Intrusion Detection Attack Patterns in Cloud Computing: Trust and Risk Assessment

Alexandros Chrysikos[1]

[1] Dr. Alexandros Chrysikos, Cyber Security Research Group, School of Computing & Digital Media, London Metropolitan University, London, UK. A.Chrysikos@londonmet.ac.uk

Abstract: Dependence on cloud services has been steadily increasing in recent years, as cloud services are an attractive option to offer flexibility and cost effectiveness through economies of scale. Cloud services are also exposed to security incidents, such as data breaches and other malicious activities. To mitigate risks to the confidentiality, integrity, and availability of assets, but also minimise loss to cloud service providers and users, the attack trust and risk elements need to be identified, classified, and prioritised. The aim of the proposed conceptual framework is to combine trust and risk assessment sources with data of risk assessment related to each attack pattern. This novel approach is a new qualitative solution to examine and determine symptoms, indicators, and vulnerabilities to detect the impact and likelihood of distributed attacks directed at cloud computing environments. The proposed framework might help to reduce false positive alarms and improve performance in Intrusion Detection Systems.

Keywords: Cloud computing, Trust Assessment, Risk Assessment, Attack Pattern, IDS, Ontology

1.1 Introduction

Cloud computing is a new emerging model in Information Technology (IT) that can enable convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources. Those resources can also be released with minimal management effort and interactions can be rapidly provisioned (Zhang et al. 2010). Cloud computing represents an opportunity for both service providers and consumers, through the improvement of IT agility, efficiency, and reliability to reduce the cost of IT technologies. Specifically, on-demand self-service, resource pooling, rapid elasticity and measured service, cloud computing systems automatically control and optimize resource usage in order to offer an alternative method to rent computing and storage infrastructure services (Zissis and Lekkas 2012).

Cloud services are provided dynamically to its users via internet, which can lead to several attacks threatening their confidentiality, integrity, and availability of the data stored in the cloud (Jadeja and Modi 2012). Detecting attacks can be challenging for security administrators. Therefore, the use of Intrusion Detection Systems (IDS) can aid both cloud providers and security administrators to monitor and analyse network traffic (Aikat et al. 2017). The reason for using such systems is to prevent attacks by employing detection algorithms. Such algorithms monitor symptoms, analyse attack patterns, and then produce a multitude of alarms known as false alarms (Duque and bin Omar 2015).

The proposed framework aims to analyse risks related to each attack pattern. Specifically, it calculates risks related to each symptom, indicator and vulnerability in order to define the attack risk score, and then generate an alert.

In the subsequent sections a review of related detection approaches in cloud computing is provided. The underpinning systems required for the recommended solution are also presented. Then, the author describes the proposed framework. In the concluding section, a discussion about recommendations for further research is presented.

1.2 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 (2005) 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 (2010) 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. (2013) proposed a four dimensions approach 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 (1998) approach. The fourth dimension, addresses the effects of the attack.

Ficco et al. (2013) 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 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.

1.3 Intrusion Detection System (IDS)

An 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 (Bace and Mell 2001).

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, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

1.4 Trust Assessment System

Trust assessment in cloud computing facilitates a variety of information sources at different levels of abstraction and several deployment models (SaaS, PaaS, IaaS). Therefore, trust evaluation and changing nature of trust relationships among different entities in the cloud paradigm become important points to be addressed (Subashini and Kavitha 2011). Specifically, trust assessment models include a collection of rules, elements, and process' to develop trust amongst the different entities in any computing paradigm. 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. These models are applied to the cloud computing paradigm and are further developed through their connection with trust assessment techniques (Moyano et al. 2012).

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. There are four main trust assessment information sources. Specifically, direct and indirect interaction, Cloud Service Provider declarations, and Third Party assessment (Mouratidis et al. 2013).

Trust dimensions is the other significant area that 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 (Huang and Nicol 2013).

1.5 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 (Duque and bin Omar 2015).

Risk = Impact * Likelihood (Humphreys 2008)

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 (Duque and bin Omar 2015). 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.

1.6 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 1 presents a correlation process that consists of a sequence of activities that are designed to analyse all network traffic through cloud layers (Valeur et al. 2004). 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.

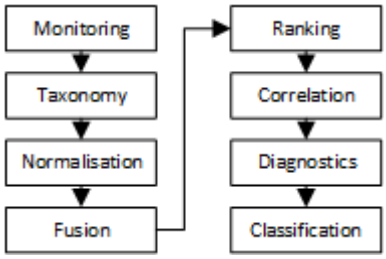

Figure 1: Correlation Process (Valeur et al. 2004)

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 (Shin et al. 2013). 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 2 shows the proposed framework's three essential security functions: (1) Monitoring & Data Collection, (2) Analysing & Detecting, and (3) Alarm & Respond.

(1) Monitoring & Data Collection. As a first step, the requirements of the organisation are defined based on monitoring the event management logs of all cloud layers (IaaS, PaaS, and SaaS). The next step is to collect data through Risk Software Agent (RSAg) programs. An RSAg is a goal-oriented computer program that reacts to its environment and operates without continuous direct supervision to perform its function. The RSAg programs store data from IaaS, PaaS, and SaaS. 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 (Bolognini and Bistolfi 2017). The pseudonymised information from those two databases is then combined in the Self-Learning Knowledge Base, which feeds with data the next function.

(2) Analysing & Detecting. 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).

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

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).

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

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). All this information is processed and stored in the Processing Knowledge Base.

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

(3) Alarm & Respond. The risk of the attack is calculated and a response is sent whether it represents a suspicious threat or a false positive alarm. This is conducted with mechanisms that classify information about all attacks and determine the impact of each attack pattern and the risk of the attack. Specifically, the use of machine-learning procedures, such as supervised classification and clustering, and analytic algorithms has been proven useful to similar proactive detection and defense models (Fu et al. 2010; Osako et al. 2016). The respond function is conducted in the Decision Making server that determines the impact of every attack and serves as an Advice as a Service for the organisations.

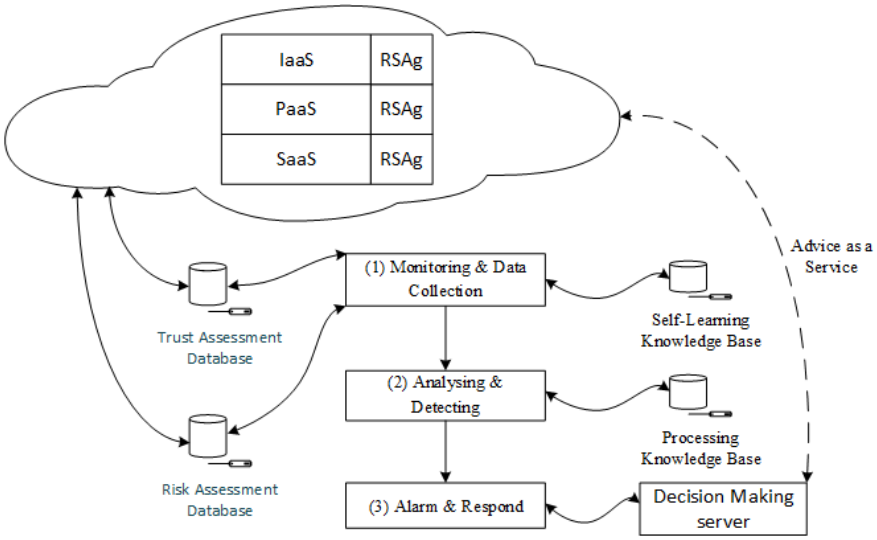

Figure 2: Proposed Framework for Attack Pattern Detection

1.7 Conclusion

In the current study 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. Moreover, 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. Therefore, a taxonomy and analysis of risk and trust assessment techniques in the cloud computing paradigm is required. Finally, future work should test the implementation of the suggested framework in an actual cloud computing environment.

References

Aikat J, Akella A, Chase JS, Juels A, Reiter M, Ristenpart T, Sekar V, Swift M (2017) Rethinking security in the era of cloud computing. IEEE Security & Privacy.

Amer SH, Hamilton J (2010) Intrusion detection systems (IDS) taxonomy-a short review. Defense Cyber Security, 13(2), 23-30.

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

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.

Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Computer Science, 61, pp.46-51.

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.

Fu, T., Abbasi, A. and Chen, H., 2010. A focused crawler for Dark Web forums. Journal of the Association for Information Science and Technology, 61(6), pp.1213-1231.

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

Howard JD, Longstaff TA (1998) A common language for computer security incidents (No. SAND98-8667). Sandia National Labs, Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US).

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

Huang J, Nicol, DM (2013) Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2(1), 9.

Jadeja Y, Modi K (2012) Cloud computing-concepts, architecture and challenges. In Computing, Electronics and Electrical Technologies (ICCEET), International Conference on (pp. 877-880). IEEE.

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.

Mouratidis H, Shareeful I, Kalloniatis C, 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.

Osako, T., Suzuki, T. and Iwata, Y., 2016. Proactive Defense Model Based on Cyber Threat Analysis. FUJITSU Sci. Tech. J, 52(3), pp.72-77.

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

Shin JS, Son HS, 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).

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.

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

Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), pp.7-18.

Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Generation computer systems, 28(3), pp.583-592.

Index