

## Intrusion detection in cloud computing based attack patterns and risk assessment

Ben Charhi Youssef<sup>\*1</sup>, Mannane Nada<sup>1</sup>, Bendriss Elmehdi<sup>2</sup>, Regragui Boubker<sup>2</sup>

<sup>1</sup> TIES Team, ENSIAS, Mohammed V University Rabat 1000, Morocco

<sup>2</sup> Professors ENSIAS, Mohammed V University Rabat 1000, Morocco

### ARTICLE INFO

Article history:

Received : 10 April, 2017

Accepted : 11 May, 2017

Online: 24 May, 2017

Keywords :

Intrusion detection

Cloud computing

Risk assessment

Attack pattern

IDS

IPS

### ABSTRACT

*This paper is an extension of work originally presented in SYSCO CONF. We extend our previous work by presenting the initial results of the implementation of intrusion detection based on risk assessment on cloud computing. The idea focuses on a novel approach for detecting cyber-attacks on the cloud environment by analyzing attacks pattern using risk assessment methodologies. The aim of our solution is to combine evidences obtained from Intrusion Detection Systems (IDS) deployed in a cloud with risk assessment related to each attack pattern. Our approach presents a new qualitative solution for analyzing each symptom, indicator and vulnerability analyzing impact and likelihood of distributed and multi-steps attacks directed to cloud environments. The implementation of this approach will reduce the number of false alerts and will improve the performance of the IDS.*

## 1. Introduction

Cloud computing is a new emerging model in Information technology which can enable ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources released with minimal management effort and can rapidly be provisioned. It represents a new opportunity for both customers and service providers, by improving IT efficiency, agility and reliability to reduce the cost of IT technologies. This technology allows customers to create an elastic environment with a multitude number of services, optimize resources and offer an alternative way for renting computing and storage infrastructure services.

Cloud computing services are the most vulnerable target for intruder's attacks due to their distributed environment and the accessibility of cloud services via the internet threatening data and services security.

Detect and deter attacks can be difficult task for security administrators. Therefore, the use of IDS (Intrusion Detection system) can help both cloud providers and security administrator in order to monitor and analyze network traffic.

The goal of using such system is to detect and prevent attacks, using different algorithm of detection. Nevertheless, analyzing and

monitoring symptoms produces a multitude alarms with a huge number of false ones impacting the effectiveness of such systems. The distributed and open structure of cloud layers makes the implementation of traditional IDS inefficient to be deployed in cloud environment.

In the aim of reducing the number of false alarms this paper proposes a correlation approach by analyzing risks related to each attack pattern. The approach consists of calculating risk related to each attack steps by analyzing symptoms, indicators and vulnerability to define the attack risk score then yield alert. This paper propose to include customers as part of security protection. It demonstrate how the implementation of risks can decrease the number of false alarms. Our work is extended by presenting the initial results of the implementation of the approach in cloud computing specially in SaaS layer.

The remainder of the paper is structured as follows: in section II we present the prior work done in this field. Section III presents the intrusion detection system and risk assessment methodology, in section IV, we describe our proposed detection process based on attacks patterns analysis by risk assessment. Section V presents the initial finding results of the implementation of our approach to detect an SQL injection attack in SaaS layer. The last section of this article will present a conclusion and future works.

<sup>1</sup> Corresponding Author: Ben Charhi Youssef, ENSIAS University Mohamed V Rabat 1000, MOROCCO | Email: [bencharhi.youssef@gmail.com](mailto:bencharhi.youssef@gmail.com)

## **2. Related Works**

Intrusion detection system has an important role in the security and perseverance of active defense system against intruder hostile attacks. Through the past few years several papers have been presented with the purpose of detecting malicious threat against cloud with different approaches. Security researchers need to have a seamless mechanism to integrate and analyze various information generated by heterogeneous sources implemented in cloud environment with the aim to detect intrusion and reduce false positive alerts. [1]

Kleber, schulter et al. [2] have proposed an IDS service at cloud middleware layer with an audit system designed to cover attacks that Network IDS and Host IDS cannot detect. In [3] authors presented an approach of detection using five major classifiers to characterize the nature of an attack, classification by attack vector, attack target, operational impact, informational impact and by defense, which provide the network administrator with information of how to mitigate an attack.

With similar methodologies to those used in the AVOIDIT [4] taxonomy, S. A. and J. Hamilton [5] developed an ontology-based attack model to assess the security of an information system from the angle of an attacker. Goal of the assessment process is the evaluation of attack effects. Thus, the difference of system performance before and after an attack is calculated. The process consists of four phases. The first step consists in identifying system vulnerabilities by using automated vulnerability tools. Such tools assess computer system, applications or network regarding their vulnerabilities and generate sets of scan results. In the second phase, the developed ontology is used to determine which attacks might occur due to the identified vulnerabilities. By querying the ontology, the possible effects are obtained. Finally, in the last phase the attack effect is calculated. In [6] authors proposed a taxonomy with four dimensions that provides a classification covering network and computer attacks. Their taxonomy provides assistance in improving computer and network security as well as consistency in language with attack description. The first dimension being attack vector is used to classify the attack. The second dimension classifies the target of the attack. The third dimension consists of the vulnerability classification number, or criteria. The fourth and final dimension highlights the payload or effects involved.

Massimo Ficco in [7] proposes a hybrid and event correlation approach for intrusion detection in cloud computing. It consists of detecting intrusion symptoms by collecting diverse information at several cloud levels to perform complex event analysis presented in an ontology.

In [15] song et al propose a model which is based on behavioral and contextual analysis. Authors present two sets of attributes to be used for anomalies detection contextual attribute and behavioral attribute based on a probabilistic analysis.

Wang et al in [16] present an approach for TCP/IP Reassembly in Network Intrusion Detection and Prevention Systems to be used as DPI (Deep Packet Inspection) for network intrusion monitoring.

For risk assessment several methods exist. In [8] author proposes a method for a probabilistic model driven risk assessment with security requirements. The security requirements and their causal relationships are represented using MEBN (Multi-Entities Bayesian Networks) logic that constructs an explicit formal risk

assessment model that supports evidence-driven arguments. In [9] author proposes security ontology for organizing knowledge on threats, assets and safeguards measures. This work constructs classification for each of these groups and creates a method for quantitative risk analysis, using its own framework.

In our previous work [10] we presented a new intrusion detection approach based on risk assessment for traditional IDS.

Although all of the previous works present useful taxonomy and ontology that can provide an informative baseline for cyber intrusions and attacks analysis, they lack the details needed to analyze all symptoms of attacks which can provide many false positive alerts in cloud environment. Moreover, this work proposes a detection approach based on risk assessment analysis related to attack pattern initially presented in [1], which means that the data owner and cloud provider will participate in attacks analysis.

For example the same attack against two different clients of the same services may have different impacts. However, IDS will detect both connections as malicious actions. That's could bring IDS to miss the impact analysis, and generate many false alarms.

Our solution addresses this issue in cloud services through the implication of risk assessment in the detection and analysis processes.

## **3. Intrusion detection and risk assessment**

This section presents the Intrusion detection systems, the correlation process and the risk assessment methodology.

### *3.1. Intrusion detection systems*

An IDS (Intrusion detection system) is used for monitoring the network or a host for suspicious or malicious activities. Next to an IDS there is also an Intrusion Prevention System (IPS). An IPS will do more than just monitoring the traffic t will also prevent malicious activities from taking place. IDS/IPS perform a diagnosis of system security to detect all suspicious actions and discover various security breaches based on different algorithms of detection. IDS is used to detect flaws and the different possible threats that attempt to compromise the confidentiality, integrity or availability of a resource with a capability to block malicious attacks using functionalities of prevention.

Providing an analysis of all network traffic with IDS will catch intruders and block multiple suspicious actions threatening the security of IT systems. But will also lead to a great number of false positives and can identify authorized users as intruders, especially in cloud environment where all resources are shared between customers.

In order to withhold attacks and reduce the number of false alerts and improve efficiency of IDS, our solution defines both CSP (Cloud Services Provider) and the customers as part of the monitoring process by implementing a risk agent related to all cloud layers (IaaS, PaaS, SaaS).

### *3.2. Risk assessment*

Risk assessment is the process of identifying security risks related to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact. Risks can be defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or

damage to the assets. The main objective of risk assessment is to define appropriate controls for reducing or eliminating those risks

Based on the 27005[11] standard risk is evaluated by looking at the probability of successful attacks and the consequent severity of that attacks.

Generally there are four steps of risk assessment. The four steps are as follow:

- Threat Identification
- Vulnerability Identification
- Risk Determination
- Control Recommendation

The general equation of risk determination is:

$$Risk = Impact * Likelihood \quad (1)$$

**Impact:** (or consequence) refers to the extent to which a risk event might affect the enterprise expressed in the terms of: Confidentiality, Integrity and Availability

**Likelihood:** represents the possibility that a given event occurs.

This equation (1) will be implemented in our approach with the aim to encourage customers to assess the security risks related to their information and to simplify the analysis of all detected events for intrusion detection systems in cloud computing.

#### 4. Attack pattern analysis in cloud with risk assessment

An attack pattern is an abstraction mechanism for describing how a type of observed attack is executed. Following the pattern paradigm, it also provides a description of the context where it is applicable and then, unlike typical patterns, it gives recommended methods of mitigating [10].

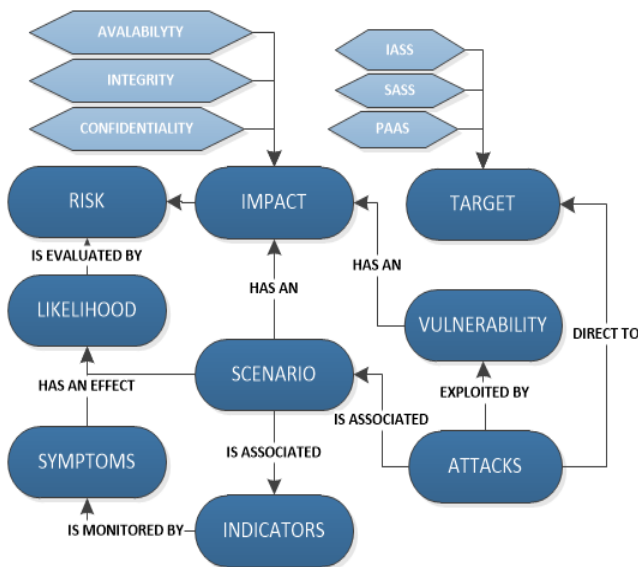


Figure 1: Attack ontology

Figure 1 shows a simplified view of our attack ontology designed to cloud environment.

When an attack occurs, it uses several paths (from reconnaissance to exploitation) by using scenarios defined in the process by indicators and symptoms, in the aims to gain unauthorized access to data. The analysis of impact simplifies the monitoring process and minimizes false-alarms.

Each attack scenario has an impact in either confidentiality, availability or/and integrity. The data owner on the risk-agent will define the impact of each indicator, symptom and vulnerability depending on the nature of the data.

The possibility that a given event will occur is defined as Likelihood. The risk score of the detected attack changes and simplifies the diagnostic of alarms (false positive or successful attack), in the same time symptoms and attack indicators scenario upturn the likelihood in the risk agent.

The analysis of attack pattern uses the risk agent to calculate the score of all indicators and symptoms then to define the nature of the packet. We propose a definition for risk (Re) as a product of the Probability (Pe) of a security compromise, a threat event, and its potential Impact or Consequence (Ie):

$$Re = Pe * Ie \quad (2)$$

The correlation is used to aggregate attack scenarios and symptoms produced by all the probes in the cloud environment.

Equation (2) represents the formula of risk assessment, the likelihood Pe, whereas (Ie) may be assigned a value on a numerical scale. Each indicator Is, Vulnerability Ve, Symptoms Sy have different impact. The value of Pe will be increased related to each detection of an attack pattern.

By using the formula of risk assessment of all suspicious actions we can get a risk score related to each attack:

$$Ra = 1/n \sum Ie * Pe \quad (3)$$

$$Ie = \sum (Is + Ve + Se + Sye) \quad (4)$$

The impact Ie and likelihood Pe of each symptom and attack will be defined by the data owner and cloud provider in a risk agent deployed in all cloud layers. The goal of such correlation is to get attacker's behavior and risk related to each action to by calculating impact and lure a potential attacker from critical system.

The value of Ra related to each attack will determine if the action is a successful attacks or a false positive depending of the sensitivity of targeted data related to risk values.

IDPSs serve four essential security functions: they monitor, analyze detect and respond to all suspicious activities as depicted in the functional layer.

The IDS/IPS detects intrusion by analyzing the collected data in all cloud layers based on knowledge base and the attack pattern ontology, calculates the risk of the attack then decides if it represents a suspicious action or a false-positive.

A software Agent is related with each probe defining the impact and likelihood of each detected symptoms. The risk server will determine the impact of each attack pattern then the risk of the attack. Implementing, such methodology can minimize the number of false-positive alarms and increase the effectiveness of Intrusion Detection System.

## 5. Implementation of approach

In this chapter we present the initial finding while implementing the discussed idea in cloud environment in the aims to decrease the number of false-alarms and to improve the reaction in the detection intrusion system in cloud.

### 5.1. Architecture of implementation

IDS implementation in cloud computing requires an efficient, scalable and virtualization-based approach. In cloud computing, user data and application is hosted on cloud service provider's remote servers and both cloud user and CSP (Cloud Services Provider) has a limited control over data and resources.

In the implementation of the proposed approach we have used OPENSTACK [12] as cloud platform with a collection of open source software project that developers and cloud computing technologist can use to setup and run their cloud compute and storage infrastructure.

SURICATA [17] was used as intrusion detection system which is a free and open source, fast and robust threat detection engine.

The simulation setup is a Cloud with different layers. We have chosen a fixed value in risk agent. The main goal is to analyze all actions based on the impacts and likelihoods of vulnerabilities and detected symptoms to evaluate the efficiency of our works.

The architecture of implementation and the used correlation process is presented in Figure 2:

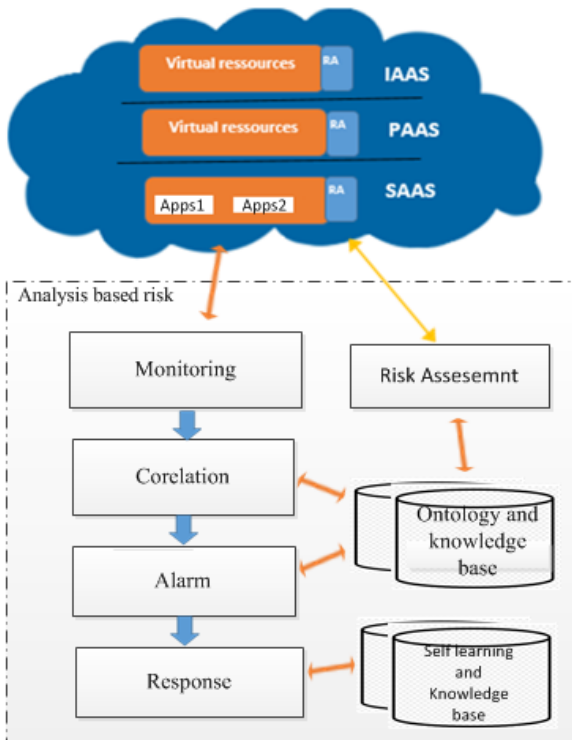


Figure 2: Architecture of implementation

### 5.2. Detection of SQL injection in SaaS

An attack based on SQL injection can be defined as an attack which consists of insertion of a SQL query via the input data from [13].

In this attack malicious user will use several steps to gain an access to a SaaS service and a successful SQL injection exploit can threat the confidentiality, integrity and availability of database. However the same attack in two application in a SaaS service could have different impact.

Based on the SQL injection attack pattern defined in [14] the scenario can be presented as below:

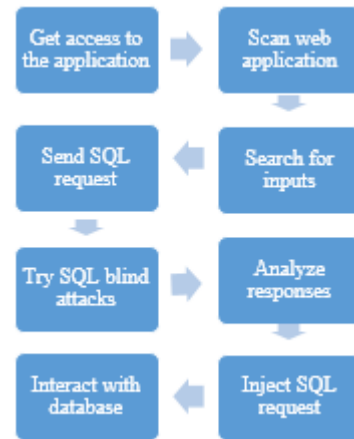


Figure 3: SQL injection attack pattern

In the scenario of implementation each cloud client must define a risk related to this attack pattern

- **Vulnerabilities:** Input validation ,Inputs are not properly validated by the application
- **Scenario :** Try different approaches for adding logic to SQL queries
- **Indicators :** Scan a website application, analyze responses positive or negative
- **Symptoms:** Use automated scan tools, try "Blind SQL Injection" techniques to extract information about the database, Send different requests

The Table below shows a simplified use of risk assessment used to estimate an SQL injection attack impact against two SaaS applications with a fixed values:

Attack pattern	Likelihood in app1	Likelihood in app2	Impact in app1	Impact in app2	Ra app 1	Ra app 2
Vulnerability	1	3	3	1	3	3
Scenarios	3	2	4	3	12	6
Indicators	2	2	4	3	8	6
Symptoms	2	3	4	1	8	4
Attack risks					7,75	4,75

Table 1: Attack analysis

Attack Pattern against SaaS services is composed of 4 attributes: Vulnerability, Scenarios, Indicators of attack and symptoms. Each attribute define an impact and has an initial value of likelihood determined by customers in risk agent.

Ra app 1 present the risk of each attribute, while attack risks is calculated using the equation (3). Table1 demonstrate how the same attack against two customers in the same Cloud service should have different impact.

The graphs below show results, before and after the use of risk analysis, obtained while exploiting the SQL injection vulnerability directed to two customers data in the same SaaS service with the use a static risk agent related to this attack pattern as presented in table 1.

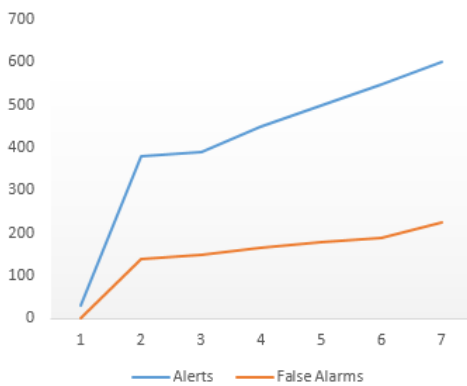


Figure 4: Number of false alarms before implementation

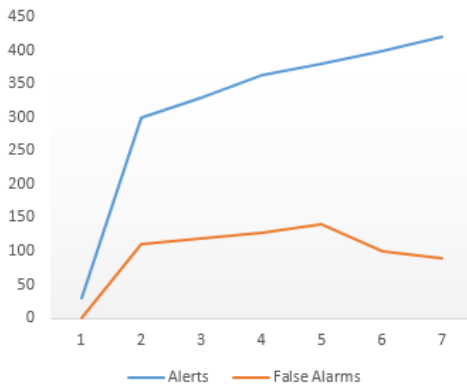


Figure 5: Number of false alarms after implementation

### 5.3. Discussion

The specific and complex characteristics of cloud computing environment make the implementation of intrusion detection system more difficult with the multitude of alarms and the huge number of false alarms. Therefore, there is a need of new approach of detection and analysis of malicious activities for both cloud consumers and CSP to check the effectiveness of the current security controls that protect data stored in cloud.

Figure 5 demonstrates how the implementation of risk assessment in cloud layer for two customers reduces the number of false positive alarms. With such an approach, the cloud consumers can check the effectiveness of the current security controls that protect an organization’s assets and the service providers can maximize and win the trust of their cloud consumers

if the level of risk is not high. Also the cloud consumers can perform the risk assessment to be aware of the risks and vulnerabilities present in the current cloud computing.

### 6. Conclusion and future works

Based on the observation that consumers must be involved in data protection and attack deterrence in cloud computing, this paper provides a novel approach in the disposition of intrusion detection system. We suggest a model to recognize and analyze malicious actions by using a risk assessment related to attack pattern.

The same attack should have different impact on different customer’s data. This paper classifies attacks by target, symptoms, scenarios, impact and likelihood defining the attack pattern than estimate impact and risk related to all malicious activities against cloud services. Both CSP and consumer will participate in the correlation process. This classification will help to provide a methodology of analysis in depth of all suspicious actions in the aim to minimize the number of false alarms and increases the efficiency of intrusion detection system in cloud services.

The initial implementation for securing a SaaS service and detecting an SQL injection attack against two customers data’s has demonstrated the efficiency of our approach in both decreasing the huge number of false alarms and increase the effectiveness of the IDS system.

Future works will be focused on the implementation of our approach to detect sophisticated attacks in all cloud layers with the implementation of distributing risk agent.

### References

- [1] S. Mumtaz, L. Khan, “Performance of Grid-Integrated Photovoltaic/Fuel Cell/Electrolyzer/Battery Hybrid Power System” in 2nd International Conference on Power Generation Systems and Renewable Energy Technologies, Islamabad Pakistan, 2015.
- [2] Youssef, Ben Charhi, Bendriss E. "Intrusion detection in cloud computing based attacks patterns and risk assessment." Systems of Collaboration (SysCo), International Conference on. IEEE, 2016.
- [3] Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, in IEEE Journal: IT Professional, 19 July 2010.
- [4] HANSMAN, Simon HUNT, Ray. “A taxonomy of network and computer attacks. Computers & Security”, vol. 24, no 1, p. 31-43,2005.
- [5] SIMMONS, Chris, ELLIS, Charles, SHIVA, Sajjan, et al. AVOIDIT: “A cyber attack taxonomy”, IEEE, 2009.
- [6] Hafez Amer, S., & hamilton Jr, J. A. “Intrusion Detection Systems (IDS) Taxonomy-A Short Review” in STN 13-2 Defensive Cyber Security: Policies and Procedures 2, 23, 2010.
- [7] Patel, Ahmed, et al. "An intrusion detection and prevention system in cloud computing: A systematic review." Journal of network and computer applications 36.1, 25-41, 2013.
- [8] Ficco, M., Tasquier, L., & Aversa, R. (2013, October). Intrusion detection in cloud computing. In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Eighth International Conference on (pp. 276-283). IEEE, 2013.
- [9] Z. Xuan,N. Wuwong , et al., “Information security risk management framework for the Cloud computing environments,” in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), pp. 1328-1333, 2010.
- [10] Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E “Security ontologies: Improving quantitative risk analysis” in System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on (pp. 156a-156a). IEEE,2007.

- [11] Bencharhi, Y., Bendriss, E., & Reragui, B. "Intrusion Detection System Based on Risk Assessment in Cloud Environment" in International Journal of cloud computing JCC, ICACON (4ICACON),2016.
- [12] ISO/IEC 27005, Information Technology-Security techniques -Information security risk management. International Organization for Standardization, Geneva,2008
- [13] Yadav, S. "Comparative study on open source software for cloud computing platform: Eucalyptus, openstack and opennebula" in international Journal Of Engineering And Science, 3(10), 51-54,2013.
- [14] OWASP [sql injection definition](https://www.owasp.org/index.php/SQL_Injection)  
[https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection)
- [15] Khatri, Jaimin K., and Girish Khilari. "Advancement in Virtualization Based Intrusion Detection System in Cloud Environment." International Journal of. Science, Engineering and Technology Research (IJSETR) 4.5,1510-1514, 2015.
- [16] LIANG, Zhenkai, YIN, Heng, et SONG, Dawn. HookFinder: Identifying and understanding malware hooking behaviors. Department of Electrical and Computing Engineering, p. 41,2008.
- [17] Wang, X., & Cronin, B "TCP/IP Reassembly in Network Intrusion Detection and Prevention Systems". International Journal of Information Security and Privacy (IJISP), 8(3), 63-76,2014.
- [18] Hoque, M. S., Mukit, M., Bikas, M., & Naser, A. "An implementation of intrusion detection system using genetic algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, 2012.