A Multi-Dimension Taxonomy of Insider Threats in Cloud Computing

Mohannad J. Alhanahnah[1], Arshad Jhumka[2] and Sahel Alouneh[3]

[1]*iTrust Center for Research in Cyber Security, Singapore University of Techology and Design, Singapore*
[2]*Department of Computer Science, University of Warwick, Coventry, UK*
[3]*School of Computer Engineering and Information Technology, German Jordanian University, Amman, Jordan*
Email: mohannad_jamal@sutd.edu.sg

Security is considered a significant deficiency in cloud computing, and insider threats problem exacerbate security concerns in the cloud. In addition to that, cloud computing is very complex by itself, because it encompasses numerous technologies and concepts. Apparently, overcoming these challenges requires substantial efforts from information security researchers to develop powerful mitigation solutions for this emerging problem. This entails developing a taxonomy of insider threats in cloud environments encompassing all potential abnormal activities in the cloud, and can be useful for conducting security assessment. This paper describes the first phase of an ongoing research to develop a framework for mitigating insider threats in cloud computing environments. Primarily, it presents a multidimensional taxonomy of insider threats in cloud computing, and demonstrates its viability. The taxonomy provides a fundamental understanding for this complicated problem by identifying five dimensions, it also supports security engineers in identifying hidden paths, thus determining proper countermeasures, and presents a guidance covers all bounders of insiders threats issue in clouds, hence it facilitates researchers' endeavours in tackling this problem. For instance, according to the hierarchical taxonomy, clearly many significant issues exist in public cloud, while conventional insider mitigation solutions can be used in private clouds. Finally, the taxonomy assists in identifying future research directions in this emerging area.

Keywords: Insider Threats; Taxonomy; Cloud Computing

Received 00 Month Year; revised 00 Month Year

1. INTRODUCTION AND MOTIVATION

The usage of cloud computing is rapidly growing; however, security concern is the main obstacle to this growth [1]. According to a recent survey conducted by RightScale in 2015, [2] security was the first significant cloud challenge, and the concern about this challenge has increased, compared to the survey which was conducted in the previous year. Moreover, according to the INFOSEC Research Council [3], insider threats provide some very hard challenges. In the cloud computing era, this insider threat problem has started to affect this area too. This observation is supported by the Cloud Security Alliance reports [4,5],as they list insider threats among the top threats to cloud computing.

Despite the increased awareness of internal threats at both the enterprise level and in the cloud computing infrastructure, little research work has been done in this space for classifying and addressing this issue. Initially, this was due to the absence of an agreement on the definition of insiders and their taxonomies. Therefore, there is a pressing need for developing relevant and accurate taxonomies of insider threats to contribute towards the understanding of this complex issue and to help towards developing techniques to combat the insider threat problems. Along this line of research, Magklaras' PhD thesis [6] developed a taxonomy of insider threat while developing a language for detecting and predicting insider attacks.

Developing attack taxonomies is the process of classifying attacks in categories based on common characteristics, i.e., identifying the common patterns of different attacks. This provides a more granular understanding about the "components" of each attack and improves the discovery of hidden vulnerabilities [7]. Thus, it was suggested at a RAND workshop that the development of an insider threat taxonomy

[8] would be important because this underpins the understanding and building of models for tackling this intricate problem. Therefore, at the next workshop, taxonomies have been presented, based on different factors (such as observables, insider actions and so on [9]. The workshop described different taxonomies for each factor and the workshop also made an additional taxonomy by mapping insider actions taxonomy and vulnerabilities and exploits. Attacks could be classified based on several criteria such as the impact, cause or fix [7]. Another dimension of classification considers the target of the attack, e.g., attacks targeting financial institutions, the location of the attack, e.g., external attacks & internal attacks, or the scope of the attack. Igure & Williams [7] described general properties and guidelines for developing taxonomies, with the most important among these being 1) that a hierarchical taxonomy is better than linear classification to obtain a firm understanding, 2) the taxonomy needs to target specific applications, i.e., operating system attacks are different than network or cryptographic attacks.

In fact, very few taxonomies of insider threats in the cloud computing environment have been developed in the literature, where the main intention of the existing works was not mainly for developing a classification. These existing taxonomies are thus limited to a specific issue in the cloud and do not cover all aspects of this emerging problem. These taxonomies are also not hierarchical and do not follow the guidelines for developing taxonomies. On the other hand, we propose a multi-dimensional, hierarchical taxonomy that covers fundamental aspects of insider threats in a cloud computing environment to provide an overall insight into the insider threat security problem. Further, as the taxonomy being proposed focuses on high-level concepts (rather than implementation details), multiple attacks can be captured and be attributed to a given attack class. In this way, the taxonomy becomes dynamic in the sense that, when new insider attacks emerge, they can be analyzed at a high level and be assessed on the overall impact they have on the system. Specifically, the taxonomy will allow attacks to be represented using signatures and many attacks may carry the same signature, meaning that they *may* be handled using similar mechanisms.

The contributions of this work are a) identifying the dimensions of the taxonomy. Section 3 introduces this contribution and describes it in a formal way b) converting the dimensions into the hierarchy form. Section 4 maps the literature surveyed and the taxonomy dimensions in order to present the taxonomy in hierarchy structure c) presenting the viability of the taxonomy d) describing future research directions in this area. Section 5 describes in detail the last three contributions.

2. TERMINOLOGY

In this section, we briefly explain the relevant concepts of cloud computing and insider threats that underpin the taxonomy that is developed in this paper.

Cloud computing is a distributed computing model that comprises all the necessary computing resources to store, manage and process data to deliver services [10]. Section 3 describes in detail the various types of cloud deployment and cloud services. We consider a cloud computing environment as one that provides for elastic resource provisioning. This tremendously reduces operational and administrative costs and potentially saves time. Insider threats are attacks that are carried out by individuals who possess the inside knowledge of the system and they have the required permissions to access the system [1], i.e., the attacks are carried out by inside users or insiders.

Therefore, in this paper, we define insiders as those trusted and authorized users who misuse the given permissions. Insiders are divided into two types: malicious insiders and non-malicious insiders [11], the former is an authorized user who intentionally misuses the granted access. This in turn can cause a violation of the confidentiality, integrity or availability properties of the organization data or information systems [12, 13]. In a similar way, insiders pose the similar harm to the cloud infrastructure, but the employed techniques are different than the approaches utilized in traditional environments. This has significant influences on the types of countermeasures used to mitigate these threats. Thus, the identification of different classes of insider threats in cloud computing environments is imperative, for building the fundamental knowledge about both the vulnerabilities and their respective countermeasures.

Our taxonomy can cover both types of insider threats (malicious and non-malicious) because the focus of this work is on the properties of the attack, i.e., the impact the attack has on the system. This can be represented using the five dimensions that are proposed in the next section.

3. DIMENSIONS OF THE TAXONOMY

At the first stage, we identify the properties which should be provided by the taxonomy, and according to these, the five dimensions have been selected. The criteria are summarized as follows:

1. Reduction of the confusion and overlapping between categories as much as possible.
2. Description of the fundamental concepts of insider threats and cloud computing.
3. Maintainance of the elasticity, effectiveness and expandability features. Therefore, the taxonomy provides an abstract insight into insider threats in the cloud and, at the same time, it can be adapted in the future.

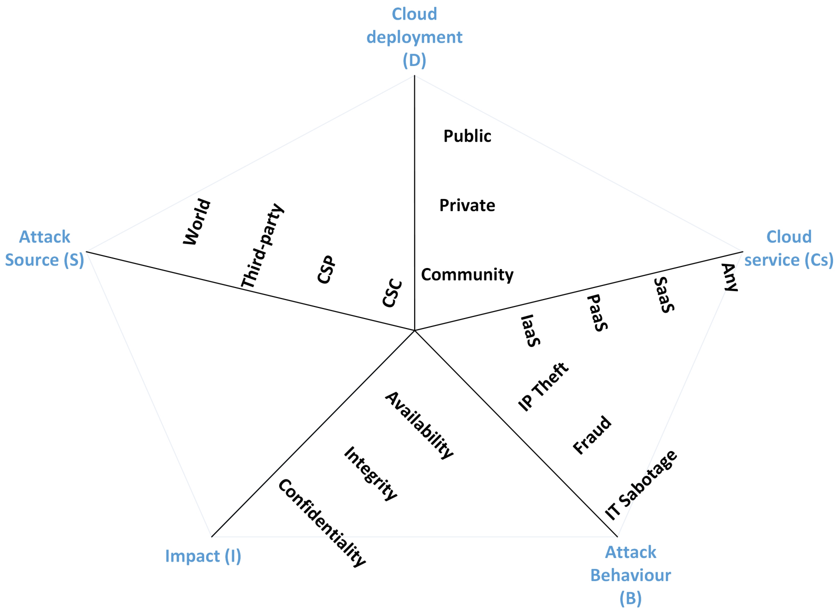

FIGURE 1. Dimensions of the taxonomy

Additionally, we followed the guidelines for developing a taxonomy, presented in [7], which was previously explained in Section 1. Accordingly, the paper identifies five dimensions for building the taxonomy, as depicted in Figure 1. The five dimensions identified are:

1. Cloud deployment,
2. Source of the attack,
3. Attack impact,
4. Insider attack approach, and
5. Susceptible cloud service.

We detail each dimension in the next coming few sections.

3.1. Cloud deployment (D)

In general, there are three forms of cloud deployment, namely public, private and community clouds. The conjunction of those previous types of cloud systems forms a hybrid cloud [10]. When the cloud is called public, this means that services are handled over an open public network. Therefore, in public cloud deployment, the Cloud Service Provider (CSP) owns and controls the resources and these resources are shared between Cloud Service Consumers (CSC). Although the CSP hosts the CSC's data, this does not mean that the CSP become the owner of the hosted data.

On the other hand, the cloud system is called a private cloud system when all resources and infrastructure are operated by a single organisation and the system is dedicated to that single organization and within its premises. However, from a security point of view, this does not imply that a private cloud system is more secure than a public cloud system. Rather, it means that security threats to the public cloud system may not apply to private clouds.

Finally, a community cloud model is similar to the public cloud model except for some differences, such as the access, which is limited here to a specific community of cloud members or users. Also, it is possible for a community cloud to be owned by more than one community member or by a third party. In other words, a cloud community deployment shares some non-cloud resources between entities (third-parties), and therefore there is no dedicated CSP which possesses cloud resources. Figure 2 depicts the relation between the type of cloud deployment and its threat exposure.

In our taxonomy only public, private and community clouds are considered. Since hybrid cloud is a mixture of the previous types, thus it inherits the security issues of the other types of cloud deployments [14].

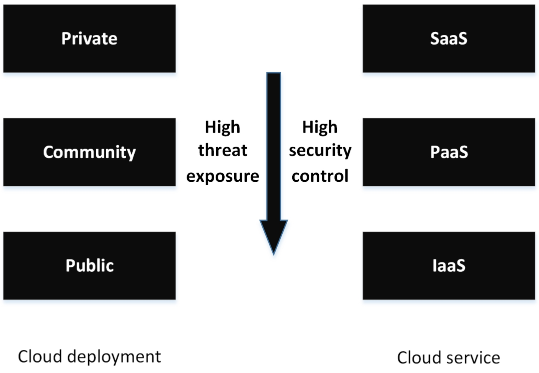

FIGURE 2. Security level based on cloud service and cloud deployment

3.2. Attack Source (S)

Cloud deployment significantly influences attack sources. In general, in private clouds, insiders from company itself, therefore the company employees constitute the source of insider attacks. While in public clouds, there are two sources of insider attacks, insiders from the CSC side and insiders from the provider side, particularly CSP employees. Also, insiders from CSC party and insiders from third-parties are attack sources in community cloud. Finally, world is a common attack source between the types of cloud deployment, it includes anyone managed to gain unauthorized access, and impersonate as insider. Hence, Duncan et al. [13] consider advanced persistent threats (APT) as a potential source of insider threats, though APTs are initiated by external attackers, because at some phases the APT acts as authorized user for making a damage or performing data exfiltration [15].

3.3. Attack Behavior (B)

CERT at Carnegie Mellon University (CMU) categories insider threats based on the behaviour of the insider attack [12]. Three out of four categories will be considered for the taxonomy purposes: Intellectual Property (IP) theft, Fraud and IT sabotage. Whereas CERT called the fourth category espionage. While in another report, CERT describes a new category (miscellaneous), which includes behavioral patterns that do not fall in the other three types. They also keep the aforementioned three categories, and link espionage to IT sabotage [16]. In fact, the difference between espionage and IT sabotage has been investigated in [17], and the result was that there is no distinction between espionage and IT sabotage, even same or simliar countermeasures can be used for mitigating both categories. Furthermore, espionage can be considered as a motivation for committing insider attacks [18]. Also, by referring back to the repercussions of Hanssens espionage incident which was the disclosure of secret information to former Soviet Union [19]. Hence, espionage is considered as IT sabotage in our taxonomy.

Other names of IP theft attack are data exfiltration or data leakage [20, 21]. In essence, these three categories of insider attacks are generic, and encompass many attacks, for instance, insider might carry out identity theft before committing financial fraud attacks.

3.4. Impact (I)

An attack can have several consequences on a system. A malware such as a cryptovirus may affect the integrity of the system as well as making part of it unavailable. In effect, several attacks will have several impacts on the system, i.e., they will cause violation of different security properties. When considered in this fashion, several attacks may end up being deemed “similar”. To avoid such cases, we focus on the direct impact of insider threats on systems, i.e., the first observable impact is the security properties. According to Silowash et al. [16], fraud is any unauthorized manipulation, deletion or addition of data, where fraud attacks break data integrity. Also, they define IT sabotage as the usage of IT to establish and direct a harm, which in the first place affects, the availability. While the immediate consequence of IP theft attack is the breaching of confidentiality, because the forefront action of this attack is a disclosure of information. It might be that these attacks can have other consequences, but the reason for focusing on the first or direct impact is practicing the early containment of attacks, in order to avoid and alleviate additional damaging consequences, which is an ultimate goal. In fact, this can encourage researchers and security engineers to capture initial abnormal implications for mitigating the attacks at early stages.

3.5. Cloud service (Cs)

Ordinarily, the main cloud services are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each service has its own security concerns, for instance usually end users use SaaS applications (i.e. Gmail), which is developed through PaaS APIs (i.e. Google App Engine), which are hosted on IaaS. Figure 2 depicts the relation between a cloud service and the level of security control. Through this dimension we can build some elicitations, speculate which kind of applications are dealing with, and determine the level of control possessed by the insider. IaaS specifies the configuration of storage, hypervisors and Virtual Machines (VMs), whereas PaaS is used for developing different applications using the provided API, but SaaS utilizes cloud applications. We noticed that performing insider attacks at the IaaS and PaaS levels require high skilled insiders. As explained later, the demonstrated attack in [22] requires professional skills

3.6. Formalizing the taxonomy

We propose the following formalization for representing our taxonomy, this opens the horizon for future utilization and development of our taxonomy. Also this formalization assisted us for making a comparision between our taxonomy and the taxonomies presented in the literature.

The taxonomy and its five dimensions can be formalized using the approach:

Taxonomy T is described by T= <D, S, I, B, Cs> where:

- Cloud deployment (D) $\in$ {public, private, community}
- Source of the attack (S) $\in$ {CSC, CSP, third-party, world}
- Impact of the attack (I) $\in$ {availability, integrity, confidentiality}

- Insider attack behavior (B) ∈ {IP theft, fraud, IT sabotage}
- Cloud Service (Cs) ∈ {SaaS, PaaS, IaaS, any}

For example T1 = <public, CSC, availability, IT sabotage, IaaS>, this taxonomy describes an insider attack in public cloud, originated from the data CSC side, affects the availability, and performed from IaaS environment. This formalization method will be used in subsection 5.3 for showing that the taxonomies developed in the literature can fit in our taxonomy.

4. HIERARCHICAL STRUCTURE OF THE TAXONOMY

According to the proposed five dimensions, and the literature surveyed, Figure 3 crystallizes the taxonomy in a hierarchal based. The five dimensions have been utilized for building the taxonomy hierarchy as follows: (1) cloud deployment (2) source of the insider attack (3) attack impact (4) insider attack behaviour (5) cloud service. Such hierarchy provides the fundamental criteria, and shows the relation between them. While the last layer provides examples of insider attacks according to the upper layers.

The first layer of this taxonomy relies on the Cloud Deployment. Accordingly, this layer provides general directions, for example in Community cloud, it is expected that several entities (third-parties) share the cloud resources, and highly probable these entities are implementing federation techniques for authenticating users of each entity. But in private clouds, all resources are owned by the company itself, and the CSC holds a full control over its data. While in public clouds, all resources are owned by the CSP, but these resources are shared between CSCs; but, in this case there is no need to implement federation techniques. Hence, security concerns are varies according to the cloud deployment.

The second layer divides the attacks based on the source of the attack. There are several sources of attack in cloud environments especially public and community clouds, for example insiders can be from the CSC side or the CSP in public clouds. But users from member companies in the community cloud can pose potential insider threats. While insiders in private clouds are in general under the control of the organizations, thus potential insider threats can be treated as standard insider attacks. This layer specifies sources of insider attacks.

According to the impact of the attack, insider threats have been classified in the third layer. Indeed, each attacks could have many consequences. As shown in Figure 3, insider attacks from the CSP side affect the confidentiality and availability. This directs the CSP organization about the mitigation techniques which are required to be implemented. On the other hand, the CSC should seriously seek integrity protection solutions, in addition to the implementation of confidentiality and availability solutions. This layer has a reflection on the fourth layer, which specifies categories of insider attacks that violate the security triangle.

In the light of the previous layer, the fourth layer utilizes CMU's classification of insider threats (IP theft, Fraud, and IT sabotage). Subsection 3.3 mentions the immediate impact of the CMU insider threat categories. Therefore, CSP employees do not pose fraud attacks, but they can carry out data exfiltration and IT sabotage attacks. Where authorized users in private cloud can commit all three types of insider threats. Furthermore, this layer and next layers unveil the dearth of research in this field, including lack in the availability of substantial volume of documented insider incidents, especially in public and community clouds (private cloud insider attacks considered as standard insider attacks but with the utilization of different means).

The fifth layer narrows down to specify the type of cloud service. In fact, according to the collected insider threat incidents, which are presented in Section 5.1, we think the cloud service does not have significant influences on insider threats in private and community clouds, as long as the insider possesses the access credentials and can perform the attack regardless of the type of cloud deployment. Since resources (asset and data) are owned only by the organization in a private cloud, thus the insider can perform the attack at IaaS, PaaS or SaaS. While in the community cloud, resources are shared between the parties. Also in public cloud, each cloud service specifies the control level of the CSC, where the CSP possesses the ultimate control. Therefore, the cloud deployment could influence the attacks that the insider can perform.

Though both CSP side and CSC side pose IP theft attack, but the cloud service influences the strategy which will be used by each party for performing this attack. For example, since the CSP hosts the cloud service (regardless its of type, because all types rely on IaaS), hence it has higher control compare to the CSC, so CSP insiders can attack hypervisors, network or storage devices, even they have physical access, but CSC's insiders have limited control and cannot easily attack these assets.

Accordingly, as stated at the end of Figure 3, below the taxonomy, that traditional mitigation solutions (e.g. monitoring) for insider attacks in public and community clouds are insufficient, and should be adopted based on the previously described circumstances. As will be described later in the future work section. Where in private cloud computing some conventional mitigation techniques can be utilized (e.g. audit).

In general, customers of IaaS cloud have superior control than PaaS and SaaS, and the same rule implies between PaaS and SaaS, so as we move to the application level, the customers control is diminished as depicted in Figure 2. Similarly, the achieved security in private cloud is greater than community and public, in other words, as we move towards publicity, threat

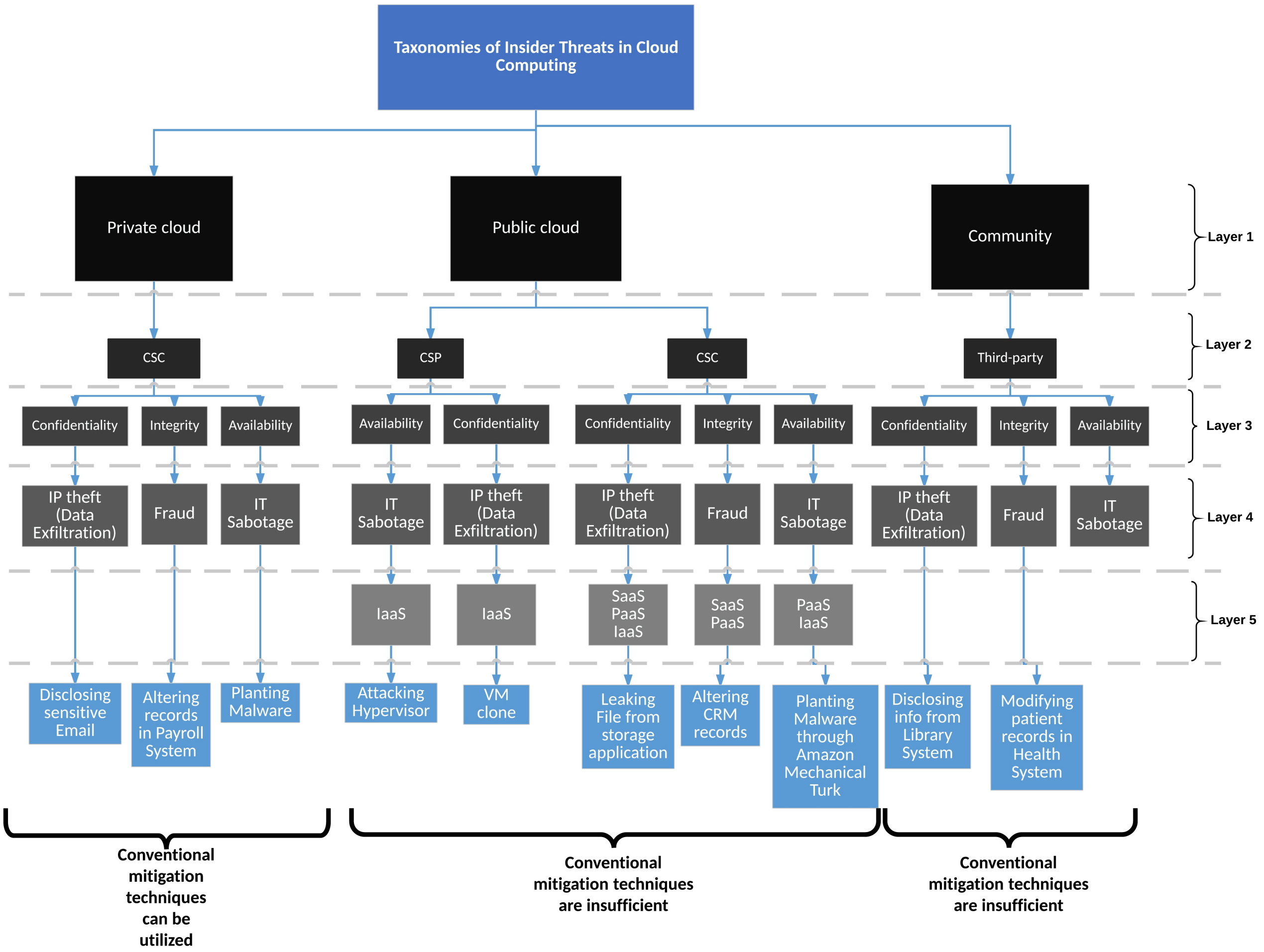
Taxonomies of Insider Threats in Cloud Computing
Private cloud
Public cloud
Community
Layer 1
CSC
CSP
CSC
Third-party
Layer 2
Confidentiality
Integrity
Availability
Availability
Confidentiality
Confidentiality
Integrity
Availability
Confidentiality
Integrity
Availability
Layer 3
IP theft (Data Exfiltration)
Fraud
IT Sabotage
IT Sabotage
IP theft (Data Exfiltration)
IP theft (Data Exfiltration)
Fraud
IT Sabotage
IP theft (Data Exfiltration)
Fraud
IT Sabotage
Layer 4
IaaS
IaaS
SaaS PaaS IaaS
SaaS PaaS
PaaS IaaS
Layer 5
Disclosing sensitive Email
Altering records in Payroll System
Planting Malware
Attacking Hypervisor
VM clone
Leaking File from storage application
Altering CRM records
Planting Malware through Amazon Mechanical Turk
Disclosing info from Library System
Modifying patient records in Health System
Conventional mitigation techniques can be utilized
Conventional mitigation techniques are insufficient
Conventional mitigation techniques are insufficient

FIGURE 3. Hierarchical taxonomy

exposure is increased [10].

Noticeably, PaaS services are susceptible for the three types of insider attacks, because it is an intermediated layer between IaaS and SaaS, however, this does not mean the techniques that are used to carry out IP theft attacks in SaaS are the same as in PaaS, also as emphasized earlier, this does not imply same attack can be committed by the insiders from each party. In other words, IP theft attacks from PaaS CSC are different than IP theft attacks from PaaS CSP. According to the hierarchy, IP theft attacks are common between all cloud services, with the consideration of various approaches are taken in each cloud service, for example as for leaking information in IaaS, the insider may target the hypervisor or storage, while in PaaS, the application itself will be targeted, and in SaaS, simply download actions, or spoofing techniques may be utilized. This could explain why majority of the surveyed publications are confined in proposing solutions against IP theft attacks/data leakage as described in the next section.

5. CASE STUDY AND VIABILITY OF THE TAXONOMY

In a nutshell, this section shows evident insider threat examples (the last layer of the taxonomy), which distinguishes the difference in the layers of the proposed taxonomy.

5.1. Demonstrated insider attacks in the cloud

This subsection shows the conformity of the proposed taxonomy with the insider attacks demonstrated in the literature. Consequently, this substantiates the meaningful results of developing taxonomy of insider attacks.

Table 1 summarizes the attacks. Rocha & Correia [22] demonstrate four insider attacks in IaaS for accessing users data, hence the ability to leak confidential and IP data. Likewise, three malicious insider attacks in IaaS have been demonstrated for proofing the ability of the malicious insider accessing and extracting users data [23]. Also, Duncan et al. [13] present several examples, where the administrator can employ forensic techniques for extracting sensitive information (i.e. usernames, passwords) from a VM on

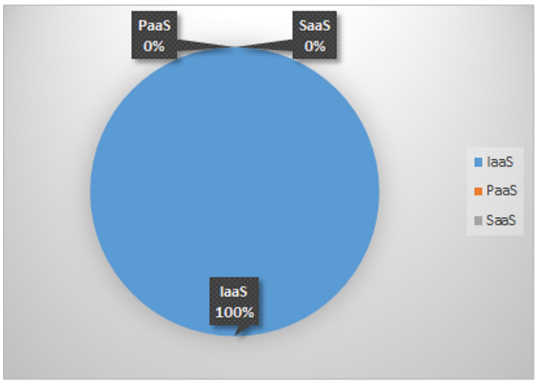

FIGURE 4. Distribution of the incidents based on cloud service

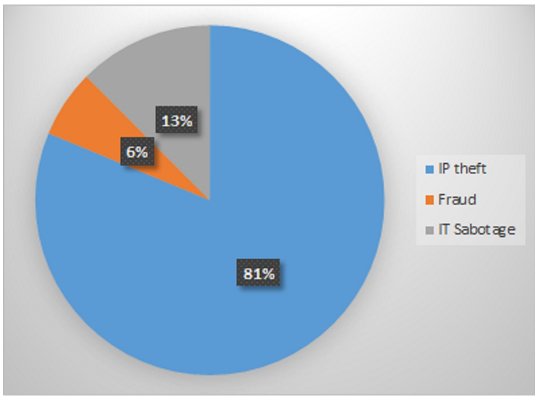

FIGURE 5. Distribution of the incidents based on insider attack behaviour

the CSP side in IaaS.

Moreover, in IaaS, especially public cloud, since cloud resources are shared between CSCs, there is a possibility for a conflict of interest, which leads to information disclosure [24]. Wei et. al. [25] present cloud app store scenarios of customers who plant Malware on their VMs before publishing them. In cloud app store environments there are three entities: one CSP entity and two CSCs entities (Publisher and Retriever). In fact, this behaviour has negative implications on the confidentiality and integrity of the information hosted on the VM. Since the infected VM could be shared with other customers, or could be employed for infecting the VMs located in the same network. Therefore, two entities are affected by this case, the CSP and the retriever customer. Other attacks also can be performed by one customer against other customers' VMs [26]. Initially, the malicious customer performs reconnaissance check for verifying the existence of his VM and the victim's VM on the same physical machine. Subsequently, the malicious CSC can extract cryptographic keys or perform DoS attacks against other CSCs [26].

Furthermore, mitigation techniques for fraud attacks have been described in SaaS private clouds, in addition to unauthorized access activities [28]. In the surveyed literature, we have not found insider attacks that have been shown in PaaS, but this does not mean PaaS is immune against insider threats. For example Amazon Mechanical Turk (AMT) allows researchers and companies recruiting people for performing some tasks[29]. This valuable PaaS cloud service might be utilized maliciously for committing insider attacks are in layer three of the taxonomy, especially when workers are requested to perform external hits, this example can be considered as a potential insider attack in PaaS. Figure 4 and Figure 5 summarizes using pie diagram the distribution of the insider threat incidents demonstrated in the literature based on cloud service and insider attack behaviour respectively.

5.2. How to use the taxonomy

The taxonomy can be utilized for defining the appropriate approach for mitigating insider attacks. In other words, similar approaches can be used for mitigating insider attacks that share the same dimensions (the attacks that have the same signature). For instance, according to the proposed taxonomy, IT sabotage and espionage are considered the same attack, therefore, similar approaches can be used for mitigating these attacks. This has been shown in [17], which recommends performing security audit, since insiders in both attacks have gone beyond the need to know principle. Moreover, Malicious Hypervisor attack described in [13] and virtual machine relocation attack presented in [22] share the same signature <**public, CSP, Confidentiality, IP Theft, IaaS**>, thus a mitigation solution can be implemented at the hypervisor level (e.g. access control or Provenance Tracking [25]).

On the other hand, as presented in Table 1, though the same attack presented in [25], but it has different signatures, due to the diversity of its consequences. The first signature is <**public, CSC, Confidentiality, IP Theft, IaaS**>, while the second signature is <**public, CSC, Integrity, Fraud, IaaS**>. Accordingly, different mitigation solutions are required to be implemented. The taxonomy has the ability to capture this variation, because it has been designed based on multidimensional approach.

Also as we are heading downwards in the taxonomy, we are eliminating and specifying the factors and technical aspects which should be ignored or considered while developing the mitigation solution, and conducting security assessment. This increases the effectiveness of the proposed taxonomies. For example, if the insider attack violates the integrity in IaaS environments, then the company should think about integrity solutions on the storage level for example, while if the violation was in PaaS platform, then the company should deploy integrity preserving solutions at the application level instead of the storage level. Also, the CSC in public cloud

TABLE 1. Summary of demonstrated insider attacks in the cloud, and their compliance with the proposed taxonomy

Reference	Attack/vulnerability	Compliance with the developed taxonomy				
		Layer1	Layer2	Layer3	Layer4	Layer5
[22]	Clear text passwords in memory snapshots	Public	CSP	Confidentiality	IP theft	IaaS
	Obtaining private keys using memory snapshots	Public	CSP	Confidentiality	IP theft	IaaS
	Extracting confidential data from the hard disk	Public	CSP	Confidentiality	IP theft	IaaS
	Virtual machine relocation	Public	CSP	Confidentiality	IP theft	IaaS
[23]	Memory Dump Scanning	Public	CSP	Confidentiality	IP theft	IaaS
	Public Templates Poisoning	Public	CSP	Confidentiality	IP theft	IaaS
	Snapshot Cracking	Public	CSP	Confidentiality	IP theft	IaaS
[24]	Conflict-of-interest	Public	CSP	Confidentiality	IP theft	IaaS
[13]	IaaS Virtual Machine Cloning	Public	CSP	Confidentiality	IP theft	IaaS
	DaaS File Copy	Public	CSP	Confidentiality	IP theft	IaaS
	Malicious Hypervisor	Public	CSP	Confidentiality	IP theft	IaaS
	Denial Of Service (DOS)	Public	CSP	Availability	IT sabotage	IaaS
[25]	Planting Malware on the VM	Public	CSC	Confidentiality	IP theft	IaaS
	Planting Malware on the VM	Public	CSC	Integrity	Fraud	IaaS
[26]	Cache-based side channels	Public	CSC	Confidentiality	IP theft	IaaS
	Denial Of Service (DOS)	Public	CSC	Availability	IT sabotage	IaaS

TABLE 2. Summary of exist taxonomies in the literature

Reference	Dimension taxonomy				
	Cloud deployment	Source	Attack Behavior	Impact	Cloud service
[1]	$\{public\}$	$\{CSP, CSC\}$	ϕ	ϕ	ϕ
[13]	ϕ	$\{world, third-party, CSP, CSC\}$	ϕ	ϕ	ϕ
[27]	$\{public\}$	$\{CSP, CSC\}$	ϕ	ϕ	ϕ

can not deploy any solution if the attack from the CSP side, as the CSC has no control over the CSP infrastructure. Hence, the taxonomy works as a road map for specifying the ability to adopt or reuse existing solutions. This facilitates the security engineers mission in implementing the appropriate mitigation approaches.

Another flexibility feature of this taxonomy is the ability for further classification after layer number five, additionally it provides a powerful guidance for combining similar attack under one umbrella and foreseeing potential internal threats. Furthermore, this taxonomy can be integrated with threats modeling frameworks such STRIDE[30], because the listed insider attacks in the fourth layer fall under the STRIDE categories, namely Spoofing, Tampering, and Information Disclosure.

As exemplified in Table 1, the vast majority of demonstrated insider attacks can be expressed using the proposed formula t= <public, CSP, confidentiality, IP theft, IaaS>. This could be due to the high potential for performing IP theft attacks from the CSP side, especially by the administrators (they have massive level of control), and the lower complexity in comparison with IT sabotage and fraud attacks.

5.3. Locating related works in the Taxonomy

As intimated earlier, information about insider threats in cloud computing is not widely available. Therefore, the endeavours developing taxonomies in this area are limited. Table 2 summarizes the taxonomy available in the literature, and places them on our taxonomy.

5.4. Future Research Directions

This subsection is aiming to highlight research trends in this area, and identify major techniques can support sorting out this issue. We will employ the dimensions and hierarchical structure of the taxonomy for achieving this goal.

- Access Control: this topic is broadly discussed in the literature, but there are many limitations when it comes to mitigating insider attacks. Crampton & Huth [31] discuss the limitation of detecting insiders using access control techniques, they emphasised the insufficiency of relying only on static access and predefined access rules, and they show the press need for considering the context in the access rules. Also we recommend investigating dynamic access control approaches such as Attribute-Base Access Control (ABAC), Risk based adaptive access control [32], and Trust based access control [33]. However, these approaches need be adopted for cloud environments.
- Trust: many works consider trust as one of the significant issues to the cloud [34–36]. Also, as mentioned in the previous point employing trust in access control can assist in mitigating insider attacks. Therefore, according to the presented

taxonomy, we proposed to trust paradigms for public clouds. Firstly, developing mechanisms for evaluating the trust level of CSP administrators, this approach assists the CSP in detecting malicious administrators. Secondly, consider the CSP or CSC as insiders, because each party constitutes a potential threat to the other party.

6. LIMITATIONS IN THE STATE-OF-THE-ART

This section does not aim to comment on the value of these researches, because developing a taxonomy was not their main concern. Claycomb & Nicoll [1] describe three categories of insider threats in the cloud based on insider type, namely the rogue cloud provider administrator, the employee in the victim organization that exploits cloud weaknesses for unauthorized access, and the insider who uses cloud resources to carry out attacks against the companys local IT infrastructure. Then, only under the rouge administrator, four types of administrators (system, application, virtual image and hosting company administrator) have been allocated with their associated potential attacks. Majority of these administrator categories fall under the CSP, but for instance application administrators are common between CSP and the CSC, therefore, this taxonomy covers also public cloud. The taxonomy can be formalized t1= <public, {CSP, CSC}, ϕ, ϕ, ϕ>. Though the proposed categories pose the highest risk due to the high privilege the administrators possess, but these categories do not manifest all aspects of insider attacks against the cloud, they are not on a multi-dimension form and only based on the insider type.

Duncan et al. [13] built a holistic view of insiders in the cloud ecosystem. This holistic view describes insider attacks from insider location/source and data location. Indeed, sources of the insider attacks have been discussed in detail, namely, APT, familial insiders, benign insider coercion, client side, ISP and third-parties. All these sources come under the defined set of attack sources world, third-party, CSP, CSC. But the location of data which either in motion or at rest was discussed briefly. The taxonomy can be expressed t2=<ϕ, {world, third-party, CSP, CSC}, ϕ, ϕ, ϕ>. However, the classification is not systematic, does not provide an insight and clear perception and is linear not on multidimensional base.

Kandias et al. [24] describe two categories of insider threat, malicious insider activities either on the CSP side or the outsourcer side. Indeed, this classification can fit only for public cloud, does not consider technical aspects and concerns in each types of cloud deployment and services; hence this approach does not break down the intricacies of insider threats in cloud environments. On the other hand, classification based on the attack source is implicitly considered in the first layer of the proposed taxonomy, and explicitly defined in the second layer, therefore it is expressed t3=<public, {CSP, CSC}, ϕ, ϕ, ϕ>.

The benefits have been shown in this section about our taxonomy, but also the taxonomy can be used as a tool for framing future research and placing current research. Therefore, researchers can use it for identifying potential aspects that will be considered in their work.

7. CONCLUSION AND FUTURE WORK

In this paper, we propose a novel taxonomy of insider threats for the cloud computing environment. The importance of such a taxonomy was recognised way back to 2000 by RAND. Indeed, developing the taxonomy was a strenuous mission, because of the scarcity of reported insider threat incidents, especially in community clouds. This work has been significantly influenced by the availability of research in this area, where the taxonomy evinces major shortcomings in the literature about insider threats in cloud environments. Hence, further work can be conducted in this research area. The contributions provided in this paper are:

- According to the taxonomy hierarchy, there are no fraud attacks in public cloud from CSP insiders. Thus, it is highly recommended to investigate this issue.
- In public clouds, the cloud service does not have impact while specifying potential mitigation solutions, because the data are physically stored on the CSP site regardless the type of the subscribed cloud service.
- The taxonomy shows its applicability to classify real world and the demonstrated insider attacks against the cloud. In tandem, we demonstrate the taxonomy ability to frame existing research. Hence, we argue that this taxonomy provides a better understanding of all aspects about insider threats in cloud computing, this underpinning ongoing research for addressing this problem.
- Researchers can use the taxonomy as a framework for identifying all attributes that will be considered in their work.
- The taxonomy can be utilized for conducting security assessment, and discover hidden areas.

A potential future work is to expand the dimension of the taxonomy, with more attention to community clouds. Also, the development of an application to include all possible types of insider threats in a cloud computing environment will definitely offer a big contribution towards risk management, security assessment and modelling of insider threats (i.e. developing attack patters as presented in [37]). Furthermore, we will also perform additional experiments for further validation of the taxonomy. Another major area for further investigation is the potential deployment of the taxonomy for actual risk assessment of cloud systems. Given that the taxonomy does not focus on detailed system implementations or specific nature of attacks (rather it focuses at an abstract level), it offers support for such risk assessment analysis.

REFERENCES

[1] Claycomb, W. R. and Nicoll, A. (2012) Insider Threats to Cloud Computing: Directions for New Research Challenges. *2012 IEEE 36th Annual Computer Software and Applications Conference*, July, pp. 387–394. IEEE.

[2] RightScale (2015) RightScal. Technical report.

[3] INFOSEC Research Council (2005). Hard Problem List. Accessed: 2014-12-15.

[4] Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Technical Report March. Cloud Security Alliance. Accessed: 2014-12-15.

[5] Cloud Security Alliance (2013) The Notorious Nine Cloud Computing Top Threats in 2013. Technical Report February. Cloud Security Alliance. Accessed: 2014-12-15.

[6] Magklaras, G. V. (2011) An Insider Misuse Threat Detection and Prediction Language. Phd thesis University of Plymouth.

[7] Igure, V. M. and Williams, R. D. (2008) Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys and Tutorials*, **10**, 6–19.

[8] Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., and Van Wyk, K. (2000) Research on Mitigating the Insider Threat to Information Systems - #2. *RAND Conference Proceedings*.

[9] Brackney, R. and Anderson, R. (2004) Understanding the Insider Threat. *Proceedings of the March 2004 Workshop* 137.

[10] Winkler, J. R. V. (2011) *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Syngress Publishing.

[11] Greitzer, F., Strozer, J., Cohen, S., Moore, A., Mundie, D., and Cowley, J. (2014) Analysis of unintentional insider threats deriving from social engineering exploits. *Security and Privacy Workshops (SPW), 2014 IEEE*, May, pp. 236–250.

[12] Flynn, L., Porter, G., and DiFatta, C. (2014) Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase II, Expanded Analysis and Recommendations. Technical Report CMU/SEI-2013-TN-030. Carnegie Mellon University.

[13] Duncan, A. J., Creese, S., and Goldsmith, M. (2012) Insider attacks in cloud computing. *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Washington, DC, USA TRUSTCOM '12, pp. 857–862. IEEE Computer Society.

[14] Balasubramanian, R. and Aramudhan, M. (2012) Security Issues: Public vs Private vs Hybrid Cloud Computing. *International Journal of Computer Applications*, **55**, 35–41.

[15] Juels, A. and Yen, T.-F. (2012) Sherlock Holmes and The Case of the Advanced Persistent Threat. *5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET'12)*. USENIX Association.

[16] Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., and Flynn, L. (2012) Common Sense Guide to Mitigating Insider Threats. Technical Report 4th edition. Carnegie Mellon University.

[17] Band, S., Cappelli, D., Fischer, L., Moore, A., Shaw, E., and Trzeciak, R. (2006) Comparing insider it sabotage and espionage: A model-based analysis. Technical Report CMU/SEI-2006-TR-026. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

[18] Munshi, A., Dell, P., and Armstrong, H. (2012) Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents. *2012 45th Hawaii International Conference on System Sciences*, January, pp. 2402–2411. IEEE.

[19] FBI (2001). FBI Robert Philip Hanssen Espionage Case.

[20] Bishop, M., Conboy, H. M., Phan, H., and Simidchieva, B. I. (2014) Insider Threat Identification by Process Analysis. *The 2014 Workshop on Research for Insider Threat (WRIT)*.

[21] Mathew, S., Upadhyaya, S., Ha, D., and Ngo, H. Q. (2008) Insider abuse comprehension through capability acquisition graphs. *Proceedings of the 11th International Conference on Information Fusion, FUSION 2008*, pp. 698–705.

[22] Rocha, F. and Correia, M. (2011) Lucy in the sky without diamonds: Stealing confidential data in the cloud. *Proceedings of the International Conference on Dependable Systems and Networks*, June, pp. 129–134. IEEE.

[23] Nguyen, M.-D., Chau, N.-T., Jung, S., and Jung, S. (2014) A Demonstration of Malicious Insider Attacks inside Cloud IaaS Vendor. *International Journal of Information and Education Technology*, **4**, 483–486.

[24] Wu, R., Ahn, G.-J., Hu, H., and Singhal, M. (2010) Information flow control in cloud computing. *2010 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, pp. 1–7.

[25] Wei, J., Zhang, X., Ammons, G., Bala, V., and Ning, P. (2009) Managing security of virtual machine images in a cloud environment. *Proceedings of the 2009 ACM workshop on Cloud computing security - CCSW '09*, New York, New York, USA 91. ACM Press.

[26] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (2009) Hey, you, get off of my cloud. *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*, New York, New York, USA 199. ACM Press.

[27] Kandias, M., Virvilis, N., and Gritzalis, D. (2013) The insider threat in cloud computing. In Bologna, S., Hmmerli, B., Gritzalis, D., and Wolthusen, S. (eds.), *Critical Information Infrastructure Security*, Lecture Notes in Computer Science, **6983**, pp. 93–103. Springer Berlin Heidelberg.

[28] Fujinoki, H. and Dehkordi, S. M. (2012) Split Clouds: New Security Architecture for Protecting User Information from Cloud Insiders - Designs, Implementation, and Performance Evaluations. *2012 6th International Conference on New Trends in Information Science and Service Science and Data Mining (ISSDM)*, pp. 824–829.

[29] Layman, L. and Sigurdsson, G. (2013) Using Amazon's mechanical turk for user studies: Eight things you need to know. *International Symposium on Empirical Software Engineering and Measurement*, pp. 275–278.

[30] Swiderski, F. and Snyder, W. (2004) *Threat Modeling.* Microsoft Press.

[31] Crampton, J. and Huth, M. (2009) Detecting and Countering Insider Threats : Can Policy-Based Access Control Help ? *Proceedings of 5th International Workshop on Security and Trust Management.*

[32] Chen, L. and Crampton, J. (2012) Risk-aware role-based access control. *Security and Trust Management* , **?**, 140–156.

[33] Baracaldo, N. and Joshi, J. (2012) A trust-and-risk aware RBAC framework. *Proceedings of the 17th ACM symposium on Access Control Models and Technologies - SACMAT '12* 167.

[34] Pearson, S. and Benameur, A. (2010) Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, pp. 693–702.

[35] Habib, S. M., Ries, S., and Mühlhäuser, M. (2010) Cloud computing landscape and research challenges regarding trust and reputation. *Proceedings - Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing in Conjunction with the UIC 2010 and ATC 2010 Conferences, UIC-ATC 2010*, pp. 410–415.

[36] Fernandes, D. a. B., Soares, L. F. B., Gomes, J. a. V., Freire, M. M., and Inácio, P. R. M. (2014) Security issues in cloud environments: A survey. *International Journal of Information Security*, **13**, 113–170.

[37] Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., and Goldsmith, M. (2015) Identifying attack patterns for insider threat detection. *Computer Fraud & Security*, **2015**, 9–17.