IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 31, 2020, accepted April 18, 2020, date of publication April 23, 2020, date of current version May 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2989739

Empirical Detection Techniques of Insider Threat Incidents

RAKAN A. ALSOWAIL AND TAHER AL-SHEHARI
Deanship of Common First Year, King Saud University, Riyadh 12373, Saudi Arabia
Corresponding author: Taher Al-Shehari (talshehari.c@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research at King Saud University through research group no. RG-1441-401.

ABSTRACT Vital organizations have faced increasing challenges of how to defend against insider threats that may cause a severe damage to their assets. The nature of insider threats is more challenging than external threats, as insiders have a privileged access to sensitive assets of an organization. In fact, there are several studies that reviewed the insider threat detection approaches from taxonomical and theoretical perspectives. However, the protection against insider threat incidents requires empirical defense solutions. Hence, our study uniquely focuses on empirical detection approaches that are validated with empirical results. We propose a 10-question model that highlights different prospective of empirical detection approaches. Significant factors are also proposed to reveal the extent to which the detection approaches are effective against insider threat incidents (e.g., feature domains, protection coverage, classification techniques, simulated scenarios, performance and accuracy metrics, etc.). The objective of this paper is to enhance researchers' efforts in the domain of insider attack by systemizing the detection techniques in comparable manner. It also highlights the challenges and gaps for further research to institute more effective solutions that can predict, detect, and prevent emerging attack incidents. Some recommendations for future research directions are also presented.

INDEX TERMS Insider threat, rigorous literature review, 10-question model, insider attack detection, information security.

I. INTRODUCTION

Currently, insider threats become a major concern for many organizations around the world. The main challenge behind insider threat is that, insiders are authorized users who have legitimate access to sensitive assets of an organization. This has made the detection and prevention of insider attack more challenging than external attack. A large body of work exists in the literature to secure organizations' assets against insider attacks.

A. INSIDER THREAT DEFINITION

An insider threat has been defined in the literature from different perspectives. Cappelli *et al.* [1] defined insider threat as ''a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems''. This definition is derived from hundreds of cases studies conducted by Computer Emergency Response Team (CERT). Pfleeger *et al.* [2] also defined the insider threat as actions of an insider that creates a risk for an organization's resources in a disruptive way. Theoharidou *et al.* [3] defined the insider threat as the originating threat from an individual who has been given an authorized access to an information system and misuse their privileges by violating the organization's security policy.

The insider threat definition in [2], [4]–[6] differentiated between the accidental and intentional aspects of insider threat incidents. While in [1], [3], and [7] the focus was on intentional threat of insiders who intentionally exceed or misuse their access negatively. Furthermore, Schultz [8] assured that only the intentional malicious incidents should be considered in insider threat topic of studies. We refer to the survey in [9] for detailed overview of various definitions of insider threat.

B. INSIDER ATTACKS, TRENDS AND CONSEQUENCES

Recent studies have shown that insider attacks are costlier for organizations than external threats. This section summarizes

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

the major trend and consequences of insider attack incidents according to the up-to-date surveys and technical reports. Ponemon Institute [10] benchmarked the insider incidents over a 12-month period by interviewing 717 IT security practitioners in 159 organizations from United States, Canada, Europe, Asia-Pacific, Africa and Middle East. The targeted organizations of the study were in business sector with more than 1,000 employees each. According to the study, the organizations experienced a total of 3.269 incidents with an average cost of $8.76 million.

IBM published an X-Force® Threat Intelligence Index report [11] that illustrated the most common types of attacks. According to the report, insider threats are the source of 60 % of cyberattacks which caused two-third of compromised data. In addition, over 2 billion records are exposed by misconfiguring the servers and backup incidents of insiders.

Crowd Research Partners [12] conducted a survey based on 472 cybersecurity professionals to reveal the latest trends on insider attacks. It found that 90% of organizations still feel vulnerable to insider attacks. Also, 33% of organizations experienced five or less insider attacks, and 27% expressed that insider attacks have become more frequent. The survey indicated that regular employees (56%) and privileged IT users (55%) are the biggest insider threats to organizations, followed by contractors with (42%). In addition, the cost of insider incidents is ranged from $100,000 to $500,000 per a successful attack. To address such attacks, 94% of organizations implemented some methods for monitoring their employees, whereas 93% of organizations deployed mechanisms for monitoring the access to their sensitive data. Besides, 43% of organizations allocated over 8% of their IT budget to detect, prevent, and mitigate insider threat incidents.

The CERT and the U.S. Secret Service evaluated the actual insider attack incidents. In [13], they presented 1,500 malicious insider crimes as categorized in Figure 1.

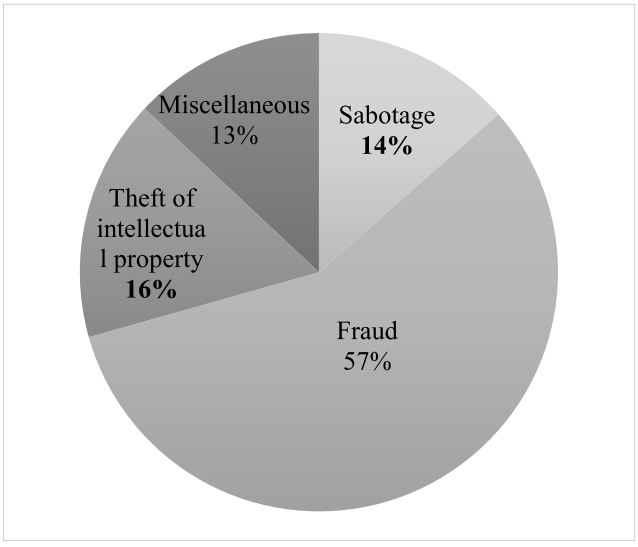

FIGURE 1. Categories of insider attack incidents.

The observed attacks are categorized into four classes: First, 156 sabotage cases are directed toward an individual or an organization for the aim of disrupting their business. Second, 659 fraud cases where executed to modify, add or delete the data assets for personal gains. Third, 189 theft cases were conducted to steal IP for violating the intellectual property of their organization. They also found that 85 cases overlapped and fell into more than one class. The last class is the miscellaneous (65 cases) in which the activity of the insider was not included in sabotage, fraud or IP theft.

The most dangerous insider attacks that caused an immense damage to the reputation of the U.S. and French bank Societe Generale [5] as follows. Robert Hanssen, one of the employees of the U.S. Federal Bureau of Investigation (FBI), who abused his access to a confidential data and sold FBI's secrets to Russian agencies which resulted in much damage to the public image of FBI and the U.S. as well. It was considered as the most dangerous spy in the U.S. history. Bradley Manning, one soldier of the U.S. army who leaked numerous of sensitive documents about the U.S. government to WikiLeaks. In addition, French bank Societe Generale lost $7 billion by a fraud act committed by one of its employees.

Apart from aforementioned attacks and their implications, several insider attacks are not reported for various reasons. Kuheli [14] illustrated four reasons of why insider attacks are not being reported by organizations: (1) to avoid the negative publicity and reputation; (2) the difficulty of detecting criminal insiders; (3) the ignorant of insider attacks; (4) the low impact of incidents the do not deserve a warrant prosecution. Furthermore, Shaw *et al.* [15] noted that to avoid any bad impact toward individuals or organizations, insider incidents are often addressed internally without reporting them to the public. So, although the severe damage of insider threat incidents that was reported above, many incidents were not announced for the above mentioned reasons.

C. DEFENSE SOLUTIONS AGAINST INSIDER ATTACKS

The huge financial, reputational and operational impacts of insider attacks require significant attention from individuals and organizations. To address such issues, researchers have made insider threat an active area of research by proposing several solutions, especially in the last decade. Likewise, several organizations, like the U.S. Secret Service, invested largely in this area of research. Although many approaches have been proposed to address insider threat problems, insider attack incidents still have not been addressed effectively. So, there is a need for strong and more accurate solutions to encounter insider threat issues efficiently.

Through our survey on the current solutions, they can be categorized into both prevention and detection approaches. The prevention approaches prevent unauthorized actions of confidential data (e.g., access, copy, edit, delete, etc.). They deploy access control mechanisms like authentication to prevent insiders' misuses. A prevention solution includes a detection mechanism to identify a suspicious activity and takes an action to stop potential attacks [16]. It was noted

in [17] and [16] that there is a little work in the literature that prevent insider attacks. The most prevention approaches known as Data Leakage Prevention Systems (DLPS) are focused to prevent data leakage incidents. This category is covered in [18], as the focus of our article is insider threat detection approaches.

This paper concentrates on detection approaches that address insider threat incidents from different prospective. The contributions of this paper are summarized as follows:

- It presents the trends and consequences of real insider attacks that resulted in severe financial and reputational losses for various organizations. It also demonstrates the major necessity for effective and robust solutions to predict, detect and prevent insider threat incidents.
- It proposes a unified model compound of 10 research questions that highlight significant factors of detection systems (e.g., types of addressed attacks, the range of violating security goals confidentiality/integrity or availability, detection mechanisms, datasets, feature domains, classification algorithms, implemented scenarios, limitations, OS platforms and tools, accuracy and performance metrics). These factors are also extended to more fine-grained elements (e.g., malicious insiders, masqueraders, anomaly-based, signature-based, etc.). Such factors are discussed in details in Section 5.
- It demonstrates the challenges of applying effective and real-world insider threat detection solutions, and shows the limitations of existing approaches.
- It recommends the future researchers on insider threat domain with some guidelines for developing robust solutions. Some research gaps observed from the literature are also highlighted.

The rest of the paper is organized as follows; Section 2 reviews the existing surveys on insider threat detection theme, and shows how our approach varies from them. Section 3 summarizes the research methodology that we adopted in this study. Our research approach and the scope of our study are clarified in Section 4. The detailed demonstration of our proposed model and findings are illustrated in Section 5. Finally, the paper concludes with challenges, limitations and recommendations.

II. RELATED WORK

The insider threat is a nascent research field, so there is a couple of surveys in the area that categorized existing approaches from different perspectives. In this section we provide a brief outline of existing surveys and show how our paper differs from them. We summarize them in ascending chronological order from the oldest to the most recent one. Bertacchini and Fierens [19] proposed a categorization of masquerader detection approaches in Unix command domain. They classified the available UNIX command line datasets and masquerader detection approaches based on different criteria. They also compared between measures and results achieved by the reviewed approaches.

In [20], the authors conducted a literature review by categorizing the malicious insiders into two classes: traitors (a legitimate user within an organization) and masqueraders (attackers who steal the credentials of legitimate users). They classified the auditing sources and different machine learning algorithms based on host-based, network-based and integrated user profiling.

Hunker and Probst [5] discussed the definitions of insiders, insider threats and relevant issues. They also categorized the insider threat approaches into different domains (organizational, socio-technical and technical). The authors concluded that the qualified system to detect and mitigate insider threats requires a combination of psychological, socio-technical and technical techniques. In [21], some of detection approaches are discussed briefly from a variety of perspectives (Intrusion-detection-based, System-call-based, Data-centric, Honeypot, Dynamical-system-theory-based, Anti-indirect-exfiltration and Visualization) as well as presenting some of their pros and cons. Azaria *et al.* [22] categorized insider threat detection techniques into different classes: anomaly-based, psychological and social theories, honeypot-based, graph-based and game theory-based. They also presented their behavioral analysis of insider threat (BAIT) framework using a game on Amazon Mechanical Turk (AMT) to measure the behavior of honest insiders and malicious ones who attempt to leak the data from their organization.

Ophoff *et al.* [23] classified the insider threat articles into five categories: Theoretical Perspective, Insider Threat Behavior, Insider Threat Mitigation, Insider Threat Management, Insider Threat Overview and Miscellaneous. This work categorized the insider threat articles from 1997 to 2013 as numbers only rather than giving an overview about the underlined approaches. Gheyas and Abdallah [24] conducted a systematic literature review by applying the method of [25] for systematic reviews and meta-analyses. The authors presented the research trends in insider threat detection and prediction just only by reviewing 13 articles.

In [17], the insider threat detection methods are classified according to the techniques and features used for the detection. They presented their taxonomy into Anomaly based, Role Based Access Control, Scenario-Based, etc. Thing *et al.* [26] categorized the behavior of insiders into four classes: biometric behaviors, psychosocial behaviors, communication behaviors and cyber behaviors. They also summarized the approaches that produced public datasets with malicious data.

In [16], the authors compiled the definitions of insider threat based on three types (traitor, masquerader, and unintentional perpetrator). They also categorized the insider threat approaches according to the auditing data source into host, network, and contextual data-based analytics. The most recent survey conducted in [9] where the structural taxonomy of insider threat incidents are categorized based on 5W1H questions [27] for information gathering problem. They also identified the approaches based on discrete events, system

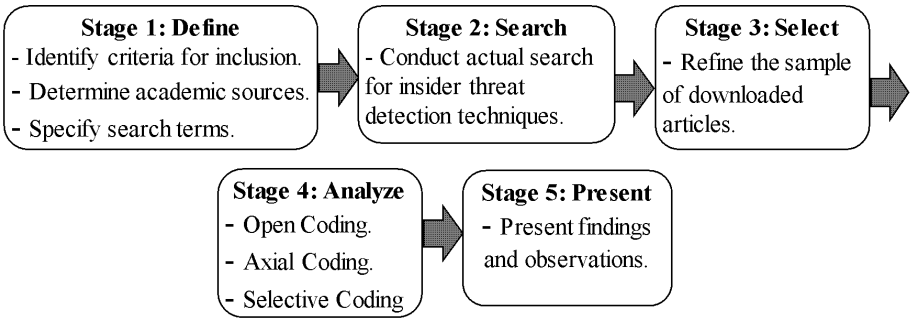

FIGURE 2. Grounded theory methodology employed in our study.

dynamics, game theory and defense solutions. The authors paid more attention to the definitions and taxonomies of insider threats incidents.

However, the main challenge in insider threat area is to build highly accurate systems that can predict, detect and prevent insider attacks on a real-time basis. The area of insider threats and their defense solutions is still not understood very well. Several surveys tried to facilitate the field by focusing exclusively on theoretical and conceptual taxonomies. Some surveys concentrated on a specific topic, for example: Bertacchini and Fierens [19] focused on masquerader detection approaches; Thing *et al.* [26] and Hunker and Probst [5] paid attention to behavioral approaches. Other surveys reviewed the current approaches in a coarse-grained level without going deeply to highlight the main factors that stand behind the effectiveness of defense solutions. Therefore, we realized that there is a pressing need for a systematic review to figure out the main characteristics that have a direct impact on the efficiency of empirical solutions such as dataset, feature domain, utilized algorithms, accuracy and performance metrics, etc. So, the objective of our paper is to focus on such factors by proposing a classification model comprised of 10 research questions as detailed in section 4. By answering those questions, we believe that our paper introduces a better understanding of the field, and provides a comprehensive and updated reference for future work.

III. METHODOLOGY

Starting a review with a well-defined methodology allows us to analyze and answer our research questions adequately. This section illustrates the grounded-theory methodology [28] that we follow in our study, as summarized in Figure 2.

The employed methodology contains of five stages that enable us to review the selected articles and analyze them for addressing our research questions. Such stages are summarized as follows:

1) Define: In the initial stage, the criteria for including and excluding the articles is identified. The field of insider threat is quite broad, so the scope of our research topic is specified as ''insider threat detection techniques that are validated with empirical results''. Thus, theoretical approaches are beyond the scope of our study. For theoretical approaches, we refer the readers to [9]. In this stage, academic sources (Web of science, Google Scholar and Scopus databases) are also determined. Furthermore, appropriate search terms are also specified with various forms (e.g., ''insider threat detection'', ''insider attack detection'', ''detecting insider attack'' and ''detecting insider threat'') in order to reflect the entire scope of our selected topic.
2) Search: The second stage is aimed to the actual search for articles using specified academic sources and search terms. During our search, synonyms of search terms (e.g., attacks, threats, issues, incidents, insiders, internal attackers, etc.) are also considered to ensure that the scope of our study is covered widely. Moreover, while we are searching, separated terms like ''insider attack'' are included between quotes inside the search box to narrow down the obtained articles. This is for not retrieving irrelevant articles that may contain separated words of the search terms. Bibliographies of downloaded articles are also scanned to search further for any relevant work. As a result of the search stage, 152 articles of insider threat detection approaches are gained.
3) Select: Not all retrieved articles are appropriate for inclusion, so the resulted articles are examined. This is achieved by reading the title, abstract, and some sections of each article in the sample set. We included only articles that are supported with experimental results, as our focus is the empirical techniques. After filtering

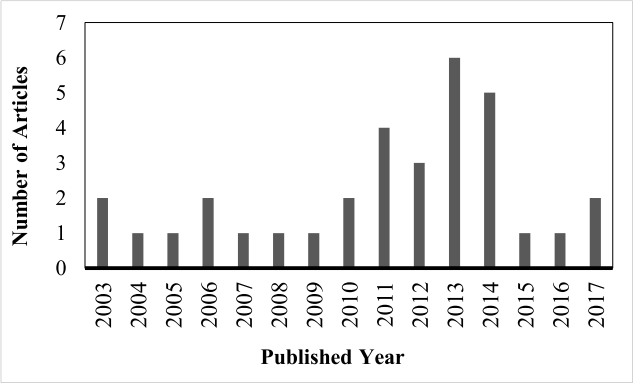

FIGURE 3. Articles' distribution of insider threat detection approaches.

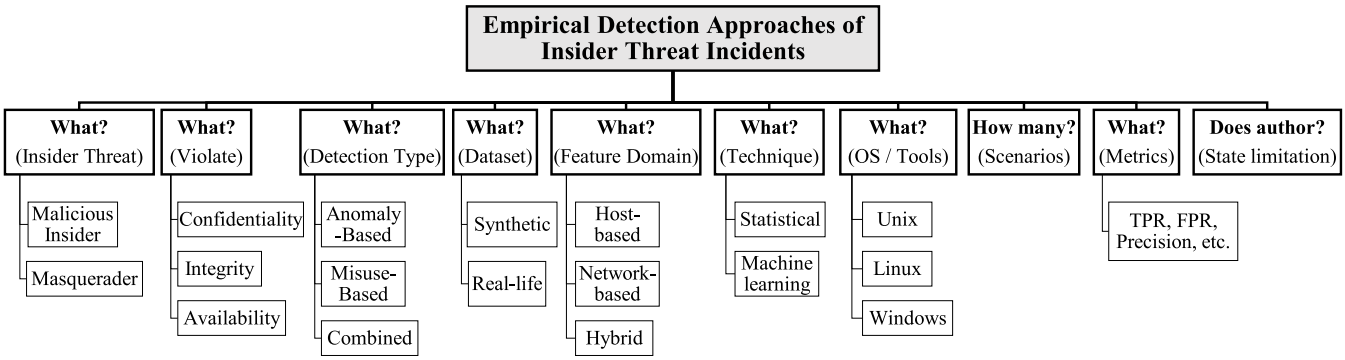

FIGURE 4. The proposed question model10 proposed questions of empirical detection approaches of insider threat incidents.

out theoretical and duplicate articles, the sample set is refined more by selecting articles that are published on journals and conference proceedings. To this point, 33 papers are selected for analysis. The distribution of selected articles is shown in Figure 3. It shows a rising interest in this area over the last two decades.

4) Analyze: After the articles have been selected, the actual analytical work is conducted. This is achieved by reading the articles line by line carefully and highlighting the findings that are relevant to our research questions. Every selected article eventually undergoes this highlighting process. Thus, each highlighted sentence represents excerpt or selection. Then, the three Grounded Theory steps (open coding, axial coding, and selective coding) are implemented: In open coding, each individual article has been read again line by line to identify 55 open codes. In axial coding, 23 codes are synthesized based on their conceptual similarities. Then, the selective coding step is executed. To conduct such processes, we utilize the Saturate tool,[1] a web-based open coding tool that is used to enable the traceability between codes and data. An overview of resulted codes is presented in Appendix A.
5) Present: After continuous iterative analysis, the findings, observations and discussion of our 10-question model are described in detail in the next sections.

IV. CLASSIFICATION MODEL

In fact, there is a need for a comprehensive study to demonstrate the empirical factors of insider threat detection techniques. This section outlines such factors in terms of 10-question model. An overview of our model is depicted in Figure 4.

The aim of this article is to assist the researchers in assessing the existing approaches from empirical prospective. In our model, we first classify and refine the articles of the studied topic (resulting with 33 empirical studies). Then, we formulate 10 research questions that highlight some quantitative and qualitative factors of the existing works. The research questions being addressed are as follows:

- What is the addressed threat?
- Which "CIA" is/are violated?
- What is the detection method?
- What is the dataset for validating an approach?
- What is the feature domain?
- What is the classification technique?
- How many threat scenarios in each approach?
- Do the authors mention the limitation of their approach?
- What are the utilized platforms and tools?
- What are the accuracy and performance metrics?

The answering and analyzing of such questions will enable a clear understanding of existing approaches for the possibility of devising more effective solutions. The detailed analysis and characterization of the model are explained in the next section.

V. OBSERVATIONS, ANALYSIS, AND DISCUSSION

As mentioned above, the focus of our study is the insider threat detection approaches that are validated with empirical results. The effectiveness of a defense solution depends on many factors, such as the dataset used to validate an approach, the feature domain, the classification algorithm, the number of simulated scenarios, the accuracy and performance metrics, etc. In this section, the answers of the proposed questions are represented as 10 factors and discussed thoroughly in a comparative way. The discussion of (33 empirical studies) with respect to such factors can give insights to overcome the limitations of the current solutions. The following sections discuss and analyze the findings presented in (Appendix B).

A. INSIDER THREAT INCIDENTS

Organizations have various assets (e.g. Data, Systems/ Software and Networks), and they struggle to keep them safe from possible attacks. The focus of this article is the attacks that are conducted by insiders. So, insider attacks can be executed by two actors (Malicious Insiders or Masqueraders). The malicious insiders who perform an attack using their authorized access, whereas the masqueraders

[1] www.saturateapp.com

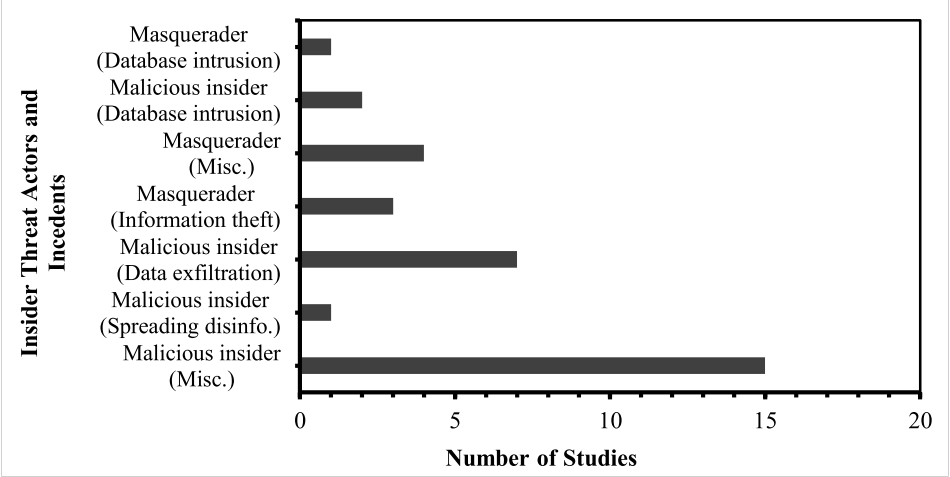

FIGURE 5. Insider threat actors and incidents addressed by existing detection approaches.

conduct an attack by gaining the access of legitimate insiders illegitimately.

Both actors can carry out various malicious actions (e.g., data exfiltration, information theft, database modification, need-to-know violation, etc.). Figure 5 summarizes the type malicious actors and attack incidents that the detection approaches attempted to address. It is noted that eight detection approaches studied (database intrusion, data theft and miscellaneous) attacks that might be conducted by masqueraders. On the other hand, most of the detection approaches (25 articles) focused on addressing various attacks (data exfiltration, need-to-know, spreading disinformation, etc.) that might be carried out by malicious insiders. Table 1 specifically shows those studies, the addressed attacks, and the actors.

TABLE 1. The insider threat actors, attack types, and their detection approaches.

Malicious Actor	Malicious Action	Detection Approach
Masquerader	Database intrusion.	[30].
Malicious insider	Database intrusion	[31].
Masquerader	Information theft.	[32], [33] and [34].
Malicious insider	Data exfiltration.	[35], [7], [36], [37], [22], [38], [39] and [40].
Malicious insider	Spreading disinfo.	[41].
Masquerader	Miscellaneous	[42], [43], [44] and [45].
Malicious insider	Miscellaneous	[46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59] and [60]

B. VIOLATED CONFIDENTIALITY, INTEGRITY OR AVAILABILITY

The confidentiality, integrity and availability of an asset known as (CIA Triad) are the major goals of information security. So, if there is an attack to a network, system, or data then it will violate one or more of CIA Triad. For example, the approaches in [7], [22], [35]–[40] addressed the data exfiltration attack that violates the confidentiality of data asset. In [41] the focus was on an attack that modifies the data to mislead the decision maker inside an organization, which at the end violates the integrity of the data. Figure 6 presents the distribution of detection approaches according to the CIA that they proposed to protect.

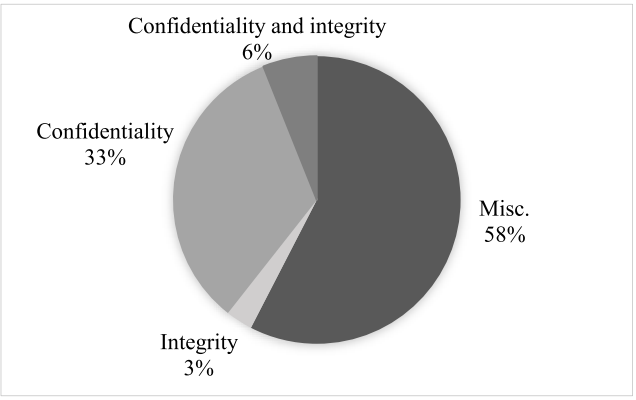

FIGURE 6. The percentage of detection approaches for addressing the CIA triad of assets.

Figure 6 shows that most of the detection approaches (19 articles) focused on detecting the malicious tendency of insiders without specifying particular type of attacks. The second set of approaches (11 articles) concentrated on detecting insiders who violate the confidentiality of assets (data exfiltration). The classification of the detection approaches based on their CIA focus is summarized in Table 2. Notably, the current detection approaches focused on addressing specific type of CIA without considering them as whole. Therefore, the designing of real-world detection system, that tackles various types of insider threats and cover all (CIA triad) security elements, is still a gap.

TABLE 2. The insider threat detection studies vs the CIA Triad.

The violated CIA	Detection Study
Confidentiality	[35], [7], [36], [37], [22], [38], [32], [33], [61], [39] and [30].
Integrity	[41].
Availability	NA.
Confidentiality &Integrity	[44] and [40].
Misc.	[46], [47], [48], [49], [50], [42], [51], [43], [52], [53], [45], [54], [31], [55], [56], [57], [58], [59] and [60].

C. DETECTION MECHANISMS

The current detection approaches are implemented using three major mechanisms (Anomaly-based, Signature-based and Combined). The anomaly-based approaches detect unexpected variation of insiders' activities from their normal activities. In such approaches the normal patterns of users are defined, so when a system detects abnormal pattern, a threat will be raised [50]. The other detection mechanism uses Misuse or Signature based method, where the system is provided with rules/signatures of previous attacks. Then, the system detects new attacks by matching with the signatures of predefined attacks. The third type of detection mechanisms is the combined/hybrid, where both the Anomaly-based and Misuse/Signature-based are involved.

However, in the literature, we noticed that most of the detection approaches (26 articles) deployed Anomaly-based detection mechanism. In contrary, little works in [7], [36], [41], [55] and [60] implemented Misuse-based detection mechanism, while the combination of the two mechanisms were applied in [48] and [37]. A graphical representation of detection mechanisms that are implemented by existing approaches is shown in Figure 7.

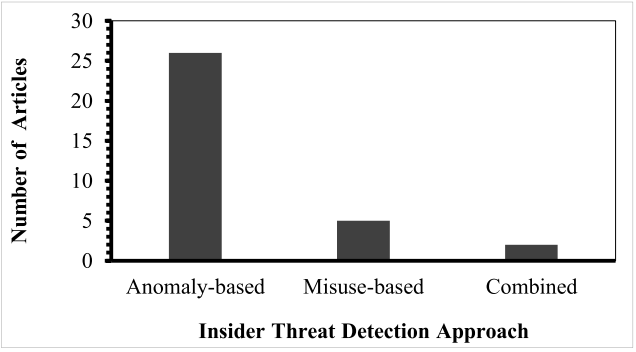

FIGURE 7. The insider threat detection mechanisms of current approaches.

Table 3 classifies the current approaches based on their detection mechanisms (Anomaly-based, Misuse-based, or Combined).

D. DATASETS OF APPROACHES' VALIDATION

The availability of datasets in a research field has a positive impact on the advancement of that field. In fact, there is a lack of real-life datasets with regard to insider threat area for two reasons [5]: First, the absence of a precise definition of insider threat complicates specifying the requirements of insider threat datasets more accurately. Second, most organizations that encountered insider attacks are unwilling to share attacks' data as they afraid of bad impacts toward their reputation or accountability issues. Therefore, researchers have faced a challenge of finding real datasets to test the effectiveness of their approaches. This triggers some researchers to create synthetic datasets and make them publicly available on the field. Such efforts facilitate testing and validating of insider threat detection approaches using artificial datasets. This section illustrates the datasets utilized by current detection approaches. In the literature, we noticed that 12 studies validated their detection approaches by deploying (CERT, RUU, SEA and Enron datasets) as summarized in Table 4.

TABLE 3. The distribution of insider threat detection studies according to their detection mechanisms.

Detection Mechanism	Research Study
Anomaly-based	[22], [46], [47], [35], [49], [50], [38], [32], [33], [42], [51], [61], [39], [43], [44], [40], [52], [53], [45], [54], [31], [56], [57], [58], [59] and [30].
Misuse-based	[7], [41], [36], [55] and [60].
Combined	[48] and [37].

TABLE 4. Available datasets of insider threat detection approaches.

Dataset	# of Insiders	Auditing Domain	Utilized By
CERT [62]	4000	General observables	[36], [48], [49], [56] and [57].
RUU [32]	78	System logs	[32] and [42].
SEA [63]	70	UNIX commands	[45] and [43].
Enron [64]	151	Email traffic	[48],[55] and [59]

The most widely used dataset in insider threat field was created by CERT [62] as a project at Carnegie Mellon University (CMU). It was collected from 4000 users who were involved in over 700 insider threat incidents for a period of 18 months. The dataset includes various activities of users (e.g. logon/logout, file operations, email, web, USB, etc.). It was generated by simulating three attacks scenarios: In the first one, malwares were injected by malicious insiders using removable devices which resulted in systems sabotage. Second, data exfiltration was conducted by malicious insiders through cloud or removable media. The last scenario was a data leakage attack that was conducted by masqueraders using email attachments. This dataset is utilized to validate the detection approaches in [36], [48], [49], [56] and [57].

Are You You (RUU) Dataset was created by Ben Salem and Stolfo [32] in 2011. It was collected from 18 normal users and 60 masqueraders. More than 500,000 records were captured per a user during 4 days. The users were distributed into three groups to simulate three attack scenarios (malicious, masquerader and neutral). This dataset was approved by

the Human Subjects protocol IRB-AAAC4240 at Columbia University [32]. It comprises of system-level features (e.g. number of created processes, unique processes, number of destroyed processes, number of registry actions, etc.). Two detection approaches in [42] and [32] employed this dataset to test the their performance.

SEA dataset [63] was captured from 70 users during several months. It contains of 15,000 UNIX commands collected per each user. In data collection, 50 users represented benign users, and 20 users represented masqueraders. This dataset is applied by two detection approaches [43] and [45].

Enron dataset [64] is a corpus of email data collected from 151 users. It comprises of over 250000 email messages. Massachusetts Institute of Technology (MIT) made this dataset available for researchers who are interested in email research topics. In insider threat area, it was utilized in [48], [55] and [59] to test their detection approaches.

The Lincoln Laboratory Intrusion Detection dataset [65] is created also by MIT. It includes all the daily system logs for a period of 7 weeks. Each log contains of tokens for every system call that are displayed as a plaintext. This dataset is too old as it was created in 1998. It was used to test the detection approach in [52]. Nevertheless, using such old dataset reflects the difficulty of finding real-life dataset in insider threat field.

Some organizations made their systems available to be used for insider threat research topics, for example, Chen *et al.* [38] assessed their detection approach on electronic health record (EHR) system at Vanderbilt University Medical Center. They used data records of more than 1.5 million patients for a period of three months. The system processed the daily workflows of more than 300,000,000 operations. Such data is used to detect anomalous insiders in collaborative systems.

Apart from utilizing the publically available datasets of others, 15 detection approaches (listed in Table 10) created their own datasets. For example, Camiña *et al.* [33] generated their private dataset namely, windows-users and intrusion simulation logs (WUIL). It was collected from 20 users over a period of ten weeks. They simulated the malicious activity of information theft that might be committed by insiders. Figure 8 shows the various types of datasets employed by current approaches. Notably, the largest number of approaches (15 articles) generated their own datasets. Some studies like in [48] tested their approach using several datasets, including their in-house dataset, CERT dataset, Enron dataset and the dataset provided by the Centre for the Protection of National Infrastructure (CPNI).

However, some approaches tried to exploit some web services to validate their detection techniques. For instance, the approaches in [47] and [22] used the dataset of online surveys. They conducted psychological surveys on Amazon's Mechanical Turk, an online service for hiring people to do online tasks. It was used to simulate insiders who leak the data from their organization. Also, the approach in [46] validated the detection technique on World of Warcraft (WoW), the massive multiplayer online game. The dataset used to measure the psychological behaviors of players using over 350,000 characters observed during 6 months. Such data used to identify the malicious behaviors of users and predict their personal characters.

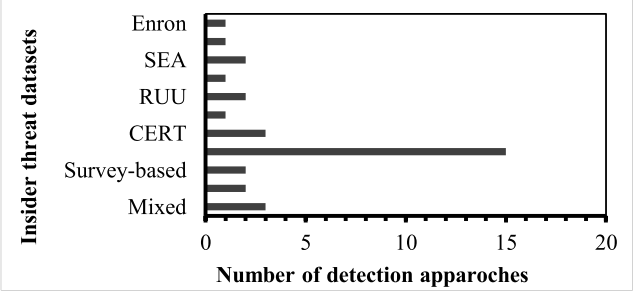

FIGURE 8. Datasets used to validate insider threat detection approaches.

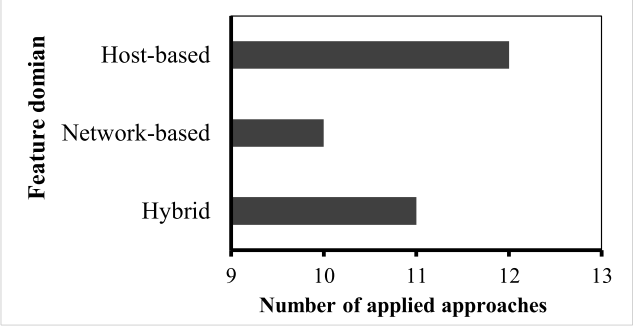

FIGURE 9. The detection approaches and their feature domain.

Although there are restrictions to find out real-life datasets about insider attack incidents, researchers tried to overcome this limitation by creating synthetic datasets and using some online platforms. However, there are some concerns related to synthetic datasets as they do not truly simulate the motivations/intentions of actual insider attacks. Furthermore, we believe that the synthetic datasets, especially that were created in authors' homes, might be affected by subjective and biased environments. So, the lack of real insider threat datasets is still a challenge.

E. FEATURE DOMAIN

When the datasets are captured from insiders' activities (e.g., log in/out, modify, delete, send, print, etc.), the feature domain is extracted from raw data and turned into a representation form that can be classified using classification algorithms. In detection systems, vast amounts of data are collected by distributed sensors across an organization. In this section, we categorize the feature domains into three classes: Host-based, Network-based and Hybrid. Using such domains, a detection system builds an activity pattern for each insider by capturing the feature set at host and/or network levels. Then the system figures out any deviation from the normal behavior compared to previous activity patterns. In our analysis, we observed that most of the approaches (12 articles) focused on Host-based feature domain. The other

TABLE 5. The domain, observables and feature set of insider threat detection approaches.

Domain	Observables	Features Set	Used By
Host-based	Log In/Out	User ID, PC ID, timestamp, login duration time, login frequency, logout time, etc.	[41], [50], [32], [33], [42], [61], [39], [43], [44], [52], [53] and [45].
	File/Folder	Search, open, create, copy, move, edit, read, rename or delete.	
	USB	Device ID, duration, associated action (copy, paste, delete, etc.).	
	System calls	Processes, registry and file system actions.	
Network-based	Email	Time, source address, destination address, attachments, size.	[7], [22], [46], [47], [38], [40], [31], [55], [30] and [60].
	HTTP	URL, http requests/responses, browser type, upload/download.	
	TCP/IP	Source and destination IPs, traffic size, packets (sync/ack), connection duration.	
Hybrid	Miscellaneous	Miscellaneous	[35], [36], [48], [49], [37], [51], [54], [56], [57], [58] and [59].

approaches concentrated on Network-based and Hybrid features as presented in Figure 9.

It is noted that 12 approaches detected insider attacks utilizing data features at host domain. For instance, Liu *et al.* [50] monitored the activities of insiders by tracking the system calls at operating system level. Also, Sankaranarayanan *et al.* [44] used Microsoft® Word Plug-In Logging Tool to detect the modification attacks on sensitive documents. We believe that tracking the activities of insiders at system level will deter malicious insiders as all insiders' actions are recorder. On the other hand, tracking the activities of insiders across enterprise level is an exhausted process: first, logging tools should be installed and run automatically in every node across an organization; second, such tools generate a huge amount of logged data that need to be processed and analyzed effectively. Moreover, experienced insiders may fly under the radar by disabling or bypassing the logging tools [20].

The other 10 approaches detected malicious activities at network level (HTTP and TCP). For example, in [66] malicious actions of insiders are detected using TCP data log (e.g., number of opened connections over a time window, duration of the connections and size of transferred data). Likewise, network based data (e.g., sent/received packets, time stamp, etc.) are used in [67] and [68] to detect the visited websites and operating system fingerprints over encrypted networks. Thus, by aggregating network-based features over a given time period, important features are derived to detect malicious activities of insiders.

The detection approaches in [36], [48], [49], [56] and [57] extracted feature set from both host and network levels, we classified them as a hybrid feature domain. Such approaches are based on a wide range of insider activities such as log in/out, file operations, USB devices, e-mails, websites, etc. It is worth noting that by combining diverse data features from different domains, the significance of individual features will be varied during the classification process. In the literature, we noticed that the approach in [48] took this factor into account. That was by associating a weight score with each individual feature to emphasize the features of a greater importance. So, based on weighted combinations of features, the most accurate model was chosen. Table 5 summarizes the feature domain, sources of data features (observables), features set and the associated detection approaches. As presented, researchers tried to exploit data features spanned from the host activities (e.g., log in/out, file operations, system calls, etc.) to the network activities (e.g., browsing, downloading, uploading, email, etc.). Such features are used as potential risk indicators to detect malicious insiders.

F. CLASSIFICATION TECHNIQUES

There are various machine learning algorithms employed in insider threat detection approaches (e.g., Support Vector Machines (SVMs), Naïve Bayes, J.48 Decision Tree, K-Means Clustering, K-Nearest Neighbor (KNN), Gaussian Mixture Models (GMM), etc.). Most of them are openly available by different platforms such as Weka [72] machine learning framework. The accuracy of a detection approach depends highly on selecting the right machine learning algorithm [24]. This section summarizes the classification techniques implemented on insider threat detection approaches. Figure 10 shows the trend of employing various classification techniques by existing approaches. As depicted in Figure 10, most of the approaches (9 articles) utilized SVM followed

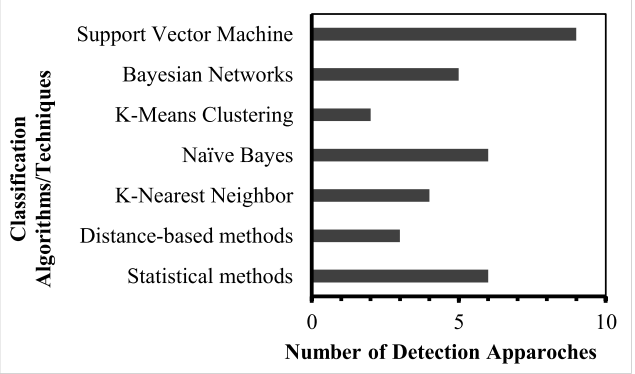

FIGURE 10. The classification techniques implemented by insider threat detection approaches.

TABLE 6. The classification algorithms used by insider threat detection approaches.

Classification Technique	Implemented By
Bayesian Networks	[46], [47], [36], [37] and [40].
Support Vector Machine (SVM)	[41], [22], [32], [33], [42], [51], [52], [45] and [30].
K-Nearest Neighbor (KNN)	[41], [50], [38] and [33].
Naïve Bayes	[22], [44], [45], [54], [31] and [30].
Gaussian mixture models (GMM)	[42].
Instance-Weighted Naive Bayes (IWNB)	[43].
Incremental Probabilistic Action Modeling (IPAM)	[44].
Dempster–Shafer theory (EDST)	[40].
Littlestone's Winnow Algorithm	[54].
Deep Neutral Network (DNN)	[56].
The Isolation Forest (IF) Algorithm	[57].
K-Means Clustering	[58] and [30].
Markov Chain	[58].
Minimum Descriptive Length (MDL)	[59].
Recurrent Neural Network(RNN)	[56].
J.48 Decision Tree	[30].
Statistical	[35], [7], [48], [53], [55] and [60].
Distance-based methods	[50], [61] and [39].
Graph-based methods	[59].
Misc.	[49].

by Naïve Bayes and other statistical techniques. Notably, the SVM has been used widely by insider threat detection community compared to other algorithms. The attractive aspect of using SVM in cyber security is that it provides very low latency and high classification performance in terms of CPU-intensive processes [24].

The statistical techniques such as Linguistic Inquiry and Word Count (LIWC) are used in [7], [35], [48], [53], [55] and [60] to detect anomalous actions of insiders. The Bayesian Networks (BNs) was used in [36], [37], [40], [46], and [47] detection approaches. BN is preferred in insider threat detection studies as its multivariate time series feature behaves well on insider threat activities [24]. The approaches in [22], [44] and [58] implemented two or more classification algorithms to seek for the best accuracy. In [50], [61] and [39] the Distance-based methods are utilized. The Minimum Descriptive Length (MDL) technique was used in [59] to detect malicious activities in social networks, business and various cybercrime domains.

Table 6 summarizes the various classification techniques that are implemented in the reviewed approaches. More details about the most well-known machine learning algorithms can be found in [73]–[75]. They compared the accuracy and complexity of various classification techniques by testing them on different datasets.

G. OS PLATFORMS AND TOOLS

The insider threat detection approaches conducted several experiments utilizing different OS platforms and software tools. Specifying the used tools by previous approaches facilitate the task of future researchers to select the proper and qualified tools. Moreover, demonstrating the specifications of the experimental environments share the research knowledge and raises the quality of the research. It also triggers those who are interested in the field to re-implement the approaches and bridge possible gaps under the same technical factors. Proctor *et al.* [76] assured that research implementation approaches cannot be tested or reused without full and precise description of experiments' components. So, in this section we summarized the software tools that are used in the experiments of implemented approaches as presented in Table 7. In the 33 studies included in this paper, we noticed that most of the approaches specify the testing platform and software tools of their experiments except the approaches in [36], [38], [57] and [58].

H. ATTACK SCENARIOS

The insider threat detection approaches are tested by simulating attack scenarios under different situations. We observed that there are considerable variations in the number of simulated scenarios by existing approaches as depicted in Figure 11. Ramirez *et al.* [77] assured that implementing various scenarios using scholarly methodology will open up research paths that empower and enable new research opportunities to arise. Additionally, the revisions and iterations of applied scenarios may generate novel lines of research and produce interesting outcomes. Moreover, when a detection approach is trained with various types of attack scenarios, it will protect against wide range of insider attacks. Notably, in the literature we observed that the largest number of scenarios were conducted in [49]. Their simulation was carried out on 5500 users with 48 attack scenarios. Other detection approaches varied in the number of conducted scenarios which ranged from 1 to 12 as presented in Figure 11.

I. ACCURACY & PERFORMANCE METRICS

To evaluate the insider threat detection approaches, diverse evaluation metrics have been utilized. Most of the detection approaches were assessed using the metrics (TPR, FPR, FPR, FPR, ROC, AUC, Precision and Anomaly Score) as

TABLE 7. The platform and software tools of implementing insider threat detection approaches.

Software Tools	Applied by	Software Tools	Applied by
Multi-Player Online Game (WoW)	[46].	OPNET Modeler	[51].
LISREL Software	[47].	File Access Monitor, Eclipse, Visual Studio, etc.	[61].
IARPA & CASE	[41].	Configuration Management & Version Control (CMVC)	[39].
Own Matrix Analysis	[35].	Unix	[43] and [45].
Splunk & Power Shell AD Modules	[7].	Microsoft® Word Plug-In Logging Tool	[44].
Linux (FSOBSERVER kernel)	[53].	LIBSVM Tool	[51], [52] and [45].
Python & D3 JavaScript Library	[48].	PostgreSQL & QStatProfiler	[30].
SureView®(Raytheon Oakley Systems, Inc.)	[49].	OMNeT++	[59].
Ethereal	[37].	Confidential Operations Simulation (iCOS)	[60].
Unix & Orca Software Package	[50].	Tensorflow	[56].
AMT's Online Service	[22].	MS-SQL Server	[40] and [31].
Enron's Software Packages, Unify, SAP, and Sitara	[55].	Standard Transactional Web Benchmark	[40].
Windows, Programming APIs, Google Desktop Search, etc.	[32].	MS Windows, FileSystemWatcherEx Class & .NET	[42].
MS Windows and Audit Tool	[33] and [54].	NA	[36], [38], [57] and [58].

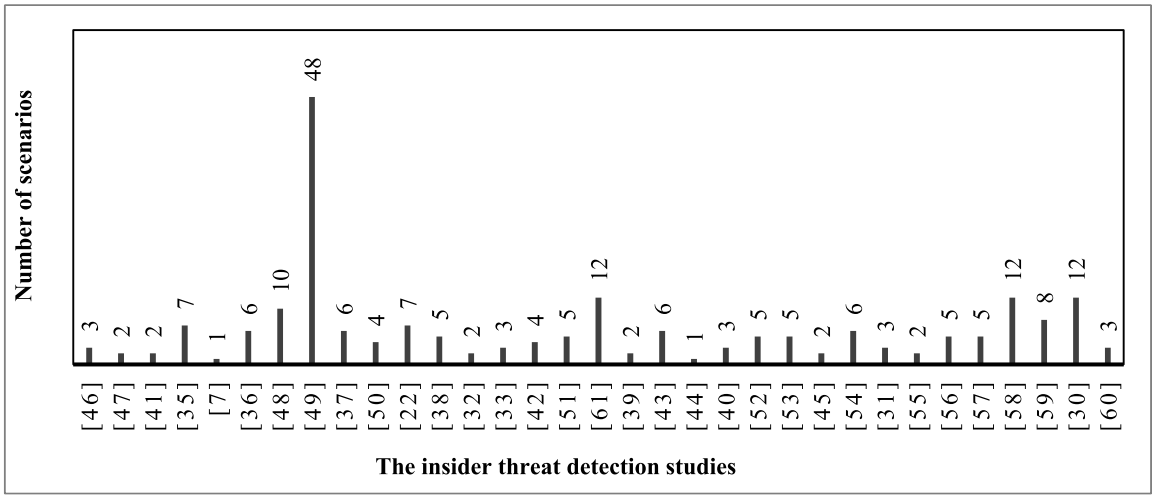

FIGURE 11. Number of scenarios applied by insider threat detection approaches.

TABLE 8. The evaluation metrics of insider threat detection approaches.

Accuracy Metric	Description	Deployed By
TPR	True Positive Rate (TPR) is the percentage of correctly detected attacks, sometimes known as detection/accuracy rate or recall.	[46], [41], [36], [48], [37], [22], [38], [32], [33], [51], [61], [39], [44], [40], [52] and [30].
FPR	False Positive Rate (FPR) is the percentage of incidents classified as attacks incorrectly known as false alarm rate.	[41], [36], [37], [32], [33], [61], [39], [44], [40], [53], [54], [31] and [30].
FNR	False Negative Rate (FPR) is the percentage of positives that produce negative test results.	[52], [53], [54] and [31].
ROC	Receiver Operating Characteristic (ROC) curve is a graphical plot of false positive rate represented on the X axis against the true positive rate on the Y axis.	[49], [50], [43] and [45].
LC	Lift Curve (LC) measures the performance of the classifier by plotting the relation between detected positives and those are actually positives.	[49].
AUC	Area Under Curve (AUC) score is the area under ROC curve, so the high AUC score indicates better accuracy.	[37] and [42].
Precision	It is the fraction of elements that are labelled as malicious correctly.	[36], [48] and [22].
Anomaly Score	It is the score of insider's abnormal changes compared to his/her coworkers.	[56], [57], [58] and [59].
Frequency	Frequency patterns of insider activities (Search Frequencies).	[35].

described in Table 8. In our analysis, we observed that the most of the approaches (16 articles) used TPR for measuring the ratio of correctly detected attacks expressed as True Positive Rate. The FPR metric was used in 13 approaches to evaluate the average of incorrectly detected attacks that generated false alarms as False Positive Rate. In [47] three

evaluation metrics are used; Logarithmic Loss Values (LLV), Quadratic Loss Values (QLV) and Error Rate. The LLV and QLV have five levels for measuring the counterproductive patterns of incidents which ranged from the lowest incident to the highest one. The Error Rate metric indicates to the extent in which the counterproductive variables are varied from the actual one. However, the accuracy of some detection approaches was assessed using other evaluation methods. In [7] the signature matching was used to detect suspicious actions. The authors argued that this method can be applied to a particular insider not all insiders as it generated high false alarms. Also, in [55] language indicators were used to detect suspicious insiders. That was by calculating words statistics of insiders and matching their interests to the email words dictionary of Enron dataset. Likewise, in [59] the language indicators are also used to detect malicious insiders using personal pronouns, negative emotion, etc.

We believe that the accuracy metrics (TPR, FPR, FNR and TNR) are the clearest ones to assess the detection rate of insider attacks. Table 9 exhibits a brief overview of such metrics.

TABLE 9. Fair accuracy metrics of insider attack detection systems.

Action \ Reaction	Detected	Not Detected
Malicious act	TPR	FNR
Legitimate act	FPR	TNR

Accordingly, the most accurate insider threat detection solution should minimize (FPR and FNR) and maximize (TPR and TNR). In other words, the perfect detection system should rise alerts for all malicious actions and do not rise alerts for any legitimate actions. Therefore, we recommend the future work to use such metrics for more fair evaluation.

VI. LIMITATIONS

Although there is a plethora of insider threat detection approaches developed over the last decade, they still face a number of limitations. Some authors pointed to the limitation of their works explicitly. So, mentioning the limitations is a critical part of a research. It is a good practice as it highlights a number of research windows and inspire interested researchers to bridge the gaps of the field. Furthermore, mentioning the research limitations explicitly is vital for other researchers to replicate and extend on a study [78]. This section summarizes the limitations of existing approaches to provide future researchers with an updated reference of research opportunities for improving insider threat body of knowledge. Camiña *et al.* [33] stated two points to improve their dataset, Windows-Users and Intruder simulations Logs (WUIL). First, they indicated that their dataset does not include important data about input devices (e.g., keyboard, mouse, etc.). So, they suggest that adding such data may improve the detection rate, as the insider access behavior will be measured not only the accessed objects. Second, to keep the validity of the dataset, an updated data of insiders' profiles and operating systems should be added continuously.

Three points of limitation are also pointed out in [38]. Firstly, the low performance of their anomaly detection method need to be tuned to avoid alerting too many false positives, especially in a complex collaborative environment. Secondly, the performance of their MetaCADS model is sensitive to the number of simulated insiders and accessed objects. When the number of accesses to particular subjects grows, the system fails to detect them. So, such performance issue need to be addressed. Also, their CADS model detects anomalies that access objects randomly, which may be vulnerable to traditional attacks, such as imitating behavior of another user. Thirdly, the approach needs to integrate additional semantic data (e.g., roles and affiliations) to establish more meaningful patterns about insiders.

A limitation was also highlighted in [50], when they proposed an approach to detect insider threat using system call features. They mentioned a limitation for their approach as the system call parameter-based features are still not sufficient to detect the malicious activities of insiders. That is because that many normal activities are detected as outliers, which resulted in a large number of false alarms. So, they concluded that the system calls feature-based are not appropriate for insider threat detection, as the probability of changing the activity pattern of insiders is less than the change of activity pattern exhibited by external attacks.

Similarly, in [53] a system was proposed to detect the insider misbehaviors by examining system calls processes. The authors presented two limitations of their system. Firstly, the proposed system was not able to detect an insider attack, if the buffer overflow occurs on programs without a fixed list of process children. Secondly, they evaluated the performance of their system utilizing a limit number of files accessed per a process which created some gaps: their system can be fooled by a malicious insider who may open only a small number of files without reaching the threshold of accessed files specified by their system. So, the system requires to take into account various number of files that may opened by several processes of malicious insiders. Another gap is that the difficulty of the system to define the perfect time window for analyzing an attack as insiders did not have a fixed working time pattern.

In [55] some points are highlighted for improvement. The authors proposed an approach to detect malicious insiders based on analyzing their interests using Enron e-mail corpus. The proposed system was not able to identify some categories of insiders' interests based on most probable words of their interests. Another point of improving the system is to expand the work to be deployed on the Internet activity which is not available on Enron e-mail corpus. In [60], the authors conducted a simulation to detect insider threats using language changes. They showed two factors that were absent in their approach. Firstly, the outside activities of insiders with individuals outside their own organization were not elaborated. Secondly, the participants in the simulation were

TABLE 10. An overview of coding processes from papers included in our study.

Selective codes	Axial codes	Open codes
Insider Threats	Malicious Insider	Database intrusion
	Masquerader	Data exfiltration
		Spreading disinformation
		Information theft
Violated CIA	Confidentiality	Opening secured assets
	Integrity	Unauthorized Modification
	Availability	Damaging assets
Detection Methods	Anomaly Based	Abnormal behavior transactions
	Misuse Based	Predefined Rules/Signatures
	Combined	
Datasets	Synthetic	General observables
	Real-life	System logs
		UNIX commands
Feature Domains	Host-based	Log in/out
	Network-based	File/Folder
	Hybrid	USB
		System calls
		Email
		HTTP
		TCP/IP
Classification Techniques	Machine learning algorithms	Bayesian Networks
	Statistical methods	Support Vector Machine (SVM)
	Distance-based methods	K-Nearest Neighbor (KNN)
	Graph-based methods	Gaussian mixture models (GMM)
		Instance-Weighted Naive Bayes (IWNB)
		Incremental Probabilistic Action Modeling (IPAM)
		Dempster–Shafer theory (EDST)
		Deep Neutral Network (DNN)
		The Isolation Forest (IF) Algorithm
		K-Means Clustering
		Minimum Descriptive Length (MDL)
		Recurrent Neural Network(RNN)
		J.48 Decision Tree
OS Platforms and Tools	Operating System (OS) platforms	Own Matrix Analysis Tool
	Software tools	Splunk & Power Shell AD Modules
	Programming languages	Linux (FSOBSERVER kernel)
	Databases	Python & D3 JavaScript Library
		SureView® (Raytheon Oakley Systems, Inc.)
		Unix OS & Orca Software Package
		AMT's Service
		Enron's Software Packages, Unify, SAP and Sitara
		OPNET Modeler
		File Access Monitor, Eclipse, Visual Studio.
		Configuration Management
		Microsoft® Word Plug-In Logging Tool
		PostgreSQL & QStatProfiler
		Confidential Operations Simulation (iCOS)
		Standard Transactional Web Benchmark
		Windows, Programming APIs, Google Desktop
		MS Windows, FileSystemWatcherEx Class & .NET
Accuracy Metrics	Positives	True Positive Rate (TPR)
	Negatives	False Positive Rate (FPR)
	Precision	False Negative Rate (FPR)
	Anomaly Score	Receiver Operating Characteristic (ROC) curve
		Area Under Curve (AUC) score
		Frequency

TABLE 11. The factors of insider threat detection approaches.

Refs.	Insider Threat	Violated CIA	Detection Method	Dataset	Feature Domain	Classification Technique	OS / Tools	# Of Scenarios	Stated Limitation	Accuracy Metrics
[46]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Network-based (Psychological Data)	Bayesian Networks	Multi-Player Online Game (WoW)	3	No	Accuracy Rate (89 %)
[47]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Network-based (Psychological Data)	Bayesian Networks	LISREL Software	2	Yes	Logarithmic Loss Values (1 & 1.7) Quadratic Loss Values (0.6 & 0.8)
[41]	Malicious insider (Spreading disinformation)	Integrity	Misuse-Based	Synthetic	Host-based (Tasks matching)	K-Nearest Neighbor (KNN) and Support Vector Machine (SVM)	IARPA & CASE	2	No	Recall and False Positive Rates (FPR) (Various Scenario Results)
[39]	Malicious insider (Data exfiltration)	Confidentiality	Anomaly-Based	Real-life	Hybrid (Search, Send, Copy, etc.)	Statistical	Own Matrix Analysis Tool	7	No	Frequency Rate (Various Scenarios Results)
[7]	Malicious insider (Data exfiltration)	Confidentiality	Misuse-Based	Real-life	Network-based (Email Data, From, Size, To, Address, Time and IPs)	Signature Matching	Splunk & Power Shell AD Modules	1	No	Signature matching
[36]	Malicious insider (Data exfiltration)	Confidentiality	Misuse-Based	Real-life	Hybrid (USB device, Email, Logins, HTTP, etc.)	Bayesian Networks	NA	6	No	Precision, Recall, and FPR (Various Scenarios Results)
[48]	Malicious insider (Misc.)	Misc.	Combined	Combine d	Hybrid (Login, USB, Emails, Files, HTTP)	Content Parser and Linguistic Inquiry Word Count (LIWC)	Python & D3 JavaScript Library	10	No	Precision & Recall (Various Scenarios Results)
[49]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Real-life	Hybrid (File events, URL and Logins)	EGMM, VSM, RIDE and CP	SureView®(Raytheon Oakley Systems, Inc.)	48	No	ROC Curve and Lift Curve (Various Scenarios Results)
[37]	Malicious insider (Data exfiltration)	Confidentiality	Combined	Synthetic	Hybrid (Searching, Browsing, Downloading and Printing)	Bayesian network	Ethereal	6	No	TPR (84%), FPR (1.5%) and AUC value (0.92)
[50]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Host-based (System calls)	K-Nearest Neighbor Algorithm and Hamming Distance	Unix & Orca Software Package	4	Yes	ROC curve (Various Scenarios Results)
[22]	Malicious insider (Data exfiltration)	Confidentiality	Anomaly-Based	Synthetic	Network-based (Fetch, Edit, Save, Print and Send)	SVM and Naïve Bayes	AMT's Service [91]	7	No	Recall (0.6) Precision (0.3)
[38]	Malicious insider (Data exfiltration)	Confidentiality	Anomaly-Based	Real-life	Network-based (Subjects Accesses)	K-Nearest Neighbors (KNNs)	NA	5	Yes	TPR (Various Scenarios Results)
[32]	Masquerader (Information theft)	Confidentiality	Anomaly-Based	Real-life	Host-based (No. of search-related records, File access, etc.)	One-Class SVM (OC-SVM)	Windows, Programming APIs, Google Desktop Search, etc.	2	No	TPR (100%) FPR (1.1%)
[33]	Masquerader (Information theft)	Confidentiality	Anomaly-Based	Real-life	Host-based (Directories, Access, Time, etc.)	SVM and k-NN	MS Windows and Audit Tool	3	Yes	SVM (87.9% TPR at 20.1% FPR) kNN (88.7% TPR at 17.0% FPR)
[42]	Masquerader (Misc.)	Misc.	Anomaly-Based	Real-life	Host-based (Processes, Registry and File system actions)	Gaussian Mixture Models (GMM) and OC-SVM	MS Windows, FileSystemWatcherEx Class & .NET	4	No	AUC (Various Scenarios Results)
[51]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Hybrid (User profile, File and Database Servers)	SVM	OPNET Modeler & LIBSVM	5	No	Detection rates (Various Scenarios Results)
[45]	Masquerader (Information theft)	Confidentiality	Anomaly-Based	Synthetic	Host-based (Files search logs)	Distance-Based Clustering	Windows, File Access Monitor, Eclipse, Visual Studio, etc.	12	No	TPR (100%) and FPR(3.85%)
[39]	Malicious insider (Data exfiltration)	Confidentiality	Anomaly-Based	Synthetic	Host-based (File access logs)	Mean Distance	Configuration Management Version Control (CMVC)	2	No	TPR (80%) and FPR (2.5%)
[43]	Masquerader (Misc.)	Misc.	Anomaly-Based	Real-life	Host-based (Unix commands)	Instance-Weighted Naive Bayes (IWNB)	Unix OS	6	No	ROC curve (Various Scenarios Results)
[44]	Masquerader (Misc.)	Confidentiality and Integrity	Anomaly-Based	Synthetic	Host-based (MS Word Editing, Copy and Save)	Incremental Probabilistic Action Modeling (IPAM) and Naïve Bayes	Microsoft® Word Plug-In Logging Tool	1	No	Avg. Detection Rate (58%) FPR (14%)
[40]	Malicious insider (Database intrusion)	Confidentiality and Integrity	Anomaly-Based	Synthetic	Network-based (Database transactions)	Dempster–Shafer theory (EDST) & Bayesian Learning	MS-SQL Server & Standard Transactional Web Benchmark	3	No	TPR (98%) FPR (10%)
[52]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Real-life	Host-based (System calls)	OC-SVM & TC-SVM	LIBSVM	5	No	TPR & FNR (Various Scenarios Results)
[53]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Host-based (System calls)	Statistical	Linux (FSOBSERVER kernel)	5	Yes	FPR & FNR (Various Scenarios Results)
[45]	Masquerader (Misc.)	Misc.	Anomaly-Based	Real-life	Host-based (Unix commands)	OC-Naïve Bayes & OC-SVM	Unix OS and LIBSVM 2.4	2	No	ROC curve (Various Scenarios Results)
[54]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Hybrid (Network activity, CPU usage, Files access)	Littlestone's Winnow & Naïve Bayes	MS Windows	6	No	TPR & FNR (Various Scenarios Results)
[31]	Malicious insider (Database intrusion)	Misc.	Anomaly-Based	Synthetic	Network-based (Database transactions)	Naïve Bayes Classifier	SQL Server	3	No	FPR & FNR (Various Scenarios Results)

TABLE 11. *(Continued.)* **The factors of insider threat detection approaches.**

Refs.	Insider Threat	Violated CIA	Detection Method	Dataset	Feature Domain	Classification Technique	OS / Tools	# Of Scenarios	Stated Limitation	Accuracy Metrics
[55]	Malicious insider (Misc.)	Misc.	Misuse-Based	Real-life	Network-based (Email data)	Statistical	Enron's Software Packages, Unify, SAP, and Sitara	2	Yes	Avg. Linking Probability of Words by Individuals' Interests
[56]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Real-life	Hybrid (Log in/off, File, Email, Device and HTTP)	DNN and Recurrent Neural Network(RNN)	Tensorflow	5	No	Avg. anomaly score of (95.53) Percentile
[57]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Real-life	Hybrid (Login, USB, URL, etc.)	The Isolation Forest (IF)	NA	5	No	Anomaly score (Various Scenarios Results)
[58]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Synthetic	Hybrid (Log in/off, USB, File, etc.)	K-Means Clustering and Markov Chain	NA	12	No	Anomaly score (Various Scenarios Results)
[59]	Malicious insider (Misc.)	Misc.	Anomaly-Based	Combined	Hybrid (Email, Cell phone logs, etc.)	Minimum Descriptive Length (MDL)	OMNeT++	8	No	Anomaly Score (Various Scenarios Results)
[30]	Masquerader (Database intrusion)	Confidentiality	Anomaly-Based	Synthetic	Network-based (SQL Server queries)	SVM, J.48 Decision Tree, Naïve Bayes, K-Means Clustering	PostgreSQL & QStatProfiler	12	No	TPR & FPR (Various Scenarios Results)
[60]	Malicious insider (Misc.)	Misc.	Misuse-Based	Synthetic	Network-based (Email messages)	Logistic Regression Classifier & Linguistic Inquiry and Word Count (LIWC)	Confidential Operations Simulation (iCOS)	3	Yes	Language Predictors

selected randomly without reflecting various types of motivations, personalities, etc. in the experimental population.

In sum, it is worth mentioning that the summarized limitations stated by previous research is highly important for future research. They can serve as an inspiration for future researchers to bridge research gaps and design more effective solutions in the field.

VII. CHALLENGES AND RECOMMENDATIONS

Most of the detection approaches were tested through extensive simulation experiments, so implementing a real-world detection system would be accompanied by several challenges. Those challenges have to be considered carefully when building practical systems. This section recapitulates some challenges and offers a set of recommendations (some are placed throughout discussed factors accordingly) to enhance the field based on lessons learned from 33 reviewed approaches.

- Some authorized activities of users were detected as malicious acts, which resulted in a lot of false alarms. So, we recommend that before building an insider threat detection system, the security policy should be defined clearly and the permissions should be specified accurately. For example, the violation of need-to-know principle by an insider (e.g., fetching unauthorized files) would be avoided by preventing the access of insiders using access control mechanisms. Thus, the access control management according to a clear security policy plays a key role in minimizing false alarm rates.
- Collecting insider threat datasets from real-world environment is still a major challenge due to the privacy concerns of organizations. As a result, several researchers synthesized their own datasets, which may lead to bias and subjective interventions. We recommend that the insider threat detection approaches to be validated using the available dataset (presented in section V., D) in order to obtain fair and unbiased results.
- In an enterprise-level detection system, insider activities (e.g., login/out, emails, web actions, file operations, etc.) might be collected from diverse and heterogeneous environments. Thus, collecting, analyzing and classifying such data from different domains are still technically challenging. So, in section V., E, we classified the collected data from different domains for better understanding the diversity of collected data to help overcoming this challenge.
- Some detection approaches simulated low number of attack scenarios (illustrated in section V., H), which at the end will not protect against various types of attacks. Consequently, implementing an insider threat detection approach based on large and different number attack scenarios, will provide large-scale protection system with more confident results.
- Some detection approaches did not specify the accuracy and performance metrics of their approach. This make it difficult to evaluate how the effectiveness of a detection solution is. Therefore, utilizing the standard evaluation metrics (summarized in section V., I) for assessing the detection systems, clarifies the efficiency of proposed solutions and the significance of the achieved results.
- The privacy concern while observing insiders is also another challenge. This is because the monitoring of daily activities of insiders revealing their private data, which may result in bad impacts toward the business goals of an organization in case if noticed by insiders. It may destroy the trust between an organization and its employees, and may trigger some insiders to create backdoors or disable monitoring tools. However, the surveillance of insiders by using robust analytical tools is an important part of detection systems, but they should be installed carefully and unnoticeably using trusted supervisors to avoid the aforementioned issues.

VIII. CONCLUSION

The insider threat incidents have increased in the last decade resulting in a huge reputable and financial losses. This makes insider threat an active research area. This paper reviews insider threat detection approaches that are validated with empirical evidences. It proposes a question model compound of 10 research questions that highlight the fundamental factors of detection approaches. The detection approaches are also classified and discussed in terms of 10 factors in comparable manner. Such factors include

- the type of actors who committed the attacks whether they are malicious insiders or masqueraders;
- the violated CIA of an asset (confidentiality, integrity and/or availability);
- the detection method of an attack (anomaly-based, misuse-based or combined);
- the dataset for validating an approach;
- the feature domains of detection approaches (host-based, network-based or hybrid);
- the statistical/machine learning technique of classification;
- the OS platform and software tools of experimental work;
- the number of simulated scenarios;
- the performance and accuracy metrics; and
- the limitations.

Finally, the challenges for deploying the real-world insider threat detection systems and some recommendations are also presented. The findings of the paper are summarized in Appendix B. This paper will serve as a guide for future researchers to observe insider threat detection body of knowledge from different prospective. The underscored factors, gaps and recommendations will help interested researchers to devise protection systems that can predict, detect and prevent the emerging attacks.

APPENDIX A

The coding processes (open codes, axial codes and selective codes) of ground theory analyze stage are presented in Table 10.

APPENDIX B

This section summarizes the answers of our 10-question model that are represented as important factors of detection approaches. Such factors are discussed and compared thoroughly in Section 5.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no. RG-1441-401.

REFERENCES

[1] D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes* (Theft, Sabotage, Fraud). Reading, MA, USA: Addison-Wesley, 2012.

[2] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, "Insiders behaving badly: Addressing bad actors and their actions," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 169–179, Mar. 2010.

[3] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799," *Comput. Secur.*, vol. 24, no. 6, pp. 472–484, Sep. 2005.

[4] M. Bishop, "Position: 'Insider' is relative," in *Proc. Workshop New Secur. Paradigms*, 2005, pp. 77–78.

[5] J. Hunker and C. W. Probst, "Insiders and insider threats-an overview of definitions and mitigation techniques," *J. Wireless Mobile Netw., Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 4–27, 2011.

[6] F. L. Greitzer and D. A. Frincke, "Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation," in *Insider Threats in Cyber Security*. Boston, MA, USA: Springer, 2010, pp. 85–113.

[7] M. Hanley and J. Montelibano, "Insider threat control: Using centralized logging to detect data exfiltration near insider termination," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2011-TN-024, 2011.

[8] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Comput. Secur.*, vol. 21, no. 6, pp. 526–531, Oct. 2002.

[9] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," *ACM Comput. Surv.*, vol. 52, no. 2, p. 30, 2018.

[10] Ponemon Institute LLC. (2018). *Cost of Insider Threats?: Global Sponsored by ObserveIT*. Accessed: Jun. 6, 2019. [Online]. Available: https://www.observeit.com/ponemon-report-cost-of-insider-threats/

[11] C. Lee, A. Iesiev, M. Usher, D. Harz, and D. McMillen. (2019). *IBM X-Force Threat Intelligence Index*. Accessed: May 12, 2019. [Online]. Available: https://www.ibm.com/downloads/cas/ZGB3ERYD

[12] CA Technologies. (2018). *Threat Report: 2018–C. Technologies*. Threat Report 2018. Accessed: May 22, 2019. [Online]. Available: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

[13] C. N. I. T. Center. (2018). *Common Sense Guide to Mitigating Insider Threats, Sixth Edition*. Carnegie Mellon University. Accessed: Jun. 6, 2019. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf

[14] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Inf. Secur. Tech. Rep.*, vol. 15, no. 3, pp. 112–133, Aug. 2010.

[15] E. D. Shaw, K. Ruby, and J. Post, "The insider threat to information systems," *Secur. Awareness Bull.*, vol. 2, no. 98, pp. 1–10, 1998.

[16] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[17] A. Sanzgiri and D. Dasgupta, "Classification of insider threat detection techniques," in *Proc. 11th Annu. Cyber Inf. Secur. Res. Conf. (CISRC)*, 2016, pp. 1–4.

[18] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on data leakage prevention systems," *J. Netw. Comput. Appl.*, vol. 62, pp. 137–152, Feb. 2016.

[19] M. Bertacchini and P. Fierens, "A survey on masquerader detection approaches," in *Proc. 5th Congr. Iberoamericano de Seguridad Informática, Univ. de la República de Uruguay*, 2009, pp. 46–60.

[20] M. Ben Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research," in *Insider Attack and Cyber Security*. Boston, MA, USA: Springer, 2008, pp. 69–90.

[21] S. Zeadally, B. Yu, D. H. Jeong, and L. Liang, "Detecting insider threats: Solutions and trends," *Inf. Secur. J., Global Perspective*, vol. 21, no. 4, pp. 183–192, 2012.

[22] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, "Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data," *IEEE Trans. Comput. Social Syst.*, vol. 1, no. 2, pp. 135–155, Jun. 2014.

[23] J. Ophoff, A. Jensen, J. Sanderson-Smith, and M. Porter, "A descriptive literature review and classification of insider threat research," in *Proc. InSITE Conf.*, 2014, pp. 211–223.

[24] 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 Anal.*, vol. 1, no. 1, p. 6, Dec. 2016.

[25] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Group, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Med.*, vol. 6, no. 7, 2009, Art. no. e1000097.

[26] V. L. L. Thing, Y. S. Liau, D. M. Divakaran, and L. L. Ko, "Insider threat detection and its future directions," *Int. J. Secur. Netw.*, vol. 12, no. 3, p. 168, 2017.

[27] L. Yang, Z. Hu, J. Long, and T. Guo, "5W1H-based conceptual modeling framework for domain ontology and its application on STPO," in *Proc. 7th Int. Conf. Semantics, Knowl. Grids*, Oct. 2011, pp. 203–206.

[28] J. F. Wolfswinkel, E. Furtmueller, and C. P. M. Wilderom, "Using grounded theory as a method for rigorously reviewing literature," *Eur. J. Inf. Syst.*, vol. 22, no. 1, pp. 45–55, Jan. 2013.

[29] Z. S. H. Abad, M. Noaeen, and G. Ruhe, "Requirements engineering visualization: A systematic literature review," in *Proc. IEEE 24th Int. Requirements Eng. Conf. (RE)*, Sep. 2016, pp. 6–15.

[30] S. Mathew *et al.*, "A data-centric approach to insider attack detection in database systems," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Berlin, Germany: Springer, 2010, pp. 382–401.

[31] G. Z. Wu, S. L. Osborn, and X. Jin, "Database intrusion detection using role profiling with role hierarchy," in *Proc. 6th Workshop Secure Data Manage.*, 2009, pp. 33–48.

[32] M. Ben Salem and S. J. Stolfo, "Modeling user search behavior for masquerade detection," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Berlin, Germany: Springer, 2011, pp. 181–200.

[33] J. B. Camiña, C. Hernández-Gracidas, R. Monroy, and L. Trejo, "The windows-users and -Intruder simulations logs dataset (WUIL): An experimental framework for masquerade detection mechanisms," *Expert Syst. Appl.*, vol. 41, no. 3, pp. 919–930, Feb. 2014.

[34] X. B. Wang, Y. J. Wang, and Y. L. Sun, "Abnormal file access behavior detection based on FPD: An unsupervised approach," *Appl. Mech. Mater.*, vols. 713–715, pp. 2212–2216, Jan. 2015.

[35] J. S. Park and J. Giordano, "Role-based profile analysis for scalable and accurate insider-anomaly detection," in *Proc. IEEE Int. Perform. Comput. Commun. Conf.*, Apr. 2006, pp. 463–469.

[36] S. C. Roberts, J. T. Holodnak, T. Nguyen, S. Yuditskaya, M. Milosavljevic, and W. W. Streilein, "A model-based approach to predicting the performance of insider threat detection systems," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2016, pp. 314–323.

[37] M. A. Maloof and G. D. Stephens, "ELICIT: A system for detecting insiders who violate need-to-know," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Berlin, Germany: Springer, 2007, pp. 146–166.

[38] Y. Chen, S. Nyemba, and B. Malin, "Detecting anomalous insiders in collaborative information systems," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 3, pp. 332–344, May 2012.

[39] C. Gates *et al.*, "Detecting insider information theft using features from file access logs," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2014, pp. 383–400.

[40] S. Panigrahi, S. Sural, and A. K. Majumdar, "Two-stage database intrusion detection by combining multiple evidence and belief update," *Inf. Syst. Frontiers*, vol. 15, no. 1, pp. 35–53, Mar. 2013.

[41] E. Santos, H. Nguyen, F. Yu, K. J. Kim, D. Li, J. T. Wilkinson, A. Olson, J. Russell, and B. Clark, "Intelligence analyses and the insider threat," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 42, no. 2, pp. 331–347, Mar. 2012.

[42] Y. Song, M. Ben Salem, S. Hershkop, and S. J. Stolfo, "System level user behavior biometrics using Fisher features and Gaussian mixture models," in *Proc. IEEE Secur. Privacy Workshops*, May 2013, pp. 52–59.

[43] S. Sen, "Using instance-weighted naive bayes for adapting concept drift in masquerade detection," *Int. J. Inf. Secur.*, vol. 13, no. 6, pp. 583–590, Nov. 2014.

[44] V. Sankaranarayanan, S. Pramanik, and S. Upadhyaya, "Detecting masquerading users in a document management system," in *Proc. IEEE Int. Conf. Commun.*, vol. 5, Jun. 2006,pp. 2296–2301.

[45] K. Wang and S. Stolfo, "One-class training for masquerade detection," in *Proc. Workshop Data Mining Comput. Secur. (ICDM)*, Melbourne, FL, USA, 2003, pp. 10–19.

[46] O. Brdiczka, J. Liu, B. Price, J. Shen, A. Patil, R. Chow, E. Bart, and N. Ducheneaut, "Proactive insider threat detection through graph learning and psychological context," in *Proc. IEEE Symp. Secur. Privacy Workshops*, May 2012, pp. 142–149.

[47] E. T. Axelrad, P. J. Sticha, O. Brdiczka, and J. Shen, "A Bayesian network model for predicting insider threats," in *Proc. IEEE Secur. Privacy Workshops*, May 2013, pp. 82–89.

[48] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Automated insider threat detection system using user and role-based profile assessment," *IEEE Syst. J.*, vol. 11, no. 2, pp. 503–512, Jun. 2017.

[49] T. E. Senator, H. G. Goldberg, A. Memory, W. T. Young, B. Rees, R. Pierce, and D. Huang, "Detecting insider threats in a real corporate database of computer usage activity," in *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2013, p. 1393.

[50] A. Liu, C. Martin, T. Hetherington, and S. Matzner, "A comparison of system call feature representations for insider threat detection," IN *Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop*, Jun. 2005, pp. 340–347.

[51] M. Raissi-Dehkordi and D. Carr, "A multi-perspective approach to insider threat detection," in *Proc. Mil. Commun. Conf. (MILCOM)*, Nov. 2011, pp. 1164–1169.

[52] P. Parveen, Z. R. Weger, B. Thuraisingham, K. Hamlen, and L. Khan, "Supervised learning for insider threat detection using stream mining," in *Proc. IEEE 23rd Int. Conf. Tools with Artif. Intell.*, Nov. 2011, pp. 1032–1039.

[53] N. Nguyen, P. Reiher, and G. H. Kuenning, "Detecting insider threats by monitoring system call activity," in *Proc. IEEE Syst., Man Cybern. Soc. Inf. Assurance Workshop*, Jun. 2003, pp. 45–52.

[54] J. Shavlik and M. Shavlik, "Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage," in *Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2004, p. 276.

[55] J. S. Okolica, G. L. Peterson, and R. F. Mills, "Using PLSI-U to detect insider threats by datamining e-mail," *Int. J. Secur. Netw.*, vol. 3, no. 2, p. 114, 2008.

[56] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," in *Proc. 31st AAAI Conf. Artif. Intell.*, 2017, pp. 1–8.

[57] A. Gamachchi, L. Sun, and S. Boztas, "A graph based framework for malicious insider threat detection," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 2638–2647.

[58] H. Eldardiry, E. Bart, J. Liu, J. Hanley, B. Price, and O. Brdiczka, "Multi-domain information fusion for insider threat detection," in *Proc. IEEE Secur. Privacy Workshops*, May 2013, pp. 45–51.

[59] W. Eberle, J. Graves, and L. Holder, "Insider threat detection using a graph-based approach," *J. Appl. Secur. Res.*, vol. 6, no. 1, pp. 32–81, Dec. 2010.

[60] P. J. Taylor, C. J. Dando, T. C. Ormerod, L. J. Ball, and M. C. Jenkins, "Detecting insider threats through language change.," *Law Hum. Behav.*, vol. 37, no. 4, p. 267, 2013.

[61] X. Wang, Y. Sun, and Y. Wang, "An abnormal file access behavior detection approach based on file path diversity," in *Proc. Int. Conf. Inf. Commun. Technol. (ICT)*, 2014, pp. 1–5.

[62] CERT. (2016). *Insider Threat Test Dataset*. Software Engineering Institute, Carnegie Mellon University. Accessed: May 6, 2018. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099

[63] M. Schonlau. (2001). *Masquerading User Dataset of Unix Command Line Sequences*. Accessed: May 6, 2019. [Online]. Available: http://schonlau.net/

[64] C. Project. (2015). *Enron Email Dataset*. Federal Energy Regulatory Commission. Accessed: Jun. 19, 2019. [Online]. Available: https://www.cs.cmu.edu/~enron/

[65] M. L. Laboratory. (2018). *1998 DARPA Intrusion Detection Evaluation Data Set*. Massachusetts Institute Of Technology. Accessed: May 23, 2019. [Online]. Available: https://www.ll.mit.edu/r-d/datasets

[66] V. Paxson, "Bro: A system for detecting network intruders in real-time," *Comput. Netw.*, vol. 31, nos. 23–24, pp. 2435–2463, Dec. 1999.

[67] T. Al-Shehari and S. Zhioua, "An empirical study of Web browsers' resistance to traffic analysis and website fingerprinting attacks," *Cluster Comput.*, vol. 21, no. 4, pp. 1917–1931, 2018.

[68] T. Al-Shehari and F. Shahzad, "Improving operating system fingerprinting using machine learning techniques," *Int. J. Comput. Theory Eng.*, vol. 6, no. 1, p. 57, 2014.

[69] M. Bishop, S. Engle, S. Peisert, S. Whalen, and C. Gates, "We have met the enemy and he is us," in *Proc. Workshop New Secur. Paradigms (NSPW)*, 2008, pp. 1–12.
[70] F. L. Greitzer and R. E. Hohimer, "Modeling human behavior to anticipate insider attacks," *J. Strategic Secur.*, vol. 4, no. 2, pp. 25–48, 2011.
[71] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *Proc. IEEE Secur. Privacy Workshops*, May 2014, pp. 214–228.
[72] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software," *ACM SIGKDD Explor. Newslett.*, vol. 11, no. 1, pp. 10–18, Nov. 2009.
[73] R. D. King, C. Feng, and A. Sutherland, "STATLOG: Comparison of classification algorithms on large real-world problems," *Appl. Artif. Intell.*, vol. 9, no. 3, pp. 289–333, May 1995.
[74] R. Caruana and A. Niculescu-Mizil, "An empirical comparison of supervised learning algorithms," in *Proc. 23rd Int. Conf. Mach. Learn. (ICML)*, 2006, pp. 161–168.
[75] L. Tjen-Sien, L. Wei-Yin, and Y.-S. Shih, "A comparison of prediction accuracy, complexity, and training time of thirty-three old and new classification algorithms," *Mach. Learn.*, vol. 229, no. 3, pp. 203–228, 1992.
[76] E. K. Proctor, B. J. Powell, and J. C. Mcmillen, "Implementation strategies: Recommendations for specifying and reporting," *Implement. Sci.*, vol. 8, no. 1, p. 139, Dec. 2013.
[77] R. Ramirez, M. Mukherjee, S. Vezzoli, and A. M. Kramer, "Scenarios as a scholarly methodology to produce 'interesting research,'" *Futures*, vol. 71, pp. 70–87, Aug. 2015.
[78] E. B. Cohen, "Growing information: Part I," in *Proc. Informing Sci. Inf. Technol. (IISIT)*, CA, USA, 2009, pp. 326–327.

RAKAN A. ALSOWAIL received the B.Sc. degree in computer science from King Abdulaziz University, in 2008, and the M.S. degree in information technology and the Ph.D. degree in informatics from the University of Sussex, U.K., in 2011 and 2016, respectively. He is currently an Assistant Professor with King Saud University. His research interests include language-based security, information flow, program analysis, programming languages, information security, insider threats, and file sharing.

TAHER AL-SHEHARI received the B.S. degree in computer science from King Khalid University, in 2007, and the M.S. degree in computer science from the King Fahd University of Petroleum and Minerals, in 2014. From 2011 to 2014, he was a Research Assistant with the Deanship of Graduate Studies, King Fahd University of Petroleum and Minerals. Since 2015, he has been a Senior Lecturer with King Saud University (KSU). His research interests include information security and privacy, traffic analysis and website fingerprinting attacks, insider threat detection and prevention systems, and data analysis. He has published a couple of journal articles and conference papers. His awards and honors include the Honor Award from King Khalid University's Rector and the Best Designed Curriculum Award from CFY's Dean, KSU.