electronics

MDPI

Article

A Multi-Tiered Framework for Insider Threat Prevention

Rakan A. Alsowail * and Taher Al-Shehari *

Deanship of Common First Year, King Saud University, Riyadh 11362, Saudi Arabia
* Correspondence: ralsowail@ksu.edu.sa (R.A.A.); talshehari.c@ksu.edu.sa (T.A.-S.)

Abstract: As technologies are rapidly evolving and becoming a crucial part of our lives, security and privacy issues have been increasing significantly. Public and private organizations have highly confidential data, such as bank accounts, military and business secrets, etc. Currently, the competition between organizations is significantly higher than before, which triggers sensitive organizations to spend an excessive volume of their budget to keep their assets secured from potential threats. Insider threats are more dangerous than external ones, as insiders have a legitimate access to their organization's assets. Thus, previous approaches focused on some individual factors to address insider threat problems (e.g., technical profiling), but a broader integrative perspective is needed. In this paper, we propose a unified framework that incorporates various factors of the insider threat context (technical, psychological, behavioral and cognitive). The framework is based on a multi-tiered approach that encompasses pre, in and post-countermeasures to address insider threats in an all-encompassing perspective. It considers multiple factors that surround the lifespan of insiders' employment, from the pre-joining of insiders to an organization until after they leave. The framework is utilized on real-world insider threat cases. It is also compared with previous work to highlight how our framework extends and complements the existing frameworks. The real value of our framework is that it brings together the various aspects of insider threat problems based on real-world cases and relevant literature. This can therefore act as a platform for general understanding of insider threat problems, and pave the way to model a holistic insider threat prevention system.

Keywords: insider threat prevention; multi-tiered approach; information security; data privacy

Citation: Alsowail, R.A.; Al-Shehari, T. A Multi-Tiered Framework for Insider Threat Prevention. *Electronics* **2021**, *10*, 1005. https://doi.org/10.3390/electronics10091005

Received: 18 March 2021
Accepted: 20 April 2021
Published: 22 April 2021

1. Introduction

With the endless use of technological devices during the last decades, security and privacy threats have been increasing. Both organizations and individuals have different types of sensitive assets such as personal data, business plans, intellectual property, etc. The breach of such assets may cause devastating damage to their reputational image and business objectives. As a consequence, finding effective mechanisms to protect the confidentiality, integrity and availability of sensitive assets is a crucial necessity for individuals and organizations alike. One of the major concerns in the information security field is the insider threats [1]. IBM X-Force® Threat Intelligence Index [2] showed that insider attacks were the most common type of cyberattacks in 2017 which was around 60%.

1.1. Insider Threat Definition

Sinclair et al. [3] defined the insider as "any person who has some legitimate privileged access to internal digital resources, i.e., anyone who is allowed to see or change the organization's computer settings, data, or programs in a way that arbitrary members of the public may not. This includes full-time employees, but may also include temporary workers, volunteers, and contractors, depending on the nature of the business." Therefore, insider threats are the malicious activities that are conducted by entities who have authorizations, which may cause serious consequences to the physical and digital assets of an organization. The Computer Emergency and Response Team (CERT) defined the insider threat as "a current or former employee, contractor, or business partner who has or had

authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" [4].

1.2. Insider Threat Incidents

The intentional or accidental actions of insiders can cause an equal harm to their organization, i.e., the leakage and removal of sensitive data or even creating backdoors for external attackers. This section highlights the severity of insider attacks by presenting major insider incidents [5]: firstly, an insider attack against The U.S. National Security was carried out by one employee of the U.S. Federal Bureau of Investigation (FBI), who leaked high confidential data to Russian agencies. This attack is counted as the most dangerous insider spy, as it resulted in a huge damage to the image of FBI and the U.S as well; secondly, one of the U.S. army leaked numerous sensitive documents of the government to WikiLeaks; thirdly, the most serious fraud incident was carried out by one employee of Societe Generale French bank which resulted in an estimated loss of $7 billion.

Moreover, the U.S. Security Service and CERT [6] reported 1154 real insider incidents and categorized them into different categories, i.e., sabotage, fraud, theft and miscellaneous incidents. The largest volume was 659 fraud incidents that modified or deleted data assets for the aim of personal gain. The data thefts came after with 189 incidents that stole the intellectual properties of organizations. The remaining incidents fell under sabotage and miscellaneous for the aim of disrupting business operations.

Although the insider attack incidents that are mentioned above, several insider incidents have not been reported. That is because, attacked organizations are afraid from the negative impacts toward their business in case of attacking incidents are announced [7]. Overall, the seriousness and losses of occurred attacks have formed a pressing need to develop insider threat prevention systems. In the remainder of the paper, we will refer to the insider threat prevention as ITP.

1.3. The Protection against Insider Threats

The highly-dependent usage on digital assets brings an actual challenge to protect them from possible breaches. Such assets may reside in PCs, removable devices, emails, servers and so on. The protection of such assets is a paramount importance to the progress and survival of organizations. Some organizations have taken extreme precautions to mitigate insider threats, such as employees vetting, authentication mechanisms, training, monitoring, separation of duty, and so on [8]. The insider threats are the most difficult to detect and the mitigation of their impacts is not easily done by traditional procedures [9]. Throughout the last decade, there has been an increased focus on how to detect and prevent insider attacks. Significant steps have been taken by CERT as they issued periodic guides that provide the best practices and standards to alleviate insider attacks, i.e., the Common Sense Guide to Mitigating Insider Threats [10].

The approaches against insider threats can be divided into detection, detection and prevention, or prevention. In detection approaches, malicious activities are detected while or after an attack has occurred. In detection and prevention approaches, an attack is detected first, and then it is prevented but after or while some aspect of an attack has occurred. In prevention approaches, an attack is prevented before occurring, which is the ideal solution for insider threat problems. However, in the literature, we noticed that most of the work, such as [11–17] have been primarily focused on how to "detect" insider threats rather than "prevent" them. Interested readers in insider threat detection approaches are referred to [18–22], as the focus of this paper is the prevention approaches.

The prevention of insider threats is crucial for sensitive organizations due to the great harm that can happen if an insider attack succeeds. Therefore, this study is attempting to deal with the problem to find the most suitable solution for it. The key contributions of this paper are summarized as follows:

- It classifies, discusses and compares the existing ITP approaches. That is by proposing a classification model that categorizes the existing approaches into two main classes: biometric-based and asset-based. The biometric-based approaches are further classified into physiological and behavioral, whereas the asset-based approaches are classified into host, network and combined. The existing approaches are reviewed, classified and discussed to provide a better understanding of the literature, and highlight the gaps for the aim of devising more optimal solutions.
- It proposes an integrated ITP framework that incorporates several countermeasures that serve as multi-tiered protection layers spanning from the pre-joining of insiders to an organization until after they leave. It includes different technical, behavioral, psychological and cognitive measures (e.g., vetting, access and usage privileges, security awareness training, technical/psychological/behavioral profiling, etc.) to track the activities of insiders throughout their employment lifespan in order to address insider threats in a proactive manner.
- It presents the employing of the framework in real-world insider threat cases. It also compares our framework with the existing theoretical frameworks, and shows how ours extends upon them.

The remainder of the paper is organized as follows: The classification model of related work is presented in Section 2. The proposed framework for ITP is illustrated in Section 3. The utilization of the framework on CERT's insider threat cases is exemplified in Section 4. The discussion of the framework and how it extends upon the existing ones are shown in Section 5. Finally, the conclusion and future work are summarized in Section 6.

2. Related Work Classification

As mentioned above, insider attacks have been increasing, and as a result different approaches have been proposed to counter them. Much of the literature, which have been reviewed in [18–22], focused primarily on "how to detect insider threats". However, this section reviews and classifies the approaches focused on "how to prevent insider threats". It classifies the ITP approaches into two main classes (biometric-based and asset-based). Following this, the biometric-based approaches are further classified into behavioral and physiological, while the asset-metric approaches are also categorized into host-based, network-based and combined. In this section, we review the existing approaches according to the proposed classification model depicted in Figure 1.

2.1. Biometric-Based

As a matter of fact, insider threats are human-driven, therefore, they should be addressed using biometric features. Biometrics is a science for recognizing individuals based on their physical, physiological or behavioral characteristics [23]. It has been implemented in various authentication techniques to validate legitimate users from those who are not. In the ITP field, some approaches have employed some biometrics of insiders, e.g., brain signals, typing behaviors, head and eye motions, etc. Such approaches are discussed in the following subsections.

2.1.1. Behavioral Biometrics

To reinforce the protection against insider attacks, some approaches implemented various behavioral biometrics (e.g., typing patterns, head and eye motions). Keystroke dynamics is a science of biometrics, where insiders are continuously authenticated based on their typing patterns. In the insider threat context, Babu et al. [24] integrated the typing patterns of insiders with access control models to prevent insider attacks. The aim of the approach was to detect and prevent masquerader attack. The model consisted of two stages. In the first one, risk scores are associated with resources using a common vulnerability scoring system (CVSS). In the second, a continuous validation of insiders' typing is monitored (using key-loggers) throughout an entire session. The simulation testing was conducted utilizing the insider threat database of CERT, while the support vector machine

(SVM) is used as a classifier. The idea was to calculate the differences between presses and releases of keystroke patterns of insiders. When anomalous typing patterns are detected, an operated task will be blocked as it is counted as a masquerader's attack.

In Reference [9], an approach was proposed to predict an insider intention of access based on behavioral biometrics (head micro-movements) for preventing insider threats. The experiments are implemented using two visual stimuli scenarios (accessing secured files and burning a lab) by 40 participants. To predict the access intention of participants, their head motions were tracked utilizing gyro sensors mounted on their heads. The collected data are automatically sent to Testbench–Emotiv EEG software for analysis. The results show that when head micro-movements of insiders are lower, the likelihood of executing their intentions is higher. Their findings indicate that there is a relation between the number of insiders' head micro-movements and the motivation toward executing intentions. The approach was able to prevent malicious actions with an accuracy of 70%.

Another behavioral approach was adopted by Eberz et al. [25] to perform a user authentication for preventing an insider attack based on eye motion features. The focus was on a threat that might come from masqueraders. The approach aimed to build a continuous authentication system that distinguishes between users based on their gaze features. To test the applicability of the approach, an experiment with 30 participants (20 males and 10 females) was conducted. The participants were recruited to conduct tasks while the data of their gazing features were collected using SMI RED500 eye tracking device. A number of 21 gaze features was extracted (e.g., pupil diameters, temporal, spatial, etc.). The scenarios of wearing eye glasses or contact lenses were also tested. The classification was implemented using k-Nearest-neighbors (kNN) and support vector machine (SVM). The accuracy of the approach reached 84.56%.

The discussed behavioral-based approaches reveal a new trend of implementing biometrics for providing more accurate solutions. Eye-tracking technologies [25–27] have been implemented also in several areas (advertisements, attracting people's attention, etc.). Such techniques can give further insights to implement more advanced eye-tracking tools in ITP context.

2.1.2. Physiological Biometrics

The objective of access control models is to protect assets using various authentication methods, i.e., passwords, tokens, fingerprints, etc. Those methods are robust for granting or rejecting the access to authorized users with assigned permissions. At enterprise-level, the main concern of such methods is that when a user is granted full access to an asset he will be trusted throughout the session [28]. Therefore, if an insider misuses his privileges, he will proceed undetected. Therefore, to protect against threats posed by authorized users, the new mechanisms of intent-based access control (IBAC) have been developed. The purpose of IBAC is to verify the honesty of insiders' intentions rather than their identities. The logic behind IBAC is that, as insider threats are human-driven, physiological features (e.g., brain signals) can be employed to detect the intentions of insiders for the possibility of preventing threats.

The implementation of IBAC in the insider threat area was proposed by Almehmadi et al. [28]. The authors applied brain signal features as an intention detection mechanism for granting or rejecting the access of insiders to organization's assets. A risk level was assessed based on verified knowledge of insiders' motivation. Following this, based on a threshold of risk level, the granting or rejecting an access to an asset was determined. The risk level is calculated to assess the likelihood of executing the insider's intention according to brain signals amplitude. The approach was validated by several experiments of 30 participants. Two malicious intentions were simulated (opening secured files and burning physical resources). The intentions of participants were detected using P300-based concealed information test (CIT) and brain–computer interface (BCI), the two main foundations of IBAC techniques. In addition, an Emotiv EPOC, the wireless 14-channel electroencephalogram (EEG) acquisition device, was used to collect brain signal responses from participants.

The collected data were analyzed using an EEGLAB—Open Source Matlab Toolbox for Electrophysiological Research [29]. The results of this approach achieved an accuracy of 100% by using a support vector machine (SVM) classifier. However, the authors suggested more investigation to be deployed in real life, as it is the first IBAC approach applied in the insider threat field.

Although this approach achieved promising results, it has some points that need to be considered in terms of deployment, acceptability, and scalability which are as follows:

- The deployment of the approach depends on brain signals, so it may be influenced by outside factors that could skew the obtained results.
- Concerning the scalability factor, the implementation of the approach can be suitable to protect against a small number of malicious intents, but for protecting against large volume of malicious intents, it will be more complex. The rationale is that IBAC depends on huge categories of intents, and this approach considers only two types of malicious intents, namely opening secured files and damaging physical assets. Hence, scalability concerns can be addressed by combining role-based access control (RBAC) with the IBAC model. By having clear knowledge of authorizations and roles of insiders, large categories of intents can be reduced, and the high accuracy can be achieved.
- The acceptability of the approach in the real environment is another concern. When an organization needs to implement such an approach, brain signal sensors need to be mounted on the heads of their employees. This practice would not be accepted by insiders, and if it is enforced, it may negatively affect the trust and productivity in the work environment.

Although the IBAC (physiological-based technique) showed promising results, as corroborated in [28], further works need to be done to overcome its limitations, in particular the deployment, scalability and acceptability factors.

2.2. Asset-Based Metrics

In previous sections, we demonstrate the approaches that are based on behavioral and physiological biometrics. This section will present the asset-based approaches. These approaches are classified into host-based, network-based and combined.

2.2.1. Host-Based

Earlier work in the insider threat area focused on preventing malicious activities at database application level. Chagarlamudi et al. [30] proposed a model to prevent malicious activities on databases based on certain tasks and transactions. In such a model, insiders have access to a database for conducting a task that executes one or more transactions. The model was validated using Petri nets, a directed bipartite graph that consists of nodes and transitions [31]. The objective of the modeling was to prevent unauthorized modifications of data by matching the transactions patterns with predefined ones. In the experiment, two parameters (normal and malicious tasks) were simulated. The results show that the false negatives were as high as (100%) for a single-transaction task and as low as (0%) for a five-transaction task. The findings conclude that the false negative rate is dependent on the number of transactions per task.

Ragavan et al. [32] proposed an approach to prevent unauthorized modifications on a database. That is by associating a variable "threshold" with every data item on the database. The threshold defines a limit to which extent a data item could be modified. If an update operation on a data item exceeds the threshold, that operation is prevented. In the experiment, two models were employed (log entries and dependency graphs). These models checked 5000 data items using various parameters (e.g., number of data items, transactions, and dependencies). We observed that the authors focused on the number of checked operations and their delay, rather than the number of prevented or unprevented operations compared to the total number of operations (e.g., accuracy). In this regard, they found that tracking the updates for each item in a huge database, introduces delay and

slows down the system. To address such performance issues, they labeled each item based on its importance to an organization. The priority was to prevent malicious updates on critical data items (CDI), and then periodically track operations on regular data items (RDI). The results show that the dependency graph models catch malicious operations faster than log entry models on different scenarios.

A data leak attack that could be carried out by insiders may cause serious consequences for organizations. To prevent such attacks, Costante et al. [33] proposed a hybrid data leak prevention framework. It involves two engines, signature-based and anomaly-based. The framework monitors the activities of insiders to detect anomalous transactions. Then, the anomaly-based engine raised an alert to the security operator who confirmed whether a detected transaction is malicious or not. Subsequently, the framework automatically creates signatures, which are used to prevent the execution of similar transactions in the future. The framework was validated using both synthetic and real-life datasets. The synthetic dataset was obtained from a healthcare management system containing 30,490 SQL transactions spanned over 15 days. The real dataset consisted of 12,040,910 SQL transactions from the Oracle database of a large IT company in the Netherlands. The results showed various false positive rates of data leak prevention on both datasets.

As USB ports are available in most computer systems, it can be exploited by insiders to execute malicious actions. To address USB attacks, Erdin et al. [8] proposed a hardware-based scheme to combat USB malicious code attacks. They applied their approach on an attack scenario when insiders inject malicious code into the PCs of their colleagues utilizing USB devices. The simulation was tested on ZedBoard [34], a development board for USB studies. On such a board, USB packets can be customized and monitored via a logic analyzer. Hence, USB packets are observed to collect features of USB devices (e.g., vendor IDs, device IDs, number of endpoints, type of endpoints, etc.). To prevent the attack, descriptors are defined through USB configuration input. To verify the hardware independency of the scheme, they implemented experiments on different OS platforms Linux and Windows.

2.2.2. Network-Based

The increase of networking environments produces many challenges, especially the prevention of data leak attacks that may be conducted by insiders. Some insiders have more privileges over systems and networks of an organization. The packet pattern of network traffic has been utilized in traffic analysis attack and operating system fingerprinting (e.g., [35,36]). Sibai et al. [37] proposed autonomic violation prevention system (AVPS) to prevent insider threats over networks. This work is an extension of their previous framework [38] for providing more scalable protection. The framework employs in-line components to limit and control the access to a network. It monitors events, and then takes actions based on conditions associated with data leak incidents. This was done by applying event–condition–action (ECA) autonomic policies [39] that are used commonly in security-centric systems. Several experiments were conducted to assess the performance of the framework over various network applications (e.g., FTP, database, and web server). The experiments were carried out on RedHat, Ubuntu Linux, and Fedora OS platforms. They utilized Snort to filter the packets of network traffic and extract the attributes (e.g., IP, user, application type, request, response, etc.). The collected data were processed and normalized to be matched against policies and rules. Once there is a violation, an action was triggered to prevent malicious action. The performance was measured using several metrics like throughput, CPU utilization, and transfer time with 95% of confidence intervals.

2.2.3. Combined

As insiders are authorized to use different services of an organization, various features can be used to prevent their malicious actions. The increasingly pervasive use of mobile devices and social media offers an opportunity to utilize them in protection systems. In particular, geo-social contexts of insiders can provide supportive information

related to their workplace environments, which can help to detect suspicious insiders and therefore prevent possible attacks. Such information can also be used to determine whether to grant the access to organizations' assets or not [25]. For example, an insider who stands frequently at places that he is not supposed to be in, an ideal protection system would flag him as suspicious and restrict him from accessing sensitive assets. In this regard, Baracaldo et al. [40] proposed a Geo-Social Insider Threat Resilient Access Control Framework (G-SIR) to detect how trustworthy an insider is, before granting him access to particular assets. The proposed framework considered current, and historical geo-social information of insiders that are associated with access control decisions. Such information included social networks, which are represented as social graphs, and the user mobility was represented as locations on maps. To validate the framework, a synthetic dataset was created using Jung API [41]. The simulations were tested using 250 insiders and repeated 30 times to confirm the stability of the framework. The approach was capable of preventing insider attacks with 76%.

Sawatnatee et al. [42] designed an insider threat detection and prevention protocol to authenticate insiders. It was suggested as a solution to detect and prevent a malicious insider "intruder" who may imitate an authorized IT user's access to an obligation application program. The approach was evaluated on thirty IT users utilizing their knowledge and computer usage behavior. Several activities logs are employed (e.g., website visits, database logs, etc.). The malicious acts were classified using decision tree classifiers (e.g., J.48 and Random Forest) and discriminant analysis techniques. The best classification accuracy was achieved on linear binary discriminant function with 98.3%.

Tukur et al. [43] proposed an edge-based blockchain enabled anomaly detection framework for preventing insider threats in the IoT. The aim was to preserve the availability and integrity of the IoT system data. The availability was maintained to avoid a single point of failure by employing the power of edge computing to reduce the latency and bandwidth requirements on the IoT nodes. The integrity of the data was also protected to be compromised by possible malicious insiders (e.g., system admins) who may violate data integrity without leaving traces of their malicious acts. Thus, to prevent such malicious acts, the framework leveraged a sequence-based anomaly detection and employed Ethereum blockchain's smart contracts to perform detection and correction of anomalies in an inbound sensor data. The framework was evaluated over Remix Development Environment utilizing dataset obtained from collected sensor data (e.g., laptops, PCs, network, etc.). The results show that the framework is able to ensure the security of transaction processing and maintain data integrity for the IoT system.

The ITP approaches that are categorized and discussed in the previous sections are summarized in Table 1.

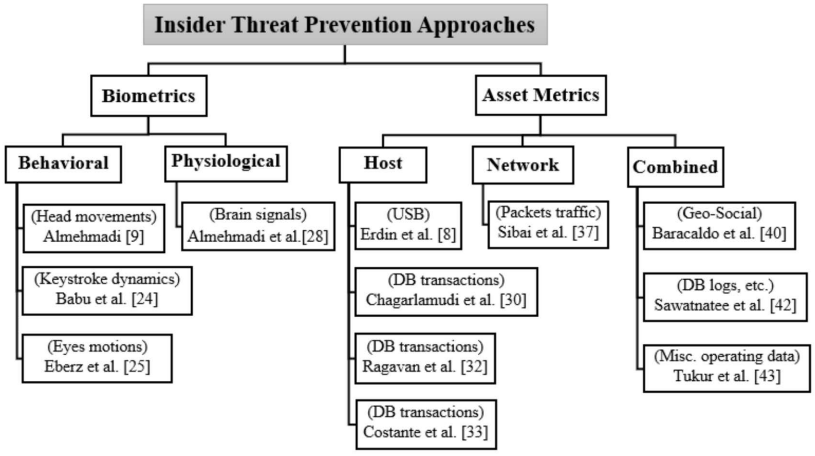

Figure 1. Classification model of ITP approaches.

Table 1. A summary of ITP approaches.

Ref.	Approach	Domain	Addressed Threat	Features
Babu et al. [24]	Biometrics	Behavioral-based	Masquerader	Typing patterns
Almehmadi [9]	Biometrics	Behavioral-based	Malicious Insider	Head micro-movements
Eberz et al. [25]	Biometrics	Behavioral-based	Masquerader	Eyes motions
Almehmadi et al. [28]	Biometrics	Physiological-based	Malicious Insider	Brain signals
Chagarlamudi et al. [30]	Asset-metrics	Host-based	DB modifications	DB Transactions
Ragavan et al. [32]	Asset-metrics	Host-based	DB modifications	DB transactions, and dependencies
Erdin et al. [8]	Asset-metrics	Host-based	USB malicious codes	USB device
Costante et al. [33]	Asset-metrics	Host-based	Data leakage	SQL queries
Sibai et al. [37]	Asset-metrics	Network-based	Data leakage	Packets traffic
Baracaldo et al. [40]	Asset-metrics	Combined	Suspicious insiders	Geo-Social
Sawatnatee et al. [42]	Asset-metrics	Combined	Masquerader	DB logs, Computer logs and Websites visits
Tukur et al. [43]	Asset-metrics	Combined	Data modification and removal	Miscellaneous operating data

The classification model, summarized in Table 1, considers both insider threats as well as the approaches to prevent them. The work in [24,25] utilized behavioral-based approaches to prevent masquerader threats utilizing typing patterns and eyes motions features, respectively. In References [9,28], the malicious acts of insiders (unauthorized access and sabotaging a lab) are addressed using behavioral and physiological approaches. That is by employing head micro-movement and brain signal features to detect the malicious behavior of an insider. Data leakage threats are addressed in [33,37] by employing asset-based metrics, namely the SQL queries and packet traffic pattern. Moreover, asset host based approaches are also applied in [8,30,32] to prevent unauthorized modifications and USB malicious codes. To reinforce the protection against insider threats, various behavioral biometric approaches are implemented (e.g., typing patterns, head and eye motions). More advanced eye-tracking technologies [25–27] have been implemented in several areas (advertisements, attracting people's attention, etc.) which can give further insights to be employed in insider threat prevention area. Moreover, a new physiological biometric approach that is based on intent-based access control (IBAC) has been proposed in [28]. The purpose of IBAC is to verify the integrity of an insider's intention rather than his/her identity utilizing physiological features (e.g., brain signals). Although this approach achieved promising results, it needs a further investigation in terms of deployment, acceptability, and scalability, which are pointed out in Section 2.1.2. The classification model shows that various insider threats are addressed utilizing individual approaches (behavioral, physiological or asset), in which an integrated approach can be developed.

However, the subject of insider threats has recently acquired considerable attention in the literature. The approaches concerning the "detection" of insider threats are reviewed in the recent survey [44]. On the other hand, the approaches concerning the "prevention" of insider threats (categorized above) focused primarily on monitoring and profiling certain aspects of insiders' activities. For instance, in References [9,24,25] the behavioral biometrics of insiders are employed (e.g., typing patterns, head micro-movements and eye motions), whereas in [8,30,32,33,37,40] the asset-based metrics are utilized (e.g., DB Transactions and dependencies, USB events, network packets, etc.).

3. The Framework

As clarified above, the monitoring and profiling the activities of insiders using certain aspects (e.g., technical monitoring) is not sufficient to prevent a wide range of insider incidents. Thus, we propose an all-encompassing framework that integrates technical, psychological, behavioral and cognitive factors of insiders to cover all surrounding aspects of insider threat problems. In addition, it considers both the pre and post aspects of insiders

by going beyond just technical monitoring at work. Figure 2 shows the components of the framework and their associated modules.

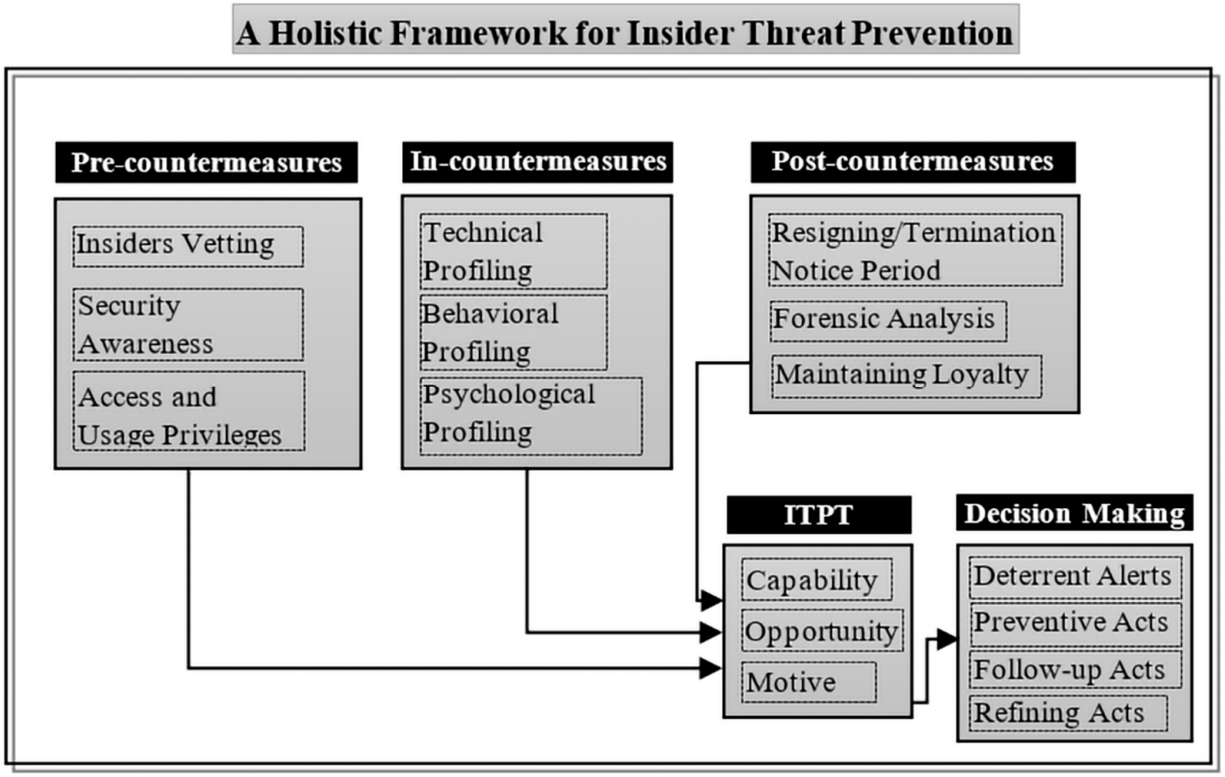

Figure 2. Insider threat prevention framework.

The framework incorporates virtual, non-virtual and contextual factors of insiders from their pre-joining period to an organization until after they leave, to provide a comprehensive view of insider threat problems. The goal is to consider "proactive" measures that need to be taken to prevent insider threats rather than "reactive" ones. The framework encompasses five main components: pre-countermeasures; in-countermeasures; post-countermeasures; an Insider Threat Prevention Team (ITPT); and decision making.

The ITPT component represents an insider threat response team who is responsible for the insider threat countermeasures such as detection, prevention, remediation, etc. They are a group of cross-functional employees within an organization consisting of IT specialists, psychologist and HR, who have the authority to act quickly and proactively. At the core of the framework, the pre/in/post-countermeasure components act as three protection layers to deter and prevent potential insider threats. This is by integrating a set of modules (e.g., insider vetting, security awareness training, technical and psychological monitoring, etc.). The objective of these components is to provide technical, behavioral and psychological profiles of insiders' activities to the ITPT component. Then, the ITPT component evaluates insiders' profiles according to their motive, opportunity and capability to carry out an attack. Finally, the decision making component activates various deterrent and preventive acts according to calculated risk score. The notification and alert management system called PRISER [45], can be adapted in the decision making component to alert possible malicious insiders as a deterrence mechanism within an organization. The next sections illustrate each component of the framework and its associated modules.

3.1. Pre-Countermeasures

The observant ITP system should have continuum countermeasures that range from the employment stage of insiders until after they leave an organization. It should apply proactive measures before providing insiders an access to organization assets. This

can be achieved by conducting various pre-countermeasures (e.g., insiders vetting, fine-granularity of access and usage privileges, security awareness training). These can be effective methods and serve as proactive strategies within the ITP system. The modules of pre-countermeasures components are presented in the next subsections.

3.1.1. Insiders Vetting

The optimal prevention system of insider threats should be very conscious about the integrity of insiders before granting them access privileges to organization assets. This is by involving the ITPT in the employment stage of insiders in an organization. Significant measures can take place at this stage (e.g., criminal background check, psychological or personality traits test, etc.). Such measures can result in potential risk indicators. This screening process is essential as it should be applied to all insiders from different levels. Furthermore, rigorous vetting process should be applied to insiders with higher privileges, especially for system admins and those who will deal with sensitive assets (e.g., intellectual property data, research and development data, accounts credentials, financial assets, etc.).

The background check of insiders can be done by investigating their previous employment, references and social media. Additionally, several indicators can be anticipated through interview questions, such as why they leave their previous job, why they need to work for, and so on. In the UK, the Centre for the Protection of National Infrastructure (CPNI) deploys comprehensive vetting guidelines [46]. They provide pre-employment vetting practices to ensure the trustworthiness of individuals.

3.1.2. Granularity of Access and Usage Privileges

Unlike external threats, insider threats are coming from users working within an organization. Therefore, if they have unfettered access to organization assets, the potential threats can be very high. An easy access to an asset that is not relevant to insiders' duties, may encourage malicious insiders to carry out an attack. Therefore, the mitigation of insider threats can be done by assigning the least privileges for performing the solely required tasks. Beebe et al. [47] proved that the decreasing of benefits that might be gained by cybercriminals will deter them from committing attacks. Similarly, the lowering of access and usage privileges will restrict malicious insiders from carrying out possible attacks. When allocating privileges for insiders, the following factors should be considered.

- Insiders vetting stage outcomes: the potential indicators resulted from the background checks of insiders should be highly considered while allocating access and usage privileges.
- Insiders roles: the insiders, who will be allocated roles with high privileges, can have a greater opportunity to commit an attack. Therefore, granting privileges should be based on RBAC and least privilege principle.
- Knowledge and skills: the insiders who are assigned specific access and usage privileges should be equipped with required knowledge and skills to avoid any unintended harmful acts. They should be grouped as per the assigned roles and privileges, and directed to a focused training program (Section 3.1.3).
- Fine-granularity: The precise assigning of access and usage privileges can be an effective threat-reducing measure. Hence, attention should be paid to apply a granular allocation of access and usage privileges (e.g., open, modify, copy, move, delete, etc.) in order to mitigate the possibility of conducting threats.

However, more measures can be done in this module to narrow the malicious activities of insiders and close the doors for their attack chances. This can be accomplished by applying some strategies: risk-adaptive access control (RAAC) [48]; using trust for assigning users to roles [49,50]; and IT responsibility alignment [51]. There are also some techniques (e.g., property watermarking, digital signatures, etc.) that can be applied to discourage malicious insiders from perpetrating attacks. In addition, encryption applications that are verified in [52], can be employed in this module to secure the privacy and communication

of data within an organization. The automatic data destruction and incident continuity administration are also effective mechanisms to prevent insider threats [53].

3.1.3. Security Awareness Training

Insider threats can be more challenging to prevent, if insiders lack the awareness of hacking, phishing, and social engineering attack methods. The novice insiders can be exploited by malicious attackers to harm the sensitive assets of an organization. Thus, the training of insiders on security measures, policies and regulations is highly imperative. The security awareness training is not taken with great interest by several organizations. It has been shown that about 40% of organizations only provide ongoing security awareness training to their staff, while 21% of organizations are just thinking to conduct it in their future plans [54].

Without significant attention to the security awareness training of insiders, an organization might be exposed to a high risk. Therefore, our framework encompasses the security awareness training as a module of pre-countermeasure components. This is to avoid unintentional threats that might have occurred by unaware insiders. The Information Technology Security Awareness and Training Program [55] that is designed by National Institute of Standards and Technology (NIST) provides the essential procedures and training techniques to secure IT resources. It identifies the necessary skills for users to conduct their management, operational, and technical tasks properly. It presents key responsibilities to ensure that an effective security awareness training program is conducted at an enterprise-level.

The aim of the pre-countermeasure component is to act as the first protection layer in the ITP framework. That is by ensuring that the integrity of insiders, the granularity of assigned access/usage privileges and the security awareness are taken place in the workplace of an organization. Such measures can also serve as a contextual dimension to deter malicious insiders from committing attacks. For example, when insiders perceive strict vetting measures, precise access privilege assigning and targeted security awareness training, they can feel that the workplace is reinforced with robust countermeasures, which at the end deter them from engaging in malicious acts.

3.2. In-Countermeasures

After ensuring that the insiders are trustworthy, the access/usage privileges are allocated accurately and the security awareness is deployed, the in-countermeasure component acts as the second protection layer. The primary functions of this component are the monitoring and profiling of technical, behavioral and psychological activities of insiders. The technical measures monitor the digital activities of insiders that can be recorded on an operational level, while the behavioral measures track the behaviors of insiders in their workplace (e.g., their commitment to the policy of working hours and assigned tasks). The psychological measures evaluate the mindsets and motivations of insiders that may lead them to engage in malicious acts. The modules of in-countermeasure components are illustrated in the following subsections.

3.2.1. Technical Profiling

In this module, the interaction of insiders with information systems is monitored and profiled. The digital activities of insiders can be aggregated and analyzed utilizing various monitoring tools (e.g., sysmon, NetFlow, Active Directory, etc.). They can track the interaction of insiders with operating systems, applications, networks and databases. This can be conducted continuously and in real-time, and therefore generates more representative records of insiders acts. To create technical monitoring profiles of insiders, system calls and application execution analysis are employed. They have been used also to monitor and profile digital activities of users in several approaches (e.g., [56–59]).

A system call runs when a program requests a service from the operating system kernel to access computer resources, such as memory, CPU, processes and network [60].

Therefore, the technical activities of insiders can be profiled through system calls utilizing different tools (e.g., * nix syslog, audit daemon and Windows event logs). They can be leveraged to identify a broad range of cyber security threats related to (e.g., authentication, file operations, processes, kernel messages, policy change, etc.). This is due to that system call-based analytics show insiders activities at the kernel level. For example, by inspecting file operation-related processes, the threats of privilege alterations can be detected. Furthermore, system call-based analytics have been used in [61] to address malware attacks, and also in [62] to uncover a malicious insider who is attempting to violate the policy of access privileges.

Magklaras et al. [63] proposed a technique to measure the computer skills of a user (user sophistication) at system level. This technique is used in our framework to assess the parameter of an insider sophistication as follows.

$$Insider\ Sophistication = Fbreadth + Fappscore + Fresutil \quad (1)$$

The *Fbreadth* parameter indicates the number of applications that are concurrently operated by an insider, whereas the *Fappscore* parameter represents the type of applications. The *Fresutil* parameter represents the consumption of resources. Therefore, the insider sophistication is used to assess the capability factor of an insider in (Section 3.4).

The honeypot technique is used to evaluate an opportunity that an insider may exploit to conduct a threat. This can be done by preparing digital resources (e.g., system, file, database, etc.) to catch malicious insiders who are trying to exceed their assigned privileges. The insiders' access to such resources reflects their motivation toward malicious acts. The honeypot technique has multiple features, such as adaptability, flexibility and requires a small amount of data [64]. For example, a honeypot file can be created and named as "Names_Passwords_of_Users.txt" to attract malicious insiders for accessing it. Thus, the honeypot use parameter is utilized to assess the opportunity factor of insiders in (Section 3.4).

3.2.2. Psychological and Behavioral Profiling

The technical profiling alone is not adequate, as insider threats are a human-centric problem. Thus, behavioral and psychological factors of insiders should be inspected in order to develop a holistic prevention system. This section focuses on behavioral and psychological aspects of insiders. As the technical profiling provides a snap of the virtual activities of insiders, behavioral and psychological profiling are essential to decrease false positive rates and make accurate decisions. Moreover, they are beneficial, as they provide contextual information for intent analysis to address insider threats in a proactive manner. In the literature, it is commonly believed that a malicious intent of an insider can be well captured through contextual data [65].

The behavioral and psychological profiling of insiders require various procedures (e.g., questionnaires, HR and psychologist monitoring, following-up social networks, etc.). Multiple techniques can be applied to profile the behavioral and psychological changes of insiders. The anomalous behaviors of insiders can provide potential risk indicators about their deviations from the policy of an organization. This can be measured using the workplace deviance scale [66]. It has acceptable internal reliabilities, and provides evidence from confirmatory analysis [67]. Thus, it can be employed in our framework to assess the anomalous behaviors of insiders. The first 12-items evaluate the deviance behaviors of insiders that can harm the organization such as: "taking assets without an organization permission"; "using illegal things on the job"; "forward the work to someone else to finish it without a permission"; "working on a personal matter instead of working for employer"; "discussing confidential information with an unauthorized person," etc. The second set of seven-items assess the deviant of interpersonal behaviors that can harm other individuals within an organization. For example: "acting rudely toward co-workers"; "making an ethnic, religious, or racial remark at work"; "repeating a rumor or gossip about boss or coworkers," etc.

The mindset of an insider could be affected by workplace factors. The stress level or workload (e.g., financial crises, workplace stressors, etc.) can cause an insider to carry out malicious acts. This can be assessed using psychometric test [68]. It evaluates various factors: personal stressors (e.g., financial stress, family illness and conflicts, etc.); and professional stressors (e.g., conflicts with supervisor, layoffs threats, unfair benefits and promotion, unspecified responsibilities, etc.). The test was selected based on the multidimensional model [69]. The output represents a snapshot of an insider stress level as "low", "medium", or "high". An insider with a high stress level is considered a high potential risk indicator for launching an attack. Therefore, the stress level is used to measure the motive factor of an insider in (Section 3.4).

The tendency of an insider toward malicious acts can be assessed using CCISLQ technique [70]. It measures the following parameters of an insider:

- The illegal computer activities of an insider in the past.
- The ability of an insider to imitate and reproduce ideas.
- The influence level of family, peers, bosses and media on the behaviors of an insider.
- The intensity of insiders' differential association with their friends.
- The attitude of an insider's family and friends toward illegal activities.
- The insider perception about the likelihood of being caught for any criminal computer activities.
- The perceived punishment and rewards.
- The scale of moral disengagement.
- The common sense toward collective responsibility.
- The vilifying, devaluing and blaming the victim.
- The social demographic information of an insider.

Depending on the results given, the tendency level of an insider to conduct an attack can be categorized as: "low", "medium", or "high". Therefore, it is utilized in measuring the motive factor of an insider in (Section 3.4).

3.3. Post-Countermeasures

The previous components focus on applying different countermeasures from the pre-joining period of insiders to their work environment at an organization. The post-countermeasures look ahead to the notice period of resignation/termination as well as after the insiders leave an organization. Moore et al. [71] presented several attacks that are carried out by insiders within a period of 60 days before departure. They stole top-secret information from their organization (e.g., financial reports, business plans, research and development strategies, etc.). The reason was to gain advantages at the new job or in their own business. Thus, different post-countermeasures can be applied to ensure a further level of protection during the end and after the employment of an insider on an organization.

3.3.1. Resigning/Termination Notice Period

As the notice period of resignation/termination is highly critical, a module in the framework is tasked to observe the activities of insiders in the pre-departure period. The module can be triggered from HR records as soon as a notice period of an insider is commenced. The notice period is the length of time an insider will continue working between delivering a resignation letter until the final day of work on an organization. When an insider puts in his/her notice period, there are two common cases that can be specified by ITPT:

1. The insider might be dissatisfied with his/her situation on an organization. In this case, the monitoring measures should be more and an immediate action should be taken. For example, during the notice period, an insider may copy sensitive data from organization's systems either at the workplace or remotely. Moreover, an insider may install sophisticated attacking tools on the PCs of an organization, which can act as a backdoor for him/her after departure. In Reference [72], it is shown that 26% of insider attacks are carried out after insiders leave, since an organization did

not disable their access. In response to that, several necessary precautions should be applied to make sure that there is any gap that might be exploited by malicious insiders which are as follows:

- Disabling all accounts to which an insider can access to any asset of an organization, as he/she might access sensitive assets that negatively affect an organization in a variety of ways.
- Changing any passwords or credit cards' PINs that might be shared with insiders within an organization.
- Invalidating the access to an organization's email address associated with an insider, as he/she may exploit the email address of an organization to carry out potential malicious acts.

2. An insider could be pleased with his/her work in an organization, but he/she might leave for any reason. In addition to the previous measures, different proactive strategies should be applied. This is by maintaining loyalty and constructing strong grateful relations with insiders who left an organization as presented in the next section.

3.3.2. Maintaining Loyalty

It is common to break the contact with an insider who left an organization. However, insiders who left an organization can constitute potential threats, as they may have highly competitive information (e.g., intellectual proprietary, trade secrets, etc.) about the former employer. Thus, in addition to the post-employment obligations, non-competition obligation (NCO) and non-disclosure obligation (NDO) concerning the information protection of former employers, keeping the loyalty with an insider provides an additional layer of protection. Maintaining the loyalty of insiders should be considered by an organization as a post-countermeasure to minimize any possible malicious act (e.g., disclosing proprietary information). As a departing insider is out of an organization's technological-based control, several procedures should take place by ITPT to preserve his/her loyalty and establish a long-term relationship:

- Rewards can be a powerful loyalty builder, so to keep an insider loyalty, he/she should be rewarded for his/her work on an organization. This makes an insider feel appreciated as a return favor for keeping and continuing the instantiated trust with an organization.
- Providing an excellence post-employment service, as a departing insider might need some services (e.g., work experience certificate, etc.). Such services can be available for them through a post-employment service portal to make their experience simpler and faster.
- Constructing strong grateful relationship with departing insiders. The technology has made it easy and it can be achieved by sending system-generated personalized congratulations (e.g., birthday, wedding, achievements anniversary, etc.). Such things speak to the emotional needs and can be an effective mean for constructing the loyalty.

Therefore, through maintaining the loyalty with a departing insider, a high level of respect for the organization can be established. This can act as preemptive measures for any possible malicious acts of post-employment.

3.3.3. Forensic Analysis

It is also important for ITP systems to employ forensic analysis techniques to figure out possible vulnerabilities for future improvements. The aim of this module is to conduct continuous evaluations and improve the undertaken measures constantly. This can be achieved by routinely inspecting the applied measures through ITPT component. The proactive ITP system should have the capability to collect and retain evidences that can be utilized later for inspection and improvement. This is considered in the framework by integrating forensic analysis solutions (e.g., [73,74]), to perform deep forensic analysis and fast triage analysis. Thus, the modules of the framework (e.g., insiders vetting, fine-granularity of

access and usage privileges, security awareness training, technical profiling, etc.) can be inspected by ITPT to make sure that effective methods are applied. The ITPT can find areas that need to be improved within pre/in/post-countermeasure modules continuously. For example, in technical profiling module, the selection of appropriate data features that reflect the actual behavior of insider act is significant. The major challenge facing the ITP approaches is whether false alarms can be reduced with reasonable cost. Therefore, with a forensic analysis module, more effective mechanisms can be introduced to improve the ITP system.

3.4. ITPT

As insider threat is a human-centric problem, a technical based solution is not sufficient to prevent insider threats perfectly. Thus, the ITPT component could be composed of security analyst and psychologist. This component assesses the above pre-, in-, and post-countermeasure components and their associated modules. The combination of technical, behavioral and psychological profiles of insiders through an advanced analytics platform reinforces the ITPT to determine the motive, capability and opportunity factors of insiders. These factors are adopted from [75] for modeling malicious activities of insiders. The idea is that each attacker requires motive, capability and opportunity to launch an attack. Therefore, each of these factors is assessed as follows:

MOTIVE: This factor represents the motive *Mi* of an insider to perform an attack. It is measured using the following equation.

$$Mi = f(Ti, Si, Vi) \tag{2}$$

The parameter *T* represents the tendency level of an insider *i* to carry out a malicious act. This can be assessed using the technique mentioned in (Section 3.2.2). The parameter *S* represents the stress level of an insider *i* as assessed using the psychometric test mentioned in (Section 3.2.2). The parameter *V* represents the skills verification of an insider *i* deduced from assessing the tendency of an insider to initialize malicious acts. Overall, the three parameters can determine the motive factor of an insider as shown in Table 2. It is utilized to measure the threat score of an insider in (Section 3.5).

Table 2. Motive Score.

Skill Verification	Stress Level	Malicious Tendency		
		Low	Medium	High
False	Low	1	2	3
	Medium	2	3	4
	High	3	4	5
True	Low	2	3	4
	Medium	3	4	5
	High	4	5	6

OPPORTUNITY: This factor represents the opportunity *O* that a malicious insider *i* can exploit to launch an attack. It can be assessed utilizing the following equation.

$$Oi = f(Bi,Ri,Hi) \tag{3}$$

The parameter *B* represents the change in the working behavior of an insider *i*, whereas *R* and *H* represent the insider role and honeypot use, respectively. The role of an insider on a system *Ri* can be categorized as "novice", "advanced" or "admin". Thus, the opportunity factor can be evaluated using Table 3.

Table 3. Opportunity Score.

Behavior Change	Honeypot Use	Insider Role		
		Novice	Advanced	Admin
False	False	1	2	3
	True	2	3	4
True	False	3	4	5
	True	4	5	6

CAPABILITY: This factor *Ci* represents the skills of an insider who may execute an attack. It can be assessed using the following equation.

$$Ci = f(Di, Si) \tag{4}$$

The *Di* represents the demonstrated capability parameter evaluated, while the *Si* represents the insider sophistication parameter. Therefore, the capability factor can be measured as shown in Table 4.

Table 4. Capability Score.

Insider Sophistication	Demonstrated Capability			
	Low	Medium	High	Very High
Low	1	2	3	4
Medium	2	3	4	5
High	3	4	5	6

3.5. Decision Making

After the motive, opportunity and capability factors have been assessed, the framework has a component that decides the threat score of an insider and takes multiple actions accordingly. Table 5 shows the motive, opportunity and capability factors that are utilized to calculate a threat score of an insider.

Table 5. Motive, Opportunity and Capability.

Motive	Opportunity	Capability		
		Low	Medium	High
Low	Low	3	4	5
	Medium	4	5	6
	High	5	6	7
Medium	Low	4	5	6
	Medium	5	6	7
	High	6	7	8
High	Low	5	6	7
	Medium	6	7	8
	High	7	8	9

The threat score *Ti* of an insider is specified based on the following equation.

$$Ti = Mi + Oi + Ci \tag{5}$$

where *Mi* represents the Motive factor, while *Oi* and *Ci* represent opportunity and capability factors, respectively. A simple scoring system is proposed to demonstrate the role of this component. As shown above, every factor classifies insiders into three categories: low (1), medium (2) or high (3). For example, if a threat score *Ti* of an insider is equal to 9, this

means that the factors (Mi = 3), (Oi = 3) and (Ci = 3). Therefore, several decisions can be taken based on the threat score of an insider specified in Table 6.

Table 6. The threat score, risk level and decision made.

Threat Score	Risk Level	Decision
3–4	Low	Rise Monitoring Measures
5–6	Medium	Deterrence Alerts
7–9	High	Preventive Acts

After assessing the threat score of an insider, the scoring system is used to classify the risk level of an insider. Three intervals can be used (3–4), (5–6) and (7–9) to map the risk level of an insider as "low", "medium" or "high", respectively. This scoring system can be adaptive as an organization who may adopt the framework can set its own scoring system based on its own requirements. Several actions (monitoring measures, deterrent alerts and preventive acts) can be taken accordingly. For example, if the risk level of an insider is flagged as "low", the monitoring and profiling module should be triggered. Similarly, if the risk level is reached to "medium", deterrent alerts should be issued. This can also play an important role in preventing malicious activities in an indirect way. There is a phenomenon known as diffusion of benefits [76] which hypothesizes that when a person is deterred in one situation, it is assumed that the deterrent measure applies to other situations as well. Likewise, if the system alerts insiders about possible malicious behaviors, it gives them a sense that the deterrent measures are applicable on all other situations. Thus, the deterrent alerts can also serve as preventive measures in the framework. It is also important that the taken decisions should be inspected to determine how accurate the prevention system is. For example, some preventive acts may block normal activities of insiders (false positives). Therefore, frequent refining measures should be taken for future improvements.

In the previous sections, we illustrate the components of the framework and their respective modules. Table 7 summarizes the components, modules and their related concerns.

Table 7. A summary of the components and modules of the framework.

Component	Module	Remarks (Continued . . .)
Pre-countermeasures (1st protection level)	Insider Vetting	As defined by CERT [4] that an insider can be a current or former employee, contractor, or business partner. An organization that would adopt this framework should apply the procedures of this module on all actors who will interact with an organization's system.
	Granularity of Access and Usage Privileges	The access and usage privileges should be assigned according to the techniques mentioned in the module (e.g., RBAC, RAAC, etc.). The usage control is highly critical and should be considered, especially with insiders who are engaged as contractors or business partners.
	Security Awareness Training	After assigning roles, access and usage privileges, the security awareness training should be directed according to assigned privileges and roles, not using a one-size-fits-all approach.
In-countermeasures (2nd protection level)	Technical Profiling	This module should profile all digital activities of insiders on operating systems, applications, databases and networks in real time basis. This is by configuring monitoring and logging tools as mentioned in the module. The storage space for the logging data should be considered, especially in production environments. More focus should be put on highly skilled users who may disable logging tools or bypass security controls. Such insiders can be identified through the assessed capability factor.
	Behavioral and Psychological Profiling	The behavioral and psychological monitoring could be conducted by the collaboration of supervisors, psychologist and HR. It should be done routinely and on a regular basis by considering the critical period (e.g., notice period of resigning/termination).

Table 7. *Cont.*

Component	Module	Remarks (Continued . . .)
Post-countermeasures (3rd protection level)	Resigning/Termination Notice Period	This module should be triggered as soon as the notice of an insider is commenced especially for disgruntled insiders. The shared accounts and exfiltration ports (e.g., e-mail and USB) should be highly monitored. All access and usage credentials should be disabled before their departure.
	Forensic Analysis	This module should be triggered routinely to find out any vulnerabilities that might be exploited by malicious insiders. Therefore, the modules of the framework can be improved accordingly. The social media platforms (e.g., Facebook, Twitter, LinkedIn, etc.) are also significant and available data sources for analyzing the malevolent tendencies of insiders. They can also establish a new dimension in the insider threat area of research.
	Maintaining Loyalty	The insiders may reside within an organization for a long period, so when they leave they may carry sensitive information to the competitors. Beside technical measures, this threat can also be mitigated by constructing the loyalty with insiders who will leave an organization. This is by maintaining loyalty and trust through applying the procedures of this module.
ITPT	Motive, Opportunity and Capability	This component should be aware of the various modules of the framework. It evaluates the motive, opportunity and capability factors of insiders utilizing specified parameters (Section 3.4). It can also ensure the alignment of applied measures with an organization's policy.
Decision Making	Deterrent Alerts	As per the calculated threat score and corresponding risk level, this module should generate automatic alerts to the concerned insider.
	Preventive Acts	As per the calculated threat score and corresponding risk level, this module should prevent an insider from conducting a specific task.
	Follow-up Acts	The procedures of the maintaining loyalty module are driven by this module as part of the decision making component.
	Refining Acts	The objective of this module is to improve the accuracy and efficiency of the framework constantly. This can be achieved according to ITPT recommendations and the feedback from taken decisions.

4. Applying the Framework on Insider Threat Cases

To demonstrate the use of the devised framework in preventing insider threat incidents, we apply it on three insider threat incidents (sabotage, fraud and theft). These incidents are adopted by the U.S. Security Service and CERT [10]. We develop an ontology adapted from the existing approaches [77,78] to show how the framework can be applied in practice. The ontology presents the concepts and relationships of insider threat factors (operational, behavioral, psychological, etc.). The CERT provides data for the three insider threat incidents. It includes information about the organizations involved, the perpetrator of malicious acts, and the insider threat indicators. Each incident includes a natural language description of operational and behavioral observables. Therefore, they are utilized as the primary data source for our framework ontology.

In the first step of ontology development, the approach in [79] is implemented for concept mapping to ensure the coverage of an information in the repository of insider threat incidents. The resulted triples from the descriptions of insider incidents are utilized as the basis for deriving the classes and object properties of the ontology. To validate our design, a catalog of common ontology development [80] has been utilized. We have used the web ontology language (OWL) for ontology implantation, as it is mature, extensible, and widely used [81]. Figure 3 shows the top-level classes of the ontology: actor, asset, action and incident.

The actor class represents people and organizations, which can contain various subclasses (e.g., an insider as an employee in an organization). The asset class represents different types of objects an organization may has (e.g., devices, data, etc.). The action class involves subclasses of acts an actor can conduct. The incident class represents multiple types of acts an actor can perform to carry out a malicious incident. For example, deleting backup files, changing passwords and shutting down server acts are modeled in the

ontology as subclasses of action class, which represent a sabotage incident that might be carried out by a malicious insider. The object properties (e.g., hasActor) are also provided to express different types of relationships between associated classes.

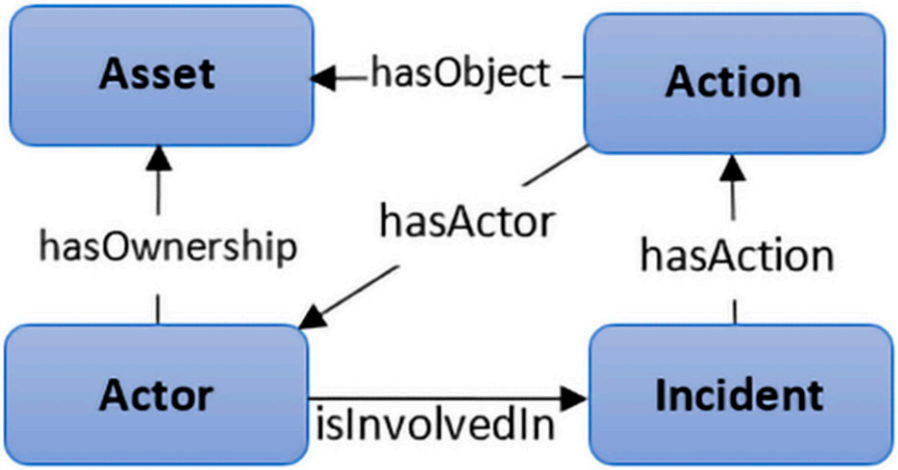

Figure 3. The top-level ontology classes and object properties.

To demonstrate the use of the ontology, the descriptions of the insider threat incidents are translated into the ontology entities as depicted in Figure 4. The concepts are identified, the instances of classes are created, and the object properties are put in to relate the instances of classes to one another.

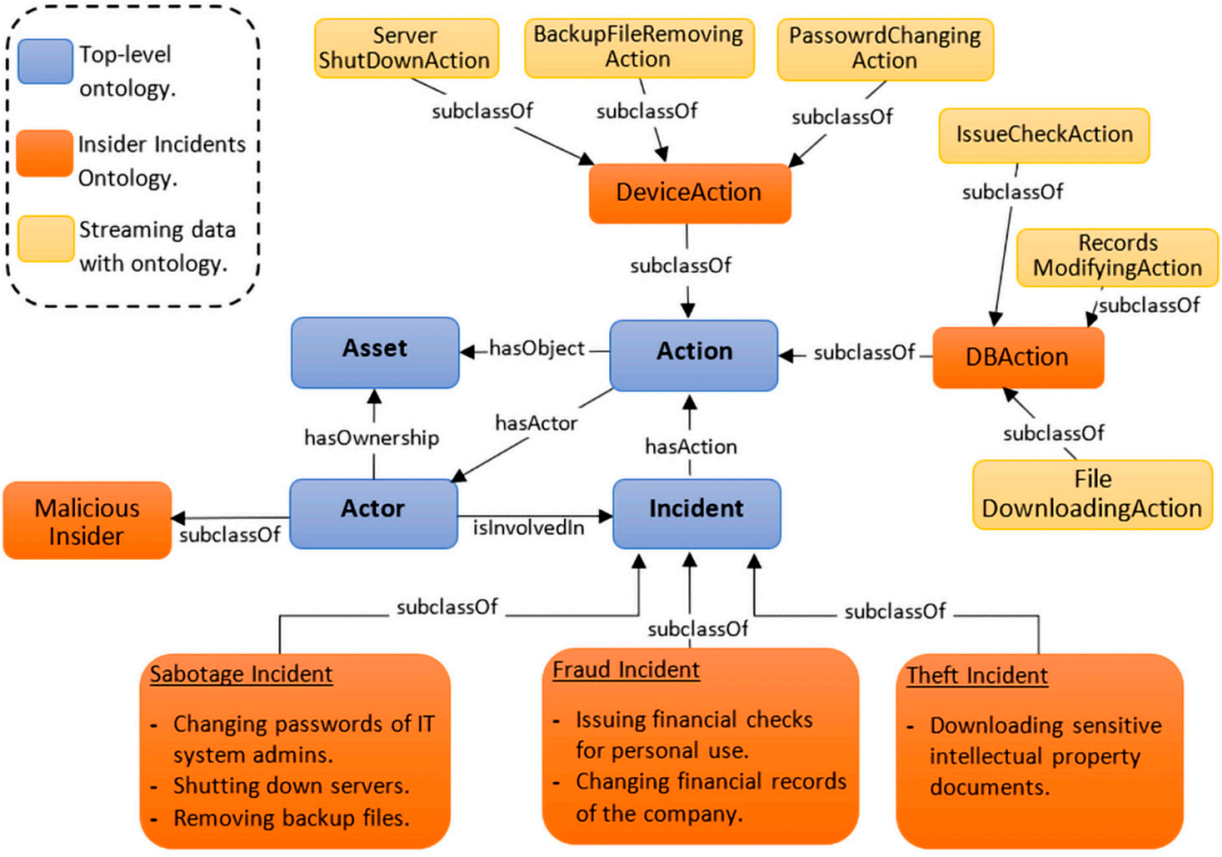

Figure 4. The framework ontology of the insider threat incidents.

The insider threat incidents can be prevented utilizing various types of indicators that are figured out by analyzing the collected observables of insider acts within an organization. Utilizing framework ontology, a semi-automated approach is designed as presented in Figure 5. The data are collected from multiple sources within an organization (operational, behavioral, psychological, etc.). The framework provides different modules (Section 3) for collecting the observed data of insiders' acts, which can be reasoned and analyzed for inferring potential indicators.

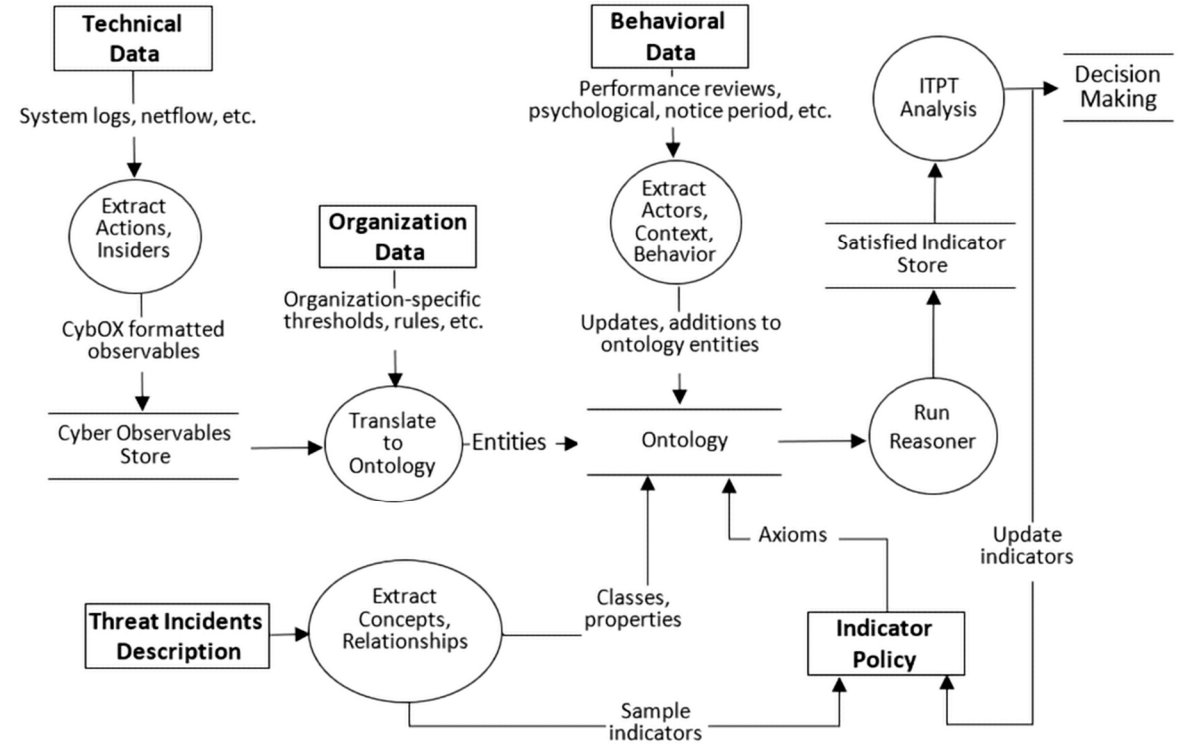

Figure 5. Data flow diagram of the framework.

The suspicious activities of insiders on the systems of an organization are derived from the operational data. They include technical observables (e.g., system event logs) associated with potential threat indicators of malicious acts. As technical data are generally originated in structured or semi-structured log files, it can be translated into ontology entities utilizing Cyber Observable Expression (CybOX) [82]. CybOX provides an API for translating various input data into XML file format. Thus, technical data are translated into the OWL XML code to create entities of ontology classes. The behavioral and psychological data about insiders are typically reside within HR data (e.g., background checks, performance reviews, policy violations, termination notice, etc.).

They provide a rich source of behavioral, psychosocial and contextual information regarding insiders. HR data are less structured than technical data as they include heteronymous behavioral, psychosocial and contextual observables. Thus, enterprise solutions for HR information management, such as human resource information systems (HRIS), could be utilized to develop an automated ontology translation process. In our design, some behavioral data are provided in the description of the threat incidents (e.g., a former fraud incident was conducted by an insider before the current incident).

Once the technical, behavioral and psychological data are described within the framework ontology and the indicators are in place, a semantic reasoner is used to make interpretations and categorize ontology entities as instances of classes. Then, a group of ontology entities that satisfy indicators can provide useful data set for ITPT. After they are analyzed, different decisions can be made, such as finding false positives, refining indicators and

taking countermeasures. Table 8 shows the observables, indicators and countermeasures of the three insider threat incidents.

The ontology provides the description of the insider threat incidents. The indicators are described at a level of details that omit sensitive information of victim company while providing enough information about observables of malicious acts. The conceptual components are provided, and the modular collection of ontology axioms (concepts, definitions, and indicators) are introduced. This section illustrates how the proposed framework can be applied on real-world insider threat cases in which various insider threat incidents can be modelled.

Table 8. A summary of applying the framework on insider threat incidents.

Case	Observables	Indicators	Countermeasures (Continued . . .)
Sabotage Incident	- Changing passwords of system admins. - Shutting down servers. - Removing backup files. - Suspicious behavior.	- High level of admin privileges. - Leaving the company without removing insider's access privileges. - Accessing the asset of the company during off working time "weekend at mid night". - Insider motivation toward destructive actions.	- Applying the module of access and usage privileges in the pre-countermeasure component (Section 3.1.2) to specify very fine-grained access control policies. - Applying the procedures of the resigning/termination notice period in the post-countermeasure component (Section 3.3.1) to remove any access to the assets of the organization by departing insiders. - Applying technical profiling module in the in-countermeasure component (Section 3.2.1) to detect and prevent anomalous acts of insiders that deviate from the baseline (accessing, changing and removing sensitive data from outside organization's network domain during off working time). - Applying the behavioral and psychological profiling module in the in-countermeasure component (Section 3.2.2) to detect and predict the offensive behavior of the insider proactively.
Fraud Incident	- Issuing financial checks for personal use. - Changing the accounting records of the company.	- Previous fraud attack incident. - Anomalies in electronic accounting checks. - Motivation for illegal personal gains.	- Applying the insider-vetting module in the pre-countermeasure component (Section 3.1.1) to conduct strict criminal background checks Before assigning roles to an insider. By applying this module, this fraud incident could have been avoided, as the previous fraud incident can be disclosed and the malicious insider can be disqualified. - Applying the technical monitoring and profiling module in the in-countermeasure component (Section 3.2.1). Thus, the disinformation changes in the electronic accounting records can be prevented. - Applying the behavioral and psychological profiling module in the in-countermeasure component (Section 3.2.2) to observe various behavioral aspects (e.g., financial stressors, workplace stressors, etc.) that trigger the insider to conduct such fraud incident. Thus, detecting such aspects beforehand can lead to prevent the fraud incident from occurring.

Table 8. *Cont.*

Case	Observables	Indicators	Countermeasures (Continued . . .)
Theft Incident	- Downloading huge intellectual property documents.	- Downloading files not relevant to an insider's duties. - Accepting the offer from a competitor. - Downloading large volume of intellectual property files. - Leaving the company without inspection.	- Applying the granularity of access and usage privileges in the pre-countermeasure component (Section 3.1.2). In this theft case, the insider downloaded large volume of sensitive files that are not relevant to his duties. This module can prevent this theft incident by restricting the insider to solely access the assets that are required for his duties. - Applying the behavioral and psychological profiling module (Section 3.2.2), as it considers various behavioral aspects surrounding the insider's context. In this theft incident, the insider decided to leave the company and move to a competitor. Therefore, downloading large intellectual property data before his departure is more likely to be exploited by the new employer. Thus, this module can detect some behavioral and psychological aspects (e.g., level of job satisfaction) that ultimately led the insider to carry out this theft incident and leave the company. - Applying the technical profiling module in the in-countermeasure component (Section 3.2.1), as the anomalous acts on company's systems (downloading excessive number of sensitive files) can be detected. Furthermore, the intellectual property data should be sustained at a very secured place and the interaction with them should be highly monitored. Thus, by applying this module, this theft incident can be prevented before the insider downloaded the intellectual property data and leave the company. - Applying the module of resigning/termination notice period in the post-countermeasure component (Section 3.3.1). When the insider introduced the notice of resigning, this module alongside with the forensic analysis module should take place. The insider's acts on the network and systems of the company should be inspected during the notice period of resigning, especially the interactions with highly sensitive files (intellectual property data). By doing so, this theft incident can be avoided.

5. Discussion

Thus far, we have illustrated the modules of the framework and showed how real-world insider threat cases can be mapped on to it. While we believe that this framework introduces a rich foundation for facilitating insider threat problems, it is important to recognize that there are other proposed frameworks. In this section, we present an overview of relevant conceptual frameworks and show how our framework extends upon them. It is observed that earlier work focused primarily on technical profiling measures. For example, Althebyan et al. [83] presented a model to address insider threats based on monitoring insider actions on various objects in a system. Agrafiotis et al. [84] presented a framework that utilized active directory services to detect policy violations or suspicious activities of insiders that follow a pattern of previous attacks. Bertino et al. [85] proposed a pattern matching model. That is by creating typical technical activities of insiders and addressing the data leakage based on observed anomalies.

Considering both technical and psychological profiling, Raskin et al. [86] proposed a model to address social engineering threats of insiders using various technical and

psychological factors that could be derived from social media and conversations. Kandias et al. [75] presented a model that could employ psychometric assessments and technical indicators to address malicious insiders according to threat scores. Gritzalis et al. [87] proposed a framework to address insider threats based on performance deviations of insiders' activities that can be assessed using psychometric evaluations on social media and technical controls.

The other frameworks integrated some factors that fall between the first two components of our framework (pre-countermeasure and in-countermeasure). For instance, Magklaras et al. [88] proposed a framework that models the behaviors of insiders based on some characteristics (e.g., role, knowledge, access, previous records, and network activity). Ali et al. [89] proposed a technical profiling model where access decisions of insiders are taken according to predefined role-based matrix. Ray et al. [90] proposed a model to compact insider threats by monitoring insider activities utilizing the concepts of attack trees. That is by assessing the psychological characteristics of an insider and his system actions based on the minimal attack tree. Bhilare et al. [91] proposed a framework to address insider threats using a rule-based concept. That is by monitoring insiders' activities on a network and correlating them with their role-based directory context. Similarly, Park et al. [92] proposed a role-based model to counter insider threats through monitoring their actions on an organization as well as applications and operating systems. Buford et al. [93] presented an architecture for compacting insider threats based on behavioral activities and misinformation of insiders. Nurse et al. [94] proposed a framework that is based on technical and behavioral indicators of potential insiders. It also considered psychological factors that may stand behind the motivation of malicious insiders. Finally, Legg et al. [95] proposed a framework to model the insider-threat problem utilizing some technical, psychological and behavioral observations from insider actions. However, Table 9 summarizes the existing frameworks and shows how our approach extends upon them.

Table 9. The existing frameworks compared to ours.

Framework	Pre-Countermeasures			In-Countermeasures			Post-Countermeasures		
	Vetting	Granularity of Access/Usage Privileges	Security Awareness Training	Technical Profiling	Psychological Profiling	Behavioral Profiling	Resigning and Termination Notice Period	Forensic Analysis	Maintaining Loyalty
Kandias et al. [75]				✓	✓				
Magklaras et al. [88]		✓	✓	✓					
Ali et al. [89]		✓		✓					
Bertino et al. [85]				✓					
Raskin et al. [86]				✓	✓				
Althebyan et al. [83]				✓					
Gritzalis et al. [87]				✓	✓				
Ray et al. [90]				✓	✓	✓			
Bhilare et al. [91]				✓		✓			
Agrafiotis et al. [84]				✓					
Buford et al. [93]				✓		✓			
Park et al. [92]		✓		✓		✓			
Nurse et al. [94]	✓			✓	✓	✓		✓	
Legg et al. [95]		✓	✓	✓	✓	✓			
Our Framework	✓	✓	✓	✓	✓	✓	✓	✓	✓

As it is shown in Table 9, most of the existing frameworks such as [75,83–87] focused mainly on technical profiling measures that consider the digital working frame of insiders. However, insider threats are a more challenging problem, so the optimal solution for them is not purely technical one that focuses on a limited work-span of insiders. Rather, it is a people-centric problem, which requires a holistic solution that includes technical and nontechnical measures. Moreover, it should cover the actual working time of insiders as well as the surrounding periods of their employment lifespan. This is what our framework aims to achieve. It considers pre-countermeasure components before establishing the technical monitoring module (vetting, granularity of assigning access/usage privileges and security awareness training).

It is observed that the frameworks in [87–89,92,94] just consider individual elements of such pre-countermeasures while our framework includes all of them within the pre-countermeasure component. Moreover, the technical, psychological and behavioral profil-

ing modules are all covered by our framework through in-countermeasure components. These modules are also covered in [90,94,95], while in the other frameworks they are considered individually. Noticeably, the post-countermeasures are neglected by the existing frameworks, except in [94] where forensic analysis factor was considered.

The implementing of technical profiling measures solely can lead to a suboptimal system that lacks significant factors (psychological, behavioral and cognitive). The technical profiling should be viewed as a single countermeasure in a broader set of all-inclusive countermeasures. Table 9 shows that our framework integrates an array of countermeasures that bridge the gaps of the existing framework for the ultimate goal of addressing the insider threat problem in multiple dimensions. Moreover, while the existing frameworks did not show how they can be employed on insider threat cases, our framework is applied on three real-world insider threat cases to show its applicability in practice.

6. Conclusions

As insider threats are continuing to be an increasing concern for public and private organizations, there is a critical need for effective ITP systems. The ITP topic is an emerging area of research. Therefore, building an optimal system for ITP remains an open challenge. In the literature, there are several approaches, each focusing on a particular aspect of the problem. In spite of such advances in insider threat research, there is no an integrated framework that incorporates various significant factors of insider threat problem (e.g., previous criminal incidents, unfettered access and usage privileges, lack of security awareness training, termination/resignation notice period, etc.). Previous research considered some individual factors, but a broader integrative perspective has been needed. Therefore, this paper integrates all such aspects in a unified framework. The framework is based on a multi-tiered approach that correlates pre-countermeasures, in-countermeasures and post-countermeasures for the goal of addressing insider threats in an all-encompassing perspective. We illustrate how different modules of the framework can act throughout the lifespan of insiders' employment by correlating various factors spanning across technical, behavioral, psychological and cognitive domains. We show how real-world insider threat cases can be addressed to confirm the soundness of the framework. Three insider threat cases are modeled (sabotage, fraud and theft) to show the applicability of the framework in practice. Using observations of the insider threat cases, an ontology/knowledge presentation of the framework is presented (e.g., actors, actions, observables, threat indicators, countermeasures, etc.).

We compare the framework with the previous ones to highlight how we extend and contribute to insider threat research. There is a limitation of obtaining various real-world data from organizations that are attacked by their insiders. It is hard to obtain a permission, from attacked organizations, to survey and collect data in the domain of their information security. In addition, attacked organizations are afraid from negative impacts toward their business, if they announce carried out attacks by their insiders. However, to mitigate this limitation, three insider threat cases were employed which simulated sabotage, fraud and theft insider threat incidents. Looking towards the future, there are several avenues to advance the ITP area:

- Providing an insider threat taxonomy (malicious and negligent), as each one should have different strategies. For example, negligent insiders who make errors and disregard policies without an intent to do harm for an organization, can be avoided through security awareness and training programs.
- Employing non-technical/psychological factors, such as what is known as big five personality traits (extraversion, agreeableness, openness, conscientiousness and neuroticism) for preventing insider threats proactively. An insider's personality is one of the contributing factors to his/her general motivation. Therefore, the employing of psychological measures (personality traits) can lend a hand in early detection and prevention of insider threat crimes.

- Exploring root causes behind insider threats concerning motives and behaviors to detect malicious intents early for the goal of preventing any possible harmful acts proactively.

Our study highlights opportunities for future research. Practitioners and academicians can draw on to incorporate into the ITP area. We expect the proposed framework will provide rich insights on the insider threat field toward the ultimate goal of devising more comprehensive solutions.

Author Contributions: Conceptualization, R.A.A. and T.A.-S.; formal analysis, T.A.-S.; investigation, R.A.A.; methodology, T.A.-S.; software, R.A.A.; supervision, R.A.A.; writing—original –draft preparation, T.A.-S.; writing—review and editing, R.A.A. and T.A.-S. All authors have read and agreed to the published version of the manuscript.

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

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

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AVPS	Autonomic Violation Prevention System
BCI	Brain–Computer Interface
CDI	Critical Data Items
CERT	Computer Emergency and Response Team
CIT	Concealed Information Test
CPNI	Centre for the Protection of National Infrastructure
CVSS	Common Vulnerability Scoring System
ECA	Event-Condition-Action
IBAC	Intent-Based Access Control
ITP	Insider Threat Prevention
ITPT	Insider Threat Prevention Team
NIST	National Institute of Standards and Technology
RAAC	Risk-Adaptive Access Control
RBAC	Role-Based Access Control
RDI	Regular Data Items

References

1. Yaseen, Q.; Panda, B. Insider threat mitigation: Preventing unauthorized knowledge acquisition. *Int. J. Inf. Secur.* **2012**, *11*, 269–280. [CrossRef]
2. Lee, C.; Iesiev, A.; Usher, M.; Harz, D.; McMillen, D. IBM X-Force Threat Intelligence Index. Available online: https://www.ibm.com/security/data-breach/threat-intelligence (accessed on 7 February 2021).
3. Sinclair, S.; Smith, S.W. Preventative Directions For Insider Threat Mitigation Via Access Control. In *Insider Attack and Cyber Security*; Springer US: Boston, MA, USA, 2008; pp. 165–194. ISBN 978-0-387-77322-3.
4. Claycomb, W.R.; Nicoll, A. Insider threats to cloud computing: Directions for new research challenges. In Proceedings of the International Computer Software and Applications Conference, Izmir, Turkey, 16–20 July 2012; pp. 387–394.
5. Hunker, J.; Probst, C. Insiders and insider threats—an overview of definitions and mitigation techniques. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2011**, *2*, 4–27.
6. Theis, M.; Trzeciak, R.F.; Costa, D.L.; Moore, A.P.; Miller, S.; Cassidy, T. Common Sense Guide to Mitigating Insider Threats, Sixth Edition. Available online: https://doi.org/10.1184/R1/12363665.v1 (accessed on 21 April 2021).
7. Roy Sarkar, K. Assessing insider threats to information security using technical, behavioural and organisational measures. *Inf. Secur. Tech. Rep.* **2010**, *15*, 112–133. [CrossRef]
8. Erdin, E.; Aksu, H.; Uluagac, S.; Vai, M.; Akkaya, K. OS Independent and Hardware-Assisted Insider Threat Detection and Prevention Framework. In Proceedings of the MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 926–932.

9. Almehmadi, A. Micromovement behavior as an intention detection measurement for preventing insider threats. *IEEE Access* **2018**, *6*, 40626–40637. [CrossRef]
10. Silowash, G.J.; Cappelli, D.M.; Moore, A.P.; Trzeciak, R.F.; Shimeall, T.; Flynn, L. *Common Sense Guide to Mitigating Insider Threats*, 4th ed.; Technical Report CMU/SEI-2012-TR-012; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2012.
11. 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 Symposium on Security and Privacy Workshops (SPW 2016), San Jose, CA, USA, 22–26 May 2016; pp. 314–323.
12. Chen, Y.; Nyemba, S.; Malin, B. Detecting anomalous insiders in collaborative information systems. *IEEE Trans. Dependable Secur. Comput.* **2012**, *9*, 332–344. [CrossRef] [PubMed]
13. Gates, C.; Li, N.; Xu, Z.; Chari, S.N.; Molloy, I.; Park, Y. Detecting insider information theft using features from file access logs. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Cham, Switherland, 2014; Volume 8713, pp. 383–400.
14. Axelrad, E.T.; Sticha, P.J.; Brdiczka, O.; Shen, J. A Bayesian network model for predicting insider threats. In Proceedings of the 2013 IEEE Security and Privacy Workshops, San Francisco, CA, USA, 23–24 May 2013; pp. 82–89.
15. 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]
16. Raissi-Dehkordi, M.; Carr, D. A multi-perspective approach to insider threat detection. In Proceedings of the IEEE Military Communications Conference MILCOM, Baltimore, MD, USA, 7–10 November 2011; pp. 1164–1169.
17. Parveen, P.; Weger, Z.R.; Thuraisingham, B.; Hamlen, K.; Khan, L. Supervised learning for insider threat detection using stream mining. In Proceedings of the International Conference on Tools with Artificial Intelligence, Boca Raton, FL, USA, 7–9 November 2011; pp. 1032–1039.
18. Bertacchini, M.; Fierens, P.I. A Survey on Masquerader Detection Approaches. *Cibsi* **2009**, 46–60.
19. Salem, M.B.; Hershkop, S.; Stolfo, S.J. A Survey of Insider Attack Detection Research. *Adv. Inf. Secur.* **2008**, *39*, 69–70.
20. Zeadally, S.; Yu, B.; Jeong, D.H.; Liang, L. Detecting insider threats solutions and trends. *Inf. Secur. J.* **2012**, *21*, 183–192. [CrossRef]
21. 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]
22. 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]
23. Jain, A.K.; Ross, A.; Pankanti, S. Biometrics: A tool for information security. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 125–143. [CrossRef]
24. Babu, B.M.; Bhanu, M.S. Prevention of Insider Attacks by Integrating Behavior Analysis with Risk based Access Control Model to Protect Cloud. In *Procedia Computer Science*; Elsevier: Amsterdam, The Netherlands, 2015; Volume 54, pp. 157–166.
25. Eberz, S.; Rasmussen, K.B.; Lenders, V.; Martinovic, I. Looks Like Eve: Exposing insider threats using eye movement biometrics. *Acm Trans. Priv. Secur.* **2016**, *19*, 1–31. [CrossRef]
26. Rayner, K.; Rotello, C.M.; Stewart, A.J.; Keir, J.; Duffy, S.A. Integrating text and pictorial information: Eye movements when looking at print advertisements. *J. Exp. Psychol. Appl.* **2001**, *7*, 219–226. [CrossRef] [PubMed]
27. Meißner, M.; Oll, J. The Promise of Eye-Tracking Methodology in Organizational Research: A Taxonomy, Review, and Future Avenues. *Organ. Res. Methods* **2019**, *22*, 590–617. [CrossRef]
28. 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]
29. Brunner, C.; Delorme, A.; Makeig, S. Eegla–an Open Source Matlab Toolbox for Electrophysiological Research. *Biomed. Eng. Biomed. Tech.* **2013**, *58*. [CrossRef]
30. Chagarlamudi, M.; Panda, B.; Hu, Y. Insider threat in database systems: Preventing malicious users' activities in databases. In Proceedings of the ITNG 2009-6th International Conference on Information Technology, New Generations, Las Vegas, NV, USA, 27–29 April 2009; pp. 1616–1620.
31. Murata, T. Petri Nets: Properties, Analysis and Applications. *Proc. IEEE* **1989**, *77*, 541–580. [CrossRef]
32. Ragavan, H.; Panda, B. Mitigating malicious updates: Prevention of insider threat to databases. In Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 16–18 July 2013; pp. 781–788.
33. Costante, E.; Fauri, D.; Etalle, S.; den Hartog, J.; Zannone, N. A Hybrid Framework for Data Loss Prevention and Detection. In Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 22–26 May 2016; pp. 324–333.
34. Monal, P.; Parmar, Y.; Valderrama, C. Evaluating synthesis tools for hardware implementation on ZYBO board. In Proceedings of the 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 18–19 July 2017; Volume 2018, pp. 712–716.
35. Al-Shehari, T.; Shahzad, F. Improving Operating System Fingerprinting using Machine Learning Techniques. *Int. J. Comput. Theory Eng.* **2014**, *6*, 57–62. [CrossRef]
36. Al-Shehari, T.; Zhioua, S. An empirical study of web browsers' resistance to traffic analysis and website fingerprinting attacks. *Clust. Comput.* **2018**, *21*, 1917–1931. [CrossRef]

37. Sibai, F.M.; Menascé, D.A. A Scalable Architecture for Countering Network-Centric Insider Threats. Available online: https://cs.gmu.edu/~{}menasce/papers/securware_2011_published.pdf (accessed on 21 April 2021).
38. Sibai, F.M.; Menascé, D.A. Defeating the insider threat via autonomic network capabilities. In Proceedings of the 2011 3rd International Conference on Communication Systems and Networks (COMSNETS 2011), Bangalore, India, 4–8 January 2011; pp. 1–10.
39. Huebscher, M.C.; McCann, J.A. A survey of autonomic computing—degrees, models, and applications. *Acm Comput. Surv.* **2008**, *40*, 1–28. [CrossRef]
40. Baracaldo, N.; Palanisamy, B.; Joshi, J. G-SIR: An insider attack resilient geo-social access control framework. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 84–98. [CrossRef]
41. Madadhain, J.; Fisher, D.; Smyth, P.; White, S.; Boey, Y. Analysis and visualization of network data using JUNG. *J. Stat. Softw.* **2005**, *10*, 1–35.
42. Sawatnatee, A.; Prakancharoen, S. Insider Threat Detection and Prevention Protocol: ITDP. *Int. J. Online Biomed. Eng.* **2021**, *17*, 69. [CrossRef]
43. Tukur, Y.M.; Thakker, D.; Awan, I. Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2020**, e4158. [CrossRef]
44. Alsowail, R.A.; Al-Shehari, T. Empirical detection techniques of insider threat incidents. *IEEE Access* **2020**, *8*, 78385–78402. [CrossRef]
45. Silva, L.A.; Leithardt, V.R.Q.; Rolim, C.O.; González, G.V.; Geyer, C.F.R.; Silva, J.S. PRISER: Managing Notification in Multiples Devices with Data Privacy Support. *Sensors* **2019**, *19*, 3098. [CrossRef]
46. Crown. *Ongoing Personnel Security: A Good Practice Guide*; The Centre for the Protection of National Infrastructure (CPNI): London, UK, 2014.
47. Beebe, N.L.; Rao, V.S. Using situational crime prevention theory to explain the effectiveness of information systems security. In Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, USA, 1 December 2005; Volume 2005, pp. 1–18.
48. Cheng, P.C.; Rohatgi, P.; Keser, C.; Karger, P.A.; Wagner, G.M.; Reninger, A.S. Fuzzy Multi-Level Security: An experiment on quantified risk-adaptive access control. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007; pp. 222–227.
49. Chakraborty, S.; Ray, I. TrustBAC. In *Eleventh ACM Symposium on Access Control Models and Technologies-SACMAT'06*; ACM Press: New York, NY, USA, 2006; Volume 2006, p. 49.
50. Lee, A.J.; Yu, T. Towards a dynamic and composite model of trust. In Proceedings of the ACM Symposium on Access Control Models and Technologies, SACMAT, Stresa, Italy, 3–5 June 2009; ACM Press: New York, NY, USA, 2009; pp. 217–226.
51. Feltus, C.; Petit, M.; Sloman, M. Enhancement of Business IT Alignment by Including Responsibility Components in RBAC. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.178.791&rep=rep1&type=pdf (accessed on 21 April 2021).
52. Saraiva, D.A.F.; Leithardt, V.R.Q.; de Paula, D.; Mendes, A.S.; González, G.V.; Crocker, P. PRISEC: Comparison of symmetric key algorithms for IoT devices. *Sensing* **2019**, *19*, 4312. [CrossRef]
53. Li, H.; Zhang, J.; Sarathy, R. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decis. Support Syst.* **2010**, *48*, 635–645. [CrossRef]
54. Colwill, C. Human factors in information security: The insider threat-Who can you trust these days? *Inf. Secur. Tech. Rep.* **2009**, *14*, 186–196. [CrossRef]
55. Wilson, M.; Hash, J. *Building an Information Technology Security Awareness and Training Program*; NIST: Gaithersburg, MD, USA, 2003; Volume 800.
56. Forrest, S.; Hofmeyr, S.A.; Somayaji, A.; Longstaff, T.A. Sense of self for unix processes. In Proceedings of the Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 6–8 May 1996; IEEE Comput. Soc. Press: Minneapolis, MN, USA, 1996; pp. 120–128.
57. Hofmeyr, S.A.; Forrest, S.; Somayaji, A. Intrusion detection using sequences of system calls. *J. Comput. Secur.* **1998**, *6*, 151–180. [CrossRef]
58. Liao, Y.; Rao Vemuri, V. Using text categorization techniques for intrusion detection. In Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, USA, 1 August 2002; Volume 12, pp. 51–59.
59. Nguyen, N.; Reiher, P.; Kuenning, G.H. Detecting insider threats by monitoring system call activity. In Proceedings of the IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, West Point, NY, USA, 18–20 June 2003; pp. 45–52.
60. Manu, G. Sysenter Based System Call Mechanism in Linux 2.6. Available online: http://articles.manugarg.com/systemcallinlinux2_6.html (accessed on 13 February 2021).
61. Liu, A.; Martin, C.; Hetherington, T.; Matzner, S. A comparison of system call feature representations for insider threat detection. In Proceedings of the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, West Point, NY, USA, 15–17 June 2005; Volume 2005, pp. 340–347.
62. 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 International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing, Boston, MA, USA, 9–11 October 2011; pp. 1102–1110.

63. Magklaras, G.B.; Furnell, S.M. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Comput. Secur.* **2005**, *24*, 371–380. [CrossRef]
64. Spitzner, L. Honeypots: Catching the insider threat. In Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 8–12 December 2003; Volume 2003, pp. 170–179.
65. 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*, 1397–1418. [CrossRef]
66. Bennett, R.J.; Robinson, S.L. Development of a measure of workplace deviance. *J. Appl. Psychol.* **2000**, *85*, 349–360. [CrossRef]
67. Mount, M.; Ilies, R.; Johnson, E. Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. *Pers. Psychol.* **2006**, *59*, 591–622. [CrossRef]
68. Puleo, A.J. *Mitigation Insider Threat Using Human Behavior Influence Models*; Air Force Institute of Technology (U.S.): Wright-Patterson, OH, USA, 2006.
69. Salkind, N. Probabilistic Models for Some Intelligence and Attainment Tests. *Inf. Control* **1961**, *4*, 382.
70. Rogers, M.K. *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study*; University of Manitoba: Winnipeg, MB, Canada, 2001.
71. Moore, A.P.; McIntire, D.; Mundie, D.; Zubrow, D. *Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders*; Software Engineering Institute: Pittsburgh, PA, USA, 2013.
72. Keeney, M.; Kowalski, E.; Cappelli, D.; Moore, A.; Shimeall, T.; Rogers, S. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*; National Threat Assessment Ctr: Washington DC, USA, 2005.
73. Clarke, J. The Coroners Toolkit. Available online: https://www.sans.org/reading-room/whitepapers/incident/paper/651 (accessed on 22 January 2021).
74. Carrier, B. The Sleuth Kit (TSK): Open Source Digital Forensic Tools. Available online: https://www.sleuthkit.org/sleuthkit/docs.php (accessed on 17 February 2021).
75. Kandias, M.; Mylonas, A.; Virvilis, N.; Theoharidou, M.; Gritzalis, D. An Insider Threat Prediction Model. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Heidelberg/Berlin, Germany, 2010; Volume 6264, pp. 26–37. ISBN 3642151515.
76. Clarke, R.V. Opportunity makes the thief. Really? And so what? *Crime Sci.* **2012**, *1*, 3. [CrossRef]
77. Villalon, J.J.; Calvo, R.A. Concept Map Mining: A definition and a framework for its evaluation. In Proceedings of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology-Workshops, Sydney, NSW, Australia, 9–12 December 2008; pp. 357–360.
78. Costa, D.L.; Collins, M.L.; Perl, S.J.; Albrethsen, M.J.; Silowash, G.J.; Spooner, D.L. An ontology for insider threat indicators development and applications. In Proceedings of the CEUR Workshop Proceedings, Rome, Italy, 24–25 November 2014; Volume 1304.
79. Starr, R.R.; Oliveira, J.M.P. de Conceptual Maps as the First Step in an Ontology Construction Method. In Proceedings of the 2010 14th IEEE International Enterprise Distributed Object Computing Conference Workshops, Washington, DC, USA, 25–29 October 2010; pp. 199–206.
80. Poveda-Villalón, M.; Suárez-Figueroa, M.C.; Gómez-Pérez, A. *Validating Ontologies with OOPS! In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7603, pp. 267–281.
81. Antoniou, G.; Van Harmelen, F. OWL: Web Ontology Language. In *SpringerReference*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 67–92.
82. Labs, C. Cyber Threat Intelligence. Available online: https://cyware.com/educational-guides/cyber-threat-intelligence/what-is-cybox-how-do-you-use-a-cybox-object-af90 (accessed on 13 January 2021).
83. Althebyan, Q.; Panda, B. A Knowledge-Base Model for Insider Threat Prediction. In Proceedings of the 2007 IEEE SMC Information Assurance and Security Workshop, West Point, NY, USA, 20–22 June 2007; pp. 239–246.
84. Agrafiotis, I.; Erola, A.; Goldsmith, M.; Creese, S. A Tripwire Grammar for Insider Threat Detection. In Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats; ACM: New York, NY, USA, 2016; pp. 105–108.
85. Bertino, E.; Ghinita, G. Towards mechanisms for detection and prevention of data exfiltration by insiders. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security-ASIACCS '11, Hong Kong, China, 22–24 March 2011; ACM Press: New York, NY, USA, 2011; p. 10.
86. Raskin, V.; Taylor, J.M.; Hempelmann, C.F. Ontological semantic technology for detecting insider threat and social engineering. In Proceedings of the 2010 Workshop on New Security Paradigms-NSPW '10, Concord, CA, USA, 21–23 September 2010; ACM Press: New York, NY, USA, 2010; p. 115.
87. Gritzalis, D.; Stavrou, V.; Kandias, M.; Stergiopoulos, G. Insider Threat: Enhancing BPM through Social Media. In Proceedings of the 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, United Arab Emirates, 30 March–2 April 2014; pp. 1–6.
88. Magklaras, G.; Furnell, S. Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Comput. Secur.* **2001**, *21*, 62–73. [CrossRef]

89. Ali, G.; Shaikh, N.A.; Shaikh, Z.A. Towards an automated multiagent system to monitor user activities against insider threat. In Proceedings of the 2008 International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, 23–24 April 2008; pp. 1–5.
90. Ray, I.; Poolsapassit, N. Using Attack Trees to Identify Malicious Attacks from Authorized Insiders. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3679, pp. 231–246. ISBN 3540289631.
91. Bhilare, D.S.; Ramani, A.K.; Tanwani, S.K. Protecting intellectual property and sensitive information in academic campuses from trusted insiders. In Proceedings of the ACM SIGUCCS fall conference on User services conference-SIGUCCS '09; ACM Press: New York, NY, USA, 2009; p. 99.
92. Park, J.S.; Ho, S.M. Composite Role-Based Monitoring (CRBM) for Countering Insider Threats. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3073, pp. 201–213. ISBN 9783540221258.
93. Buford, J.F.; Lewis, L.; Jakobson, G. Insider threat detection using situation-aware MAS. In Proceedings of the 11th International Conference on Information Fusion, Cologne, Germany, 30 June–3 July 2008; pp. 1–8.
94. Nurse, J.R.C.; Buckley, O.; Legg, P.A.; Goldsmith, M.; Creese, S.; Wright, G.R.T.; Whitty, M. Understanding Insider Threat: A Framework for Characterising Attacks. In Proceedings of the 2014 IEEE Security and Privacy Workshops, San Jose, CA, USA, 17–18 May 2014; Volume 2014, pp. 214–228.
95. Legg, P.; Moffat, N.; Nurse, J.R.C.; Happa, J.; Agrafiotis, I.; Goldsmith, M.; Creese, S. Towards a conceptual model and reasoning structure for insider threat detection. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2013**, *4*, 20–37.