from 30 to 40. The effect size remained statistically significant despite decreasing from -0.41 to -0.17. Additionally,

the Q-value increased, indicating greater variability among the studies; however, this variability reflects inherent differences in study designs and does not undermine the primary findings [50]. In sum, while the presence of publication bias is likely, it does not fundamentally alter the conclusions of this meta-analysis. Even after adjusting for bias, the primary findings remain robust and valid, thereby reinforcing the reliability of the results [48, 55, 80].

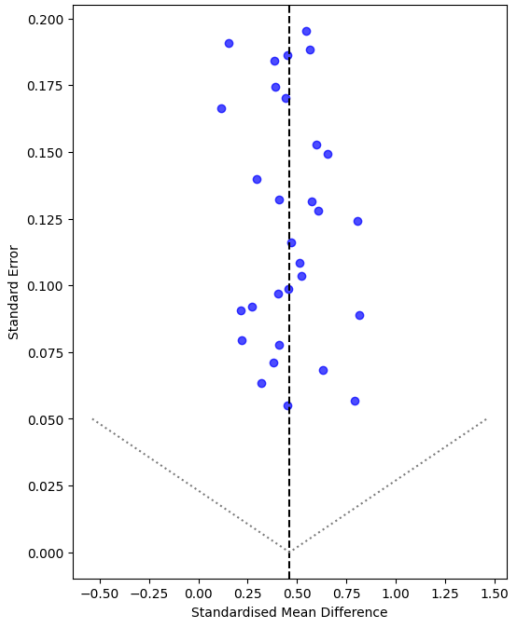


Fig. 3. Funnel plot for publication bias analysis.

Table 6. Results of Egger's regression test

t-value	df	*p*-value
-2.08	28	0.038

Table 7. Results of Trim-and-Fill method analysis

Category	K	Effect size	95% CI		Q
			Lower	Upper	
Observed	30	-0.4128	-0.5784	-0.2397	47.12
Adjusted	40	-0.1695	-0.3215	0.0384	109.85

4.2 Overall Effect Size

4.2.1 Heterogeneity analysis and model selection

To evaluate the consistency of the results across all studies included in this analysis, we conducted a test known as Higgins' I^2. This test measures the degree to which the results from different studies vary due to genuine differences between them, rather than random chance. In this instance, the I^2 value was 76.2%, which was considered quite high. This indicated that the studies differed significantly from one another in aspects such as their design, methods of measuring stress, and participant demographics [46].

Because of this significant variation, we decided against using a fixed effects model. This type of model assumes that all studies measure the same construct in the same manner, which is clearly not applicable in this case. Instead, we employed a Random Effects Model, which accounted for the

differences among studies. This model provides a more realistic, accurate estimate of how stress influences insider behavior when the studies exhibit considerable variability [47, 57, 58]. For instance, some studies primarily examined the effects of time pressure, but others focused on task complexity or external distractions. The methods used to measure stress varied significantly, including keystroke dynamics, mouse movement, and HRV [45–81]. Furthermore, the participants in these studies and the environments in which the research was conducted differed. These variations prompted us to select the Random Effects Model as the most appropriate option. Table 8 presents the results of our variability analysis. The Q-value (Q(df)=125.48, p<0.0001) indicates statistically significant differences across the studies, whereas the high I^2 value (76.2%) confirms a substantial level of heterogeneity. These findings strongly support our decision to employ the Random Effects Model for analyzing the overall effect size.

Table 8. Results of the Heterogeneity analysis

K	Q	Q(df)	*p*-value	I^2
30	125.48	29	< 0.0001	76.2%

4.2.2 Calculation and interpretation of effect size

The results of this study indicate that stress significantly influences the behavior of insiders. To quantify this effect, we employed Cohen's d, a statistical measure assessing the magnitude of differences between two groups: specifically stressed versus non-stressed individuals. In this study, the Cohen's d values exceeded 1.9; hence the "very large" classification. This finding suggests that individuals experiencing stress exhibit substantial changes in their task performance, decision-making processes, and adherence to security protocols. We also utilized another measurement known as Hedges' g, a metric similar to Cohen's d but included a correction factor that enhanced its accuracy particularly when the sample size was small. In this study, the Hedges' g values ranged from 1.85 to 2.10 further indicating that stress had a very strong effect on behavior. Additionally, we assessed the effect using the OR. This statistic indicates the likelihood of an event occurring under specific conditions. Our results showed OR values ranging from 2.5 to 3.5, suggesting that individuals experiencing stress were approximately three times more likely to disclose sensitive information or violate security protocols compared to those who were not under stress. These findings reinforce the notion that stress is a significant contributor to insider threat behavior.

4.2.3 Subgroup analysis and evaluation of the effectiveness of non-invasive methods

To gain deeper understanding of how various types of stress influenced insider behavior, we categorized the stress factors into smaller groups and analyzed them individually [80]. This approach enabled us to identify which specific types of stress were more likely to trigger unusual or risky behavior among employees. We examined five major types of stress: time pressure, complex tasks, environmental distractions, competitive work conditions, and heavy workloads. Among these factors, time pressure had the most significant impact. This finding indicates that individuals facing tight deadlines, are considerably more likely to engage in risky behaviors (Cohen's d=2.61). Similarly, a sudden increase in workload also resulted in a notable change in behavior (Cohen's d=2.45), suggesting that overwhelming work demands could heighten the likelihood of rule-breaking or mistakes [39]. To ensure the reliability of these results, we employed a 95% confidence interval (CI).

This statistical method assesses whether the results are robust and are not merely due to chance. If the interval does not include zero, it suggests that the effect is likely to be genuine. Additionally, we utilized another method known as the Q-test to evaluate the variability among the studies we analyzed. A significantly high Q-test value indicates substantial differences in the results, as indeed observed (Table 9).

Next, we examined the effectiveness of various monitoring methods in detecting changes in stress-related behaviors. These methods include analyzing typing patterns (Keystroke Dynamics), mouse

movements (Mouse Movement), heart activity (HRV), eye movements (Eye Tracking), and brain activity (EEG). Most of these methods demonstrated very high effect sizes (Cohen's d>2.0), indicating their robustness in identifying behavioral changes due to stress [69, 82] (Table 10).

Table 9. Results of effect size analysis by stress factors

Stress factor	k	Effect size (Cohen's d)	95% CI		Q	*p*-value
			Lower	Upper		
Time pressure	30	2.61	2.32	2.90	5.43 (29)*	0.021
Task complexity	28	1.92	1.71	2.13	3.98 (27)*	0.045
External distraction	25	2.13	1.89	2.37	4.21 (24)*	0.039
Competitive environment	22	1.98	1.76	2.20	3.75 (22)	0.050
Workload increase	27	2.45	2.22	2.68	4.95 (26)*	0.028

Observed total variance, k=number of effect sizes, effect size=Hedge's g, 95% CI=95% confidence interval.
*$p<0.05$.

Table 10. Results of effect size analysis by non-invasive methods

Non-invasive method	k	Effect size (Cohen's d)	95% CI		Q	*p*-value
			Lower	Upper		
Keystroke dynamics	25	2.15	1.90	2.40	4.21 (24)*	0.037
Mouse movement	27	2.32	2.10	2.55	4.85 (26)*	0.028
Eye tracking	22	1.89	1.65	2.10	3.90 (21)*	0.045
Heart rate variability	24	2.41	2.20	2.62	5.10 (23)*	0.021
EEG analysis	20	2.05	1.80	2.30	3.75 (19)*	0.048

Observed total variance, k=number of effect sizes, effect size=Hedge's g, 95% CI=95% confidence interval.
*$p<0.05$.

5. Discussion, Conclusion, and Future Work

5.1 Discussion

This study employed a meta-analytic approach—a method synthesizing quantitative results from multiple independent studies—to investigate how psychological stress influenced insider behavior and to evaluate the effectiveness of non-invasive monitoring tools in detecting such behavioral changes. Traditional cybersecurity tools such as intrusion detection systems (IDS) and network log analysis often fall short in identifying threats posed by individuals who already have authorized access. With insider threats becoming increasingly complex and subtle, this research focused on examining how specific stress-related factors—such as time pressure, task complexity, workplace distractions, and increased workload—could modify employees' behaviors and contribute to security risks. Additionally, it assessed whether real-time, contactless monitoring tools could function as effective early warning systems.

The first major finding is that stress has a clear, measurable impact on insider behavior. When individuals experience stress, their cognitive resources become strained, making it more difficult to concentrate, recall information accurately, or make sound decisions. This often results in an increased likelihood of security-related errors such as clicking incorrect links, bypassing the required procedures, or mishandling sensitive data. For example, an employee striving to meet a tight deadline may inadvertently forget to encrypt a file or may use a weak password. Interestingly, the study also found that stressed individuals tended to work more quickly but with higher incidence of errors—suggesting that stress not only impaired adherence to rules but also increased the risk of operational failures. These patterns underscore the importance of recognizing stress as a critical factor in predicting and preventing

insider-related security breaches (RQ1). The second part of the analysis examined how different types of stressors varied in their impact. Among the stressors analyzed, time pressure was found to have the strongest influence on risky insider behavior (Cohen's d=2.61). This indicates that employees working under strict time constraints are significantly more likely to overlook security protocols. Heavy workloads (Cohen's d=2.45) were the next most influential factor, followed by external distractions (Cohen's d=2.13) that could diminish focus and increase the likelihood of unintended mistakes, such as environmental noise or constant notifications. Lastly, task complexity (Cohen's d=1.92) was also associated with more frequent errors, particularly in cognitively demanding tasks like access control or risk auditing. These findings demonstrate that it is not only the identity of those at risk that matters, but also the timing and specific work conditions under which such vulnerabilities are likely to arise (RQ2). The third part of this research evaluated the effectiveness of non-invasive behavioral monitoring methods in identifying stress-related insider risks. As a result, keystroke dynamics (analyzing typing patterns) and HRV monitoring demonstrated the highest accuracy. For instance, keystroke dynamics detected stress-induced changes with over 85% accuracy, whereas HRV consistently reflected physiological stress responses across various tasks. Other methods such as mouse movement tracking and eye tracking were also effective, but their performance varied depending on the specific task. Mouse dynamics proved to be more useful during distraction-heavy tasks, whereas eye tracking was more effective for visually intensive activities such as monitoring dashboards.

To assist organizations in applying these tools more effectively, this study proposes a straightforward classification framework based on the type of work:

For typing-intensive tasks → use of keystroke dynamics

For tasks that require frequent mouse use → use of mouse movement tracking

For visually demanding activities → use of eye tracking technology

For general stress detection across various tasks → use of HRV monitoring

Additionally, the analysis of ORs found that stressed employees were up to three times more likely to engage in security-compromising behavior than their non-stressed counterparts. These findings underscore the significant potential of real-time, stress-aware monitoring systems as proactive tools for preventing insider threats, especially when tailored to the user's role and work context (RQ3).

These findings not only support the cognitive overload theory—which suggests that heightened stress impairs rational decision making—but also provide practical insights for organizational security management. Implementing real-time, stress-aware monitoring can proactively mitigate insider risks before breaches occur, aligning cybersecurity practices with human-centered design principles. Overall, this research emphasized the importance of integrating behavioral and physiological monitoring into next-generation security frameworks.

5.2 Conclusion

This study conducted a meta-analysis of 30 empirical studies to examine how psychological stress influenced insider behavior and to assess the effectiveness of non-invasive behavioral monitoring methods. As a result, stress-related factors—such as time pressure, workload, distractions, and task complexity—were confirmed to increase the risk of security violations substantially.

Among the monitoring techniques evaluated, keystroke dynamics and HRV demonstrated the highest accuracy in detecting stress-induced anomalies. The study proposed a novel task-function mapping framework to guide organizations in selecting context-appropriate tools, thereby enhancing detection efficiency while respecting user privacy.

The primary contributions of this research include:

- Quantitatively established the behavioral impact of key stressors on insider threats.
- Evaluated the effectiveness of four major non-invasive monitoring tools across various task types.
- Introduced a classification framework for practical deployment in real-world settings.

- Highlighted the potential of stress-aware, real-time monitoring systems to prevent security breaches proactively.

By bridging psychology, behavioral science, and cybersecurity, this study advances the field of human-centric computing and offers actionable strategies for insider threat mitigation. Future research should focus on validating these findings in operational environments, exploring the multi-modal integration of behavioral signals, and adapting the framework to diverse industry sectors such as healthcare, finance, and government.

5.3 Limitations

While this study provided valuable insights into the detection of stress-based insider threats, several limitations must be acknowledged. First, the included studies exhibited significant variability in design, encompassing differences in stress measurement methods, sample sizes, and definitions of behavioral change. This heterogeneity, while statistically accounted for, may still impact the reliability and generalizability of the meta-analytic conclusions. Future research should prioritize methodological standardization to facilitate clearer comparisons across studies. Second, the current research focused exclusively on stress as the psychological driver of insider behavior. However, additional factors—such as fatigue, emotional instability, organizational culture, and job dissatisfaction—may also influence security-related behavior. A more comprehensive psychological model should incorporate these variables to reflect the complexity of insider threats more accurately. Third, while the statistical effectiveness of non-invasive monitoring tools (e.g., keystroke analysis, HRV, and eye tracking) has been confirmed, most evidence originates from controlled experimental settings rather than operational environments. Real-world deployment requires addressing challenges such as system integration, scalability, and incident response. Pilot implementations within actual organizations are essential to validate both feasibility and effectiveness. Fourth, ethical and privacy considerations are paramount. Although less intrusive than traditional biometrics, these tools involve continuous monitoring of behavior and physiological states. In the absence of clear governance, this could result in unintended surveillance or misuse. Organizations must establish transparent policies, obtain informed consent, and implement stringent data protection measures along with ethical oversight. Fifth, the scope of the monitoring techniques and contextual applications analyzed in this study was relatively narrow. Although supported by empirical evidence, the selected tools do not encompass the full spectrum of insider threat scenarios. Future research should broaden its focus to include a wider variety of monitoring approaches and evaluate their suitability across different organizational contexts. In summary, although the study contributes significantly to understanding stress and insider risk, advancing this field requires broader psychological modeling, real-world testing, ethical safeguards, and expanded methodological diversity.

5.4 Implications and Future Work

This study provided significant academic, organizational, and practical implications for detecting insider threats through stress-based behavioral monitoring.

From an academic perspective, the study contributed a systematic, quantitative synthesis of how psychological stressors influenced insider behavior. By analyzing data from 30 independent empirical studies, the meta-analysis provided empirical evidence that specific stressors—such as time pressure, workload, distractions, and task complexity—significantly increased the likelihood of human error and policy violations. Unlike previous research that often relied on isolated experiments or theoretical discussions, this work enables comparative evaluation of effect sizes; thus offering a clearer understanding of the psychological mechanisms underlying insider threats. Technologically, the study evaluated the detection performance of four non-invasive monitoring tools: keystroke dynamics, HRV, mouse tracking, and eye tracking. Furthermore, it proposed a task-function mapping framework to guide the selection of the most suitable detection tools based on the job characteristics. This approach not only

integrates the fields of psychology and cybersecurity domains but also opens pathways for the application of human-computer interaction (HCI) research in high-security organizational contexts. On a practical level, the findings can provide multiple real-world strategies. In high-risk environments such as research and development (R&D) where time-sensitive and cognitively intensive tasks are common, stress-based behavioral monitoring systems may serve as early warning mechanisms. Software agents could passively track input behavior or physiological indicators to detect signs of excessive stress, facilitating proactive interventions by human resources or security teams—emphasizing prevention over punishment. Dynamic access control systems can also be deployed to adjust user privileges in real time based on stress levels. For instance, if a highly stressed researcher is working on sensitive intellectual property (IP) late at night, the system may prompt secondary authentication or temporarily restrict access until cognitive indicators stabilize. Combined with real-time alerts and incident response protocols, such measures can significantly reduce the risk of security breaches. Moreover, integrating stress awareness components into security training can enhance employees' understanding of how stress influences decision making and behavior. Organizations can further mitigate insider risks by addressing systemic stressors—such as excessive workloads, ambiguous responsibilities, and lack of feedback—through coordinated efforts between human resources and cybersecurity teams.

The primary contributions of this study are as follows:

- Quantitatively linked psychological stress to insider threat behavior via a meta-analysis of 30 studies.
- Identified and ranked key stressors affecting security compliance.
- Evaluated four non-invasive detection methods across different job contexts.
- Proposed a practical framework to match detection tools with task types.
- Suggested stress-aware security measures including adaptive access control and training.
- Promoted interdisciplinary integration between cybersecurity, behavioral science, and HCI.

In conclusion, this study provided compelling evidence of psychological stress being a critical driver of insider threats. Time pressure was identified as the most influential factor, followed by workload and distractions. Additionally, keystroke dynamics and HRV emerged as the most effective detection tools when tailored to the cognitive demands of specific roles. To advance this field further, several future directions are recommended. First, real-world validation is essential to move beyond theoretical efficacy. Pilot testing in operational settings—particularly within R&D departments where the unique cognitive and emotional stress patterns of researchers require deeper investigation, and in financial sectors where high-stakes, time-critical decision-making presents another application frontier—should be conducted to assess the technical feasibility, user acceptance, and ethical governance of real-time behavioral monitoring systems. Second, future research should broaden the scope of psychological modeling to incorporate variables such as burnout, anxiety, motivational deficits, and organizational climate. These factors may interact with stress in intricate ways, and their inclusion would enhance the ecological validity of insider threat prediction models. Third, advanced detection systems should be developed to integrate multiple data streams—behavioral, physiological, and contextual. For instance, combining keystroke dynamics, HRV, task type, and time-of-day data could improve adaptive and precise access control and anomaly detection capabilities. Finally, sector-specific strategies should be developed to address the distinct risks and operational characteristics of various industries. In particular, R&D environments represent a high-risk domain where information security is critical. Given the concentration of intellectual property and early-stage innovations, even minor behavioral lapses can lead to serious data breaches. These environments are particularly vulnerable to stress-induced errors due to high cognitive load, time constraints, and autonomous working conditions. Therefore, experimental studies based on the current framework should be conducted specifically in R&D settings to validate the effectiveness of real-time stress-based behavioral monitoring empirically. Such domain-specific research may not only enhance the national research security infrastructure but also provide a scalable model for implementation across other high-stakes sectors.

Author's Contributions

Conceptualization, JP, SL, YJ, HC; Investigation, JP; Methodology, JP, HC; Software and validation, JP; Data curation, JP; Visualization, JP; Supervision, HC; Project administration, HC; Funding acquisition, HC; Writing of the original draft, JP; Writing of the review and editing, JP;

Funding

This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (RS-2024-00415520, HRD Program for Industrial Innovation).

Competing Interests

The authors declare that they have no competing interests.

References

[1] A. S. Abdullah, H. Shyam, B. Sriram, A. Ansari, and S. Selvakumar, "A holistic framework for insider threat detection and analysis upon security and privacy for data management services," in *Emerging Threats and Countermeasures in Cybersecurity*. Hoboken, NJ: John Wiley & Sons, 2025, pp. 263-301. https://doi.org/10.1002/9781394230600.ch13

[2] H. Xiao, Y. Zhu, B. Zhang, Z. Lu, D. Du, and Y. Liu, "Unveiling shadows: a comprehensive framework for insider threat detection based on statistical and sequential analysis," *Computers & Security*, vol. 138, article no. 103665, 2024. https://doi.org/10.1016/j.cose.2023.103665

[3] Z. Wei, U. Rauf, and F. Mohsen, "E-Watcher: insider threat monitoring and detection for enhanced security," *Annals of Telecommunications*, vol. 79, no. 11, pp. 819-831, 2024. https://doi.org/10.1007/s12243-024-01023-7

[4] T. A. Al-Shehari, D. Rosaci, M. Al-Razgan, T. Alfakih, M. Kadrie, H. Afzal, and R. Nawaz, "Enhancing insider threat detection in imbalanced cybersecurity settings using the density-based local outlier factor algorithm," *IEEE Access*, vol. 12, pp. 34820-34834, 2024. https://doi.org/10.1109/ACCESS.2024.3373694

[5] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of unintentional insider threats deriving from social engineering exploits," in *Proceedings of 2014 IEEE Security and Privacy Workshops*, San Jose, CA, USA, 2014, pp. 236-250. https://doi.org/10.1109/SPW.2014.39

[6] J. R. Schoenherr, "Insider threats and individual differences: Intention and unintentional motivations," *IEEE Transactions on Technology and Society*, vol. 3, no. 3, pp. 175-184, 2022. https://doi.org/10.1109/TTS.2022.3192767

[7] Y. Han and H. Chang, "Insider threat surveillance system via multimodal-based physical leak detection and optimal imbalanced augmentation in research and development environments," *Human-centric Computing and Information Sciences*, vol. 14, article no. 73, 2024. http://dx.doi.org/10.22967/HCIS.2024.14.073

[8] S. D. Gunawardhane, P. M. De Silva, D. S. Kulathunga, and S. M. Arunatileka, "Non invasive human stress detection using key stroke dynamics and pattern variations," in *Proceedings of 2013 International Conference on Advances in ICT for Emerging Regions (ICTER)*, Colombo, Sri Lanka, 2013, pp. 240-247. https://doi.org/10.1109/ICTer.2013.6761185

[9] F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, "Unintentional insider threat: contributing factors, observables, and mitigation strategies," in *Proceedings of 2014 47th Hawaii International Conference on System Sciences*, Waikoloa, HI, USA, 2014, pp. 2025-2034. https://doi.org/10.1109/HICSS.2014.256

[10] U. Saeed, K. Kumar, M. A. Khuhro, A. A. Laghari, A. A. Shaikh, and A. Rai, "DeepLeukNet—a CNN based microscopy adaptation model for acute lymphoblastic leukemia classification," *Multimedia Tools and Applications*, vol. 83, no. 7, pp. 21019-21043, 2024. https://doi.org/10.1007/s11042-023-16191-2

[11] M. Naegelin, R. P. Weibel, J. I. Kerr, V. R. Schinazi, R. La Marca, F. Von Wangenheim, C. Hoelscher, and A. Ferrario, "An interpretable machine learning approach to multimodal stress detection in a simulated office environment," *Journal of Biomedical Informatics*, vol. 139, article no. 104299, 2023. https://doi.org/10.1016/j.jbi.2023.104299

[12] D. Ackerman and H. Mehrpouyan, "Modeling human behavior to anticipate insider attacks via system dynamics," in *Proceedings of 2016 Symposium on Theory of Modeling and Simulation (TMS-DEVS)*, Pasadena, CA, USA, 2016, pp. 1-6. https://doi.org/10.23919/TMS.2016.7918809

[13] A. Kolakowska, "Towards detecting programmers' stress on the basis of keystroke dynamics," in *Proceedings of 2016 federated conference on computer science and information systems (FedCSIS)*, Gdansk, Poland, 2016, pp. 1621-1626. https://doi.org/10.15439/2016F263

[14] S. Douhou and J. R. Magnus, "The reliability of user authentication through keystroke dynamics," *Statistica Neerlandica*, vol. 63, no. 4, pp. 432-449, 2009. https://doi.org/10.1111/j.1467-9574.2009.00434.x

[15] A. N. H. Nahin, J. M. Alam, H. Mahmud, and K. Hasan, "Identifying emotion by keystroke dynamics and text pattern analysis," *Behaviour & Information Technology*, vol. 33, no. 9, pp. 987-996, 2014. https://doi.org/10.1080/0144929X.2014.907343

[16] P. Zimmermann, S. Guttormsen, B. Danuser, and P. Gomez, "Affective computing—a rationale for measuring mood with mouse and keyboard," *International Journal of Occupational Safety and Ergonomics*, vol. 9, no. 4, pp. 539-551, 2003. https://doi.org/10.1080/10803548.2003.11076589

[17] Y. Hashem, H. Takabi, and R. Dantu, Insider threat detection based on users' mouse movements and keystrokes behavior," in *Proceedings of the Secure Knowledge Management Conference 2017 (SKM)*, Tampa, FL, USA, 2017.

[18] V. A. Yerdon, J. Lin, R. W. Wohleber, G. Matthews, L. Reinerman-Jones, and P. A. Hancock, "Eye-tracking active indicators of insider threats: detecting illicit activity during normal workflow," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3838-3847, 2022. https://doi.org/10.1109/TEM.2021.3059240

[19] H. Takabi, Y. Hashem, and R. Dantu, "Prediction of human error using eye movements patterns for unintentional insider threat detection," in *Proceedings of 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis*, Singapore, 2018, pp. 1-8. https://doi.org/10.1109/ISBA.2018.8311479

[20] A. Almehmadi and K. El-Khatib, "On the possibility of insider threat detection using physiological signal monitoring," in *Proceedings of the 7th International Conference on Security of Information and Networks*, Glasgow, Scotland, UK, 2014, pp. 223-230. https://doi.org/10.1145/2659651.2659654

[21] Y. Said, A. A. Alsheikhy, H. Lahza, and T. Shawly, "Detecting phishing websites through improving convolutional neural networks with Self-Attention mechanism," *Ain Shams Engineering Journal*, vol. 15, no. 4, article no. 102643, 2024. https://doi.org/10.1016/j.asej.2024.102643

[22] B. J. Edelman, S. Zhang, G. Schalk, P. Brunner, G. Muller-Putz, C. Guan, and B. He, "Non-invasive brain-computer interfaces: state of the art and trends," *IEEE Reviews in Biomedical Engineering*, vol. 18, pp. 26-49, 2024. https://doi.org/10.1109/RBME.2024.3449790

[23] A. Alberdi, A. Aztiria, and A. Basarab, "Towards an automatic early stress recognition system for office environments based on multimodal measurements: a review," *Journal of Biomedical Informatics*, vol. 59, pp. 49-75, 2016. https://doi.org/10.1016/j.jbi.2015.11.007

[24] A. A. Laghari, V. V. Estrela, H. Li, Y. Shoulin, A. A. Khan, M. S. Anwar, A. Wahab, and K. Bouraqia, "Quality of experience assessment in virtual/augmented reality serious games for healthcare: a systematic literature review," *Technology and Disability*, vol. 36, no. 1-2, pp. 17-28, 2024. https://doi.org/10.3233/TAD-230035

[25] A. A. Laghari, V. V. Estrela, and S. Yin, "How to collect and interpret medical pictures captured in highly challenging environments that range from nanoscale to hyperspectral imaging," *Current Medical Imaging*, vol. 20, no. 1, article no. e281222212228, 2024. https://doi.org/10.2174/1573405619666221228094228

[26] J. R. Schoenherr, K. Lilja-Lolax, and D. Gioe, "Multiple approach paths to insider threat (map-it): intentional, ambivalent and unintentional insider threats," *Counter-Insider Threat Research and Practice*, 2022 [Online]. Available: https://www.researchgate.net/publication/362269405.

[27] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis," *Big Data Analytics*, vol. 1, no. 1, article no. 6, 2016. https://doi.org/10.1186/s41044-016-0006-0

[28] A. Sultanov and K. Kogos, "Insider threat detection based on stress recognition using keystroke dynamics," 2020 [Online]. Available: https://arxiv.org/abs/2005.02862.

[29] A. Harilal, F. Toffalini, J. Castellanos, J. Guarnizo, I. Homoliak, and M. Ochoa, "TWOS: a dataset of malicious insider threat behavior based on a gamified competition," in *Proceedings of the 2017 International Workshop on Managing Insider Security Threats*, Dallas, TX, USA, 2017, pp. 45-56. https://doi.org/10.1145/3139923.3139929

[30] A. A. Laghari, S. Shahid, R. Yadav, S. Karim, A. Khan, H. Li, and Y. Shoulin, "The state of art and review on video streaming," *Journal of High Speed Networks*, vol. 29, no. 3, pp. 211-236, 2023. https://doi.org/10.3233/JHS-222087

[31] D. Mladenovic, M. Antonijevic, L. Jovanovic, V. Simic, M. Zivkovic, N. Bacanin, T. Zivkovic, and J. Perisic, "Sentiment classification for insider threat identification using metaheuristic optimized machine learning classifiers," *Scientific Reports*, vol. 14, no. 1, article no. 25731, 2024. https://doi.org/10.1038/s41598-024-77240-w

[32] L. Jovanovic, J. Kaljevic, M. Zivkovic, N. Bacanin, M. Antonijevic, and M. Cajic, "Insider threat identification from accessed website content optimized by modified metaheuristic," in *Proceedings of 2024 International Conference on Circuit, Systems and Communication (ICCSC)*, Fes, Morocco, 2024, pp. 1-6. https://doi.org/10.1109/ICCSC62074.2024.10617256

[33] K. Kumpf, M. Protic, L. Jovanovic, M. Cajic, M. Zivkovic, and N. Bacanin, "Insider threat detection using bidirectional encoder representations from transformers and optimized AdaBoost classifier," in *Proceedings of 2024 International Conference on Circuit, Systems and Communication (ICCSC)*, Fes, Morocco, 2024, pp. 1-6. https://doi.org/10.1109/ICCSC62074.2024.10616526

[34] N. Bacanin, L. Jovanovic, S. Janicijevic, M. Antonijevic, M. Sarac, and M. Zivkovic, "Leveraging metaheuristic optimization to enhance insider threat detection through email content natural language processing," in *Intelligent and Fuzzy Systems*. Cham, Switzerland: Springer, 2024, pp. 569-577. https://doi.org/10.1007/978-3-031-67195-1_63

[35] G. V. Glass, "Primary, secondary, and meta-analysis of research," *Educational Researcher*, vol. 5, no. 10, pp. 3-8, 1976. https://doi.org/10.3102/0013189X005010003

[36] J. Prummer, T. van Steen, and B. van den Berg, "Assessing the effect of cybersecurity training on end-users: a meta-analysis," *Computers & Security*, vol. 150, article no. 104206, 2025. https://doi.org/10.1016/j.cose.2024.104206

[37] A. Karabacak Celik, "A reliability generalization Meta-analysis of the PERMA-Profiler," *Social Indicators Research*, vol. 177, no. 3, pp. 1027-1050, 2025. https://doi.org/10.1007/s11205-025-03547-4

[38] S. D. Walter, "Choice of effect measure for epidemiological data," *Journal of Clinical Epidemiology*, vol. 53, no. 9, pp. 931-939, 2000. https://doi.org/10.1016/S0895-4356(00)00210-9

[39] J. W. Kotrlik, and H. A. Williams, "The incorporation of effect size in information technology, learning, information technology, learning, and performance research and performance research," *Information Technology, Learning, and Performance Journal*, vol. 21, no. 1, pp. 1-7, 2003.

[40] M. Moshagen and M. Bader, "semPower: general power analysis for structural equation models," *Behavior Research Methods*, vol. 56, no. 4, pp. 2901-2922, 2024. https://doi.org/10.3758/s13428-023-02254-7

[41] Z. Hussain, M. Binz, R. Mata, and D. U. Wulff, "A tutorial on open-source large language models for behavioral science," *Behavior Research Methods*, vol. 56, no. 8, pp. 8214-8237, 2024. https://doi.org/10.3758/s13428-024-02455-8

[42] L. Theodorakopoulos and A. Theodoropoulou, "Leveraging big data analytics for understanding consumer behavior in digital marketing: a systematic review," *Human Behavior and Emerging Technologies*, vol. 2024, article no. 3641502, 2024. https://doi.org/10.1155/2024/3641502

[43] R. C. Van Aert and C. Goos, "A critical reflection on computing the sampling variance of the partial correlation coefficient," *Research Synthesis Methods*, vol. 14, no. 3, pp. 520-525, 2023. https://doi.org/10.1002/jrsm.1632

[44] C. Andrade, "Mean difference, standardized mean difference (SMD), and their use in meta-analysis: as simple as it gets," *The Journal of Clinical Psychiatry*, vol. 81, no. 5, article no. 20f13681, 2020. https://doi.org/10.4088/jcp.20f13681

[45] C. M. Faggion Jr, M. A. Atieh, M. Tsagris, J. Seehra, and N. Pandis, "A case study evaluating the effect of clustering, publication bias, and heterogeneity on the meta‐analysis estimates in implant dentistry," *European Journal of Oral Sciences*, vol. 132, no. 1, article no. e12962, 2024. https://doi.org/10.1111/eos.12962

[46] H. Zhang, W. Liu, M. Wang, and L. Wang, "A systematic review of meta‐analysis in marketing research: theme analyses, variable selections, and future directions," *Psychology & Marketing*, vol. 42, no. 7, pp. 1741-1761, 2025. https://doi.org/10.1002/mar.22199

[47] M. Borenstein, "How to understand and report heterogeneity in a meta-analysis: the difference between I-squared and prediction intervals," *Integrative Medicine Research*, vol. 12, no. 4, article no. 101014, 2023. https://doi.org/10.1016/j.imr.2023.101014

[48] S. Nakagawa, Y. Yang, E. L. Macartney, R. Spake, and M. Lagisz, "Quantitative evidence synthesis: a practical guide on meta-analysis, meta-regression, and publication bias tests for environmental sciences," *Environmental Evidence*, vol. 12, no. 1, article no. 8, 2023. https://doi.org/10.1186/s13750-023-00301-6

[49] K. Trabelsi, Z. Saif, M. W. Driller, M. V. Vitiello, and H. Jahrami, "Evaluating the reliability of the athlete sleep behavior questionnaire (ASBQ): a meta-analysis of Cronbach's alpha and intraclass correlation coefficient," *BMC Sports Science, Medicine and Rehabilitation*, vol. 16, no. 1, article no. 1, 2024. https://doi.org/10.1186/s13102-023-00787-0

[50] J. Afonso, R. Ramirez-Campillo, F. M. Clemente, F. C. Buttner, and R. Andrade, "The perils of misinterpreting and misusing "publication bias" in meta-analyses: an education review on funnel plot-based methods," *Sports Medicine*, vol. 54, no. 2, pp. 257-269, 2024. https://doi.org/10.1007/s40279-023-01927-9

[51] J. Aisbett, E. J. Drinkwater, K. L. Quarrie, and S. Woodcock, "Applying generalized funnel plots to help design statistical analyses," *Statistical Papers*, vol. 64, no. 1, pp. 355-364, 2023. https://doi.org/10.1007/s00362-022-01322-y

[52] S. Kepes, W. Wang, and J. M. Cortina, "Assessing publication bias: a 7-step user's guide with best-practice recommendations," *Journal of Business and Psychology*, vol. 38, no. 5, pp. 957-982, 2023. https://doi.org/10.1007/s10869-022-09840-0

[53] Z. Irsova, H. Doucouliagos, T. Havranek, and T. D. Stanley, "Meta-analysis of social science research: a practitioner's guide," *Journal of Economic Surveys*, vol. 38, no. 5, pp. 1547-1566, 2024. https://doi.org/10.1111/joes.12595

[54] C. Luo, A. Marks-Anglin, R. Duan, L. Lin, C. Hong, H. Chu, and Y. Chen, "Accounting for publication bias using a bivariate trim and fill meta-analysis procedure," *Statistics in Medicine*, vol. 41, no. 18, pp. 3466-3478, 2022. https://doi.org/10.1002/sim.9428

[55] X. Xing, C. Xu, F. M. Al Amer, L. Shi, J. Zhu, and L. Lin, "Methods for assessing inverse publication bias of adverse events," *Contemporary Clinical Trials*, vol. 145, article no. 107646, 2024. https://doi.org/10.1016/j.cct.2024.107646

[56] J. P. Simmons, L. D. Nelson, and U. Simonsohn, "False-positive psychology: undisclosed flexibility in data collection and analysis allows presenting anything as significant," *Psychological Science*, vol. 22, no. 11, pp. 1359-1366, 2011. https://doi.org/10.1177/0956797611417632

[57] B. Baujat, C. Mahe, J. P. Pignon, and C. Hill, "A graphical method for exploring heterogeneity in meta-analyses: application to a meta‐analysis of 65 trials," *Statistics in Medicine*, vol. 21, no. 18, pp. 2641-2652, 2002. https://doi.org/10.1002/sim.1221

[58] M. Borenstein, "Avoiding common mistakes in meta‐analysis: Understanding the distinct roles of Q, I-squared, tau-squared, and the prediction interval in reporting heterogeneity," *Research Synthesis Methods*, vol. 15, no. 2, pp. 354-368, 2024. https://doi.org/10.1002/jrsm.1678

[59] A. Kim, J. Oh, J. Ryu, and K. Lee, "A review of insider threat detection approaches with IoT perspective," *IEEE Access*, vol. 8, pp. 78847-78867, 2020. https://doi.org/10.1109/ACCESS.2020.2990195

[60] M. Yildirim and E. Anarim, "Mitigating insider threat by profiling users based on mouse usage pattern: ensemble learning and frequency domain analysis," *International Journal of Information Security*, vol. 21, no. 2, pp. 239-251, 2022. https://doi.org/10.1007/s10207-021-00544-9

[61] A. S. Anakath, R. Kannadasan, N. P. Joseph, P. Boominathan, and G. R. Sreekanth, "Insider attack detection using deep belief neural network in cloud computing," *Computer Systems Science & Engineering*, vol. 41, no. 2, pp. 479-492, 2022. https://doi.org/10.32604/csse.2022.019940

[62] X. Wang, Q. Tan, J. Shi, S. Su, and M. Wang, "Insider threat detection using characterizing user behavior," in *Proceedings of 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*, Guangzhou, China, 2018, pp. 476-482. https://doi.org/10.1109/DSC.2018.00077

[63] J. Ferreira, H. Santos, and B. Patrao, "Intrusion detection through keystroke dynamics," in *Proceedings of the 10th European Conference on Information Warfare and Security*, Tallinn, Estonia, 2011, pp. 81-90.

[64] D. Rudrapal, S. Das, N. Debbarma, and S. Debbarma, "Internal attacker detection by analyzing user keystroke credential," *Lecture Notes on Software Engineering*, vol. 1, no. 1, pp. 49-52, 2013.

[65] B. M. Babu and M. S. Bhanu, "Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud," *Procedia Computer Science*, vol. 54, pp. 157-166, 2015. https://doi.org/10.1016/j.procs.2015.06.018

[66] L. He, Z. Li, and C. Shen, "Performance evaluation of an anomaly-detection algorithm for keystroke-typing based insider detection," *Tsinghua Science and Technology*, vol. 23, no. 5, pp. 513-525, 2018. https://doi.org/10.26599/TST.2018.9010014

[67] A. Aggarwal and R. K. Dhurkari, "Association between stress and information security policy non-compliance behavior: a meta-analysis," *Computers & Security*, vol. 124, article no. 102991, 2023. https://doi.org/10.1016/j.cose.2022.102991

[68] Y. Hashem, H. Takabi, M. GhasemiGol, and R. Dantu, "Towards insider threat detection using psychophysiological signals," in *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, Denver, CO, USA, 2015, pp. 71-74. https://doi.org/10.1145/2808783.2808792

[69] A. Y. Al Hammadi, D. Lee, C. Y. Yeun, E. Damiani, S. K. Kim, P. D. Yoo, and H. J. Choi, "Novel EEG sensor-based risk framework for the detection of insider threats in safety critical industrial infrastructure," *IEEE Access*, vol. 8, pp. 206222-206234, 2020. https://doi.org/10.1109/ACCESS.2020.3037979

[70] G. Matthews, L. Reinerman-Jones, R. Wohleber, and E. Ortiz, "Eye tracking metrics for insider threat detection in a simulated work environment," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 61, no. 1, pp. 202-206, 2017. https://doi.org/10.1177/1541931213601535

[71] G. Matthews, R. Wohleber, J. Lin, L. Reinerman-Jones, V. Yerdon, and N. Pope, "Cognitive and affective eye tracking metrics for detecting insider threat: a study of simulated espionage," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 62, no. 1, pp. 242-246, 2018. https://doi.org/10.1177/1541931218621056

[72] S. Eberz, K. Rasmussen, V. Lenders, and I. Martinovic, "Preventing lunchtime attacks: fighting insider threats with eye movement biometrics," in *Proceedings of the Network and Distributed System Security (NDSS) Symposium*, San Diego, CA, USA, 2015. https://dx.doi.org/10.14722/ndss.2015.23203

[73] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: exposing insider threats using eye movement biometrics," *ACM Transactions on Privacy and Security (TOPS)*, vol. 19, no. 1, article no. 1, 2016. https://doi.org/10.1145/2904018

[74] L. Reinerman-Jones, G. Matthews, R. Wohleber, and E. Ortiz, "Scenarios using situation awareness in a simulation environment for eliciting insider threat behavior," in *Proceedings of 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Savannah, GA, USA, 2017, pp. 1-3. https://doi.org/10.1109/COGSIMA.2017.7929611

[75] Z. H. Shokishalov and H. Wang, "Applying eye tracking in information security," *Procedia Computer Science*, vol. 150, pp. 347-351, 2019. https://doi.org/10.1016/j.procs.2019.02.062

[76] A. A. Laghari, Y. Sun, M. Alhussein, K. Aurangzeb, M. S. Anwar, and M. Rashid, "Deep residual-dense network based on bidirectional recurrent neural network for atrial fibrillation detection," *Scientific Reports*, vol. 13, no. 1, article no. 15109, 2023. https://doi.org/10.1038/s41598-023-40343-x

[77] M. A. Garcia-Leon, J. M. Perez-Marmol, R. Gonzalez-Perez, M. del Carmen Garcia-Rios, and M. I. Peralta-Ramirez, "Relationship between resilience and stress: perceived stress, stressful life events, HPA axis response during a stressful task and hair cortisol," *Physiology & Behavior*, vol. 202, pp. 87-93, 2019. https://doi.org/10.1016/j.physbeh.2019.02.001

[78] J. E. Pustejovsky and M. A. Rodgers, "Testing for funnel plot asymmetry of standardized mean differences," *Research Synthesis Methods*, vol. 10, no. 1, pp. 57-71, 2019. https://doi.org/10.1002/jrsm.1332

[79] F. Bartos, M. Maier, E. J. Wagenmakers, F. Nippold, H. Doucouliagos, J. P. Ioannidis, et al., "Footprint of publication selection bias on meta-analyses in medicine, environmental sciences, psychology, and economics," *Research Synthesis Methods*, vol. 15, no. 3, pp. 500-511, 2024. https://doi.org/10.1002/jrsm.1703

[80] P. Cuijpers, J. W. Griffin, and T. A. Furukawa, "The lack of statistical power of subgroup analyses in meta-analyses: a cautionary note," *Epidemiology and Psychiatric Sciences*, vol. 30, article no. e78, 2021. https://doi.org/10.1017/S2045796021000664

[81] S. Mondal and P. Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1-22, 2017. https://doi.org/10.1016/j.neucom.2016.11.031

[82] S. Das, A. Adhikary, A. A. Laghari, and S. Mitra, "Eldo-care: EEG with Kinect sensor based telehealthcare for the disabled and the elderly," *Neuroscience Informatics*, vol. 3, no. 2, article no. 100130, 2023. https://doi.org/10.1016/j.neuri.2023.100130