A Predictive Model for Risk and Trust Assessment in Cloud Computing: Taxonomy and Analysis for Attack Pattern Detection

Alexandros Chrysikos[1] , Stephen McGuire[2]

[1] Dr. Alexandros Chrysikos, Cyber Security Research Group, School of Computing & Digital Media, London Metropolitan University, London, UK.
A.Chrysikos@londonmet.ac.uk
[2] Stephen McGuire, School of Computing, University of Huddersfield, UK.
S.Mcquire@hud.ac.uk

Abstract: Cloud computing environments consist of many entities that have different roles, such as provider and customer, and multiple interactions amongst them. Trust is an essential element to develop confidence-based relationships amongst the various components in such a diverse environment. The current chapter presents the taxonomy of trust models and classification of information sources for trust assessment. Furthermore, it presents the taxonomy of risk factors in cloud computing environment. It analyses further the existing approaches and portrays the potential of enhancing trust development by merging trust assessment and risk assessment methodologies. The aim of the proposed solution is to combine information sources collected from various trust and risk assessment systems deployed in cloud services, with data related to attack patterns. Specifically, the approach suggests a new qualitative solution that could analyse each symptom, indicator, and vulnerability in order to detect the impact and likelihood of attacks directed at cloud computing environments. Therefore, possible implementation of the proposed framework might help to minimise false positive alarms, as well as to improve performance and security, in the cloud computing environment.

Keywords: Cloud computing environment, Trust Assessment, Risk Assessment, Taxonomy, Attack Pattern, Detection, Framework

1.1 Introduction

Cloud computing environment combines known technologies, such as virtualization, big data, data warehousing and data mining. The advantages that it provides are increased performance, ease of deployment, elasticity of a service, and anytime-anywhere access. A cloud computing environment with the aforementioned benefits, as well as its dynamic resource sharing and its cost effectiveness, draws the attention of many enterprises and individual users [1]. Especially, for technological developments such as mobile applications and Internet-of-Things (IoT), a cloud computing environment becomes the preferred way of deployment.

Cloud services are provided dynamically to its users in a non-transparent manner. Due to its complex infrastructure, it exhibits heterogeneous capabilities of services and resources [2, 3]. Therefore, users might not be confident in terms of controlling the data stored in the cloud. In addition, safeguarding users' privacy and providing secure cloud based transactions is challenging. Establishing consistent operational practices and performance, as well as reliable cloud services has also a level of difficulty. Therefore, from a cloud-user point of view, the reliability of a cloud service is an important issue [4].

Every day a new announcement is released regarding cloud computing threats and security risks. Furthermore, security is highlighted as the most critical obstacle in adapting cloud computing for a service [5]. As a result, cloud computing security issues lead to difficulties in terms of developing a well-defined assessment structure regarding the actual impact on security. This is justified by two key reasons. Firstly, basic vocabulary terms, such as vulnerability, risk, and threat, are usually adopted interchangeably. Secondly, not all issues identified are specifically related to cloud computing [6, 7]. In order to establish a clear understanding about cloud-specific security issues, an analysis of how cloud computing influences security issues is required. A key factor is security vulnerabilities [8, 9]. This is important because security vulnerabilities could function as indicators that could in turn help detect cloud computing based attack patterns and vulnerabilities. Before expanding on that, though, it is important to first establish what is a 'vulnerability'?

1.2 Vulnerability: An Overview

Vulnerability is characterised as a prominent risk factor [10]. Specifically, the ISO 27000 defines risk as "*the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization*" [11]. The Open Group has developed an overview of the factors contributing to risk [12]. Specifically, as presented in Figure 1 it uses the same two top-level risk factors as ISO 27000, the likelihood of a harmful event (in diagram: loss event frequency) and its consequence (in diagram, probable loss magnitude). The probable loss magnitude's sub-factors influence a harmful event's ultimate cost (see Figure 1 on the right). On other hand, the loss event's frequency sub-factors occur when a threat agent, for instance a hacker, successfully exploits a vulnerability (see Figure 1 on the left). The frequency with which that develops is based on two factors:

1) The frequency is determined by both the agent's motivation and how much access the agents have to the attack targets. What is the level of effort? What is the risk level for the attackers? What can they gain from the attack? and

2) The difference between the threat agents' attack capabilities and the system's strength to resist the attack [11, 12].

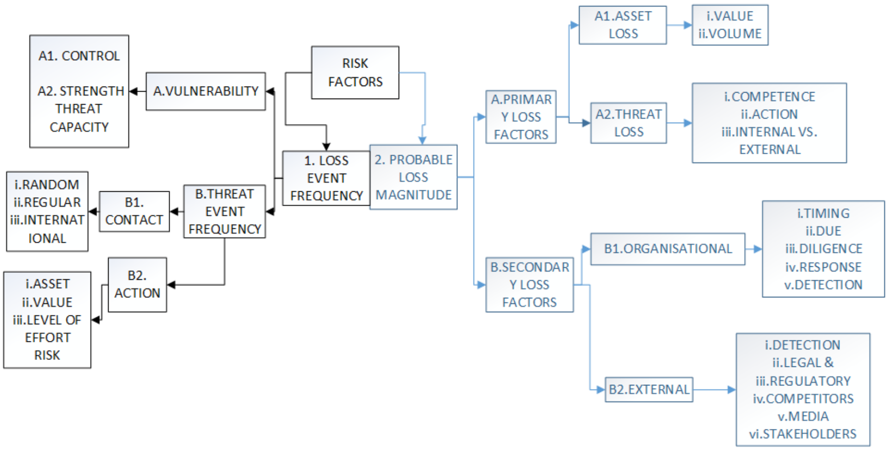

Figure 1: Taxonomy of Risk Factors (Open Group) based on [11]

1.2.1 Definition of Vulnerability

According to the aforementioned Open Group's risk taxonomy factors a useful definition of vulnerability is developed. Vulnerability is defined as *the probability that an asset will be unable to resist the actions of a threat agent. It exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force* [13].

Thus, vulnerability should always be expressed in terms of resistance to a certain attack type. For instance, in a real world example, a car is not able to protect its driver against injury when hit frontally by a truck traveling at 60mph, is a vulnerability. The resistance of the car's crumple zone is simply too weak compared to the truck's force. On the other hand, against the "attack" of a biker, or even a small car driving at a more moderate speed, the car's resistance strength is perfectly adequate [12].

Computer vulnerability can also be described as a removal or weakening of a certain resistance strength. For example, a buffer-overflow vulnerability weakens a system's resistance to arbitrary code execution. Whether attackers can exploit this vulnerability, or not, depends on how capable they are [5].

1.2.2 Vulnerabilities in Cloud Computing

Having defined and explained the term 'vulnerability', this section examines how cloud computing can influence the risk factors presented in Figure 1. From a cloud-customer perspective, the right-hand side is related to the probable magnitude of future loss. Similarly to conventional IT infrastructure, in cloud computing the consequences and ultimate cost of, for instance, data confidentiality breach, is the same [14]. From a cloud-service perspective it looks a bit different. Cloud computing systems were previously separated on the same infrastructure; therefore, a loss event could be more impactful. However, this fact can be easily included into a risk assessment, as no conceptual work is required to adapt impact analysis to cloud computing [8].

The left-hand side, in Figure 1, deals with the loss event frequency. Cloud computing could potentially alter the probability of a harmful event's occurrence. Specifically, cloud computing could cause significant changes in the vulnerability factors, because moving to a cloud infrastructure might alter the attackers' access level and motivation, as well as effort and risk [15]. To support a cloud-specific risk assessment it is important to start investigating the exact nature of cloud-specific vulnerabilities. However, is there such thing as a "cloud-specific" vulnerability? If so, certain factors in a cloud computing environment should make a vulnerability cloud-specific.

A cloud computing environment consists of many components with different roles that need to interact with each other. Depending on the context, the nature of interaction may differ. Trust is an essential aspect to achieve confidence-based interactions amongst various entities in a cloud computing environment. Therefore, the taxonomy of trust models and classification of information sources for cloud-specific risk assessment is needed for an effective trust assessment in a cloud computing environment. This in return might help identify factors that make a vulnerability cloud specific.

Trust assessment in a cloud computing environment requires facilitation of a wide range of aspects involving services; such as software, platform, and infrastructure as a service, and deployment models; such as private, public, community, and hybrid [16]. For that reason, the evolving dynamic of trust relationships amongst those entities makes trust assessment a vital area that needs addressing. In the following sections the taxonomy of trust assessment models, trust assessment information sources, and trust dimensions in cloud computing are presented.

1.3 Trust Assessment Models in Cloud Computing

A trust model is defined as a collection of rules, elements, and process' to develop trust amongst the different entities in any computing paradigm. Specifically, cloud computing environment components such as databases, virtual machines, cloud service providers, cloud service customers, and cloud services are examples of different entities. Trust models are classified in two categories, decision models and evaluation models [17]. These models are applied to the cloud computing paradigm and are further developed through their connection with trust assessment techniques. This leads to the development of taxonomy of trust models and trust assessment techniques. Figure 2 presents taxonomy of trust models, in the following sections a detailed description is provided.

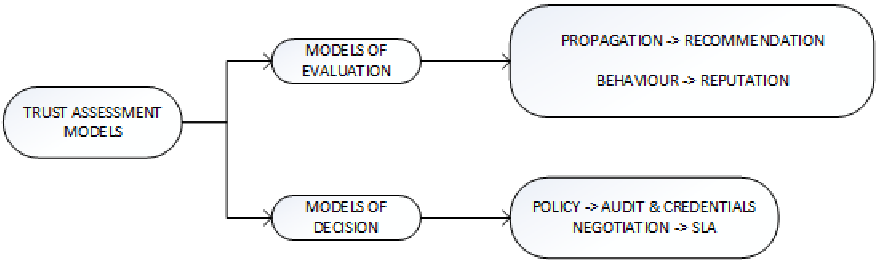

Figure 2: Taxonomy of Trust Assessment Models based on [17]

1.3.1 Decision Models

The aim of a decision model is to provide an access control decision as a unique trust decision instead of following a relatively complex mechanism that includes authentication and authorization [5]. Decision models are categorised into two types, as policy models and negotiation models. The policy model employs credentials and policies in order to control access to different resources. Specifically, credentials and policies signify the essential permissions required to access various resources. The other type is the negotiation model that applies negotiation strategies in order to establish trust between two different entities [17].

Cloud service providers may apply different audits and compliance standards to provide assurance to their users about the offered software, platforms, and services [18]. To increase the level of security third party assessment is provided by auditors. This involves issuing the audit certificates based on the audit compliance. However, cloud service providers are not required to disclose the audit reports to the users [19]. A trust assessment technique, though, can employ credentials and policies of cloud service providers to customers in order to make a trust decision. Such credentials and policies may be set by applying standards such as X.509, digital certificates, or public key infrastructure (PKI) [2, 19]. In the cloud computing environment context, a Service Level Agreement (SLA) can be applied as a policy-based method that may provide trust assessment [6]. An SLA describes the functional and quality related facets of the offered cloud service [20]. The details of those aspects are specified during the negotiation process between cloud providers and cloud customers. Nevertheless, authenticating claims made by a cloud service provider as part of the SLA documentation necessitates an experienced and trusted third party [19]. In general, establishing trust via the use of credentials and policies can be difficult to achieve. Hence, it is considered as hard trust [20]. In the following section, the second type of trust models, evaluation models, is examined.

1.3.2 Evaluation Models

Evaluation models are defined as computational trust models; this is because trust assessment is dependent on evaluation of different parameters. Specifically, these parameters categorise the evaluation models in behavior models and propagation models [6]. In behavior models, the aim is to compute the trust of the previously mentioned entities by measuring relevant factors such as reliability and performance. In propagation models, a new trust relationship is developed through the data distribution of pre-existing trust values in communication paths to other entities [21].

In the behavior model, a reputation technique may be applied as trust assessor of a cloud service. In particular, trust is measured via the combination of ratings submitted by a number of cloud users for a cloud service [19]. The measurement of trust may employ various methods like addition or averaging and fuzzy logic. The resulting value of trust signifies the degree of cloud users' trust to a specific cloud service [20].

On the other hand, the propagation models are using a recommendation based technique. Essentially, in this technique a cloud user develops a trust for a cloud service based on recommendations by trusted third party cloud users [20].

Overall, both reputation and recommendation techniques employ factors such as feedback regarding trust assessment and ratings. Therefore, establishing trust through those elements is classed as soft trust [6].

1.4 Trust Assessment Information Sources in Cloud Computing

The cloud users' service-related needs are constantly changing in the diverse environment of cloud computing. Consequently, the role of various factors, such as feedback, ratings, and Quality of Service (QoS), in trust assessment is very important. In the following paragraphs, four trust assessment information sources are examined. Specifically, direct and indirect interaction, Cloud Service Provider declarations, and Third Party assessment [6]. These information sources are, then, correlated with various factors of the cloud computing environment. The outcome was a taxonomy of information sources for trust assessment that is presented in Figure 3 and then explained in the following sections.

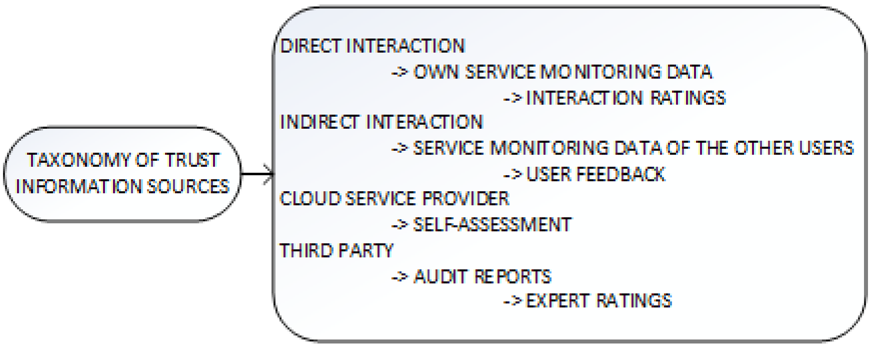

Figure 3: Taxonomy of Trust Information Sources based on [6]

1.4.1 Direct Interaction

When a cloud user has past experiences with cloud services, then the source of information is the direct interaction between those two sides. Specifically, this type of information can be expressed as ratings provided by the cloud user after interacting with a cloud service. The factors for trust assessment can be in the form of QoS parameters and can be documented though monitoring during the process of interaction between a cloud service and a cloud user. The advantage of storing and reviewing a cloud user's previous experiences is that the most relevant information can be used for trust assessment. However, such reviews will also include information that is insufficient, and as a result, not suitable for the purpose of trust assessment [19].

1.4.2 Indirect Interaction

When a cloud user has insufficient, or no past experience with cloud services, then the source of information is the indirect interaction between a cloud user and a cloud service. Specifically, assessment factors are calculated based on third party users' experiences and can be in the form of feedback and/or ratings that are provided by third party cloud users regarding their cloud service experiences. In addition, this type of information could be acquired through the processing of data recorded by the cloud service provider. Consequently, the assessment conducted by employing this type of information could be considered of better validity. On the other hand, the information retrieved by third party users may be biased in terms of feedback quality and that is a potential concern. Therefore, the feedback collected as part of indirect interaction could be employed as initial assessment until direct interaction is made available [21].

1.4.3 Cloud Service Provider declarations

A cloud service provider incorporates a set of parameters of cloud services that may include information related to privacy, security, integrity, and compliance. Nevertheless, all this information is based on the assessment conducted and published by the cloud service providers themselves. Therefore, the data authenticity needs to be confirmed [20].

1.4.4 Third Party Assessment

Third Party Auditor (TPA) in cloud computing is a mechanism that inspects cloud services by reflecting on parameters such as privacy, performance and security. The reports generated by TPA form an objective and a formal source of information that may be used for trust assessment [22].

1.5 Trust Dimensions in Cloud Computing

A trust model measures the security strength and computes a trust value. A trust value comprises of various parameters that are necessary dimensions to measure cloud services' security. In the consequent sections, the dimensions regarding effective trust assessment are identified.

1.5.1 Multi-Criteria

Trust assessment evaluation needs to entail various parameters like availability and reliability, in order to describe relevant qualities of the cloud provider and/or the cloud service [20]. Specifically, those parameters are categorised in objective and subjective parameters. The objective parameters incorporate real-time measurement or ratings provided by users. The subjective parameters incorporate factors such as feedback provided by third party cloud service customers [19]. The combination of the aforementioned parameters is a challenging task. If it is successful, though, it could lead to quality trust assessment.

1.5.2 Context

Each type of cloud service requires different performance specification based on the various applying scenarios. Therefore, a trust model should consider the different types of cloud services applied. The types that form distinct contexts for trust assessment are Platform as a Service (PaaS), and Software as a Service (SaaS) [23].

1.5.3 Pesronalisation

In the cloud computing environment, there is a wide variety of user requirements about the trust assessment of the previously mentioned cloud services. A personalised service allows users to determine suitable requirements regarding trust evaluation from their perspective [6]. This enables users' flexibility to specify their own unique preferences, needs, and information sources about trust assessment.

1.5.4 (De)-Centralised Trust Assessment

In the centralised trust assessment approach the architecture consists of a centralised repository that stores the trust assessment related data. The mechanism can be simple to implement and the trust assessment data, such as ratings and processing are conducted in a centralised entity/site. The main disadvantage is the possibility of failure of that centralised entity [21]. In the de-centralised trust assessment method the trust related data are distributed amongst various entities/sites. Furthermore, the de-centralised architecture allows computation of trust data and storage in multiple sites of the distributed cloud computing environment. Therefore, it enables the scalability and redundancy characteristic to all its users.

1.5.5 Adaptability

In the various applications of a cloud computing environment there is a number of actors, such as cloud customer, cloud provider, cloud broker, cloud carrier, and cloud auditor, who could be situated around the globe. In addition, new cloud providers may be added or current users may be withdrawn from the cloud computing environment. In such a diverse environment with the potential for rapid change, alterations in the cloud infrastructure may occur constantly. Therefore, it is important for a trust model to adapt to any change seamlessly [6]. The term adaptability signifies the degree of which a trust evaluation model adapts to the aforementioned changes.

1.5.6 Credibility

In the trust evaluation context of a cloud computing environment, credibility refers to the degree of service parameters or the data quality given as input for the trust assessment process [6, 21]. Therefore, encouraging the credibility of cloud services or the credibility of feedback provided by the cloud users is an essential task.

1.5.7 Trust Dynamics

In the dynamic cloud computing environment associations between two or more different entities are not fixed but evolve with experience. Therefore, trust amongst entities needs to be assessed and revised regularly [21].

Having completed the presentation of the dimensions to be supported by trust management systems, an analysis of trust assessment frameworks is provided.

1.6 Analysis of Trust Assessment Frameworks in Cloud Computing

In the last ten years, researchers have been investigating the various aspects of trust assessment in the cloud computing environment. A series of important trust assessment frameworks are presented in the subsequent paragraphs. Specifically, the selection of the frameworks addressed is based on those involving a holistic approach focused on cloud services. In addition, the frameworks are presented in chronological order that can be seen in Table 1.

To begin with, Noor et al. [24] proposed the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS). Specifically, it is an adaptive and robust model for measuring the credibility of user feedback to protect cloud services from malicious users. Furthermore, it offers comparison of the trustworthiness of cloud services. Ghosh et al. [25] suggested a framework that evaluates the associated risk in interacting with the cloud provider. This framework performs the trust assessment of cloud provider in the context of SaaS, PaaS and IaaS. The next framework is proposed by Qu and Buyya [26]. It is a trust evaluation framework regarding selection of cloud infrastructure services. Specifically, it evaluates the trust of cloud services based on the subjective QoS requirements and preferences of the cloud user. Noor et al. [27] recommended a generic analytical framework for trust management. In the frame work, interactions in cloud applications occur at three layers. For each layer, a set of dimensions is identified and the used as a benchmark to evaluate and analyse existing trust management research prototypes.

The next trust assessment framework is proposed by Pawar et al [28] to measure the trustworthiness of an infrastructure provider. It evaluates trust by employing factors such as SLA, satisfaction ratings, and providers' behavior values. Furthermore, it takes into account the uncertainty of information during trust evaluation. Habib et al. [21] proposed an architecture that employs a centralised method to collect trust-related data from various sources. The framework is using a numbers of QoS parameters determined by the users, to measure trust assessment of cloud providers. The final framework is suggested by Alhamad et al. [29]. It is a cloud trust framework that uses SLA and applies a business process monitoring. Specifically, it takes advantage of the SLA cloud customer categorisation in various classes to enable domain specific trust values.

Table 1 shows a comparative analysis of the aforementioned trust assessment frameworks. The table is structured by using the titles and information from the previously presented trust assessment related sections. The first column of the table includes the Existing Work. This outlines the previously explained trust assessment frameworks in chronological order. The second column, Trust Assessment Models, describes the basic trust assessment techniques used in each framework. In the third column, which is titled as Trust Assessment Information Sources, the information sources and parameters are indicated. Finally, the fourth column is the Trust Dimensions that presents the features of the several dimensions of trust assessment supported by the frameworks.

Table 1: Comparative Analysis of Trust Assessment Frameworks

Existing Work	**Trust Assessment Models**	**Trust Assessment Information Sources**	**Trust Dimensions**
Noor et al. 2016 [24]	-Reputation, -Credibility, -Credentials, -Trust assessment of cloud service using fuzzy logic	-User feedback (direct/indirect interactions, collusion attacks) -Direct interaction (Dynamic QoS parameters, such as performance, availability) -Cloud Service Provider satisfaction ratings and behavior values	-De-centralised architecture - A technique to identify credible feedback -Availability and security of Trust Management System
Ghosh et al. 2015 [25]	-SLA, -Reputation	-Cloud customer Ratings -User feedback (direct/indirect interactions)	-Context of interaction for trust assessment -SLA based competence assessment -Mathematical modeling of trust, reputation, competence and risk
Qu et al. 2014 [26]	-QoS parameters, -Trust assessment of cloud service using fuzzy logic	-Expert ratings (static parameters, such as security) -Direct interaction (Dynamic QoS parameters, such as performance, availability)	-Dynamic trust -Personalised trust evaluation
Noor et al. 2013 [27]	-Reputation, -Policy, -Credentials	-User feedback (direct/indirect interactions, collusion attacks) -Direct interaction (Dynamic QoS parameters, such as performance, availability),	-De-centralised architecture -A technique to identify credible feedback -Availability and security of Trust Management System

Pawar et al. 2012 [28]	-Reputation, -Recommendation	-Cloud Service Provider satisfaction ratings and behavior values -SLA indicators	-Context includes IaaS and multi-cloud environment
Habib et al. 2011 [21]	-Reputation, -Recommendation	-User feedback -Expert ratings -Declarations of Cloud Service Provider	-Personalised trust evaluation -Integration: Combining feedback and other trust related factors from multiple sources
Alhamad et al. 2010 [29]	-SLA, -Negotation	-Cloud Service Provider and Users experience -SLA agent reports	-De-centralised architecture

In the previous sections a classification of information related to vulnerabilities (risk factors), trust assessment models, trust assessment information sources, and trust dimensions of the cloud computing environment is presented. This analysis and taxonomy of information is considered crucial to better comprehend the novel approach recommended in the current research. Before doing that, though, a description of similar approaches is presented.

1.7 Related Detection Approaches

When it comes to detection approaches, security researchers require a mechanism that can integrate and analyse a wide variety of data sources. Particularly, they need a mechanism that can process information that is generated by heterogenous sources implemented in any cloud computing environment. These mechanisms should aim to detect attack patterns and reduce false positive alarms.

Hansman et al, [30] employed five classifiers to describe different types of attack. Specifically, classification by attack vendor, classification by attack target, classification by operational impact, classification by informational impact, and classification by defense. All this information can provide the network administrator with data on how to mitigate or deter an attack. Amer and Hamilton [31] developed an ontology based attack model to assess the security of an information system from an attacker's point of view. The aim of the assessment process is to evaluate the effects of an attack. The process consists of four stages. The first stage consists of identifying the system’s vulnerabilities using automated vulnerability tools. These tools evaluate vulnerabilities of computer systems, applications or networks and generate sets of scan results. The second stage, involves determining the attacks that might occur due to the previously identified vulnerabilities. In the third stage, the possible effects of those vulnerabilities are analysed. The fourth and final stage the attack effects are calculated.

Patel et al. [32] proposed a taxonomy with four dimensions that provides classification covering network and computer attacks. Specifically, it provides assistance in improving network and computer security, as well as language consistency through attack description. The first dimension focuses on classifying the attack. The second classifies the target of the attack. The third provides vulnerability classification or uses criteria from Howard and Longstaff’s taxonomy [33]. The fourth dimension, addresses the effects of the attack.

Ficco et al. [34] recommended a hybrid and event correlation approach for detecting attack patterns. The process involves detecting symptoms by collecting diverse information at several cloud levels in order to perform a complex event analysis presented in an ontology.

All of the previously mentioned methodologies demonstrate beneficial ontology and taxonomy that may offer informative guidelines regarding cyber intrusions and attack analysis. However, there is lack of detail required to analyse all symptoms and attacks that could in return minimise the number of false positive alarms. For instance, the same attack in two different cloud services may have a different degree of impact, but in most existing systems it would be classed as a malicious attack by both services.

The proposed framework addresses this issue, of a system generating multiple false positive alarms, through the implication of risk and trust assessment analysis in the detection process. In this approach, all actors, such as cloud providers and cloud customers participate in the data analysis to achieve a high level of information and data processing~~.~~ Before describing the proposed framework, though, the underpinning systems are presented.

1.7.1 Intrusion Detection System

An Intrusion Detection System (IDS) is very important in terms of preventing an attack against an Information Technology (IT) organisation. An IDS conducts a security system diagnosis to discover all suspicious activities based on detection algorithms. Specifically, those systems can help to deter and prevent actions related to security breaches, system flaws, as well as potential threats that may lead to system violations [35].

On the other hand, an IDS system may detect many false actions, but it may also lead to a number of false positive alarms and authorized users identified as intruders. In a cloud computing environment where all resources are shared amongst cloud customers, this point becomes even more critical. In order to minimise the number of false positive alarms and improve the efficiency of attack detection in all cloud computing environments, the proposed framework includes both cloud service providers and cloud customers as part of the correlation process in all cloud layers (SaaS, PaaS, IaaS).

1.7.2 Risk Assessment System

Risk assessment can be identified as the potential that a given attack will exploit vulnerabilities of an asset or a group of assets to cause loss or damage to the assets. According to the ISO 27005 Risk Management, risk is measured by evaluating the probability of successful attacks and the subsequent impact of those attacks, should they occur [5].

$$\text{Risk} = \text{Impact} * \text{Likelihood}\ [36]$$

Specifically, the term Impact refers to the degree of which a risk event might affect an enterprise, expressed in terms of: Confidentiality, Integrity, and Authentication. The term Likelihood refers to the possibility that a given event may occur [5]. The implementation of the aforementioned equation in the proposed framework aims to stimulate cloud customers to evaluate security risks and simplify the analysis of all identified events.

1.8 Proposed Framework for Attack Pattern Detection through Trust and Risk Assessment

The proposed framework is a predictive model that detects attack patterns based on trust assessment and risk assessment analysis. Figure 4 presents a correlation process that consists of a sequence of activities that are designed to analyse all network traffic through cloud layers [37]. The proposed framework applies a correlation process that intends to unify different steps of correlation by adding risk and trust assessment analysis in the diagnosis step, before the taxonomy step takes place.

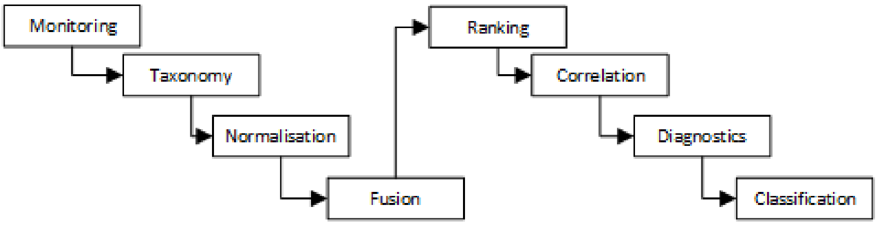

Figure 4: Correlation Process based on [37]

An attack pattern is an abstraction mechanism that describes how an observed attack type is executed. Following the lifecycle of cyber-attack, when an attack occurs it uses several paths, from reconnaissance to exploitation, and aims to gain unauthorized access to data [38]. Through studying the impact effects of an attack and simplifying the analysis of monitored events, then it could be possible to minimise false positive alarms.

Figure 5 shows the proposed framework's four essential security functions: Monitoring / Data Collection, Analysing & Detecting, Alarm, and Respond. The attack patterns are detected by collecting and analysing data from all cloud layers. The data storage is structured in two separate knowledge databases that do not communicate. These are the Trust Assessment Database and the Risk Assessment Database. The reason for recommending two isolated databases is to reassure cloud providers for data pseudonymisation. The cloud providers processing of personal data is conducted in a way that the data can no longer be attributed to a specific data subject without the use of additional information [39]. The pseudonymised information from those two databases is then combined in the Processing Knowledge Base. There, the risk of the attack is calculated and a response is sent whether it represents a suspicious threat or a false positive alarm. The calculation is conducted in the Decision Making server that determines the impact of each attack pattern and the risk of the attack. The Respond function is connected to a Self-Learning Knowledge Base that classifies information about all attacks. It serves as an Advice as a Service for the Decision Making server.

A Risk Software Agent (RSAg), a goal-oriented computer program that reacts to its environment and operates without continuous direct supervision to perform its function, is related to each function defining the impact and likelihood of each detected symptom. The Decision Making server determines the impact of each attack pattern and the risk of the attack. Employing the aforementioned framework could help minimise the rate of false positive alarms and increase the effectiveness of attack pattern detection systems.

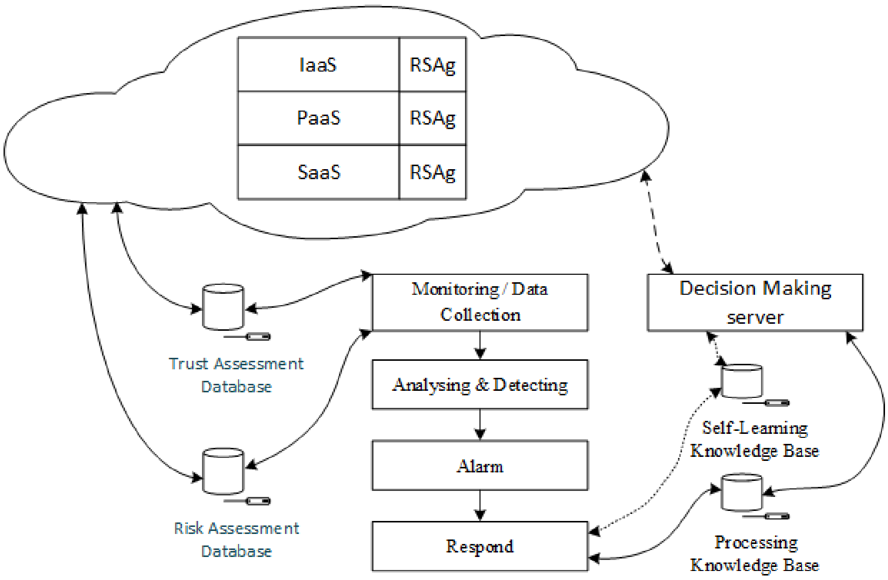
IaaS
RSAg
PaaS
RSAg
SaaS
RSAg
Monitoring / Data Collection
Analysing & Detecting
Alarm
Respond
Decision Making server
Trust Assessment Database
Risk Assessment Database
Self-Learning Knowledge Base
Processing Knowledge Base

Figure 5: Proposed Framework for Attack Pattern Detection

The analysis of attack patterns is conducted by calculating the score of all indicators. Specifically, the proposed solution includes a definition for Risk (Ri) as a product of the Probability (Po) of a security compromise and its potential Impact (Im) (see 1).

$$Ri = Po * Im \ (1)$$

The recommended correlation is used to aggregate the attack scenarios and symptoms generated by all parts in the cloud computing environment. The Impact (Im) is a value consisting of the following indicators: Trust Assessment Indicator (TaI), Vulnerability (Vu) and Symptoms (Sy). Each of these indicators has a different impact. The Probability (Po) value is increased in relation to each indicator of an attack pattern (see 2).

$$Im = TaI + Vu + Sy \ (2)$$

The Impact (Im) and Probability (Po) of each indicator is defined by the cloud customer and cloud provider using data collected from all cloud layers. The aim is to use attackers’ behavior to determine the Impact (Im) and expose a potential attacker before an attack can take place. The value of Risk (Ri) related to each attack determines whether the attack is successful or false positive alarm depending on the sensitivity of the targeted data as defined by the owner (cloud provider and cloud customer) (see 3).

$$Ri = Po * (TaI + Vu + Sy) \quad (3)$$

1.9 Recommendations for further research and Conclusion

In the current study a taxonomy and analysis of risk and trust assessment techniques in the cloud computing paradigm are presented. Risk factors for a cloud-specific risk assessment are classified. Furthermore, information sources and factors for trust assessment are categorised. The analysis of the techniques studied shows that most of the approaches should involve both cloud providers and cloud customers in the process of attack pattern detection. This could be achieved by sharing common processes of data collection and analysis.

Therefore, a new framework for attack pattern detection in the cloud computing paradigm is proposed. A framework to recognise and analyse malicious actions based on risk and trust assessment factors and information sources related to attack patterns. Specifically, the recommended framework classifies attacks by evaluating the probability of a security breach and its potential impact indicators, such as trust assessment Indicator, vulnerability, and symptoms. The outcome of this evaluation gives the likelihood of an attack pattern risk. Both cloud providers and cloud customers are involved in the data collection and correlation process. This classification might aid to protect data in the cloud and provide a method that could efficiently analyse suspicious attack actions and reduce false positive alarms.

In the cloud computing environment, risk and trust assessment need to be assessed continuously using multiple factors. These factors keep changing in the dynamic and constantly evolving cloud computing paradigm. In addition, multi-cloud environments demand a more risk and trust assessment oriented analysis. Therefore, risk and trust assessment needs of cloud providers and cloud customers’ have to be addressed in more detail. Finally, future work should test the implementation of the suggested framework in an actual cloud computing environment.

References

[1] Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on (pp. 27-33). Ieee.

[2] Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. ACM Computing Surveys (CSUR), 46(1), 12.

[3] Abbadi, I. M., & Martin, A. (2011). Trust in the Cloud. information security technical report, 16(3), 108-114.

[4] Habib, S. M., Ries, S., & Muhlhauser, M. (2010). Cloud computing landscape and research challenges regarding trust and reputation. In Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2010 7th International Conference on (pp. 410-415). IEEE.

[5] Grobauer, B., Walloschek, T. and Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy Magazine, 9(2), pp.50-57.

[6] Mouratidis H, Shareeful I, Kalloniatis C, and Gritzalis s, (2013). “A framework to support selection of cloud providers based on security and privacy requirements.” Journal of Systems and Software 86: 2276–93.

[7] Heydari, A., Tavakoli, M. A., & Riazi, M. (2014). An Overview of Public Cloud Security Issues. International Journal of Management Excellence, 3(2), 440-445.

[8] Catteddu, D. (2010). Cloud Computing: benefits, risks and recommendations for information security. In Web application security (pp. 17-17). Springer, Berlin, Heidelberg.

[9] Islam, S., Fenz, S., Weippl, E., & Kalloniatis, C. (2016). Migration Goals and Risk Management in Cloud Computing: A Review of State of the Art and Survey Results on Practitioners. International Journal of Secure Software Engineering (IJSSE), 7(3), 44-73. doi:10.4018/IJSSE.2016070103

[10] Trappey, A. J., Trappey, C. V., Govindarajan, U. H., Sun, J. J., & Chuang, A. C. (2016). A review of technology standards and patent portfolios for enabling cyber-physical systems in advanced manufacturing. IEEE Access, 4, 7356-7382.

[11] International Organization for Standardization: ISO/IEC 27000:2016: Information technology - Security techniques - Information security management systems - Overview and vocabulary. Technical report, ISO (2016)

[12] Kreger, H., & Estefan, J. (2009). Navigating the soa open standards landscape around architecture. Joint Paper, The Open Group, OASIS, and OMG.

[13] Lemoudden, M., Bouazza, N., El Ouahidi, B., & Bourget, D. (2013). A SURVEY OF CLOUD COMPUTING SECURITY OVERVIEW OF ATTACK

VECTORS AND DEFENSE MECHANISMS. Journal of Theoretical & Applied Information Technology, 54(2).

[14] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), 113-170.

[15] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.

[16] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[17] Moyano, F., Fernandez-Gago, C., & Lopez, J. (2012). A conceptual framework for trust models. In International Conference on Trust, Privacy and Security in Digital Business (pp. 93-104). Springer, Berlin, Heidelberg.

[18] Rimal, B. P., Choi, E., & Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. NCM, 9, 44-51.

[19] Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2(1), 9.

[20] Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London.

[21] Habib, S. M., Ries, S., & Muhlhauser, M. (2011). Towards a trust management system for cloud computing. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on (pp. 933-939). IEEE.

[22] Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-preserving public auditing for data storage security in cloud computing. In Infocom, 2010 proceedings ieee (pp. 1-9). Ieee.

[23] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[24] Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S., & Ngu, A. H. (2016). CloudArmor: Supporting reputation-based trust management for cloud services. IEEE transactions on parallel and distributed systems, 27(2), 367-380.

[25] Ghosh, N., Ghosh, S. K., & Das, S. K. (2015). SelCSP: A framework to facilitate selection of cloud service providers. IEEE transactions on cloud computing, 3(1), 66-79.

[26] Qu, C., & Buyya, R. (2014). A cloud trust evaluation system using hierarchical fuzzy inference system for service selection. In Advanced information networking and applications (aina), 2014 ieee 28th international conference on (pp. 850-857). IEEE.

[27] Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. ACM Computing Surveys (CSUR), 46(1), 12.

[28] Pawar, P. S., Rajarajan, M., Nair, S. K., & Zisman, A. (2012). Trust model for optimized cloud services. In IFIP International Conference on Trust Management (pp. 97-112). Springer, Berlin, Heidelberg.

[29] Alhamad, M., Dillon, T., & Chang, E. (2010). Sla-based trust model for cloud computing. In Network-Based Information Systems (NBiS), 2010 13th International Conference on (pp. 321-324). Ieee.

[30] Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31-43.

[31] Amer, S. H., & Hamilton, J. (2010). Intrusion detection systems (IDS) taxonomy-a short review. Defense Cyber Security, 13(2), 23-30.

[32] Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications, 36(1), 25-41.

[33] Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents (No. SAND98-8667). Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US).

[34] Ficco, M., Tasquier, L., & Aversa, R. (2013). Intrusion detection in cloud computing. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on (pp. 276-283). IEEE.

[35] Bace, R., & Mell, P. (2001). NIST special publication on intrusion detection systems. BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.

[36] Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. information security technical report, 13(4), 247-255.

[37] Valeur, F., Vigna, G., Kruegel, C., & Kemmerer, R. A. (2004). Comprehensive approach to intrusion detection alert correlation. IEEE Transactions on dependable and secure computing, 1(3), 146-169.

[38] Shin, J. S., Son, H. S., & Heo, G. (2013). Cyber security risk analysis model composed with activity-quality and architecture model. In International conference on computer, networks and communication engineering (pp. 609-612).

[39] Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review, 33(2), 171-181.

Index

vulnerability.. ………………2, 3, 4, 15, 17
Risk Assessment 4, 15, 16
Trust Assessment….4, 6, 10, 11, 12, 15, 16
Information sources... ....6, 7, 11, 12, 15
Trust Dimensions…………....8, 11, 12, 14
Taxonomy...................................3, 5, 7, 15
Intrusion Detection 14
attack pattern..... ……………..2, 15, 16, 15
framework ……………..10, 11, 12, 15, 16
risk factors .... ………………………2, 3, 4
Cloud Computing Environment ...………2
Risk Assessment System 15
Risk……..17
Impact…………………………………....17
Probability…...…………………………17