End-user based model for risk quantification in Cloud Computing Environment

Amal BENFATEH*  
Intelligent management of energies and information systems laboratory,  
Physics Department,  
Faculty of Sciences,  
Cadi Ayyad University,  
Marrakesh, Morocco

F. GHARNATI  
Intelligent management of energies and information systems laboratory,  
Physics Department,  
Faculty of Sciences,  
Cadi Ayyad University  
Marrakesh, Morocco

T. AGOUTI  
Computer Science Department,  
Faculty of Sciences,  
Cadi Ayyad University,  
Marrakesh, Morocco

Abstract—Cloud computing is the result of the evolution and the adoption of new technologies and paradigms. Because of its accessibility via internet, that makes it subject to a large variety of attacks. In present paper, we talk about risk quantification by focusing on a Cloud user as the main actor who affects closely on system security by taking into account more parameters based on his conducts within the system as well the state of the assets treated within business processes.

Key-Words: -Cloud computing; risk quantification; assessment; security system; threat; user stakeholders.

I. INTRODUCTION:

Today’s organizations are a target of information security attacks. More we use e-service, more we are in penetration danger. Attacks could be due to a human or software treat… maybe it is difficult to discover the kind of attacks but we know it would lead to harm our data or our system, or worst, lose a large amount of money; that’s why organizations spend millions of dollars on security of technical equipments such as firewalls, intrusion detection systems, encrypting systems, anti-virus tools to protect their systems against threats. Nevertheless, there is always a clever intruder that succeeds in sneaking or exploits unknown vulnerability. Therefore, organizations need to manage their information security risks to protect their assets and thus their business values.

What is the most challenge for these companies? The answer is simple. They don't know about what they have, and what they need. They want to know which asset or technology has a security risk and for which one, they have enough security control to protect. [1]

On the other hand, risk management is usually human activity that includes assessing task and developing security strategy… the important part of the risk management is identifying treats and vulnerabilities by taking into account all past incidents and their impacts on system. To manage this challenge we propose exploit advantages and benefits of software agents to automate this important activity.

II. CLOUD COMPUTING ENVIRONMENT:

A. Cloud characteristics:

The National Institute of Standards and Technology's definition of cloud computing identifies five essential characteristics: [2]

- On-demand self-service: give the customer the possibility to provision power of computing as needed without any human interaction.
- Large network access: make the cloud available from any type of network using any client platform.
- Resource pooling: cloud uses a multi-tenant model to serve multiple consumers. The resources have to be pooled to maximize the number of consumers.
- Measured service: cloud systems must monitor resources usage appropriate to the type of service. This can be done by using a metering capability.
- Rapid elasticity: capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

B. Service models:

The consumer has to begin by deciding the appropriate service model to select a cloud solution. The most popular services that cloud offers:

- Software as a service (SaaS): the users can rent a set of applications running on the cloud by the provider.
- Platform as a service (PaaS): the users have the service of implementing their applications on the cloud and run it.
- Infrastructure as a service (IaaS): the users can rent a specific infrastructure from the cloud and run any kind of applications even the operating system.

C. Deployment model:

After the service model, the future consumer might think about how he would benefit from the Cloud. So we have four models of the cloud deployment:

- Private Cloud: the cloud system will be used by a single consumer. The system can be maintained in the client’s local or by a third party.
- Public Cloud: the cloud is deployed by a Cloud provider for any client who wants to consume.
Risk (R) in the simplest form is the product between event probability P(E) and the possible damage, mostly described as an Impact (I) [9]:

\[ R(E) = P(E) \times I(E) \]  

Where:
- \( R(E) \) = risk of an event,
- \( E \) = Event,
- \( P \) = Probability

III. Risk assessment:

The first step in risk management is asset identification and establishing risk assessment. The potential risk identification could run after this assessment. A risk is the probability of cause of a problem when a threat triggered by vulnerabilities. The source of the problem is vulnerability and the problem itself is threats. Threats are much related to the characteristics of the assets and vulnerabilities are relevant to the security controls. [3][4].

A. Risk concepts:

An asset is defined as any element of an information system that possesses a value [5]. It includes tangible (software, hardware, personnel) and intangible assets (plans, organization, external factors, technical factors). In risk process an object is called asset when there is an effect in objects value when risk emerges. A threat is defined as any possible harm to the system, including network failures and natural disasters. Vulnerability is a weak point where the system security is susceptible to attack [6], [7]. Threats need to exploit certain vulnerability in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a measure of the risk. [8]

B. Risk estimation metrics review (related work):

1. Simplest form: [8]

\[ P(Risk) = P(Impact) \times P(Occurrence Rate) \times P(Probability) \]  

\[ P(R) = (P(Asset Value) \times P(Classification)) \times P(Occurrence Rate) \times P(Threat) \times P(Vulnerability) \]  

\[ P(R) = (P(AC1) \times P(AC2) \times P(AC3) \times P(AC4) \times P(AC5) \times P(C)) \times P(ARO) \times P(T1) \times P(T2) \times P(T3) \times P(T4) \times P(V1) \times P(V2) \times P(V3) \times P(V4) \]  

AC1, AC2, AC3 are factors related to asset value such as each asset could have one or more factors of the preceding. T1, T2, T3 are the common threats in the information system that could be categorized, according to BSI PD.

V1, V2, V3 are the common vulnerabilities from the same guideline.


In [12] the author presents a quantitative infrastructure that estimates the security of a system. The model measures the
security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. The infrastructure in question reflects the values that stakeholders have in each security requirement, the dependency of security requirements on the operation of architectural components, and the impact that security threats. Given the stakes matrix ST, the dependability matrix DP, the impact matrix IM and the threat vector PT, we can derive the vector of mean failure costs (one entry per stakeholder) by the following formula:

\[
MFC = ST \circ DP \circ IM \circ PT
\]

(7)

Where matrix ST is derived collectively by the stakeholders, matrix DP is derived by the systems architect, matrix IM is derived by the security analyst from architectural information, and vector PT is derived by the security analyst from perpetrator models. All matrixes are related by using the matrix product (\(\circ\)). In Figure 4 illustrates these matrices and their attributes (size, content, indexing, etc.).

IV. MODEL CONSTRUCTS:

A simplified illustration of the model is shown in fig 1.

A business process is a set of tasks. Let b be the vector of business processes \(p_m\) for \(m = 1 \ldots P\).

A task is a key activity in the business process, which is essential for the success of the business. Let \(t_n(p_m)\) be the vector of tasks \(t_n\) for each business process \(p_m\). Each business process \(p_m\) has \(n = 1 \ldots T(p_m)\) tasks \(t_n\). Let \(f(t_n/p_m)\) be the vector of frequencies \(f_n\) of how often a task \(t_n\) of a business process \(p_m\) is executed. For each task \(t_n\) there are \(i = 1 \ldots U(t_n)\) users responsible on performing it. Let \(u_i\) be the vector of users. To execute a task, users use some information resources.

An asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software, and confidential information.\(^{[13]}\) Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization. Let \(a_j\) be the asset used for each task \(t_n\) by the user \(u_i\) for \(j = 1 \ldots A\).

Let \(PR(A/U)\) be the vector the probabilities that an asset \(a_j\) is used by a user \(u_i\) and required for the task \(t_n\).

A threat on any asset arises when this last is not fit for the specific purpose of a task in a business process and the outcome of the task is potentially influenced by this. Each asset \(a_j\) has a vector of \(k = 1 \ldots TH(a_j)\) threats \(th_k\).

Let \(PR(TH/A)\) be the vector of the probabilities that a threat \(th_k\) appears in an asset \(a_j\).

Every threat has one or more direct consequences, and each direct consequence can has one or more intermediate consequences. Let \(c\) therefore be the vector of \(f = 1 \ldots C\) direct and intermediate consequences \(c_f\). A direct consequence is the direct effect of a threat with a likelihood attached, and might directly impact one or more business objectives. Let \(PR(C/TH)\) be the matrix of probabilities that a threat \(th_k\) leads to the direct consequence \(c_f\).

An intermediate consequence is a consequence of a consequence with likelihood attached, and also might directly impact one or more business objectives. A consequence \(c_f\) can lead to an intermediate consequence \(c_g\) with a probability of \(PR_{fg}\).

Business objective is the desired result of an organization, which are set by the executive leadership and typically formulated in the corporate mission. They can be financial goals, but may also include other aspects like product quality, customer satisfaction and environmental objectives. Formally, each organization has a vector of \(h = 1 \ldots H\) objectives \(o_h\) that it aims to achieve, which are measured quantitatively.

A consequence \(c_f\) might directly impact an objective \(o_h\), let \(\alpha(c_f)\) be the vector of the direct impacts of each consequence \(c_f\) on each of objectives \(o_1\) to \(o_h\).
V. RISK CALCULATION:

The vector of risk for each objective $o_h$ over all business processes $p_m$ can be calculated as follows:

$$R_{oh} = \prod_{j=1}^{A} PR(A / U) \times \prod_{k=1}^{TH} PR(TH / A) \times \prod_{l=1}^{C} PR(C / TH) \times \omega_f \right\} (8)$$

With $\omega_f = \varepsilon(c_f) + \sum_{g=1}^{C} PR_{fg} \times \omega_g \right\} (9)$

VI. DISCUSSION:

The proposed model aims to quantify the risk taking into account the different parameters and actors to better quantifying the risk. This model, as the title indicates, is focus on the user, his ability and stakeholders in the tasks/process. This aspect makes the evaluation more realistic by highlighting the users' responsibilities in security of information system in general and Cloud Computing in particular. Moreover, we added another parameter in the threat computing: the exposure factor of the asset. On the other hand, the model gives a space for the decision makers (leaders) to choose the criteria and objectives on which the risk will be calculated.

VII. CONCLUSION:

Cloud computing is an emerging system that offers subscribers the benefit of virtually unlimited computing resources. One advantage Cloud Computing doesn’t offer is absolute security of subscriber’s data. In this paper, we offer a quantitative model of security measurement that enables Cloud services providers and Cloud subscribers to quantify the risks they take with the security of their assets by focusing on user’s intervention on system, and to make security related decisions on the basis of business objectives proposed by decision makers (leaders).

REFERENCES:


