Computer Standards & Interfaces 38 (2015) 44–50

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Scalable risk assessment method for cloud computing using game theory (CCRAM)

Evrim Furuncu, Ibrahim Sogukpinar *

Gebze Institute of Technology Computer Engineering Department, P.K. 141, Gebze, 41400 Kocaeli, Turkey

ARTICLE INFO

Article history:
Received 13 January 2013
Received in revised form 9 November 2013
Accepted 16 August 2014
Available online 27 August 2014

Keywords:
Cloud computing security
Scalable security using cloud service models
Game theory security modeling

ABSTRACT

Cloud computing is one of the most popular information processing concepts of today's IT world. The security of the cloud computing is complicated because each service model uses different infrastructure elements. Current security risk assessment models generally cannot be applied to cloud computing systems that change their states very rapidly. In this work, a scalable security risk assessment model has been proposed for cloud computing as a solution of this problem using game theory. Using this method, we can evaluate whether the risk in the system should be fixed by cloud provider or tenant of the system.

1. Introduction

Cloud computing has been increasingly used in recent years by organizations to deliver new services, enter new markets, get closer to customers and decrease IT operation costs. Generally, cloud computing is defined as usage of another computer's resources as a service that is delivered using a network. Technological advances in broadband connections made it possible to use for normal users of the Internet for cloud computing.

Since more than one entity uses these computer resources, its security becomes more important than normal IT resources that are used by one entity. By the definition of the National Institute of Standards and Technology (NIST), typically there are three different service models presented as follows for cloud computing [1].

- Software as a Service (SaaS): Software delivery model using cloud infrastructure. Since there is no need to install anything extra, users can access to this service from anywhere where they have Internet. Some examples are mail services, office applications, Customer Relationship Management (CRM) and collaboration, etc.
- Platform as a Service (PaaS): In this service model, tenant gets a platform where he/she can develop and run their application on. Cloud provider provides complementary services and required technological infrastructure to develop and run the application. Google AppEngine, Force.com and Microsoft Azure are known PaaS providers.
- Infrastructure as a Service (IaaS): In IaaS, cloud vendors provide the infrastructure to the tenant in the form of computing power or storage. Infrastructure comes from the data centers which are used virtualization to divide and distribute its resources. Rackspace Cloud, Google Computing Engine and Amazon EC2 are some examples for IaaS service model.

In each service model, different layers are needed to execute the service stack. Since each service model requires different computing resources, security measures which are used for each of these service models may be varied. Some security measures in some service models must be implemented by the cloud provider. However, the other security implementations are not necessarily needed to be done by cloud provider; instead, they must be implemented by the tenants. These security precautions can be different depending on Service-level Agreement (SLA) which is a negotiated agreement between tenant and the cloud provider.

Security requirements for the service models that are defined by NIST [1] are given in Table 1. However, a point to be made here is that cloud computing does not consist of only three models. Apart from the NIST defined models SaaS, PaaS and IaaS, there are other models currently used by providers such as:

- Storage as a Service (STaaS or SaaS): In this model, the service provider rents space in its infrastructure to another party or individual.
- Desktop as a Service (DaaS): Delivers a “virtualized” desktop to the user; thus, all the programs, applications, processes and data are kept on centralized server.
- Network as a Service (NaaS): This model includes application accelerating, security measures or mobile device management, etc.
- Data a Service (DaaS): Providing data on demand to the tenant

* Corresponding author. Tel.: +90 262 605 2201; fax: +90 605 2205.
E-mail addresses: efuruncu@bilmuh.gyte.edu.tr (E. Furuncu), ispinar@bilmuh.gyte.edu.tr (I. Sogukpinar).

http://dx.doi.org/10.1016/j.csi.2014.08.007
0920-5489/© 2014 Elsevier B.V. All rights reserved.

Table 1
Security requirements for cloud computing.

IT security requirements (X requirement, * optional requirement)	Cloud deployment models					
	Public			Private		
	Cloud service models					
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
Availability	X	X	*	X	X	X
Authorization	X	X	X	*	*	X
Confidentiality	*	*	X	*	X	X
Integrity	X	*	X	*	X	X
Authentication	X	*	X	X	*	X

regardless of geographic or organizational separation of the provider or tenant.

Security measures for these service models are different than each other because of the requirements for different resources. For example, availability requirement for NaaS is more important than the other requirements. Because, it is the elementary need for that service to provide bandwidth and the network. The cloud provider is not responsible for ensuring confidentiality and integrity of the passing data. But, since all computation is done by the provider in SaaS model, all the security properties presented in Table 1 must be implemented by the SaaS provider.

Network attackers are generally known as intelligent and rational human beings. They consider the cost and profit of their attacks. Defenders profit when a harmful attack is blocked by their security systems. But, if such an attack doesn't happen, they can lose money because of the unnecessary security measures. These properties make it possible to model this behavior in game theory [14,15]. Like in network security, there is an important game connection between attackers and defenders in the cloud computing. Ideal defensive strategy and ideal offensive strategy may be changed depending on each other.

Game theory techniques are used in economy, biology, mathematics, psychology and other social and behavioral sciences. In computer science, many works used game theory have been realized on intrusion detection systems (IDS) [2], security scheduling [3] and network/cyber security [4,15–20]. In the recent years, studies between game theory, economic theory and computer science have given way to a new field, Algorithmic Game Theory [5].

In this work, a model has been proposed to determine defensive and offensive ideal strategies using properties of defender and attackers that are mentioned above and considered the security measures taken. Strategies increasing gain or reducing damage are presented to the corresponding players using this model. As a result, cloud computing security staff can determine which security measures should be taken depending on their gain or loss. The proposed model is a novel solution for security of cloud computing. Evaluated security risks using proposed method in the cloud computing system should be mitigated by a cloud provider or a tenant of the system.

The rest of the paper is organized as follows: Section 2 includes related works. Section 3 introduces the proposed model. Section 4 gives a brief practical example and discussion. Section 5 presents our conclusions and future work.

2. Related works

Since risk assessment in cloud computing is a hot topic, most of researches in this topic are built on grid computing infrastructure. Research that is based on grid computing generally do not cover the storage of data which is an important aspect of cloud computing because most grids are used to solve a single task and do not cover storage of the data, and also most of these research focuses on static risk assessments. In ref [6], the FPVA model applies mostly to grid middleware which is used to separate the work load of a program into more physical machines. Although it seems similar to a cloud, because users create platform or change the platform in IaaS and PaaS service models, FPVA model becomes ineffective for such targets. Basically, this model first creates a tree that consists of the interactions between applications and assets. After, each node in this tree is analyzed for relationship with each other and examined for the possible security vulnerabilities. Next, each node's programming code is manually inspected by experts considering the possible security vulnerabilities that tree relation presented. One of the biggest problems of this model is that manually inspecting the cloud APIs would take so much time considering the magnitude of IaaS and PaaS APIs. Another problem is that even though cloud and grid technologies seem similar, the risk associated with them is different with each other.

Peiyu and Dong proposed a three layered risk assessment model summarized as follows using AHP in ref. [7].

- Level one: Formulates the problem in a hierarchical structure. The overall objective is placed on the top of the level. In this model, it corresponds to the overall assessment of the cloud computing system platform.
- Level two: Includes eight attributes consisting of major factors identified for assessing level one.
- Level three: The last level is for concrete assessment factors in the decision framework. Thirty nine factors were identified corresponding to higher levels and specific local conditions.

Implementation of the AHP requires three principles: decomposition, pair-wise comparisons and synthesis of weights. Some advantages using AHP process in cloud computing are:

- Able to break problem into heretical pieces,
- Able to quantify the decision-marker's experimental judgments, particularly when the objectives lacked quantifiable data.

Decision makers evaluate the assessment considering the factors defined in level three and each one is given a weight and put together in a matrix to get a weight factor. The problem in here, decision makers have to manually change the vectors until assessments pass verification of consistency.

J. Oriol Fitò and Jordi Guitart [8] proposed a semi-quantitative approach to risk assessment for cloud computing. Decisions are made by considering business level objects such as; maximizing profit and user satisfaction. In this semi-quantitative approach, some risks even turn into gain for the business. Impact of the risks changes between two factors: benefit and threat. Before comparison, risks are grouped considering the following factors:

- The probability of occurrence of a risk event: Takes values between 1 and 5. Expressed by means of very unlikely (1, e.g. once in 20 years), unlikely (2, e.g. yearly), possible (3, e.g. monthly or weekly), likely (4, e.g. daily), and frequent (5, e.g. at any moment).
- The impact of that event: Either a threat, a benefit, or both, semi-quantified between very high (−5 or 5, for negative and positive impact, respectively), high (−4/4), medium (−3/3), low (−2/2) and very low (−1/1).
- The risk-level estimation: This is proportional to the probability of a given event and its business level object in question.

In this method, probability of the risk is multiplied with the impact of the risk to get risk level estimation which is between the values of −25 and +25 [8]. Considering the impact of the risks (benefit and threat), this is a narrow interval. In our method, considering the service model of the provider and the value of the system, our interval size is larger. Also, the proposed model does not take risks as a benefit in any way in order to eliminate any problems that may occur in the future.

M. Kiran et al. [9] explained in their paper that most proposed risk assessments in cloud computing considers heavily on user side of