EasyChair Preprint

№ 6928

Risk and Trust Models for the Cloud

Thai Nguyen

October 26, 2021

RISK AND TRUST MODELS FOR THE CLOUD

Thái Nguyễn

University of Science and Technology of Hanoi

khangthai276@gmail.com

Abstract. Risk in itself is not bad, risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity.

With the increase in the growth of cloud computing and the changes in technology that have resulted new ways for cloud providers to deliver their services to cloud consumers, the cloud consumers should be aware of the risks and vulnerabilities present in the current cloud computing environment. An information security risk assessment is designed specifically for that task. However, there is lack of structured risk assessment approach to do it.

In this paper, firstly, I provide the definition of risk, also risk analysis, assessment, and management as well as their relationship and differences. Secondly, this paper will define the term "threat" and introduce the top threats and vulnerabilities for cloud computing by Cloud Security Alliance (CSA). Next, I present a cloud risk management by European Network and Information Security Agency (ENISA). The last section is about risk and trust models, and it also introduce two models developed by A4Cloud, which are Cloud adopted risk assessment model (CARAM) and the Joint risk and trust model (JRTM).

Keywords: Cloud computing, Risk analysis, Cloud risk assessment, Trust model, Risk and trust assessment.

1 Risk Analysis, Assessment and Management

1.1 Risk analysis

According to ISO 31000, risk is the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected. Therefore, the main factor in risk analysis is about uncertainty. Uncertainties can come for many sources, but they can be classified into two classes: epistemic, which caused by lack of knowledge, and aleatory, which is based on randomness and probability.

We can also categorize risk analysis into two classes: qualitative and quantitative risk analysis. While qualitative risk analysis uses a person's subjective judgment and experience to build a theoretical model of risk for a given scenario, quantitative analysis uses mathematical models and simulations to assign numerical values to risk.

1.1.1 Quantitative analysis

When the uncertainty is classified as aleatory, we can use quantitative analysis. Although there are many well-developed industries that use quantitative risk, it is not commonly used in information technology. In fact, it is very rare indeed.

In analyzing risk, we are attempting to envision how the future will turn out if we undertake a certain course of action (or inaction). Fundamentally, therefore, a risk analysis consists of an answer to the following three questions:

- A scenario si (What can happen?)
- The probability Pi of si (How likely is that will happen?)
- The consequence xi of si (If it does happen, what is the consequence?)

To answer these questions, we would make a list of outcomes or "scenarios" as suggested in Table I. The i_{th} line in the table can be thought of as a triplet:

$$< si, pi, xi >$$

where si is a scenario identification or description; p, is the probability of that scenario; and x, is the consequence or evaluation measure of that scenario, i.e., the measure of damage.

$$R = \{< si, pi, xi >\}, i=1, 2, 3, \ldots, N$$

Scenario	Likelihood	Consequence
s1	P1	x1
s2	P2	x2
s3	P3	x3
.	.	.
.	.	.
Sn	Pn	xn

Table I. Scenario list

If this table contains all the scenarios we can think of, we can then say that it (the table) is the answer to the question and therefore is the risk. More formally, using braces, {}, to denote "set of" we can say that the risk, R, "is" the set of triplets:

$$R = \{< si, pi, xi >\}, i=1, 2, 3, \ldots, N$$

Consider $x1 < x2 < x3 < \ldots < xN$:

Scenario	Likelihood	Consequences	Cumulative probability
s1	P1	x1	P1 = P2 + P1
s2	P2	x2	P2 = P3 + P2
…	…	…	…
si	Pi	xi	Pi = Pi+1 + Pi
…	…	…	…
sn-1	Pn-1	xn-1	Pn-1 = Pn + Pn-1
sn	Pn	xn	Pn = Pn

Table II. Scenario list with Cumulative probability

1.1.2 Qualitative analysis

On the other hand, when the uncertainty is classified as epistemic, we can also conduct a qualitative risk analysis. Qualitative analysis describes likelihood of consequences in detail. This approach is used in events where it is difficult to express numerical measure of risk. It is, for example, the occurrence without adequate information and numerical data. Such analysis can be used as an initial assessment to recognize risk. Qualitative is used with the term likelihood instead of probability, therefore, this uses a qualitative scale for likelihood, for example almost, possible… and for consequences, such as major, minor, moderate, …

1.2 Risk analysis, assessment and management

Risk analysis is a systematic examination of a risk scenario to understand its probability/likelihood and consequences. Risk assessment, the next step after risk analysis, is the process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact. The main objective of risk assessment is to define appropriate controls for reducing or eliminating those risks.

Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives. According to the introduction to ISO 31000 2009, the term risk management also refers to the architecture that is used to manage risk. Risk assessment is one step in the process of risk management.

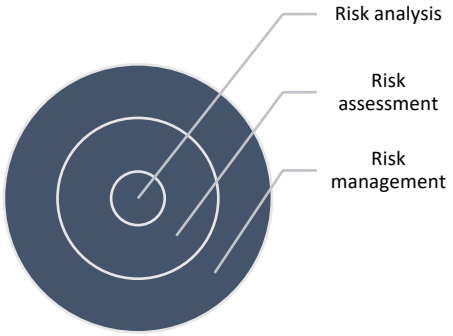

Figure I. Risk analysis, assessment and management.

2 Top Threats for the Cloud

2.1 Definition of "threat"

A threat is the potential cause of an unwanted incident, which may result in harm to a system, person, or organization. While risk focuses on incidents and the effects of those incidents, threat is about intentions and the harm that those intentions could cause.

In cloud computing, threats can be Data breaches, Account hijacking, … Every year, Cloud Security Alliance (CSA) publishes a document of top threats against the cloud, which is resulted by a survey among the experts and stakeholders to gain an insight into their perception.

2.2 Top threats by Cloud Security Alliance (CSA)

In this paper, I use the data from the document, by CSA, titled "Top Threats to Cloud Computing, The Egregious 11", in 2020 edition.

In this document, CSA introduced top eleven threats in priority order. For each threat, they included threat's description, its business impact, they also provided anecdotes, examples and security guidance.

In this paper, I do not discuss in detail each of "the egregious 11", further information can be found in the CSA's document. The list below includes, in order, the eleven top threats for cloud computing in 2020:

1 Data breaches
2 Misconfiguration and inadequate change control
3 Lack of cloud security architecture and strategy
4 Insufficient identity, credential, access and key management
5 Account hijacking
6 Insider threats
7 Insecure interfaces and APIs
8 Weak control plane
9 Metastructure and applistructure failures
10 Limited cloud usage visibility
11 Abuse and nefarious use of cloud services

3 Cloud Risk Assessment

3.1 Cloud risk assessment by European Network and Information Security Agency (ENISA)

ENISA provides a list of relevant incident scenarios, assets and vulnerabilities. It suggests estimating the level of risk on the basis of likelihood of a risk scenario mapped against the estimated negative impact, which is also the essence of the risk formulation by many others in the literature.

The level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact. The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.

The likelihood of each incident scenario and the business impact was determined in consultation with the expert group contributing to this report, drawing on their collective experience.

	Likelihood of incident scenario	Very low	Low	Medium	High	Very high
Business Impact	Very low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very high	4	5	6	7	8

Table III. ENISA's estimation of risk level, based on ISO/IEC 27005:2008

The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating:

Low risk: 0 – 2
Medium risk: 3 – 5
High risk: 6 - 8

ENISA provides 35 risk scenarios, which are identified in the assessment and classified into three categories: Policy & organizational, Technical and Legal. Each risk is presented in tables which include: Probability level, Impact level, Reference to vulnerabilities, Reference to the affected assets and Level of risk. Further information about this list is provided in (5).

3.2 Cloud risk assessment by The Commission Nationale de l'Informatique et des Libertés (CNIL)

CNIL's cloud risk assessment is another qualitative inductive scheme. Its methodology is mostly similar to the ENISA's framework. Further information can be found in (6).

4 Risk and Trust Models for the Cloud

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. These models are applied to the cloud computing paradigm and are further developed through their connection with trust assessment techniques.

4.1 Trust management

Definition of trust can be a starting point for modeling it. However, the term "trust" is a complex notion to define. In the paper (11), trust is defined as "the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trusting party, irrespective of the ability to monitor or control the trusted party." However, the paper (10) claimed that trust has hard part, which depends on the authentication and encryption, and soft part, which is based on aspects like brand and reputation.
In summary, according to (7), there are some common factors of trust, which are essential for a risky environment, used to make decisions, made based on experience, is an opinion of an individual and dependent on context. Trust management is based on four factors: Policies, Prediction, Recommendations, and Reputation.

4.2 Trust model in cloud computing

Trust model is defined as the scale of trust among two parties on each other. The idea of trust was taken from the relationship between customer and CSP. Such relation has some scope defined which is security threats. When the service provider monitors the actions of cloud system, the user or the clients generate ratings. There are two outlooks to define a trust model in computing world:

- Customer's outlook (What security does the service provider have?)

- Provider's outlook (What type of customer does it have?)

The clients must be informed about the security faults and vulnerabilities that exists in the system or that have the possibilities. Trust model is nothing but some set of protocols which are to be followed by the service provider and their users or customers. Users also have the facility to provide some rules to overpower the activities on cloud according to their choices. The syntax of the protocol must be in understandable and standard form. It must be able to interpret the instructions every time the user made a request. The continuous mentoring of the activities happening in the cloud helps the users or clients and provider to have the information about the threats breaching the security of the cloud network. The rating provided by the clients does not add much to the trust management system. It is better to make list of expectations from the cloud user's activities so that the provider will know about his expectations form the user. It also tells how the provider can manage the cloud instances. If there is an increase in the count of cloud instances within same time phase every year then the provider will allocate the resources automatically thereby increasing satisfaction. In summary, trust in cloud computing should relies on the reputation of the provider and self-estimation of their services. Trust is reputation based which is an aggregate opinion of a community, SLA verification-based trust which focuses on visible elements, Trust as a Service, which includes Cloud Trust Authority (CTA) to provide a single point for organizing security of cloud services from different CSPs, Policy based and Evidence-based trust.

There are several cloud trust models introduced by various researchers and organizations with their best parameters and efficiency. Security becomes most important criteria for the clients to choose one of the available cloud resources. When the user wants to choose a specific service, then he/she needs some ranking application to evaluate the quality of cloud service. A standard which assesses the reliability of cloud resources is the requirement of cloud clients to choose a service. In this paper, I introduce two well-known trust model, Cloud adopted risk assessment model and Joint risk and trust model.

4.2.1 Cloud adopted risk assessment model (CARAM)

CARAM is a model developed and implemented by A4Cloud recently. A4Cloud stands for Accountability for Cloud and Other Future Internet Services, and it is a European Union Seventh Framework Project.

CARAM is a qualitative and relative risk assessment model for assisting CCs to select a CSP that fits their risk profile best. It is based on the existing frameworks such as ENISA, CAIQ, CNIL developed in Europe for the last decade and complements them to provide the CC with a practical tool. For adapting the likelihood and impact assessments made in an ENISA report to a CSP and a CC, CARAM uses the information about the CSP available in STAR and assets owned by the CC, respectively. It is a decision support tool designed to help CCs in selecting a CSP that best fits their risk profile. It is a risk assessment approach such that evaluation is carried out for a specific CC, which means assessment for each CSP- CC pair is for that pair and not generic.

4.2.2 Joint risk and trust model (JRTM)

The JRTM is another model developed by A4Cloud. It is a quantitative risk assessment model that computes the probability of security, privacy, and service risks according to the CSP performance data. It calculates the probability that an event occurs and the probability that an event is eliminated before it becomes an incident, and subtracts the latter from the former. It based on statistical data is introduced for this purpose. The model addresses not only the security related risk but also the risk related to the performance of the services. It differentiates the negative performance from the positive performance in risk assessment based on the subscribers' preferences. It also takes into account the freshness of the data about the performance of the CSP again according to the parameters specified by the users. The model is simple enough to be practical for a TaaS used for MSaaS. Our initial experimentation also shows that its results are aligned with the perception of risks and trust.

References:

1 Cloud Security Alliance. Top Threats to Cloud Computing, The Egregious 11. 2020 edition.

2 S. Kaplan and B. J. Garrick. On the quantitative definition of risk. Risk Analysis 1(1): 11–27, 1981.

3 Drissi S., Houmani H. and Medromi H. Survey: Risk Assessment for Cloud Computing. Vol. 4 No.12, 2013

4 John R. Vacca - Cloud computing security_ foundations and challenges-CRC Press (2017)

5 European Network and Information Security Agency (ENISA). Cloud computing – Benefits, risks and recommendations for information security. November 09, 2009.
6 The Commission Nationale de l'Informatique et des Libertés. Methodology for Privacy Risk Management. (Translation of June 2012 edition).
7 Ramya and Priya Govindaraj, Subrata Chowdhury, Dohyeun Kim, Duc-Tan Tran and Anh Ngoc Le. A Review on Various Applications of Reputation Based Trust Management. May 2021.
8 Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan "Trust Management in Cloud Computing: A Critical Review" International Journal on Advances in ICT for Emerging Regions (ICT), ·November 2012
9 Alexandros Chrysikos, Stephen McGuire A Predictive Model for Risk and Trust Assessment in Cloud Computing: Taxonomy and Analysis for Attack Pattern Detection.
10 D. Osterwalder. Trust through evaluation and certifi- cation. Social Science Computer Review 19(1): 32–46, 2001.
11 R. C. Mayer, J. H. Davis, and F. D. Schoorman. An integrative model of organizational trust. The Academy of Management Review 20(3): 709–734, 1995
12 Erdal Cayirci, Alexandr Garaga, Anderson Santana de Oliveira and Yves Roudier. A Cloud Adoption Risk Assessment Model.
13 Erdal Cayirci. A Joint Trust and Risk Model for Msaas Mashups (2013)
14 Ritu, Sukhchandan Randhawa, Sushma Jain. Trust Models in Cloud Computing: A Review. 2017