applied sciences

MDPI

Review

A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations

Mohammed Nasser Al-Mhiqani [1,*], Rabiah Ahmad [1,*], Z. Zainal Abidin [1], Warusia Yassin [1], Aslinda Hassan [1], Karrar Hameed Abdulkareem [2], Nabeel Salih Ali [3] and Zahri Yunos [4]

1 Information Security and Networking Research Group (InFORSNET), Center for Advanced Computing Technology, Faculty of Information Communication Technology, Universiti Teknikal Malaysia Melaka, Durian Tunggal 76100, Malaysia; zaheera@utem.edu.my (Z.Z.A.); s.m.warusia@utem.edu.my (W.Y.); aslindahassan@utem.edu.my (A.H.)

2 College of Agriculture, Al-Muthanna University, Samawah 66001, Iraq; khak9784@mu.edu.iq

3 Information Technology Research and Development Centre, University of Kufa, Kufa 54001, Najaf Governorate, Iraq; nabeel@uokufa.edu.iq

4 CyberSecurity Malaysia, Selangor 63000, Malaysia; zahri@cybersecurity.my

* Correspondence: almohaiqny@gmail.com (M.N.A.-M.); rabiah@utem.edu.my (R.A.)

Received: 8 June 2020; Accepted: 2 July 2020; Published: 28 July 2020

Abstract: Insider threat has become a widely accepted issue and one of the major challenges in cybersecurity. This phenomenon indicates that threats require special detection systems, methods, and tools, which entail the ability to facilitate accurate and fast detection of a malicious insider. Several studies on insider threat detection and related areas in dealing with this issue have been proposed. Various studies aimed to deepen the conceptual understanding of insider threats. However, there are many limitations, such as a lack of real cases, biases in making conclusions, which are a major concern and remain unclear, and the lack of a study that surveys insider threats from many different perspectives and focuses on the theoretical, technical, and statistical aspects of insider threats. The survey aims to present a taxonomy of contemporary insider types, access, level, motivation, insider profiling, effect security property, and methods used by attackers to conduct attacks and a review of notable recent works on insider threat detection, which covers the analyzed behaviors, machine-learning techniques, dataset, detection methodology, and evaluation metrics. Several real cases of insider threats have been analyzed to provide statistical information about insiders. In addition, this survey highlights the challenges faced by other researchers and provides recommendations to minimize obstacles.

Keywords: cybersecurity; data exfiltration; insider threats; insider threat detection; machine learning; security

1. Introduction

Computer networks and telecommunications play a significant role in information exchange. An increase in valuable information, along with enabling technology expansions, have led to increases in threats. The sources of these threats are not only from outside but, also, from within the organization. Such threats possess a large security risk and are seemingly difficult to detect [1–3]. Insider threats can inflict critical damage on the reputation, financial assets, and intellectual property of enterprises. A 2018 report on the insider threat has stated that slightly more than half of threats (53%) in the past 12 months came from inside of organizations. Moreover, 27% of surveyed organizations have stated that attacks originated from within the organizations [4]. In the previous decade, many incidents of insider

threats have gradually reached the media; these include well-known cases of data leakage conducted by Edward Snowden and Daniel Ellsberg [1]. Thus, most organizations implement cybersecurity techniques, such as firewalls, intrusion detection, and electronic access system, to protect data not only from outsider threats but, also, from potential malicious insiders.

To fend off malicious insiders, organizations should have an insider threat detection system that can detect and mitigate malicious insiders before they perpetuate threats. Unfortunately, the insider threat field is not sufficiently understood. Moreover, the detection mechanisms or approaches that can be used and the limitations of existing solutions remain unexplored. Thus, an urgent review on available insider threat detection systems is needed [5]. The current scenario is primarily due to the lack of knowledge on insider threat and its potential damage to organizations.

This study aims to discuss the insider threat problem in a descriptive and analytic manner by studying the insider or attacker to understand its nature, such as insider access, types of insider, insider motivation, insider profiling, effect security property, level of insider, and method and actions used by the insider, and highlighting the researchers' achievements. Furthermore, our objectives in this study are, first, to summarize previous studies conducted on insider threat detection systems and, second, to categorize the field of insider threats based on insider and detection systems; we classified them mainly by the type of study, such as development scenarios based on behaviors analyzed. The detection mechanisms or approaches can differ through the type of analyzed behavior [5], techniques, datasets used to evaluate the proposed solution, detection methodology, and evaluation metrics. In this work, the major contributions are summarized as follows:

- Classifying the field of insider threats based on the insider as an actor and insider threat detection systems.
- Analyzing real insider threat cases based on the subsection of the proposed classification.
- Discussing challenges and recommendations in the field of insider threats.

Figure 1 presents the remaining sections of the article in detail.

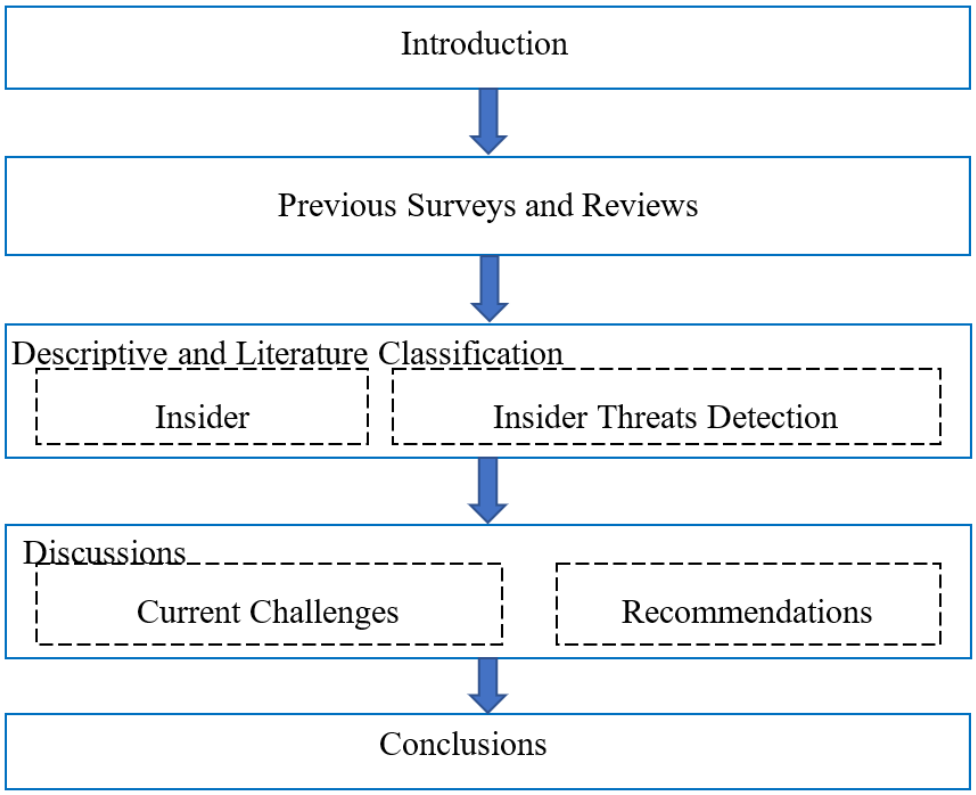

Figure 1. Article outline.

2. Related Studies

This section discusses the surveys and review articles on insider threats. Only a few papers were found, i.e., [6–16]. Walker-Roberts et al. [6] conducted a systematic review on insider threat detection; however, the scope of the review focused only on insider threats in healthcare critical infrastructures. Ullah et al. [7] and Alneyadi et al. [14] covered data exfiltration and data leakage. However, only F. Ullah et al. [7] provided in-depth details and insights into data exfiltration caused by the malicious activities of a remote attacker. In addition, the studies [10–13] and [15] described the understanding and future directions for the behavior of insider information security threats. However, Ho et al. [11] provided details on sociotechnical works with technical and behavioral evidence. Nonetheless, Nazir et al. [9] provided a comprehensive study on modeling, simulation, and related techniques that have been used to assess the vulnerabilities of the supervisory control and data acquisition (SCADA) system to cyberattacks. In addition, M. Kim et al. [16] surveyed trends and forecasts of intrusion-detection techniques by categorizing them into basic software and machine-learning techniques. Finally, L. Liu et al. [8] conducted a survey to line up and deeply discuss insider threats from several perspectives and mainly focused on three common types of insiders: traitor, masquerader, and unintentional perpetrator.

The main contributions of this review and what makes it different from the previous studies can be summarized as follows. Firstly, as far as we can possibly know, this is the first work that surveys the insider threat literature from many different perspectives and focuses on theoretical, technical, and statistical aspects of insider threats. Secondly, we study and analyze many insider threats incidents and provide statistical information about insiders. Finally, we discuss several challenges and highlight some recommendations for future research in insider threats.

3. Descriptive and Literature Classification

Classifying various aspects of insider threats into relevant classifications and forming them into a set of taxonomy is useful. The present study summarizes insider threats in such a taxonomy, as described in Figure 2. The research areas are divided into two main categories.

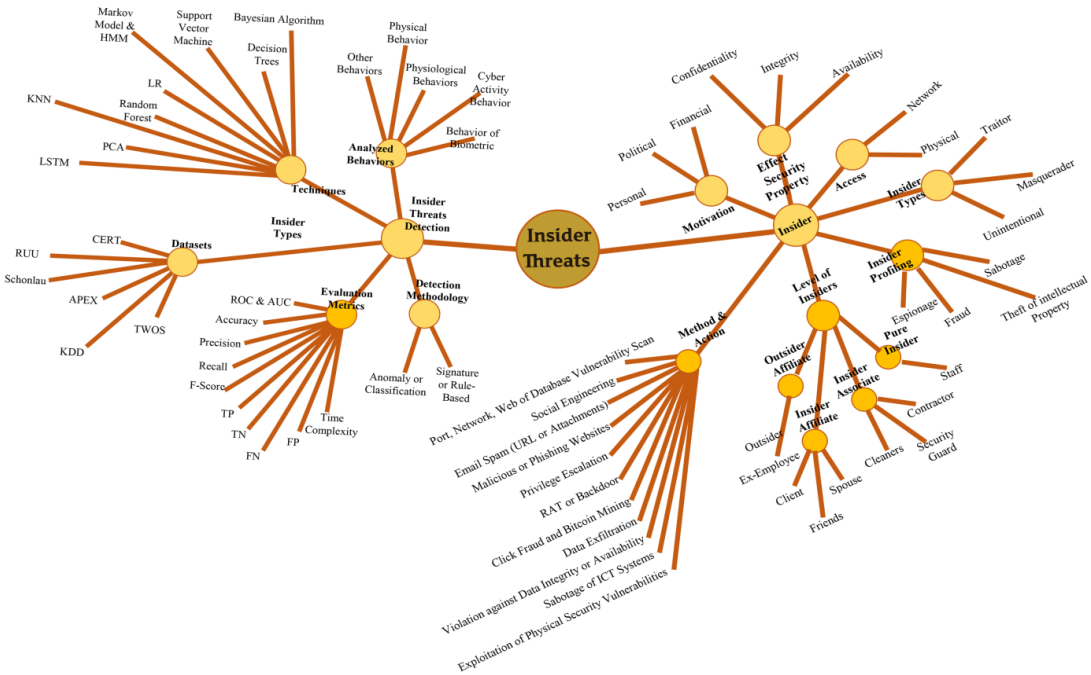

Figure 2. Classifications of insider threats.

Adopting from the cyber security principal stated in [17], the security culmination is of the interactions of people, process, and technology. Thus, our description consists of: the first describes a subject who performs an action. In this case, a potential attacker originates an attack from an internal system or authorized area. This category covers an ecosystem of insiders known as the root of access, types of insider, motivation, insider profiling, and affected security property, as well as the level, method, and actions undertaken.

The second describes the technology and state-of-the-art in detecting insider threats. The category comprises five main elements: namely, analyzed behaviors, techniques and methods, dataset, detection methodology, and evaluation matrices. This section discusses the sub-classifications of each element in detail.

3.1. Insider

3.1.1. Access

By nature, insiders have authorized access to networks, physical or both, which enable them to pose threats. Physical access describes malicious insiders who misuse data systems using physical access to infiltrate organizational data or steal devices. By having such a level of access, they are able to copy documents to a USB drive or any other removable media to steal intellectual property, sabotage data systems, or use identifiable information stored in the organizational system to commit fraud [18]. Network access involves malicious insiders who misuse their access to the organization's data/system. One of the examples for detecting insiders who use network access is network traffic, which may carry unauthorized content of interest or constitute protocols or the address of sources and destination endpoints that might be unauthorized. Abusing the network access can cause significant damage to the organization, and the majority of insider threats are caused by misusing network access, such as sabotaging and altering information, abusing authorized network access, or installing malicious software [19].

Figure 3 shows that the majority of insider threats are due to network access, which constitutes approximately 66% of the studied cases. This finding is based on the fact that insiders can easily access data and systems using the company network. In the case of data exfiltration, insiders can send data through email or upload it to the cloud service and abuse the use of data outside of the company. Although most insider cases fall under the network access scenario, however, physical access cannot be ignored, because it can cause the same damage to the organization when insiders intentionally or unintentionally exploit physical security vulnerabilities.

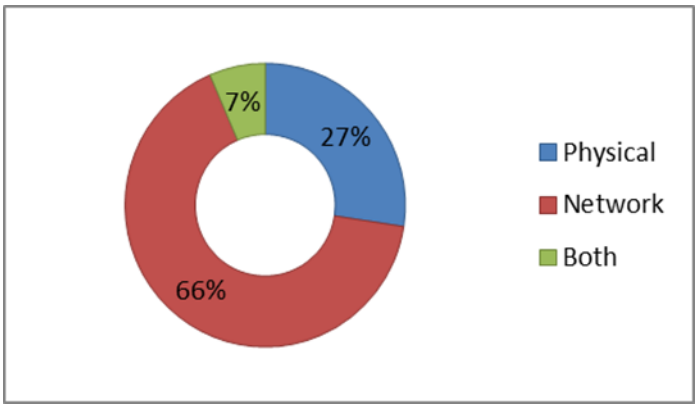

Figure 3. Types of access.

3.1.2. Insider Types and Methods

Insiders are categorized into three types: namely, traitor, masquerader, and unintentional. Traitors constitute the main category, and, as shown in Figure 4, most of the threats are posed by this type of insider.

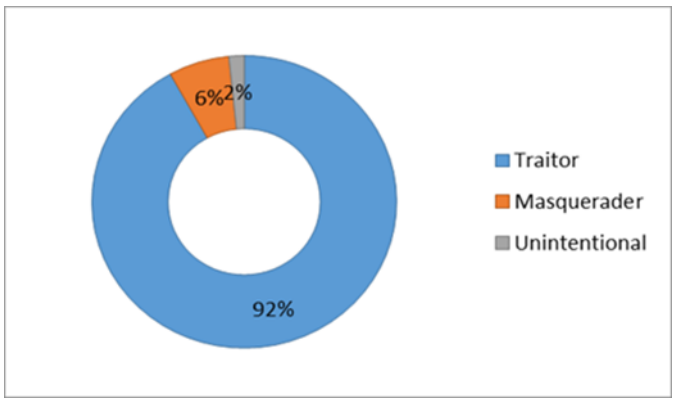

Figure 4. Types of insiders.

Traitors are also called misfeasors; the users are from within the organization and do not need to masquerade but use their access privileges to misuse the organization's systems [20].

A masquerader is an external attacker who steals the legitimate identification of an insider and uses the stolen identity to impersonate the insider for malicious intent [8].

The unintentional type pertains to a current employee who unintentionally causes harm or increases the possibility of future harm to the organization [21]. To link the type of insider with the threat or method used to conduct the attack, Liu et al. [8] introduced a taxonomy that matches the types of insider with the methods used or threats they pose. The authors have employed the Advanced Persistent Threat APT intrusion kill chain to model all types of threats, from early to late stages. Figure 5 shows the details.

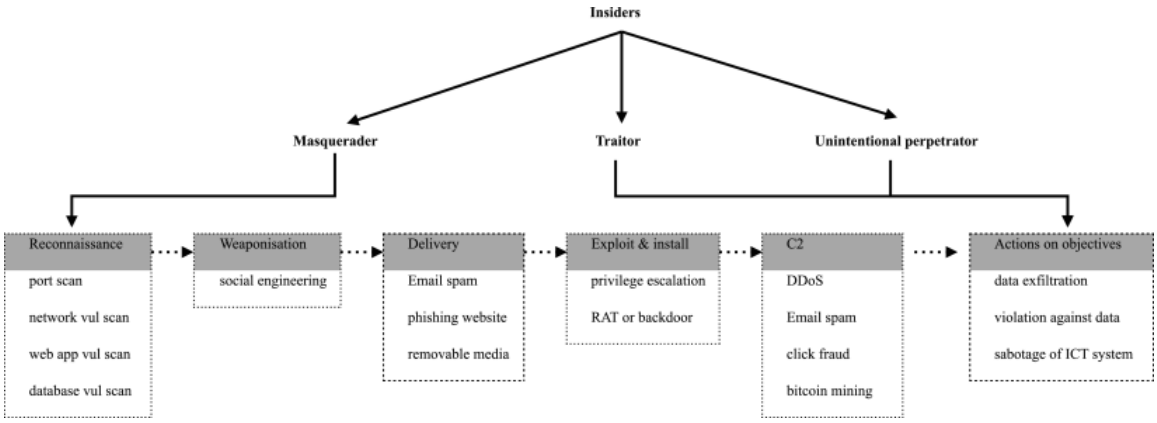

Figure 5. Insider types and methods [8].

3.1.3. Insider Motivation

Defining the motivation of the insider is highly important for facilitating detection, installing appropriate mitigation strategies, and enabling forensics [21]. Cole and Ring [22] divided the motivation into three main factors. Financial motivation is an extremely powerful matter, and it leads some people to act in manner that no one thought could be possible. Hence, it is not a big surprise that financial motivation is one of the main factors that motivate the malicious insider. Another motivation that drives people is their political views; they feel very strongly about their views, and if a company

works against their interests, this might be a strong reason that drives the employee to harm the company or cooperate with outsiders to harm the organization. There is also personal—this type of motivation can come in several shapes or sizes, but mostly, it comes in blackmail form. The attacker targets somebody with personal secrets that the target does not want anyone to know about and then threatens him/her with disclosing the personal secrets if the target does not collaborate. This is a very dangerous way and can cause a lot of trouble for the people and their organization.

3.1.4. Insider Profiling

In this review, based on the works [23,24], insider profiling is classified into four categories: namely, sabotage, theft (of intellectual property), fraud, and espionage. The malicious insider uses information technology to sabotage or direct particular harm at an organization or individual. Such malicious insiders are mainly disgruntled employees with technical knowledge and authorized access. An example of this type of profiling is the logic bomb installation, which can be activated after the termination of the employee [1]. Theft of intellectual property is the case where the malicious insider steals intellectual property that they access during daily work and takes the data with her/him outside of the organization (e.g., using intellectual property for personal business by sending it to a new employer or transferring it to a competitor organization). This act is frequently carried out by technical (e.g., developers or engineers) or nontechnical (e.g., salesmen or clerks) employees [1]. Fraud refers to the use of authorized access to misuse the organization's financial resources. In other words, fraud is a means of stealing money from the organization [25]. Lastly, espionage refers to corporate information systematic and targeted extractions by a malicious insider, which gives the malicious insider strategic economic, military, or public relation benefits [26,27].

Figure 6 indicates that the majority of analyzed cases fall under sabotage and fraud, where disgruntled employees harm the organization due to vengeful motivations after being terminated or the intention to gain financial benefits using their authorized access.

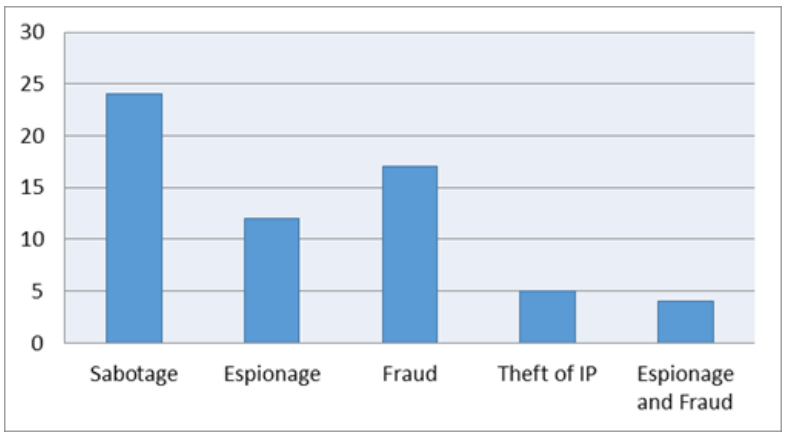

Figure 6. Insider profiling.

3.1.5. Effected Security Propriety

According to the type of access used by an insider, stated in Section 3.1.1, each insider has legitimate access to the organization's assets. This legitimate access can be a physical access, network access, or both (i.e., people who are working in an information system at the office). These different types of access can bring threats that can be done either intentionally by traitor or unintentionally by careless employee. Making this distinction is essential, due to the fact that not all insider threats are posed with the intention to cause harm to the company. All intentional malicious insiders and unintentional insider threats can be done by the misuse of authorized actions on data or by the utilization of unauthorized activity. The threats can either result in the disclosure (threat to information confidentiality), modification

(threat to information integrity), or destruction and interruption (threats to the information availability) of information [27].

3.1.6. Level of Insider

Based on the access level privileges, malicious insiders have been divided in [22,28,29] into four categories: namely, pure insider, insider affiliate, insider associate, and outside affiliate. The first category pertains to users with authorized access and badges or keys to the organization's data centers. The user has access to all information about the logical or physical structures of high-sensitivity data and access rights to such data. Compared with pure insiders, insider affiliates lack a reason or permission to access the company's resources. Insider affiliates may be friends, relatives, or clients of the company. In certain cases, employees' relatives or friends may visit the workplaces and access resources using the employees' credentials. An insider associate is not employed at the company but may have physical access to the company instead of network access. The insider associate may be a business partner, cleaner, contractor, or security guard. Outside affiliates are not a part of the organization and do not have legitimate access to organizational resources. However, they may attempt to access the resources through unprotected networks. The outsider affiliate may illegally access the network to obtain access credentials from the organization [22,28,29].

Based on the studied cases, Figure 7 shows that the majority of insiders fall under the category of outsider affiliates, who are mostly ex-employees who have been terminated and pose a unique risk because of their knowledge of the organization and their vengeful motivations.

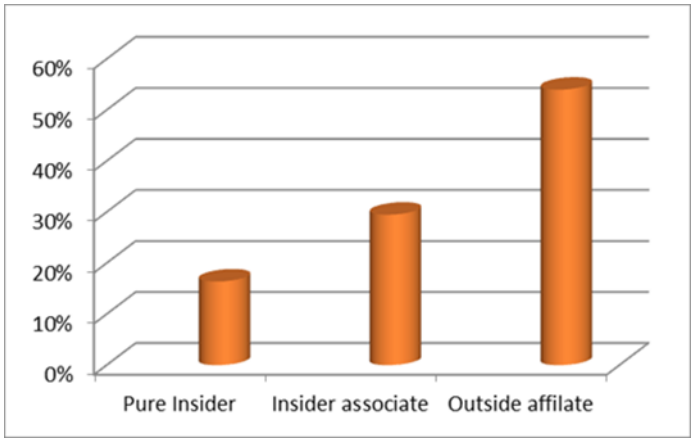

Figure 7. Level of insider.

3.2. Insider Threat Detection

This section reviews and analyzes the relevant studies on insider threat detection. Many aspects were investigated to establish a broad understanding of various studies examined through a survey of the existing literature. Such studies have been previously discussed in detail, and the types of analyzed behaviors and techniques used to model such behaviors have been categorized. The subsequent sections discuss the datasets that have been used in the literature and provide a summary of techniques, detection methodology, and evaluation metrics.

3.2.1. Analyzed Behaviors

Biometric Behaviors

X. Chen et al. [30] first identified mouse movement as the only feature for detection. The decision tree (DT), support vector machine (SVM), and probabilistic neural network (PNN) were used to model behaviors. The works [31–33] used similar features and added the keystroke biometric to model behavior;: the statistical learning algorithms, an ensemble learning classification, and the

utilization of a network access control NAC-like capability were used to build the detection approaches, respectively. Second, Y. Park et al. [34] analyzed the keystroke and typing patterns using the local outlier factor algorithm and two-class classifiers. Third, the studies [35–39] used command line and user command features with the dynamical system theory, Lempel–Ziv–Welch (LZW) algorithm, data mining techniques, incremental learning algorithm, and sequence alignment, respectively. Additionally, the works [40–43] used system call features, whereas Parveen et al. in [40] and [41] used an ensemble-based stream mining algorithm based on supervised learning and graph-based anomaly detections, while Parveen et al. [43] used the same method but with unsupervised learning, and Pitropakis et al. [42] proposed a solution that used the GPU card computational power to effectively monitor the virtual machines VMs health, detecting both the presence of malicious insiders and attacks against the infrastructure. Song et al. [44] and E. Yuan et al. [45] proposed a model by studying a user's system-level behavior using the Fisher feature selection and Gaussian mixture model (GMM) and data mining model, respectively. Fifth, Nasr et al. [46,47] highlighted the use of the system and application-level features in the SCADA system, which is molded by statistical and machine-learning techniques. The studies [48–50] utilized software and resource architecture using the model-based sequence, clustering algorithm, and the Bayesian information criterion by Lamba et al. [48], while S. Young and Dahnert [49] used the Bayesian belief network to propose a DevEyes Framework that has the capability to identify potential user actions, and in work [50], Clark et al. focused on the identification, characterization, and modeling of unintended USB channels. White and Panda's [51] proposed criticality score is based on the content sensitivity of the data item using SVM, the naive Bayes network is used to model the user's behavior information by the client, including the called process and its corresponding threads when the user is normally working [52], and a decision model called named RevMatch is proposed [53]. RevMatch made a decision based on the history of the labeled malware detection. Lastly, to identify malicious patterns in the system, Nkosi et al. [54] used a sequential pattern-mining technique.

Cyber Activity Behavior

Many articles focused on the use of cyber activity behaviors, login events, or the combination of login events with other features [55–60] using many different techniques. Nikolai and Wang [55] proposed a solution for data theft in Infrastructure as a Service IAAS Clouds; the k-nearest neighbor (KNN) is used to detect data theft in Clouds. Their monitoring system analyzed network messages patterns used to transfer data; using the similar KNN classifier technique and Dempster-Shafer theory by Punithavathani et al. [57]. Roberts et al. [56] provided a detection mechanism to counter insider threats in critical networks. W. Liu et al.'s [58] used the Bayesian networks (BNs) and novel modeling approach for the performance of insider threat detection. Research methodology was proposed to provide an approach for the construction, assessment, and optimization of the insider user normal behavior model. The framework was derived from the dynamic Bayesian perspective. Goldberg et al. [59] introduced an anomaly detection system, PROactive Detection of Insider threats with Graph Analysis and Learning PRODIGAL, to support human analysts by combining multiple machine-learning-based anomaly detection techniques. Rajamanickam et al. [60] discussed the password disclosure case and how the cryptography and, especially, the elliptic curve cryptography (ECC) worked, and because of its smaller keys, the ECC dominated the role of providing secure communication. Using ECC, it is appropriate to encrypt the users' passwords and share them when users need to communicate with Internet applications.

Another widely analyzed feature in cyber activities is the network packet or network traffic using different methods, such as machine-learning techniques, to model the behavior of insiders [61–67]. Encryption and pattern-matching techniques [68–72] and network-attached systems, such as HoneyBot and deception (i.e., a decoy network interface controller) [73–76] have also been used. Traffic monitoring tools [77,78], a behavioral analysis based on a zero-knowledge anomaly called XABA (semi-comprehensive solution) [79], and novel algorithms are beneficial for detecting insider

attacks on wireless sensor networks [80]. The industrial sector used ISA100.11a, a smart response mechanism based on wireless sensor networks [81]. Gossip protocols have been used to introduce the overlay architecture of networking designed to facilitate information sharing on mobile devices [82]. Dynamic access control [83] is a mechanism that is heavily dependent on malicious node assumption to design advanced collision attacks called random poisoning [84]. Other studies used a mathematical model [85], unknown input observers [86], Dynamic Host Configuration Protocol DHCP starvation attack and Transmission Control Protocol TCP [87–89], simple statistical measures [90], and Bayesian network model to predict insider threats [91].

Several articles focused on event log features, such as printer, system, and security logs. For example, Ambre and Shekokar [92] calculated the probability of an intrusion behavior for a given event using the Bayesian theorem. Hsieh et al., Isis Rose et al., and Nkosi et al. [93–95] analyzed active directory services and audit logs using the Markov model, hierarchical task decomposition, and a rule learning algorithm, respectively. The works [96–109] combined and analyzed multiple log features collected from multiple sources, such as email, HTTP, logon, files, and devices to detect insider threats using statistical methods and machine-learning techniques.

The features of the user database and file access patterns have been studied by Hu et al. [110] using statistical methods, a community anomaly detection system applying a relational framework [111], One-Class Support Vector Machine OCSVM to analyze features [112], rule mining [113], and cryptographic techniques and watermarking [114]. A probabilistic mechanism was used to re-encrypt files [115], the scoring function [116], the naive Bayes algorithm, and vector space model (VSM) [117]. Consensus clustering was employed to create multi-view anomaly detection methods [118], a random topic access model [119], community evolution discovery [120], orthogonal defense mechanism [121], incremental algorithms [122], and an unsupervised approach [123]. Algorithms and techniques on structured query language (SQL) queries [124–127] were used, and a malicious information flow was detected through bridge data items [128]. This approach enables the identification of deviations by reconciling the process and data perspectives [129]. A user profiling approach was used to detect suspicious transactions using a two-stage database intrusion detection system [130]. Moreover, methods for bypassing data loss prevention systems were used over trusted applications [131], and a solution for fine-grained histogram-based profiles of database usage was created [132]. Business process mining [133], neural dependency and inference graph (NDIG) [134], knowledge graph and dependency graph components [135], the triangle authentication process [136], and a provenance graph using privacy, lineage, uncertainty, and security PLUS [137] were also utilized.

Legg et al. [138] analyzed and explored device usage features using PCA, and Aditham et al. [139] used a semi-supervised approach to investigate the multiple features of memory access. For insider threat detection, Crawford and Peterson [140], Meng et al. [141], and Chiu et al. [142] used a methodology that is dependent on scanning the memory of running virtual machines, a Bayesian inference-based trust mechanism, and a frequent pattern outlier factor, respectively. The works [143–147] highlighted correlation coefficient methods and kernel density estimation (KDE) to determine CPU usage, a medium access layer MAC based solution, design science research to detect USB usage, a fuzzy multi-criteria aggregation method, and the hidden Markov model (HMM) and Baum–Welch algorithm to model resource misuse, respectively.

Jaenisch and Handley [148] analyzed email and text features using the random forest algorithm, which identifies the various behaviors of suspicious users or their abnormal derivatives. Canbay et al. [149] applied the term frequency–inverse document frequency TF-IDF numerical statistic to sensitive documents to extract sensitive words, whereas Garfinkel et al. [150] used latent semantic indexing to construct a model that documents topics based on Google's rapid response framework in monitoring disk forensic content (or other media), such as email addresses and credit card numbers.

Feng et al. [151] analyzed upload, download, and web-browsing features using a novel two-stage machine-learning system, whereas Zhang et al. [152] proposed two generic reputation-establishment algorithms. Another study by Myers et al. [153] suggested a cooperating server distributed system that

correlates log information and triggers rule-based responses. In addition, Sohal et al. [154] proposed a cybersecurity framework using the Markov model, virtual honeypots, and intrusion detection systems to detect malicious edge devices in the environments of fog computing. Nathezhtha and Yaidehi [155] proposed improvised long short-term memory (LSTM) to learns users' behaviors. The model automatically trains itself and stores behavioral data to classify user behaviors as normal or abnormal. Sharghi and Sartipi [156] explored file-sharing and access policy features using a new behavior pattern language—that is, a constraint-based pattern-matching engine, whereas Agrafiotis et al. [157] used tripwire grammar. Bao et al. [158] proposed a behavior rule-based methodology to monitor devices in a smart grid to detect insider threats. Using organizational structures, Kammüller and Probst [159] built vectors for insider attacks to identify the sequences of actions that lead to violations of security policies, whereas Dasgupta et al. [160] used a multi-token permission strategy.

Psychosocial Behaviors

Studies on psychosocial behavior analyses are few. Brdiczka et al. [161] combined psychological profiling and structural anomaly detection to build an architecture for the detection of insider threats using social networks, messages, and Internet visits. Alternatively, Suh and Yim [162] discussed the use of the power spectrum analysis of electroencephalogram EEG data to identify insiders using brain wave features. Similarly, Almehmadi and El-Khatib [163] and Almehmadi [164] proposed the use of intent-based access control that uses brain signals as intention access control. Lee et al. [165] proposed a real-time internal information leakage detection system based on emotional recognition, such as tension, agitation, and anxiety. A similar work by Taylor et al. [166] purported how self-focus, negativity, and cognitive processing can be assessed based on a linguistic inquiry and word count (LIWC) analysis.

In addition, Maasberg et al. [167] discussed a theoretical model of insider threats based on the following components: motive, opportunity, and capability. Safa et al. [168] modeled planned behavior and the dark triad personality trait theory and used motivation and opportunity modeled as presented by the social bond theory and situational crime prevention theory. Finally, studies [169–172] discussed social media and online behavior through Twitter and Facebook user comments and status updates, whereas Berk et al. [173] used opportunity and action theories.

Physical Behaviors

Marrone et al. [174] used door access and traffic server features and combined two unified modeling language models. The first addresses the physical protection of a system, whereas the second focuses on cyber protection. Another study by Zou et al. [175] used the door and sensor data features to explore the use of the failure mode and effect analysis method. Mavroeidis et al. [176] presented an ontological framework to improve physical security and insider threat detection using door access. Lastly, W. Meng et al. [177] used Euclidean distance to judge a node's reputation and combed multisource logs, such as emails, websites, and camera usage.

Other Behaviors

This section discusses the use of other behavior features or combined behaviors from previously discussed features. Durán [178] applied the reactor risk method, which includes a human reliability analysis and object-based event sequence trees developed using a probabilistic analysis approach. It integrates Material Control with Accounting (MC&A) protection and operational activities in a vulnerability assessment (VA) analysis. Kim et al. [179] discussed the modeling of game theoretics and an analysis of physical protection by incorporating insider threat implications to address the issues of interactions and intentionality. Dietzel et al. [180] suggested an approach that uses the resilient aggregation technique to leverage current communication redundancy. The data consistency technique is then applied to identify false aggregate information and filtration. Combining biometric and cyber behaviors, Fridman et al. [181] introduced a decision-level fusion technique that fused

four modalities based on stylometry (text analysis), usage patterns of application, and behaviors in web browsing. Additionally, Santos et al. [182] analyzed a combination of features, such as nonverbal behavior, biometric information, and daily activities, using machine-learning techniques. Tabash and Happa [183] combined computer emergency response team (CERT) logs with the knowledge of security experts in their system by having the analysts classify detected anomalies. Soh et al. [184] used email, personality traits, and implicit motives to profile employees using a gated recurrent unit and Skip-gram. Nithiyanandam et al. [185] proposed a layered defense based on data monitoring, activity monitoring, user authentication, resource monitoring, and an overarching defense manager. They have analyzed multiple features, such as access to use particular data, keystrokes of a particular user, printer, scanner, USB, and transfer data.

3.2.2. Techniques and Methods Used

Many techniques have been used to model insider threat behaviors. Table 1. discusses several techniques used in detecting the insider threats and highlights the general strengths and weakness. Most of the reviewed articles in this field deal with the issue of insider threats as classification-based. Thus, scholars aim to improve insider threat detection performances by developing detection systems based on existing machine learning, statistical classification, and clustering techniques. However, with valuable efforts for proposing detection methods, the performances of such methods remain challenging, and the need for feature engineering for a number of these techniques tends to be costly and time-consuming. New research requires sophisticated methods for an in-depth understanding of insider activities, where the nature of the insider is entirely different from that of the outsider.

Table 1. Techniques used.

Technique	Strengths	Weaknesses
Bayesian Algorithms	Good for mutually exclusive event probability calculation with any other event within a given sample set [92]. BN can abstract from specific details that satisfy desirable characteristics in modeling insider threat detection systems and predict their performance in enterprises in terms of simplicity, privacy, and portability [56].	Most of the detection models built on the basis of mathematical methods, such as Bayesian networks and Principal component analysis PCA, require extensive experience and in-depth knowledge for the models' development, training, and refinement. This expertise is neither cost-effective nor available for acquisition [186]. Expert disagreement may exist on the probability of a specific event or causality direction between two events. For example, certain experts might deem that A's behavior is normal, whereas the opposite is true for others [58].
Support Vector Machine (SVM)	One of the main aspects of SVMs that make it attractive for cybersecurity is that the latencies of classification are very low—that is, in the range of microseconds on modern computers. The performance of the classification is made faster by classifier training [61]. Another attractive property of SVMs is the fact that SVMs are based on a convex optimization formulation with single minima. In addition, SVMs provide a clear geometric interpretation of the classification boundaries and support vectors [112]. A better classification result can be provided by SVMs with less training data [52,63].	Although clustering k-means and SVM classifiers offer the best balance between quality and efficiency, they are not user-friendly and difficult for a human operator to understand [61]. In certain cases, parameterization can be tricky. Training can be more time-consuming for SVMs compared with other methods. SVM entails difficult communication.

Table 1. *Cont.*

Technique	Strengths	Weaknesses
One Class Support Vector Machine (OCSVM)	OCSVM can address the issue of rare class by building a model that considers nonthreat or normal data only [41,42]. It focuses on each action's semantic content, whereas the KNN method focuses on each action type. Therefore, OCSVM is selected because data are unbalanced, and which action is normal or malicious remains unclear [13].	The OCSVM approach is applicable to static data streams with bounded lengths only. By contrast, the data that relate to insider threats are typically continuous, and the pattern of the threats evolves over time. In other words, data involve unbounded length streams [41,42]
Decision Tree (DT)	A DT is easy and intuitive for human operators to interpret [61]. Easy to communicate and maintain. Simple, few, and relatively intuitive parameters are required. Can perform fast predictions.	DT consumes a large amount of memory (deep and large DT is required with additional features). DT, by nature, tends to overfit (i.e., it generates high-variance models, and the branches should be pruned to avoid such models). DT is incapable of incremental improvement.
TF-IDF	TF-IDF provides or identifies sensitive or important words in documents [43,150]. TF-IDF analyzes the importance of intercepted system calls (SCs) collected in the log file of the user [37].	It might be slow for large vocabularies, because TF-IDF directly computes document similarity in a word-count space. It assumes that different word counts provide similarity-independent evidence. TF-IDF ignores the semantic similarities between words.
Markov Model and Hidden Markov Model HMM	The Markov model effectively describes the consequent changes of the state [93]. The HMM models have been widely used in many areas, such as bioinformatics and computational linguistics, because of their capabilities on the recognition of temporal patterns. To capture sequential behavior, HMM is well-suited and has been successful in the biological sequence analysis and pattern reorganization in languages. It provides algorithms to learn the parameters from an observed sequence set, as well as the probability prediction for observing a given sequence [96].	The computational cost of the HMM increases with the number of states.
K-Nearest Neighbors KNNs	Compared with other classifiers, such as neural networks, the KNN classifier can achieve a faster speed with a lower computational burden in the training and classification phases. This quality makes it desirable when deployed in limited-resource platforms, such as the intrusion detection system node [64].	The KNN method is ineffective in certain aspects of detecting insider threat, because information can be hidden in normal actions via manipulation [182]. Using the KNN method requires advanced knowledge of how many clusters in the data may require many trials to assume the best cluster K number to define. Clusterization may differ across runs due to random algorithm initialization.

Table 1. *Cont.*

Technique	Strengths	Weaknesses
Principal component analysis PCA	PCA is used for dimensionality reduction and reduces similar cluster behaviors. It is a widely used mechanism for addressing high-dimensional data. PCA is an effective technique for identifying outliers [100,187]. Using PCA, a large feature set can be reduced into multiple anomaly assessment scores [138].	One of the drawbacks of PCA is that it is often regarded as a black-box approach, where comprehending the link between the resulting PCA space and original feature space becomes difficult [188]. Similar to the other detection models that are built on the basis of mathematical methods, such as Bayesian networks, PCA requires extensive experience and in-depth knowledge for the model development, training, and refinement. This expertise is neither cost-effective nor available for acquisition [186].
Gaussian Mixture Model GMM	By implementing the GMM approach, the model can explain why given observations are classified as anomalous [183]. Moreover, the models' parameters and the results of predictions provide analysts with a deep understanding of the decision-making process of the method. GMM is capable of modeling a dataset with a complex probability distribution.	Long computation time. Falling into the local maximum. One of the serious limitations in GMMs is its statistical inefficiency in modeling data located on or near a nonlinear manifold in the data space.
Long Short-Term Memory LSTM	LSTM is well-suited to classify a time series, because it employs an LSTM cell to learn a historical experience [99]. LSTM is suitable for capturing the long-term temporal dependencies on the user sequence of actions, because the hidden units of the LSTM can potentially record temporal behavior patterns [188].	It is inefficient when directly used to classify the insider sequence of actions, because its output only contains a single bit of information for each action sequence [188]. Compared with other techniques, such as gated recurrent units (GRU), LSTM requires a longer computation time due to its structure [189].

3.2.3. Datasets

Considering the various datasets, Table 2 shows that the majority of the recent studies have used the Computer Emergency Readiness Team CERT dataset, because such data contains many scenarios for the traitor and masquerader. We introduce the types of dataset involved as follows:

Table 2. Datasets.

Ref.	Dataset	Features
[57,97,102,104–110,188]	CERT	HTTP: ID, user, date, PC, URL, and content EMAIL: ID, user, date, PC, from, to, CC, BCC, attachments, size, and content LOGON: ID, user, date, PC, and activity (logon or off) FILE: ID, user, date, PC, filename, and content DEVICES: ID, user, date, PC, and activity (connect/disconnect)
[70,98,99,127]	NSLKDD Or KDD-99	KDD-99 and NSL-KDD data include 41 features and five normal classes and four types of attacks, namely, Dos, Probe, R2L, and U2R Denial of service attack (DoS)
[190]	Schonlau dataset	Time, user, process, registry, and file access

Table 2. *Cont.*

Ref.	Dataset	Features
[182]	APEX	
[44]	(Are You You?) RUU Dataset	Number of search and nonsearch actions, user-induced actions, window touches, new processes, running processes, and documents that edit running applications on the system.
[191]	The Wolf Of SUTD (TWOS)	KEYSTROKE: timestamp, key press/release events, key value (anonymized as a subpart of the keyboard), and username MOUSE: timestamp, mouse move/click/release events, coordinates of mouse pointer, and username HOST MONITOR: timestamp, program name, PID, parent program name, parent PID, and SC operation NETWORK TRAFFIC: HTTP request/response, method (e.g., GET and POST), status code, content length, and content type EMAIL: timestamp, header, sender, receiver, and LIWC features extracted from email body LOGON: timestamp, login attempt, login success, logout event, and username

CERT is a collection of datasets on the synthetic insider threat generated by the CERT and other partners. The dataset is generated using different scenarios that contain traitor instances and masquerade activities. The collected dataset contains logs of login data, HTTP or browsing history, emails, file access logs, device usage, LDAP data, and psychometric information.

Remote terminal unit (RTU). The RTU dataset is a collection of labeled RTU telemetry streams from a gas pipeline system at the Critical Infrastructure Protection Center at Mississippi State University. The dataset includes benign RTU transactions, data injection attacks, and command injection attacks, which were generated specifically for research on critical infrastructure protection.

NSLKDD/KDD-99. An intrusion detection evaluation dataset was collected at the Massachusetts Institute of Technology Lincoln Laboratory. The main purpose of the dataset was to improve and evaluate intrusion detection systems. However, this dataset has been used in research on insider threat detection—in particular, the "user-to-root" group of attacks—to mitigate masquerade attacks using SC logs.

Schonlau dataset. This dataset contains UNIX commands at approximately 15,000 commands per user and is generated by 50 users with different roles in the organization. In the generated dataset, the first 5000 commands for each user exclude any masqueraders, which are used for training. The next 10,000 commands are deemed as a hundred blocks of a hundred commands, which are seeded with the masquerader's user information, i.e., with the data of another user outside of the 50 users. Thus, the data used in masquerade sessions does not contain any malicious content.

APEX' 07. These datasets were introduced by the National Institute of Standards and Technology to simulate the analysts' tasks in the intelligence community. The APEX dataset contains the activities of 13 analysts, 8 benign analysts, and 5 malicious insider analysts.

RUU. This dataset for masqueraders was collected by Malek Ben Salem [192] and [193]. The datasets were collected from the PCs of 34 regular users, which consisted of host-based activities, such as Windows registry, file system access, processes, system GUI, and dynamic library loadings.

TWOS. The TWOS dataset has been collected from real user interactions with a host machine that contains legitimate user data and malicious insider instances (i.e., masqueraders and traitors). The dataset was collected during the competition organized by the Singapore University of Technology and Design in March 2017 and comprises data collected from six data sources (i.e., keystrokes, mouse, host monitor, network traffic, SMTP logs, and logon), with additional data from a psychological personality questionnaire [191].

3.2.4. Evaluation Metrics for Insider Threat Detection

Many classification metrics are used to evaluate the insider threat detection systems, and a few are known by multiple names. Table 3 discusses the most common metrics and the works where these metrics are used.

Table 3. Evaluation metrics.

Metric	Formula	Description	References
Precision	$Precision = \frac{TP}{TP+FP}$	A fraction of data entries of insider threats are labeled as a malicious insider, which indicates a truly malicious insider.	[32,46,55,57,62–68,94, 96,99,108,119,130,139, 162,170,173]
True Positive Rate (TPR)	$TPR = \frac{TP}{TP+FN}$	TPR, which is also known as sensitivity or recall, is defined as the fraction of insider threat data on malicious entries that are correctly classified.	[32,37,39–41,46,55,57, 62–68,70,94,96,99,107, 108,114,119,125–130, 133,139,143,153,161, 162,170,173]
True Negative Rate (TNR)	$TNR = \frac{TN}{TN+FP}$	Additionally known as specificity, TNR pertains to the ability of the detector to correctly identify data without malicious entries.	[55,96]
False Positive Rate (FPR)	$FPR = \frac{FP}{FP+TN}$	It is calculated as the ratio between the number of benign insiders that are incorrectly classified as malicious insiders and the total number of benign insiders.	[31,37,39–42,46,57,58, 62,66,67,75,100,102,108, 114,125–128,133,143, 153,159,161]
False Negative Rate (FNR)	$FNR = \frac{FN}{FN+TP}$	False negative indicates the fraction of the missed malicious insider that the model failed to identify but classified as a benign insider.	[31,42,125–128]
F-score	$F-score = 2.\frac{Precision.Recall}{Precision+Recall}$	Additionally known as F-measure, it is the harmonic mean between sensitivity and precision.	[32,37,46,62–68,130, 134,162,170,173]
Accuracy	$Accuracy = \frac{TN+TP}{TN+TP+FN+FP}$	It is the fraction of all negative and positive entries that are correctly classified. It can be considered the overall effectiveness of a classifier.	[37,38,41,42,62–68,94, 107,108,110,113,148, 150,151,159,161,170, 173]
ROC or AUC		The ROC curve is a graphical visualization and used to plot the TPR against the FPR. AUC is computed by taking the area under the ROC curve as the ranges of the FPR from 0 to 1.	[35,45,62–68,97,101, 105,106,110,112,117, 121,124,131,133,182, 194]
Time complexity		It pertains to the time required to complete the classification task of such a classifier.	[61]

TP: true positive, FN: false negative, TN: true negative, and FP: false positive. These terms have meanings according to the type of processes defined in Table 4.

Table 4. Definitions of statistical measures.

Statistical Measure	Process
	Insider Threat Detection
TP	Number of malicious insiders correctly classified.
FN	Number of malicious insiders incorrectly classified.
FP	Number of normal insiders incorrectly classified.
TN	Number of normal insiders correctly classified.

3.2.5. Detection Methodology

Based on the reviewed studies, two main detection methodologies are used. The first is anomaly detection, where the system makes a baseline profile of the normal system, network, or program activities. Any abnormality from the learnt baseline is labeled a malicious insider. The second is signature-based detection, which identifies a previously known malicious insider when such activities match the stored signature or rule-based protocol to model the used behaviors on the system. Figure 8 shows that the majority of existing solutions are based on anomaly-based detection or address insider threats as a classification issue. The use of anomaly-based methodologies is due to the class imbalance in insider threat datasets, where the majority of the data are composed of the daily activities of regular users, as well as concerns on the issues of zero-day malicious attacks.

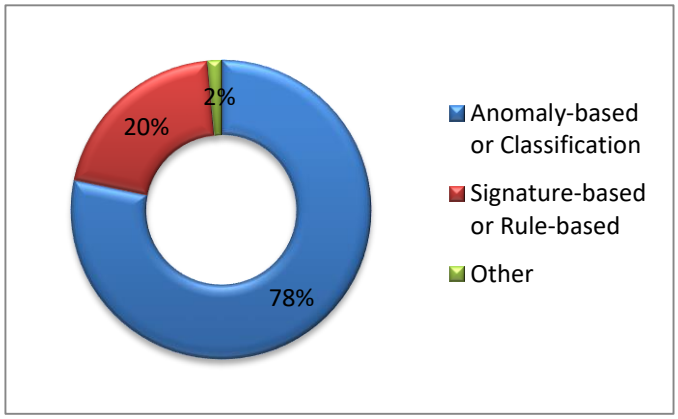

Figure 8. Detection methodology.

4. Discussion

This survey article aims to study insider threats and discuss the current detection methods and techniques in the field of insider threat. The main purpose of the study is to focus on the literature using an analysis review. The included papers were reviewed and discussed based on the analyzed behavior, techniques, and methods used, as well as datasets, evaluation metrics, challenges, and recommendations.

The previous sections indicate that the majority of previous studies have highlighted the monitoring and analysis of user activities to detect insider threats using cyber behaviors. However, other behaviors, such as physical behaviors, are attracting less attention. Despite the need for "feature engineering," which is difficult and time-consuming, machine-learning techniques are widely used for the development of insider detection methods. In terms of datasets, the majority of studies used their experiment and simulation due to the lack of real-world data for insider threats. Recently, however, synthetic datasets, such as CERT, have been used to evaluate insider threat detection systems. Appendix A sheds light on studies carried out concerning detection methodologies, methods, and datasets used; behavior features; and their results.

4.1. Challenges

This part discusses the current challenges in the detection of insider threats; these challenges are grouped into eleven categories, which are discussed as follows in Figure 9.

Figure 9. Challenges.

4.1.1. Performance

As an attacker is a legitimate user of the system, this notion poses the difficulty of drawing a clear line between what is legitimate and what is malicious [112]. Most of the existing approaches used for insider threat detection apply the anomaly detection approach, which is supervised or unsupervised methods that classify small deviations from normal activity patterns in anomaly detection as an abnormality and, thus, classify this abnormality as malicious. However, most of these abnormalities are nonmalicious activities. These methods tend to raise unnecessary false alarms in handling such cases [36]. Thus, traditional approaches suffer from the well-known issue of false positives due to this notion, which makes such approaches difficult to apply in enterprise environments [37]. In other words, reducing false positive and negative alarms for insider threat detections without affecting the detection accuracy remains a major challenge.

4.1.2. Insider Threat Datasets

Lack of Real Data

In spite of advanced research on insider threats, challenges in validating and refining the detection models remain due to the absence of real-world data from organizations [13,139,195]. The lack of actual insider threat data is also a major challenge in assessing and developing insider threat detection systems. Moreover, the present review observes that synthetically created datasets used in the surveyed articles were not created specifically for insider threats. Furthermore, a few of these datasets did not contain malicious data, whereas others were outdated [1].

Ethical and Privacy Issues

Despite the increase in the number of insider threat incidents, not all organizations report such incidents nor allow access to their data, typically due to ethical and privacy concerns. The issue of real data access is crucial for insider detection, which continues to be a significant obstacle for

validating and refining effective and scalable detection systems. As a result, most existing detection systems are tested and evaluated on synthetic and simulated datasets, with the biases that such data imply [57,100,191].

Analysis Issues on Encrypted Flows or Encrypted Data Packets

To avoid detection by tools, such as intrusion detection systems, attackers may use cryptography to mask their attacks. Such a scenario renders detection systems unable to analyze encrypted flows or encrypted data packets, which is another main limitation of the current intrusion detection systems [70].

4.1.3. High Dimensionality

Sheer Volume

The capabilities of capturing logs for the activities are an advantage that may provide insight into employee actions. Despite this advantage, the analysis of activity logs continues to be difficult for analysts because of the sheer volume of activities that employees produce every day [95,139,162]. The large number of organizational staff requires the monitoring of staff behavior properties, which results in the massive need for data to be processed [52]. The growth of this data outpaces the ability of human auditors and administrators to digest such data quantities using manual analyses [95].

Unbounded Length and Threat Patterns

Features can be found in time or frequency domains, according to the temporal phenomenon of insider threat detection. Nevertheless, any sudden changes in behaviors should be monitored to identify specific problems. Additionally, any actions can be a sign of malicious attacks by the insider. The complexity and unpredictability of malicious actions render a careful analysis difficult for the system, network, and user parameters correlated with insider threats. Therefore, a heterogeneous, high-dimensional data analysis problem in isolating suspicious users was created [41,106,107,195]. Unsupervised learning is one of the approaches applied to solve such a problem, but these approaches are limited to static, finite-length data, thereby limiting the application against insider threats. Thus, insiders tend to have unbounded length and threat patterns that evolve over time [43].

4.1.4. Physical and Cyber Behavior

Another limitation of the current insider threat detection approaches is that they only concentrate on cyber or physical security behaviors within cybersecurity [87,175,177]. Most of the previous works did not use both behaviors of the cyber and physical systems in analyzing insider threat detections. The majority of scholars aim to detect insiders by observing behaviors either from the cybersecurity or physical security aspects [86]. However, in terms of detecting physical threats, most of the existing studies applied physical access control mechanisms that may control the physical access of unauthorized users to a certain point. However, such mechanisms are ineffective against insider attacks.

4.1.5. Analysis Interval

Several insider threat detection systems were unable to provide real-time responses, which raises the need for additional research efforts [7]. In the case of offline detection tools, a drawback exists where these tools are unable to provide support and respond to a log analysis with respect to time. Therefore, most of the current systems continue to lack real-time tools, which prevents further actions from curbing the problem [92]. Large amounts of audit data are collected from organizational environments in a server log form, which potentially can play a role in access decisions. However, audit data are often used only for offline forensics, which leads to “later is too late” circumstances [61].

4.1.6. Costly and Time-Consuming

One of the detection approaches for insider threats is the supervised learning approach, which trains data to build a classification model. However, most of the introduced detection methods built are based on supervised learning. Thus, the need remains for contextual data entries about users and a training process for supervised learning methods that are specific to insider threat detections. Despite such capabilities, this approach tends to be costly and time-consuming [39,42,80,103].

4.1.7. The Policy

In general, insiders have knowledge of policies and practice such knowledge. Typically, policies are related to access rights granted to insiders, which essentially aim to circumvent regulations [159]. The development of access control policies is centered around trust regarding the access rights of legitimate users, such as reading, writing, and execution, based on the task and position hierarchy of the legitimate users in the organization. In this case, an insider with malicious intentions can have the power to destroy or steal information [43]. However, such access rights are increasingly misused by oblivious, hostile, rogue, and pseudomalicious insiders [160]. Therefore, the lack of access control systems in insider threat detection systems leaves enterprises frequently vulnerable to such threats [163].

Limitations of Static Access Control Policy

The existing access control techniques are designed on the basis of static policies that tie crypto-credentials to attributes used by the rules of access control. Dynamic events, such as behavioral changes of the actor (e.g., a user performs illegitimate activity within their privilege rights), subversion of credentials (e.g., theft of common access cards), and changes in the structures of the document (e.g., editing Wiki pages), are not detectable, which leaves systems vulnerable for a long period [62,122].

Limitations of Access Control Point Location

As countermeasures against insider threats, access control rules are more complex than those used for countermeasures against malicious outsiders. Furthermore, the challenge for countermeasures against insider threats continues to question where access control should be installed in a network. The question of the suitable location of an access control point to control insider threats is yet unanswered [83].

4.1.8. Complexity of Insider Threat Detection

Detecting insider threats is becoming a highly complex and difficult task for the following reasons. First, insiders with trusted access can perform unauthorized activities. Thus, external network security tools, such as firewalls, IDS, and antivirus software, cannot detect a malicious insider [93,147,184,189]. Second, insider attacks manifest in many forms. For example, a malicious insider may plant a logic bomb to disrupt the systems or steal intellectual property. The diversity of insider attacks increases with the complexity of detecting insider threats. Finally, insider attacks are frequently conducted by malicious insiders during daily working hours, which drown the anomalous behavior of malicious insiders in most of the normal employee behaviors [95,139,184,189].

4.1.9. Collusion Attack Detection

Most of the existing solutions for insider threats are focused on individual detections. Nevertheless, collaborative attacks can be launched by two or more insiders, which are difficult to detect. The disadvantage of these types of attacks is that the activity of each insider may look benign, but, when combined with other activities, it may result in a malicious action. Therefore, further effort is required to handle collusion attacks [128].

4.1.10. Lack of Attention and Strategy

Most organizations provide extra focus on outsider threats rather than malicious insiders [95]. Researchers in the field of cybersecurity have dealt with and identified many different security threats. Scholars emphasize that threats from malicious insiders are more dangerous than external threats; however, this statement has failed to receive sufficient attention. Another challenge is the lack of understanding of the intent and strategy of the malicious insider [45]. Most researchers in security highlight the lower layers of a software system—that is, mining data at the network and host machine or the levels of source code. As a result, these solutions mainly focus on certain signatures or threat categories that are naturally tactical. The current study deems that a piece remains lacking in the overall picture of the current understanding on the intent and strategy of malicious insiders.

4.1.11. Insider Threats in SCADA

Supervisory control and data acquisition systems (SCADA) constitute the critical infrastructures' sensitive parts. Each successful malicious incident could cause huge damages on materials economic and human [196]. Operators play an important role in SCADA systems, and their commands can have high impacts on the reliability of critical infrastructures. Therefore, insider attacks and approaches to deal with the malicious insider get more attention in SCADA security [46]. All SCADA environments are open to insider attacks, even though an insider cyberattack mostly needs more technical skills and knowledge about the targeted system. For the direct attack on remote terminal units, physical access is required to the communications channels, but when this access is obtained, mostly, at that point of access, all protections will be bypassed. The equipment of programmable logic controllers (PLC) is also more vulnerable to remote attack because of the device's inherent design and devices origins on the floor of the factory [197].

4.2. Recommendation

The research recommendations in insider threats detection are grouped into eight categories as shown in Figure 10.

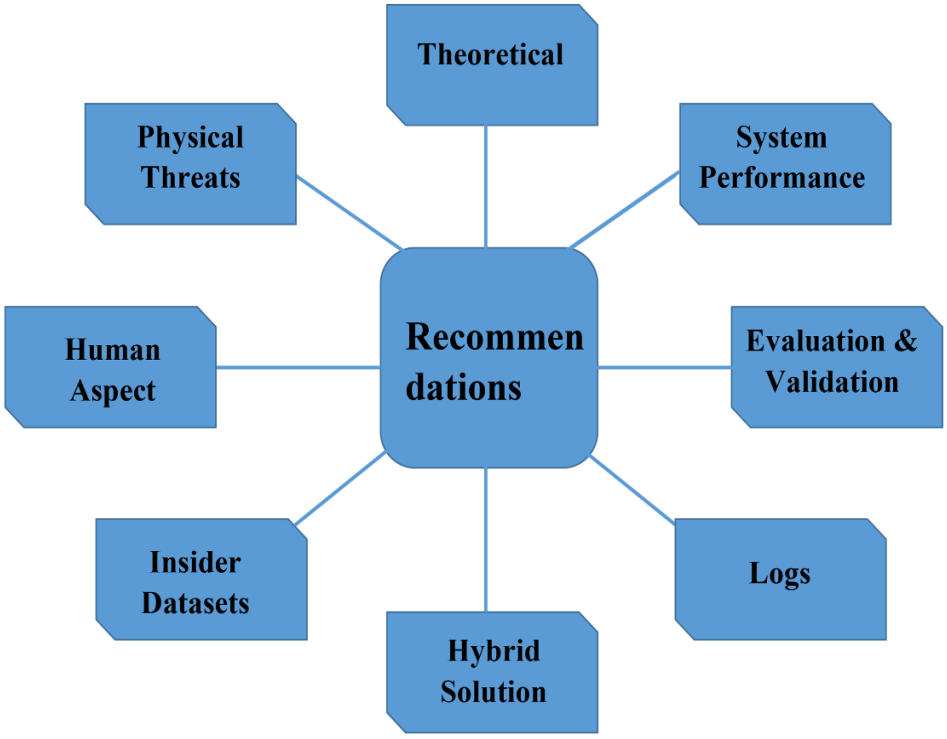

Figure 10. Recommendations.

4.2.1. Performance

For insider threat detection to be effective, improving the performance of the recall rate without sacrificing precision is extremely important [93]. Feature selection of security event data is a potential approach to improve performance. Therefore, added efforts are required for the development of feature selection technologies and tool defenses against insider threats [111]. One such example of the recommendation for selecting features is the use of complex models, such as the LSTM recurrent neural network [96] and gated recurrent unit (GRU), such that a rich representation of user behavior can be learned.

4.2.2. Dataset

Previous studies recommended that new insider datasets should be created with much larger data and stream sizes [102]. A long period is also essential to confirm whether the models can normally work with the daily updates, whereas normal user behaviors change over time [58]. The new dataset should include more malicious data, because the current datasets contain only a few malicious data, a few of which are becoming outdated. Collusion attacks should also be considered using the new insider dataset for further improvements and challenging and realistic testing of detection methods [1]. Thus, maintaining updates on insider datasets with normal and malicious activity patterns is necessary so that the proposed solutions for detecting recent insider attacks can be verified and evaluated [111].

4.2.3. Hybrid Solution

In summary, the present study observed that most of the existing solutions are based on anomaly and unsupervised approaches due to the class imbalances in datasets and other issues, such as zero-day malicious attacks. However, a good and robust insider threat detection method should use a combination of several independent approaches [1]. In terms of the first defense line, misuse-based insider detection should be considered to cover the scenarios of known insider threats. However, at the second line, anomalies and other best practices, such as prevention and mitigation techniques, should be employed.

4.2.4. Logs

One of the better techniques for mitigating insider threats is using log management, which includes log analysis and event correlation. Log analysis can pinpoint the root cause of an insider attack and protect the network from security violations at the same time [92]. Combining other sources of data for the better detection of insider threats includes Windows logs, active directory logs, printer logs, and physical security logs [151]. The statistical learning algorithms, an ensemble learning classification, and the utilization of a network access control (NAC), modern "big data" are having the ability to capture and manage the flow of logs and provide accessibility to batch processing, stream processing into the analytic tools, and also, offering interfaces queries for investigative of the ad hoc [198]. Mayhew et al. [61] discussed the well-known instance of a big data processing Splunk, which offers a capability that eased the cyber defender's task to create correlations between different pieces of log information using a specialized query language. Therefore, combining and analyzing these types of logs and applying the use of big data analytics tools can be a direction for future studies on insider threats.

4.2.5. Evaluation and Validation

Currently, no framework or standard exists that addresses the evaluation of insider threat detection systems [7]. Thus, the selection for the best detection method is still a challenging decision-making task; this is due to the multiple detection evaluation criteria, such as accuracy, Recall, FPR, time complexity, etc. Therefore, this study strongly recommends that a generic framework should be developed for the evaluation of insider threat detection systems to assist and guide researchers and practitioners in

evaluating their proposed systems. With regard to improving the evaluation standard, collaboration between researchers in the academia and practitioners in the industry is highly recommended. Such collaborations will assist researchers in seeking feedback from the industry on developed systems to be evaluated, which can lead to improved adoption and adaptation of the respective systems to real-world environments [7,188].

4.2.6. Human Aspect

Most of the existing works focused on the technical aspect of insiders, on the machine, system, and network. However, the nontechnical aspects of the insider problem are critical elements of any insider threat detection system. Therefore, many effective techniques can be used to address the human aspect of the insider problem, such as human communication (i.e., tone of voice, body language, and attitude toward others) [187].

4.2.7. Physical Features

Although cybersecurity researchers appear to be aware of the physical effects of cyber threats, most studies are conducted either on "cyber" or "logical" security. Even so, many cybersecurity threats (particularly on the Internet) originated from physical intrusions, and we still need approaches that model cyber and physical security aspects [174].

4.2.8. Theoretical

Future studies should provide information for all responsible management departments, as well as security professionals, with a deep understanding of insider characteristics, threats posed, potential risks of insider threats, and possible countermeasures. The analysis of the problem in general, including insider taxonomy development, attacks, and countermeasures, points to a particular information security threat with forecasting model developments [12].

5. Conclusions

Insider threats are among the most challenging security threats and the main concern of organizations of all sizes. Numerous studies have been conducted in this field, and efforts continue to grow, although the boundaries and descriptions of insider threats remain ambiguous. Thus, understanding and gaining insights into insider threat detection is an important research direction. This review aimed to provide an extensive view and deep understanding of the field of insider threats by surveying and categorizing the existing literature. Along with the deep investigation on the existing literature and analysis of real cases, the two distinct classes—namely, insider and insider threat detection—have been elucidated. Significant information was obtained through the intensive review and analysis of the final set of the reviewed articles, such as the challenges and issues that researchers face in the field of insider threats. In addition, important recommendations related to insider threat detection, as well as datasets and techniques that have been used, were proposed. The various recommendations can provide future researchers with a clear picture of the research direction on insider threat detection. The present review also summarizes the concepts for insider detection as presented in the previous literature, which provides a useful reference for researchers.

Author Contributions: Conceptualization, methodology, and design M.N.A.-M., and R.A.; As the first authors, M.N.A.-M. and R.A. wrote the main parts and the first draft of this study; Z.Z.A., contributed to the review analysis; W.Y. and A.H., verified the output; K.H.A. and N.S.A., 2editing and visualization; and Z.Y., industry advise. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to gratefully acknowledge the funding support provided by Universiti Teknikal Malaysia Melaka (UTeM) and the Ministry of Education Malaysia under the TRGS Program with number TRGS/1/2016/UTEM/01/3 and TRGS Project (TRGS/1/2016/FTMKCACT/01/D00006).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

To understand and categorize the previous studies on the insider threat detection domain, Appendix A provides a comparative analysis based on diverse aspects, such as **detection methodologies** which divided into: The anomaly detection and classification method, where the anomaly system makes a baseline profile of the normal network, system, or program activities, and any deviation from the created baseline is addressed as an malicious insider and the signature-based detection and rule based method detect previously known malicious insider threat when those intrusions match the stored signature. **Methods** are divided based on the approaches that used in each of the studied article to model the insider threat. **Datasets** is referring to the data that been used to evaluate the proposed solution as well as the environment used to build the insider threat detection which was divided into synthetic dataset (SY), real data (RD), case study (CS), Simulation (SE), own environment (OE). **Features**, all the reviewed articles are divided based on the analyzed behavioral features and divided into four groups: behavior of biometrics, cyber features, psychosocial behaviors and other behaviors. Finally, the **Results** that have been achieved by the studied article.

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[46]	×	√	Statistical threshold-based anomaly	SE	√	×	×	×	>20 DTR
[35]	×	√	Dynamical system theory for usage pattern	SE	√	×	×	×	N/A
[36]	×	√	Unsupervised learning techniques (LZW) algorithm	RD	√	×	×	×	ACC = 87, TPR = 58, FPR = 0.09
[40]	×	√	Supervised learning OCSVM	SY	√	×	×	×	Accuracy = 71% FPR = 31%, FNR = 0%
[41]	×	√	Multiple OCSVM models and multiple graph-based anomaly detection models	SY	√	×	×	×	SV ACC = 0.71, SV FPR = 0.31 SV FNR = 0.0, UV ACC = 0.56 UV FPR = 0.54, UV FNR = 0.42
[169]	×	√	Unsupervised flat data classification	RD	×	×	√	×	Accuracy: NBM = 79 SVM = 81, MLR = 80
[44]	×	√	Fisher feature selection and GMM	SY	√	×	×	×	Average AUC improvement of 17.6%
[32]	×	√	Ensemble reauthentication for Human Computer Interaction HCI behavioral patterns using SVM	SE	√	×	×	×	Between 20% and 100% accuracy rate

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[37]	√	×	TF-IDF	SE	√	×	×	×	Accuracy = 94.29% Response time = less than 0.45 s
[53]	√	×	Decision model named RevMatch	SE	√	×	×	×	TP = 0.927, FN = 0.073 FP = 0.007, Qu Sc = 0.920
[30]	×	√	DT, SVM, and PNN	OE	√	×	×	×	FRR = 2.86%, FAR = 3.23%
[34]	×	√	local outlier factor LOF, DT, logistic regression, random forest	OE	√	×	×	×	Best AUC = 0.979
[130]	√	×	Markov Modulated Poisson Process Module MMPPM and Malicious Transaction Generation Module (MTGM)	SE	√	×	×	×	TP = 98%, FP > 10%
[48]	×	√	Sequence clustering algorithm and Bayesian information criterion	SE	√	×	×	×	N/A
[47]	×	√	Statistical quality control technique	RD	√	×	×	×	N/A
[45]	×	√	Dynamic approach Generalized sequential pattern mining	OE	√	×	×	×	Precision = 100%, Recall = 70%
[43]	×	√	Ensemble-based stream mining and unsupervised learning	SY	√	×	×	×	Accuracy = 56%, FPR = 54% FNR = 42%
[49]	×	√	Bayesian belief network	N/A	√	×	×	×	N/A

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[54]	√	×	Sequential pattern mining framework prefix span	OE	√	×	×	×	At Minsup = 0.9, Precision = 0.9 FPR = 0.02, FNR = 0.1
[38]	×	√	Incremental learning algorithm	OE	√	×	×	×	FPR = 0.036, TPR = 0.98
[52]	×	√	Rough set theory along with machine learning (naive Bayes network)	N/A	√	×	×	×	N/A
[51]	×	√	SVM	OE	√	×	×	×	Accuracy approx. 98%
[39]	×	√	Sequence alignment	SY	√	×	×	×	TPR = 98.3%, FPR = 0.77% Success rate = 80.2%
[92]	×	√	Probabilistic approach Bayes' theorem, RE	OE	×	√	×	×	N/A
[93]	×	√	Statistical model, Markov model	OE	×	√	×	×	Recall = 67%, Precision = 99%
[79]	×	√	Zero-Knowledge Anomaly-Based Behavioral Analysis called XABA	SY	×	√	√		N/A
[156]	√	×	New behavior pattern language; a constraint-based pattern-matching engine	OE	×	√	×	×	N/A
[111]	×	√	K-Nearest neighbors and PCA	RD	×	√	×	×	Mix rate = approximately 0.91

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[36]	×	√	K-means++ clustering, dts, and SVM	OE	×	√	√	×	HTTP = 99.6, TCP = 93, Wiki = 76, Twitter = 96 Email = 93
[151]	×	√	Use graph-based Oddball and PageRank and density-based LOF	SY	×	√	×	×	N/A
[110]	×	√	Tree-structured profiles and PCA	SY & SE	×	√	×	×	Precision = 42%, Recall = 100%
[55]	×	√	KNN	OE	×	√	×	×	DT = 100%, FB = 0
[96]	×	√	HMMs	SY	×	√	×	×	AUC:10 state = 0.755 20 state = 0.784, 10 state = 0.797
[57]	√	√	KNN classifier, Dempster–Shafer theory	OE	×	√	√	×	N/A
[102]	×	√	Unsupervised KNN	SY	×	√	×	×	Recall = 0.5, Precision = 0.08
[152]	×	√	Based on a game-theoretic formulation	SE	×	√	×	×	FPR = 0.35, DTR = 90%
[104]	×	√	Unsupervised algorithms and anomaly detection language syntax	OE	×	√	×	×	AUC scores close to 1.0
[112]	×	√	OCSVM (support vector machine) and radial basis function (RBF)	SE	×	√	×	×	DB and file access = 96%, File server = 98%, DB server = 98%
[103]	×	√	PCA and Euclidean distances	SY	×	√	×	×	N/A
[157]	√	×	Grammar that can capture policies	SE	×	√	×	×	N/A

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[105]	×	√	PCA	SY	×	√	×	×	N/a
[106]	×	√	K-means, GMM, TF/IDF, and Markov model	SY	×	√	×	×	N/A
[158]	√	×	DC power flow model and state estimation model, rule-weight, compliance distance	SE	×	×	√	×	N/A
[66]	×	√	Bi-clustering and OCSVM	OE	×	√	√		FP = 1%–2%
[125]	×	√	Datacentric viewpoint	RD	×	√	×	×	N/A
[107]	×	√	Hidden Markov method	SY	×	√	×	×	DTR = 0.39, 0.36, and 0.47 detection rate of 0.8
[134]	√	×	Neural Dependency and Inference Graph NDIG	N/a	×	×	√	×	N/a
[116]	×	√	Scoring function and aggregation function	OE	×	√	×	×	N/A
[117]	×	√	Document segmentation and naive Bayes algorithm and vector space model VSM	SY	×	√	×	×	N/A
[159]	√	×	Exasym model	CASE STUDY	×	×	√	×	N/A
[108]	×	√	Graph-based optimization approach	SY	×	√	×	×	AUC, CERT = 0.9520 NATOPS = 0.7196
[88]	√	×	TCP tunneling	SE	×	×	√	×	N/A
[78]	×	√	User privileges Techniques	OE	×	√	√	×	N/A

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[127]	×	√	period detection and filter algorithm	SY	×	√	×	×	N/A
[95]	√	×	Rule-learning algorithm	OE	×	×	√		Minsup 0.9, TPR = 0.94, TNR = 0.02
[173]	×	√	Traditional notion of Motive, Means, and Opportunity	OE	×	×	√	×	N/A
[128]	×	√	Algorithm based on the basic logic for the connection	SE	×	√	×	×	FP = below 20%
[109]	×	√	Efficient Determination of Clusters regarding Attributes and Relationships "EDCAR" and (Graph & Attribute Miner "GAMER"), and the outlier ranking mechanism	SY	×	√	×	×	ROC = 0.7648
[143]	×	√	KDE and correlation coefficient methods	OE	×	√	×	×	N/A
[140]	√	×	Virtual machine introspection and the modified taxonomy of Howard and Longstaff	SY	×	√	×	×	N/A
[120]	×	√	Analysis of logs for event-related actions	OE	×	√	×	×	AUC: AVC = 0.83 and 0.91 for EHR and Wiki, respectively
[98]	×	√	Deep Belief Network DBN, OCSVM	SY	×	√	×	×	Acc = 87.79, FP = 12.18

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[64]	×	√	Trust management model, KNN, back-propagation neural networks (BPNN), and DT	SE and RD	×	×	√	×	Accuracy at 60, KNN = 96% BPNN = 89%, DT = 90%
[132]	×	√	Histogram-based profiles	SE	×	√	×	×	FPR = 0.003% enterprise dataset, and 0.50% over simulated dataset
[170]	×	×	Investigation of reported insider problems, initial characterization of insiders, and feedback from workshop participants	INTERVIEW	×	×	√	×	N/A
[165]	×	√	Emotional recognition technology Polygraph technique	OE	×	×	√	×	N/A
[166]	√	×	Linguistic Inquiry and Word Count LIWC	SE and OE	×	×	√	×	N/a
[163]	√	×	Novel intention-based authorization mechanism using EEG signals P300-based concealed information test CIT and SVM classifier	OE	×	×	√	×	
[167]	×	×	Analyzing Capability Means Opportunity CMO	N/A	×	×	√	×	N/A

Reference	Detection Methodology		Method	Dataset	Features				Results
	Signature or Rule-based	Anomaly or Classification			Behavior of Biometrics	Cyber Features	Psychosocial Behaviors	Other Behaviors	
[161]	×	√	Graph structure analysis Psychological profiling (PP)	OE	×	×	√	×	N/A
[171]	×	×	Conceptual framework	N/A	×	×	√	×	N/A
[162]	×	×	Quantitative Electroencephalogram qEEG signal	OE	×	×	√	×	N/A

Simulation (SE), own environment (OE), synthetic dataset (SY), real data (RD), and case study (CS).

References

1. Homoliak, I.; Toffalini, F.; Guarnizo, J.; Elovici, Y.; Ochoa, M. Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Comput. Surv.* **2019**, *52*. [CrossRef]
2. Al-Mhiqani, M.N.; Ahmad, R.; Abidin, Z.Z.; Yassin, W.M.; Hassan, A.; Mohammad, A.N.; Clarke, N.L. A new taxonomy of insider threats: An initial step in understanding authorised attack. *Int. J. Inf. Syst. Manag.* **2018**, *1*, 343–359.
3. Kim, J.; Park, M.; Kim, H.; Cho, S.; Kang, P. Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Appl. Sci.* **2019**, *9*, 4018. [CrossRef]
4. Crowd Research Partners Insider and Cybersecurity Insiders. In *Insider Threat 2018 Report*; Cybersecurity Insiders: Washington, DC, USA, 2018; Available online: https://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf (accessed on 7 April 2020).
5. Ko, L.L.; Divakaran, D.M.; Liau, Y.S.; Thing, V.L.L. Insider threat detection and its future directions. *Int. J. Secur. Netw.* **2017**, *12*, 168–187. [CrossRef]
6. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access* **2018**, *6*, 25167–25177. [CrossRef]
7. Ullah, F.; Edwards, M.; Ramdhany, R.; Chitchyan, R.; Babar, M.A.; Rashid, A. Data exfiltration: A review of external attack vectors and countermeasures. *J. Netw. Comput. Appl.* **2018**, *101*, 18–54. [CrossRef]
8. Liu, L.; De Vel, O.; Han, Q.-L.; Zhang, J.; Xiang, Y. Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1397–1417. [CrossRef]
9. Nazir, S.; Patel, S.; Patel, D. Assessing and augmenting SCADA cyber security: A survey of techniques. *Comput. Secur.* **2017**, *70*, 436–454. [CrossRef]
10. Farahmand, F.; Spafford, E.H. Understanding insiders: An analysis of risk-taking behavior. *Inf. Syst. Front.* **2013**, *15*, 5–15. [CrossRef]
11. Ho, S.M.; Kaarst-Brown, M.; Benbasat, I. Trustworthiness Attribution: Inquiry Into Insider Threat Detection. *J. Assoc. Inf. Sci. Technol.* **2018**, *69*, 271–280. [CrossRef]
12. Zaytsev, A.; Malyuk, A.; Miloslavskaya, N. Analysis of Research on Specific Insider Information Security Threats. In *Proceedings of the Recent Advances in Information Systems and Technologies, Vol 2*; Rocha, A., Correia, A.M., Adeli, H., Reis, L.P., Costanzo, S., Eds.; Springer: New York, NY, USA, 2017; Volume 570, pp. 725–735.
13. Zaytsev, A.; Malyuk, A.; Miloslavskaya, N. Critical Analysis in the Research Area of Insider Threats. In Proceedings of the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, Czech Republic, 21–23 August 2017; pp. 288–296.
14. Alneyadi, S.; Sithirasenan, E.; Muthukkumarasamy, V. A survey on data leakage prevention systems. *J. Netw. Comput. Appl.* **2016**, *62*, 137–152. [CrossRef]
15. Crossler, R.E.; Johnston, A.C.; Lowry, P.B.; Hu, Q.; Warkentin, M.; Baskerville, R. Future directions for behavioral information security research. *Comput. Secur.* **2013**, *32*, 90–101. [CrossRef]
16. Kim, M.; Kim, K.; Lee, H. Development trend of insider anomaly detection system. In Proceedings of the 20th International Conference on Advanced Communication Technology, ICACT, IEEE, Chuncheon-si Gangwon-do, Korea, 11–14 February 2018; pp. 373–376.
17. Andress, M. *Surviving Security: How to Integrate People, Process, and Technology*, 2nd ed.; Auerbach Publications: Boca Raton, FL, USA, 2003; ISBN 9780849320422.
18. Flynn, L.; Huth, C.; Trzeciak, R.; Buttles, P. *Best Practices Against Insider Threats in All Nations*; IEEE: Physcataway, NJ, USA, 2013.
19. Magklaras, G.B.; Furnell, S.M. Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Comput. Secur.* **2001**, *21*, 62–73. [CrossRef]
20. Greitzer, F.L.; Strozer, J.; Cohen, S.; Bergey, J.; Cowley, J.; Moore, A.; Mundie, D. Unintentional insider threat: Contributing factors, observables, and mitigation strategies. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, USA, 6–9 January 2014; pp. 2025–2034.
21. Probst, C.W.; Hunker, J.; Gollmann, D.; Bishop, M. Aspects of insider threats. In *Insider Threats in Cyber Security*; Springer: New York, NY, USA, 2010; pp. 1–15.

22. Cole, E.; Ring, S. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*; Elsevier: Amsterdam, The Netherlands, 2005; ISBN 0080489052.
23. Cappelli, D.M.; Moore, A.P.; Trzeciak, R.F. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, 2nd ed.; Addison-Wesley: Boston, MA, USA, 2012; ISBN 013290604X.
24. Collins, M.L.; Theis, M.C.; Trzeciak, R.F.; Strozer, J.R.; Clark, J.W.; Costa, D.L.; Cassidy, T.; Albrethsen, M.J.; Moore, A.P. *Common Sense Guide to Mitigating Insider Threats*, 5th ed.; CERT, Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2016.
25. Casey, T. A Field Guide to Insider Threat. Available online: http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/a-field-guide-to-insider-threat-paper.pdf (accessed on 27 April 2018).
26. Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 499–508.
27. Cornelissen, W. Investigating Insider Threats: Problems and Solutions. Masterr's Thesis, University of Twente, Twente, The Nederlands, 2009.
28. Gunasekhar, T.; Rao, K.T.; Basu, M.T. Understanding insider attack problem and scope in cloud. In Proceedings of the Power and Computing Technologies (ICCPCT), Nagercoil, India, 19–20 March 2015; pp. 1–6. [CrossRef]
29. Long, J.; Wiles, J.; Rogers, R.; Drake, P.; Green, R.J.; Kipper, G.; Blackwood, R.T.; Schroader, A. *Techno Security's Guide to Managing Risks for it Managers, Auditors, and Investigators*; Elsevier: Amsterdam, The Nederlands, 2011; ISBN 0080553974.
30. Chen, X.; Shi, J.; Xu, R.; Yiu, S.M.; Fang, B.; Xu, F. PAITS: Detecting Masquerader via Short-Lived Interventional Mouse Dynamics. In *Proceedings of the Applications And Techniques In Information Security, ATIS 2014*; Batten, L., Li, G., Niu, W., Warren, M., Eds.; Springer: New York, NY, USA, 2014; Volume 490, pp. 231–242.
31. Wang, X.; Tan, Q.; Shi, J.; Su, S.; Wang, M. Insider threat detection using characterizing user behavior. In Proceedings of the 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018, Guangzho, China, 18–21 June 2018; pp. 476–482.
32. Xiaojun, C.; Zicheng, W.; Yiguo, P.; Jinqiao, S. A Continuous Re-Authentication Approach Using Ensemble Learning. *Procedia Comput. Sci.* **2013**, *17*, 870–878. [CrossRef]
33. Gabrielson, B. Who really did it? Controlling malicious insiders by merging biometric behavior with detection and automated responses. In Proceedings of the 45th Hawaii International Conference on System Sciences Who, Maui, HI, USA, 4–7 January 2012; pp. 2441–2449.
34. Park, Y.; Molloy, I.M.; Chari, S.N.; Xu, Z.; Gates, C.; Li, N. Learning from Others: User Anomaly Detection Using Anomalous Samples from Other Users. In *Proceedings of the COMPUTER SECURITY-ESORICS 2015, PT II*; Pernul, G., Ryan, P.Y.A., Weippl, E., Eds.; Springer: New York, NY, USA, 2015; pp. 396–414.
35. Kanaskar, N.; Bian, J.; Seker, R.; Nijim, M.; Yilmazer, N. Dynamical System approach to insider threat detection. In Proceedings of the 2011 IEEE International Systems Conference, IEEE, Boston, MA, USA, 4–7 April 2011; pp. 232–238.
36. Parveen, P.; McDaniel, N.; Hariharan, V.S.; Thuraisingham, B.; Khan, L. Unsupervised ensemble based learning for insider threat detection. In Proceedings of the ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust, Amsterdam, The Netherlands, 3 September 2012; pp. 718–727.
37. Leu, F.Y.; Tsai, K.L.; Hsiao, Y.T.; Yang, C.T. An internal intrusion detection and protection system by using data mining and forensic techniques. *IEEE Syst. J.* **2017**, *11*, 427–438. [CrossRef]
38. Parveen, P.; Thuraisingham, B. Unsupervised incremental sequence learning for insider threat detection. In Proceedings of the 2012 IEEE International Conference on Intelligence and Security Informatics, IEEE, Arlington, VA, USA, 11–14 June 2012; pp. 141–143.
39. Maestre Vidal, J.; Lucila Sandoval Orozco, A.; Javier García Villalba, L. Online masquerade detection resistant to mimicry. *Expert Syst. Appl.* **2016**, *61*, 162–180. [CrossRef]
40. Parveen, P.; Weger, Z.R.; Thuraisingham, B.; Hamlen, K.; Khan, L. Supervised learning for insider threat detection using stream mining. In Proceedings of the 23rd IEEE International Conference on Tools with Artificial Intelligence Supervised, Boca Rton, FL, USA, 7–9 November 2011; pp. 1032–1039.
41. Parveen, P.; McDaniel, N.; Weger, Z.; Evans, J.; Thuraisingham, B.; Hamlen, K.; Khan, L. Evolving insider threat detection stream mining perspective. *Int. J. Artif. Intell. Tools* **2013**, *22*, 1360013. [CrossRef]

42. Pitropakis, N.; Lambrinoudakis, C.; Geneiatakis, D. Till All Are One: Towards a Unified Cloud IDS. In *Proceedings of the Trust, Privacy and Security in Digital Business*; Fischer Hubner, S., Lambrinoudakis, C., Lopez, J., Eds.; Springer: New York, NY, USA, 2015; pp. 136–149.
43. Parveen, P.; Evans, J.; Thuraisingham, B.; Hamlen, K.W.; Khan, L. Insider threat detection using stream mining and graph mining. In Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, Boston, MA, USA, 9–11 October 2011; pp. 1102–1110.
44. Song, Y.; Salem, M.B.; Hershkop, S.; Stolfo, S.J. System level user behavior biometrics using Fisher features and Gaussian mixture models. In Proceedings of the 2013 IEEE Security and Privacy Workshops System, Melbourne, Australia, 11–13 December 2013; pp. 52–59.
45. Yuan, E.; Malek, S. Mining software component interactions to detect security threats at the architectural level. In Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture Mining, Venice, Italy, 5 April 2016; pp. 211–220.
46. Nasr, P.M.; Varjani, A.Y. Alarm based anomaly detection of insider attacks in SCADA system. In Proceedings of the 2014 Smart Grid Conference (SGC), IEEE, Tehran, Iran, 9–10 December 2014.
47. Nasr, P.M.; Yazdian-Varjani, A. Toward Operator Access Management in SCADA System: Deontological Threats Mitigation. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3314–3324. [CrossRef]
48. Lamba, H.; Glazier, T.J.; Schmerl, B.; Camara, J.; Garlan, D.; Pfeffer, J. A Model-based Approach to Anomaly Detection in Software Architectures. In Proceedings of the Symposium and Bootcamp on the Science of Security, Pittsburgh, PA, USA, 19–21 April 2016; pp. 69–71.
49. Young, S.; Dahnert, A. DevEyes insider threat detection. In Proceedings of the 2011 Second Worldwide Cybersecurity Summit (WCS), IEEE, London, UK, 1–2 June 2011.
50. Clark, J.; Leblanc, S.; Knight, S. Compromise through USB-based Hardware Trojan Horse device. *Futur. Gener. Comput. Syst.* **2011**, *27*, 555–563. [CrossRef]
51. White, J.; Panda, B. Insider threat discovery using automatic detection of mission critical data based on content. In Proceedings of the 2010 Sixth International Conference on Information Assurance and Security, Napoly, Italy, 8–10 September 2010; pp. 56–61.
52. Zhang, T.; Zhao, P. Insider threat identification system model based on rough set dimensionality reduction. In Proceedings of the 2010 Second WRI World Congress on Software Engineering Insider, IEEE, Boston, MA, USA, 19–20 December 2010; Volume 2, pp. 111–114.
53. Fung, C.J.; Lam, D.Y.; Boutaba, R. RevMatch: An efficient and robust decision model for collaborative malware detection. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–9.
54. Nkosi, L.; Tarwireyi, P.; Adigun, M.O. Insider threat detection model for the cloud. In Proceedings of the 2013 Information Security for South Africa, Johannesburg, South Africa, 14–16 August 2013; pp. 1–8.
55. Nikolai, J.; Wang, Y. A system for detecting malicious insider data theft in IaaS cloud environments. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
56. Roberts, S.C.; Holodnak, J.T.; Nguyen, T.; Yuditskaya, S.; Milosavljevic, M.; Streilein, W.W. A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems. In Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW), Oxford, UK, 8 July 2016; pp. 314–323.
57. Punithavathani, D.S.; Sujatha, K.; Jain, J.M. Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Comput.* **2015**, *18*, 435–451. [CrossRef]
58. Liu, W.; Ci, L.; Liu, L. Research on Behavior Trust Based on Bayesian Inference in Trusted Computing Networks. In Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, 19–21 May 2015; pp. 1134–1138.
59. Goldberg, H.G.; Young, W.T.; Memory, A.; Senator, T.E. Explaining and Aggregating Anomalies to Detect Insider Threats. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Kauai, HI, USA, 5–8 January 2016; pp. 2739–2748.
60. Rajamanickam, S.; Vollala, S.; Amin, R.; Ramasubramanian, N. Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC. *IEEE Syst. J.* **2019**, *PP*, 1–12. [CrossRef]

61. Mayhew, M.; Atighetchi, M.; Adler, A.; Greenstadt, R. Use of machine learning in big data analytics for insider threat detection. In Proceedings of the MILCOM 2015–2015 IEEE Military Communications Conference, IEEE, Tampa, FL, USA, 26–28 October 2015; pp. 915–922.
62. Shemla, A.; Bineesh, V. An EvABCD approach for masquerade detection. In Proceedings of the Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014, IEEE, Coimbatore, India, 8 July 2014; pp. 533–537.
63. Dietzel, S.; Gürtler, J.; van der Heijden, R.; Kargl, F. Redundancy-based statistical analysis for insider attack detection in VANET aggregation schemes. In Proceedings of the 2014 IEEE Vehicular Networking Conference (VNC), Los Angeles, CA, USA, 4–6 December 2014; pp. 135–142.
64. Li, W.; Meng, W.; Kwok, L.F.; IP, H.H.S. Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *J. Netw. Comput. Appl.* **2017**, *77*, 135–145. [CrossRef]
65. Bostani, H.; Sheikhan, M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. *Comput. Commun.* **2017**, *98*, 52–71. [CrossRef]
66. Pagliari, R.; Ghosh, A.; Gottlieb, Y.M.; Chadha, R.; Vashist, A.; Hadynski, G. Insider attack detection using weak indicators over network flow data. In Proceedings of the MILCOM 2015–2015 IEEE Military Communications Conference, IEEE, Tampa, FL, USA, 26–28 October 2015; Volume 2015, pp. 1–6.
67. Debarr, D.; Sun, H.; Wechsler, H. Adversarial Spam Detection Using the Randomized Hough Transform-Support Vector Machine. In Proceedings of the 2013 12th International Conference on Machine Learning and Applications, Miami, FL, USA, 4–7 December 2013; Volume 1, pp. 299–304.
68. Shu, T.; Krunz, M. Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. *IEEE Trans. Mob. Comput.* **2015**, *14*, 813–828. [CrossRef]
69. Mohan, R.; Vaidehi, V.; A, A.K.; Mahalakshmi, M.; Chakkaravarthy, S.S. Complex Event Processing based Hybrid Intrusion Detection System. In Proceedings of the 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 26–28 March 2015; pp. 1–6.
70. Neu, C.V.; Zorzo, A.F.; Orozco, A.M.S.; Michelin, R.A. An approach for detecting encrypted insider attacks on OpenFlow SDN Networks. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016; pp. 210–215.
71. Moorthy, B.V.; Meghanathan, N.T. An efficient approach for privacy preserving and detection of selective packet dropping attacks in wireless ad hoc networks. *IIOAB J.* **2016**, *7*, 152–161.
72. Yan, Z.; Ding, W.; Niemi, V.; Vasilakos, A.V. Two Schemes of Privacy-Preserving Trust Evaluation. *Futur. Gener. Comput. Syst.* **2016**, *62*, 175–189. [CrossRef]
73. Rrushi, J.L. NIC displays to thwart malware attacks mounted from within the OS. *Comput. Secur.* **2016**, *61*, 59–71. [CrossRef]
74. Sandhu, R.; Sohal, A.S.; Sood, S.K. Identification of malicious edge devices in fog computing environments. *Inf. Secur. J.* **2017**, *26*, 213–228. [CrossRef]
75. Mtibaa, A.; Harras, K.; Alnuweiri, H. Friend or Foe? Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms. In Proceedings of the 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Vancouver, BC, Canada, 30 Novembar–3 December 2015; pp. 42–49.
76. Huayu, F.; Jun, H.; Menglin, W. Research on fog computing based active anti-theft technology. *Procedia Comput. Sci.* **2017**, *111*, 209–213. [CrossRef]
77. Kansal, V.; Dave, M. Proactive DDoS attack detection and isolation. In Proceedings of the 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 1–2 July 2017; pp. 334–338.
78. Tupakula, U.; Varadharajan, V. Trust Enhanced Security Architecture for Detecting Insider Threats. In Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, Australia, 16–18 July 2013; pp. 552–559.
79. Zargar, A.; Nowroozi, A.; Jalili, R. XABA: A zero-knowledge anomaly-based behavioral analysis method to detect insider threats. In Proceedings of the 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 7–8 September 2016; pp. 26–31.
80. Huang, X.; Ahmed, M.R.; Sharma, D. A Novel Protection for Wireless Sensor Networks from Internal Attacks. In *Proceedings of the International Multiconference of Engineers and Computer Scientists, Imecs 2012, Vol I*; Ao, S.I., Castillo, O., Douglas, C., Feng, D.D., Lee, J.A., Eds.; Spinger: New York, NY, USA, 2012; pp. 374–379.

81. Lopez, J.; Alcaraz, C.; Roman, R. Smart control of operational threats in control substations. *Comput. Secur.* **2013**, *38*, 14–27. [CrossRef]
82. Callegati, F.; Giallorenzo, S.; Melis, A.; Prandini, M. Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. *Comput. Secur.* **2018**, *74*, 277–295. [CrossRef]
83. Hori, Y.; Nishide, T.; Sakurai, K. Towards Countermeasure of Insider Threat in Network Security. In Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, 30 November–2 December 2011; pp. 634–636.
84. Meng, W.; Luo, X.; Li, W.; Li, Y. Design and Evaluation of Advanced Collusion Attacks on Collaborative Intrusion Detection Networks in Practice. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 1061–1068.
85. Cho, J.H.; Chen, I.R. Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks. *Perform. Eval.* **2010**, *68*, 58–75. [CrossRef]
86. Khorrami, L.S.; Afshar, A. Attack detection in active queue management within large-scale networks control system with information of network and physical system. In Proceedings of the 2016 24th Iranian Conference on Electrical Engineering (ICEE), Okinawa, Japan, 3–7 July 2016; pp. 714–719.
87. Tripathi, N.; Hubballi, N. Exploiting DHCP server-side IP address conflict detection: A DHCP starvation attack. In Proceedings of the 2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS), Kolkata, India, 15–18 December 2015; pp. 1–3.
88. Kim, J.S. Development of integrated insider attack detection system using intelligent packet filtering. In Proceedings of the 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, Jeju Island, Korea, 23–25 May 2011; pp. 65–69. [CrossRef]
89. Yang, J.; Ray, L.; Zhao, G. Detect stepping-stone insider attacks by network traffic mining and dynamic programming. In Proceedings of the 2011 International Conference on Advanced Information Networking and Applications Detect, IEEE, Singapore, 22–25 March 2011; pp. 151–158.
90. Suresh, N.R.; Malhotra, N.; Kumar, R.; Thanudas, B. An integrated data exfiltration monitoring tool for a large organization with highly confidential data source. In Proceedings of the 2012 4th Computer Science and Electronic Engineering Conference (CEEC), Colchester, UK, 12–13 September 2012; pp. 149–153.
91. Muchene, D.N.; Luli, K.; Shue, C.A. Reporting insider threats via covert channels. In Proceedings of the 2013 IEEE Security and Privacy Workshops Reporting, IEEE, San Francisco, CA, USA, 23–24 May 2013; pp. 68–71.
92. Ambre, A.; Shekokar, N. Insider Threat Detection Using Log Analysis and Event Correlation. In *Proceedings of the International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)*; Elsevier B.V.: Amsterdam, The Netherlands, 2015; Volume 45, pp. 436–445.
93. Hsieh, C.H.; Lai, C.M.; Mao, C.H.; Kao, T.C.; Lee, K.C. AD2: Anomaly detection on active directory log data for insider threat monitoring. In Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, 21–24 September 2015; pp. 287–292.
94. Rose, I.; Felts, N.; George, A.; Miller, E.; Planck, M. Something Is Better Than Everything: A Distributed Approach to Audit Log Anomaly Detection. In Proceedings of the 2017 IEEE Cybersecurity Development (SecDev), Cambridge, MA, USA, 24–26 September 2017; pp. 77–82. [CrossRef]
95. Nkosi, L.; Tarwireyi, P.; Adigun, M.O. Detecting a malicious insider in the cloud environment using sequential rule mining. In Proceedings of the 2013 International Conference on Adaptive Science and Technology, Pretoria, South Africa, 25–27 November 2013; pp. 1–10.
96. Rashid, T.; Agrafiotis, I.; Nurse, J.R.C. A new take on detecting insider threats: Exploring the use of Hidden Markov Models. In Proceedings of the MIST '16 Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats ACM, Vienna, Austria, 28 October 2016; pp. 47–56.
97. Meryem, A.; Samira, D.; Bouabid, E.O.; Mouad, L. A novel approach in detecting intrusions using NSLKDD database and MapReduce programming. *Procedia Comput. Sci.* **2017**, *110*, 230–235. [CrossRef]
98. Lin, L.; Zhong, S.; Jia, C.; Chen, K. Insider Threat Detection Based on Deep Belief Network Feature Representation. In Proceedings of the 2017 International Conference on Green Informatics (ICGI), Fuzhou, China, 15–17 August 2017; pp. 54–59.
99. Meng, F.; Lou, F.; Fu, Y.; Tian, Z. Deep learning based attribute classification insider threat detection for data security. In Proceedings of the 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018, IEEE, Guangzhou, China, 18–21 June 2018; pp. 576–581.

100. Dahmane, M.; Foucher, S. Combating insider threats by user profiling from activity logging data. In Proceedings of the Proceedings-2018 1st International Conference on Data Intelligence and Security, ICDIS 2018, South Padre Island, TX, USA, 8–10 April 2018; pp. 194–199.
101. Hall, A.J.; Pitropakis, N.; Buchanan, W.J.; Moradpoor, N. Predicting Malicious Insider Threat Scenarios Using Organizational Data and a Heterogeneous Stack-Classifier. In Proceedings of the 2018 IEEE International Conference on Big Data, Big Data 2018, IEEE, Seattle, WA, USA, 10–13 December 2018; pp. 5034–5039.
102. Böse, B.; Avasarala, B.; Tirthapura, S.; Chung, Y.Y.; Steiner, D. Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. *IEEE Syst. J.* **2017**, *11*, 471–482. [CrossRef]
103. Agrafiotis, I.; Erola, A.; Happa, J.; Goldsmith, M.; Creese, S. Validating an Insider Threat Detection System: A Real Scenario Perspective. In Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW), IEEE, Boston, MA, USA, 22–26 May 2016; pp. 286–295.
104. Young, W.T.; Goldberg, H.G.; Memory, A.; Sartain, J.F.; Senator, T.E. Use of domain knowledge to detect insider threats in computer activities. In Proceedings of the 2013 IEEE Security and Privacy Workshops Use, San Francisco, CA, USA, 23–24 May 2013; pp. 60–67.
105. Legg, P.A.; Buckley, O.; Goldsmith, M.; Creese, S. Caught in the act of an insider attack: Detection and assessment of insider threat. In Proceedings of the 2015 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 10–12 May 2015; pp. 1–6.
106. Eldardiry, H.; Bart, E.; Liu, J.; Hanley, J.; Price, B.; Brdiczka, O. Multi-domain information fusion for insider threat detection. In Proceedings of the 2013 IEEE Security and Privacy Workshops, IEEE, San Francisco, CA, USA, 23–24 May 2013; pp. 45–51.
107. Lo, O.; Buchanan, W.J.; Griffiths, P.; Macfarlane, R. Distance Measurement Methods for Improved Insider Threat Detection. *Secur. Commun. Netw.* **2018**, *2018*, 5906368. [CrossRef]
108. Das Bhattacharjee, S.; Yuan, J.; Jiaqi, Z.; Tan, Y.-P. Context-aware graph-based analysis for detecting anomalous activities. In Proceedings of the the IEEE International Conference on Multimedia and Expo (ICME) 2017, IEEE, Hong Kong, China, 10–14 July 2017; pp. 1021–1026.
109. Gamachchi, A.; Boztas, S. Insider threat detection through attributed graph clustering. In Proceedings of the Trustcom/BigDataSE/ICESS, 2017 IEEE, San Francisco, CA, USA, 1–4 August 2017; pp. 112–119.
110. Hu, Y.; Frank, C.; Walden, J.; Crawford, E.; Kasturiratna, D. Profiling file repository access patterns for identifying data exfiltration activities. In Proceedings of the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, France, 12–13 April 2011; pp. 122–128.
111. Chen, Y.; Nyemba, S.; Malin, B. Detecting Anomalous Insiders in Collaborative Information Systems. *IEEE Trans. Dependable Secur. Comput.* **2012**, *9*, 332–344. [CrossRef] [PubMed]
112. Raissi-Dehkordi, M.; Carr, D. A multi-perspective approach to insider threat detection. In Proceedings of the 2011-MILCOM 2011 Military Communications Conference, IEEE, Baltimore, MD, USA, 7–10 November 2011; pp. 1164–1169.
113. Hu, Y.; Panda, B. Two-dimensional traceability link rule mining for detection of insider attacks. In Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010; pp. 1–9. [CrossRef]
114. Garkoti, G.; Peddoju, S.K.; Balasubramanian, R. Detection of Insider Attacks in Cloud Based e-Healthcare Environment. In Proceedings of the 2014 International Conference on Information Technology, Zrenjanin, Serbia, 24 October 2014; pp. 195–200.
115. Blasco, J.; Tapiador, J.E.; Peris-Lopez, P.; Suarez-Tangil, G. Hindering data theft with encrypted data trees. *J. Syst. Softw.* **2015**, *101*, 147–158. [CrossRef]
116. Gates, C.; Li, N.; Xu, Z.; Chari, S.N.; Molloy, I.; Park, Y. Detecting Insider Information Theft Using Features from File Access Logs. In *Proceedings of the Computer Security-Esorics 2014, PT II*; Kutylowski, M., Vaidya, J., Eds.; Springer: Cham, Switzerland, 2014; Volume 8713, pp. 383–400.
117. Zhang, R.; Chen, X.; Shi, J.; Xu, F.; Pu, Y. Detecting Insider Threat Based on Document Access Behavior Analysis. In *Proceedings of the Web Technologies and Applications, APWEB 2014, PT II*; Han, W., Huang, Z., Hu, C., Zhang, H., Guo, L., Eds.; Springer: Cham, Switzerland, 2014; Volume 8710, pp. 376–387.
118. Liu, A.Y.; Lam, D.N. Using Consensus Clustering for Multi-view Anomaly Detection. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, 24–25 May 2012; pp. 117–124.

119. Gupta, S.; Hanson, C.; Gunter, C.A.; Frank, M.; Liebovitz, D.; Malin, B. Modeling and detecting anomalous topic access. In Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA, 4–7 June 2013; pp. 100–105.
120. Chen, Y.; Nyemba, S.; Zhang, W.; Malin, B. Leveraging social networks to detect anomalous insider actions in collaborative environments. In Proceedings of the Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, IEEE, Boston, MA, USA, 10–12 July 2011; pp. 119–124.
121. Shrivastava, S.; Adepu, S.; Mathur, A. Design and assessment of an Orthogonal Defense Mechanism for a water treatment facility. *Rob. Auton. Syst.* **2018**, *101*, 114–125. [CrossRef]
122. Zhou, D.; Wang, K.; Cao, N.; He, J. Rare Category Detection on Time-Evolving Graphs. In Proceedings of the 2015 IEEE International Conference on Data Mining, Atlantic City, NJ, USA, 14–17 November 2015; pp. 1135–1140.
123. Gafny, M.; Shabtai, A.; Rokach, L.; Elovici, Y. POSTER: Applying Unsupervised Context-Based Analysis for Detecting Unauthorized Data Disclosure. In Proceedings of the Proccedings of the 18th ACM Conference on Computer & Communication Security (CCS 11), Association for Computing Machinery, New York, NY, USA, 17–21 October 2011; pp. 765–767.
124. Rao, U.P.; Singh, N.K.; Amin, A.R.; Sahu, K. Enhancing detection rate in database intrusion detection system. In Proceedings of the 2014 Science and Information Conference, Uppsala, Sweden, 24–27 August 2014; pp. 556–563.
125. Mathew, S.; Petropoulos, M.; Ngo, H.Q.; Upadhyaya, S. A Data-Centric Approach to Insider Attack Detection in Database Systems. In *Proceedings of the Recent Advances in Intrusion Detection*; Jha, S., Sommer, R., Kreibich, C., Eds.; Springer: Berlin/Heildelberg, Germany, 2010; Volume 6307, pp. 382–401.
126. Desai, A.S.; Gaikwad, D.P. Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA. In Proceedings of the 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, India, 2–3 December 2016; pp. 291–294.
127. Sallam, A.; Bertino, E. Detection of Temporal Insider Threats to Relational Databases. In Proceedings of the 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), San Jose, CA, USA, 15–17 October 2017; pp. 406–415.
128. Viet, K.; Panda, B.; Hu, Y. Detecting collaborative insider attacks in information systems. In Proceedings of the 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, Korea, 14–17 October 2012; pp. 502–507.
129. Alizadeh, M.; Lu, X.; Fahland, D.; Zannone, N.; van der Aalst, W.M.P. Linking data and process perspectives for conformance analysis. *Comput. Secur.* **2018**, *73*, 172–193. [CrossRef]
130. Panigrahi, S.; Sural, S.; Majumdar, A.K. Two-stage database intrusion detection by combining multiple evidence and belief update. *Inf. Syst. Front.* **2013**, *15*, 35–53. [CrossRef]
131. Blasco, J.; Hernandez-Castro, J.C.; Tapiador, J.E.; Ribagorda, A. Bypassing information leakage protection with trusted applications. *Comput. Secur.* **2012**, *31*, 557–568. [CrossRef]
132. Costante, E.; den Hartog, J.; Petković, M.; Etalle, S.; Pechenizkiy, M. A white-box anomaly-based framework for database leakage detection. *J. Inf. Secur. Appl.* **2017**, *32*, 27–46. [CrossRef]
133. Zhu, T.; Guo, Y.; Ma, J.; Ju, A. Business Process Mining based Insider Threat Detection System. In *Proceedings of the Advances On P2p, Parallel, Grid, Cloud And Internet Computing*; Xhafa, F., Barolli, L., Amato, F., Eds.; Springer: Cham, Switzerland, 2017; Volume 1, pp. 467–478.
134. Yaseen, Q.; Panda, B. Enhanced Insider Threat Detection Model that Increases Data Availability. In *Proceedings of the International Conference on Distributed Computing and Internet Technology*; Natarajan, R., Ojo, A., Eds.; Springer: New York, NY, USA, 2011; Volume 6536, pp. 267–277.
135. Althebyan, Q.; Mohawesh, R.; Yaseen, Q.; Jararweh, Y. Mitigating insider threats in a cloud using a knowledgebase approach while maintaining data availability. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 12–16 December 2015; pp. 226–231.
136. Razaque, A.; Rizvi, S.S. Privacy preserving model: A new scheme for auditing cloud stakeholders. *J. Cloud Comput.* **2017**, *6*, 7. [CrossRef]
137. Allen, M.D.; Chapman, A.; Seligman, L.; Blaustein, B. Provenance for collaboration: Detecting suspicious behaviors and assessing trust in information. In Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, FL, USA, 15–18 October 2011; pp. 342–351.

138. Legg, P.A.; Buckley, O.; Goldsmith, M.; Creese, S. Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. *IEEE Syst. J.* **2017**, *11*, 503–512. [CrossRef]
139. Aditham, S.; Ranganathan, N.; Katkoori, S. Memory access pattern based insider threat detection in big data systems. In Proceedings of the 2016 IEEE International Conference on Big Data (Big Data), IEEE, Washington, DC, USA, 5–8 December 2016; pp. 3625–3628.
140. Crawford, M.; Peterson, G. Insider threat detection using virtual machine introspection. In Proceedings of the 46th Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2013; pp. 1821–1830.
141. Meng, W.; Li, W.; Xiang, Y.; Choo, K.-K.R. A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks. *J. Netw. Comput. Appl.* **2017**, *78*, 162–169. [CrossRef]
142. Chiu, C.Y.; Yeh, C.T.; Lee, Y.J. Frequent Pattern Based User Behavior Anomaly Detection for Cloud System. In Proceedings of the 2013 Conference on Technologies and Applications of Artificial Intelligence, Taipei, Taiwan, 6–8 December 2013; pp. 61–66.
143. Ramachandran, R.; Neelakantan, S.; Bidyarthy, A.S. Behavior model for detecting data exfiltration in network environment. In Proceedings of the 2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, IEEE, Bangalore, India, 12–14 December 2011.
144. Gondaliya, T.P.; Singh, M. Intrusion detection system on MAC layer for attack prevention in MANET. In Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–5.
145. Tagle, B.; Felch, H. Conclusion to an Intelligent Agent as an Economic Insider Threat Solution: Aimie. In *Proceedings of the Tackling Society's Grand Challenges with Design Science, Desrist 2016*; Parsons, J., Tuunanen, T., Venable, J., Donnellan, B., Helfert, M., Kenneally, J., Eds.; Springer: Cham, Switzerland, 2016; Volume 9661, pp. 147–157.
146. Palomares, I.; Kalutarage, H.; Huang, Y.; Miller, P.; McCausland, R.; McWilliams, G. A fuzzy multicriteria aggregation method for data analytics: Application to insider threat monitoring. In Proceedings of the IFSA-SCIS 2017, Otsu, Shiga, Japan, 27–30 June 2017.
147. Wang, C.; Zhang, G.; Liu, L. A Detection Method for the Resource Misuses in Information Systems. In *Proceedings of the Affective Computing And Intelligent Interaction*; Luo, J., Ed.; Springer: Berlin/Heildelberg, Germany, 2012; Volume 137, pp. 545–552.
148. Jaenisch, H.; Handley, J. Insider threat detection enabled by converting user applications into fractal fingerprints and autonomously detecting anomalies. In Proceedings of the Proceedings of SPIE-The International Society for Optical Engineering, Brussels, Belgium, 16–19 April 2012; Volume 8408.
149. Canbay, Y.; Yazici, H.; Sagiroglu, S. A Turkish language based data leakage prevention system. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 26–28 April 2017; pp. 1–6.
150. Garfinkel, S.L.; Beebe, N.; Liu, L.; Maasberg, M. Detecting threatening insiders with lightweight media forensics. In Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 12–14 November 2013; pp. 86–92. [CrossRef]
151. Feng, W.; Yan, W.; Wu, S.; Liu, N. Wavelet transform and unsupervised machine learning to detect insider threat on cloud file-sharing. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; pp. 155–157.
152. Zhang, N.; Yu, W.; Fu, X.; Das, S.K. Maintaining defender's reputation in anomaly detection against insider attacks. *IEEE Trans. Syst. Man, Cybern. Part B Cybern.* **2010**, *40*, 597–611. [CrossRef]
153. Myers, J.; Grimaila, M.; Mills, R. Insider Threat Detection Using Distributed Event Correlation of Web Server Logs. In Proceedings of the Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, USA, 8–9 April 2010; Armistead, E.L., Ed.; pp. 251–258.
154. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354. [CrossRef]
155. Nathezhtha, T.; Yaidehi, V. Cloud Insider Attack Detection Using Machine Learning. In Proceedings of the Proceedings of the 2018 International Conference on Recent Trends in Advanced Computing, ICRTAC-CPS 2018, IEEE, Chennai, India, 10–11 September 2018; pp. 60–65.
156. Sharghi, H.; Sartipi, K. A User Behavior-Based Approach to Detect the Insider Threat in Distributed Diagnostic Imaging Systems. In Proceedings of the 2016 IEEE 29th International Symposium on Computer-Based Medical Systems (CBMS), Dublin, Ireland, 20 June 2016; pp. 300–305.

157. Agrafiotis, I.; Erola, A.; Goldsmith, M.; Creese, S. A tripwire grammar for insider threat detection. In Proceedings of the Managing Insider Security Threats 2016, Vienna, Austria, 28 October 2016; pp. 105–108.
158. Bao, H.; Lu, R.; Li, B.; Deng, R. BLITHE: Behavior Rule-Based Insider Threat Detection for Smart Grid. *IEEE Internet Things J.* **2016**, *3*, 190–205. [CrossRef]
159. Kammüller, F.; Probst, C.W. Invalidating policies using structural information. In Proceedings of the 2013 IEEE Security and Privacy Workshops, San Francisco, CA, USA, 23–24 May 2013; pp. 76–81. [CrossRef]
160. Dasgupta, D.; Roy, A.; Ghosh, D. Multi-user permission strategy to access sensitive information. *Inf. Sci.* **2018**, *423*, 24–49. [CrossRef]
161. Brdiczka, O.; Liu, J.; Price, B.; Shen, J.; Patil, A.; Chow, R.; Bart, E.; Ducheneaut, N. Proactive insider threat detection through graph learning and psychological context. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops, IEEE, San Francisco, CA, USA, 24–25 May 2012; pp. 142–149.
162. Suh, Y.A.; Yim, M.-S. High risk non-initiating insider" identification based on EEG analysis for enhancing nuclear security. *Ann. Nucl. Energy* **2018**, *113*, 308–318. [CrossRef]
163. Almehmadi, A.; El-Khatib, K. On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC). *IEEE Syst. J.* **2017**, *11*, 373–384. [CrossRef]
164. Almehmadi, A. Micromovement behavior as an intention detection measurement for preventing insider threats. *IEEE Access* **2018**, *6*, 40626–40637. [CrossRef]
165. Lee, H.-J.; Park, M.-W.; Eom, J.-H.; Chung, T.-M. New Approach for Detecting Leakage of Internal Information; Using Emotional Recognition Technology. *KSII Trans. Internet Inf. Syst.* **2015**, *9*, 4662–4679. [CrossRef]
166. Taylor, P.J.; Dando, C.J.; Ormerod, T.C.; Ball, L.J.; Jenkins, M.C.; Sandham, A.; Menacere, T. Detecting Insider Threats Through Language Change. *LAW Hum. Behav.* **2013**, *37*, 267–275. [CrossRef]
167. Maasberg, M.; Warren, J.; Beebe, N.L. The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. In Proceedings of the 2015 48th Hawaii International Conference on System Sciences, IEEE, Kauai, HI, USA, 5–8 January 2015; pp. 3518–3526.
168. Safa, N.S.; Maple, C.; Watson, T.; Von Solms, R. Motivation and opportunity based model to reduce information security insider threats in organisations. *J. Inf. Secur. Appl.* **2018**, *40*, 247–257. [CrossRef]
169. Kandias, M.; Gritzalis, D.; Stavrou, V.; Nikoloulis, K. Stress level detection via OSN usage pattern and chronicity analysis: An OSINT threat intelligence module. *Comput. Secur.* **2017**, *69*, 3–17. [CrossRef]
170. Pfleeger, S.L.; Predd, J.B.; Hunker, J.; Bulford, C. Insiders behaving badly: Addressing bad actors and their actions. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 169–179. [CrossRef]
171. Padayachee, K. A conceptual opportunity-based framework to mitigate the insider threat. In Proceedings of the 2013 Information Security for South Africa, IEEE, Johannesburg, South Africa, 14–16 August 2013.
172. Park, W.; You, Y.; Lee, K. Detecting Potential Insider Threat: Analyzing Insiders' Sentiment Exposed in Social Media. *Secur. Commun. Netw.* **2018**, *2018*, 7243296. [CrossRef]
173. Berk, V.H.; Cybenko, G.; Gregorio-De Souza, I.; Murphy, J.P. Managing malicious insider risk through BANDIT. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, IEEE, Maui, HI, USA, 4–7 January 2012; pp. 2422–2430.
174. Marrone, S.; Rodríguez, R.J.; Nardone, R.; Flammini, F.; Vittorini, V. On synergies of cyber and physical security modelling in vulnerability assessment of railway systems. *Comput. Electr. Eng.* **2015**, *47*, 275–285. [CrossRef]
175. Zou, B.; Yang, M.; Guo, J.; Wang, J.; Benjamin, E.-R.; Liu, H.; Li, W. Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation. *Prog. Nucl. Energy* **2018**, *104*, 8–15. [CrossRef]
176. Mavroeidis, V.; Vishi, K.; Jøsang, A. A Framework for Data-Driven Physical Security and Insider Threat Detection. In Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (ASONAM), IEEE, Barcelona, Spain, 28–31 August 2018; pp. 1108–1115.
177. Meng, W.; Li, W.; Wang, Y.; Au, M.H. Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. *Futur. Gener. Comput. Syst.* **2018**, *108*, 1258–1266. [CrossRef]
178. Durán, F.A. Probabilistic basis and assessment methodology for effectiveness of protecting nuclear materials. In Proceedings of the 2012 IEEE International Carnahan Conference on Security Technology (ICCST), Boston, MA, USA, 15–18 October 2012; pp. 43–52.
179. Kim, K.-N.; Yim, M.-S.; Schneider, E. A study of insider threat in nuclear security analysis using game theoretic modeling. *Ann. Nucl. Energy* **2017**, *108*, 301–309. [CrossRef]

180. Dietzel, S.; Gürtler, J.; Kargl, F. A resilient in-network aggregation mechanism for VANETs based on dissemination redundancy. *Ad Hoc Netw.* **2016**, *37*, 101–109. [CrossRef]
181. Fridman, L.; Weber, S.; Greenstadt, R.; Kam, M. Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. *IEEE Syst. J.* **2017**, *11*, 513–521. [CrossRef]
182. Santos, E.; Nguyen, H.; Yu, F.; Kim, K.J.; Li, D.; Wilkinson, J.T.; Olson, A.; Russell, J.; Clark, B. Intelligence Analyses and the Insider Threat. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2012**, *42*, 331–347. [CrossRef]
183. Al tabash, K.; Happa, J. Insider-threat detection using Gaussian Mixture Models and Sensitivity Profiles. *Comput. Secur.* **2018**, *77*, 838–859. [CrossRef]
184. Soh, C.; Yu, S.; Narayanan, A.; Duraisamy, S.; Chen, L. Employee profiling via aspect-based sentiment and network for insider threats detection. *Expert Syst. Appl.* **2019**, *135*, 351–361. [CrossRef]
185. Nithiyanandam, C.; Tamilselvan, D.; Balaji, S.; Sivaguru, V. Advanced framework of defense system for prevetion of insider's malicious behaviors. In Proceedings of the 2012 International Conference on Recent Trends in Information Technology, Chennai, Tamil Nadu, 19–21 April 2012; pp. 434–438.
186. Walton, S.; Maguire, E.; Chen, M. A visual analytics loop for supporting model development. In Proceedings of the 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), Chicago, IL, USA, 25 October 2015.
187. Yuan, F.; Cao, Y.; Shang, Y. Insider Threat Detection with Deep Neural Network. In *Proceedings of the International Conference on Computational Science*; Springer: New York, NY, USA, 2018; pp. 43–54.
188. Legg, P.A. Visualizing the insider threat: Challenges and tools for identifying malicious user activity. In Proceedings of the 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), IEEE, Chicago, IL, USA, 25 October 2015.
189. Al-mhiqani, M.N.; Ahmad, R.; Abidin, Z.Z.; Yassin, W.; Hassan, A.; Mohammad, A.N. New insider threat detection method based on recurrent neural networks. *Indones. J. Electr. Eng. Comput. Sci.* **2020**, *17*, 1474–1479. [CrossRef]
190. Salem, M.B.; Stolfo, S.J. A comparison of one-class bag-of-words user behavior modeling techniques for masquerade detection. *Secur. Commun. Netw.* **2012**, *5*, 863–872. [CrossRef]
191. Harilal, A.; Toffalini, F.; Homoliak, I.; Castellanos, J.H. Twos: A dataset of malicious insider threat behavior based on a gamified competition. *J. Wirel. Mob. Netw.* **2018**, *1*. [CrossRef]
192. Salem, M.B.; Stolfo, S.J. *Masquerade Attack Detection Using a Search-Behavior Modeling Approach*; Technical Report CUCS-027-09; Columbia University, Computer Science Department: New York, NY, USA, 2009; Volume 9.
193. Salem, M.B.; Stolfo, S.J. Modeling user search behavior for masquerade detection. *Lect. Notes Comput. Sci.* **2011**, *6961*, 181–200. [CrossRef]
194. Salem, M.B.; Hershkop, S.; Stolfo, S.J. *A Survey of Insider Attack Detection Research*; Springe: Boston, MA, USA, 2008; ISBN 978-0-387-77321-6.
195. Gheyas, I.A.; Abdallah, A.E. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Anal.* **2016**, *1*, 6. [CrossRef]
196. El Anbal, M.; Abou El Kalam, A.; Benhadou, S.; Moutaouakkil, F.; Medromi, H. Securing SCADA Critical Network Against Internal. In *Proceedings of the International Conference on Critical Information Infrastructures Security*; Springer: New York, NY, USA, 2017; pp. 328–339.
197. William, T. Shaw SCADA System Vulnerabilities to Cyber Attack. Available online: https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm (accessed on 24 June 2020).
198. Software Engineering Institute. Analytic Approaches To Detect Insider Threats, Technical Report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA. Available online: https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_451069.pdf (accessed on 7 April 2020).