Journal of Information Security and Applications 000 (2017) 1–11

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Towards quantification and evaluation of security of Cloud Service Providers

Talal Halabi, Martine Bellaiche*

Génie Informatique et Génie Logiciel, École Polytechnique de Montréal, Montreal, Quebec, Canada

ARTICLE INFO

Keywords:
Security quantification
Security evaluation
Cloud Service Provider (CSP)
Cloud Security Services
Security metrics
Goal-Question-Metric (GQM) method

ABSTRACT

Security is still the main obstacle preventing companies and businesses which deal with private information and confidential data from migrating towards the Cloud. Cloud Service Providers should continuously perform security self-evaluation and assess the level of their security services in order to identify their limitations and improve their performance. We propose in this paper, a methodology for performance quantification and evaluation of Cloud security services, based on a set of quantitative evaluation metrics which we developed using the Goal-Question-Metric (GQM) paradigm. We also make use of a case study scenario in order to demonstrate the efficiency and practicability of the proposed methodology.

1. Introduction

The scientific and industrial communities are currently receiving Cloud Computing technology with growing attention and research efforts. Cloud Computing has many technical and financial advantages, such as scalability, resilience, performance, and portability. It forms a new business model and computing paradigm by providing the possibility of on-demand network access to an environment of shared and configurable resources (e.g., networks, servers, storage, applications, and services), the advantage of rapid provision and release with minimal management effort or service provider interaction, and the possibility of cost reduction through optimized computing [1].

According to NIST [2], the five essential characteristics of Cloud Computing are: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The Cloud Computing architecture consists of three layers: (i) Software-as-a-Service (SaaS) which is run by Cloud Service Providers (CSPs) and mostly used by organizations; (ii) Platform-as-a-Service (PaaS) which is a tool provided to develop applications without installing any software on the developer's side; and (iii) Infrastructure-as-a-Service (IaaS) which includes storage, hardware, servers, and networking services operated, maintained, and controlled by the CSPs. Four different deployment models exist in Cloud Computing: (a) public clouds in which the physical infrastructure is owned and managed by the CSP; (b) community clouds in which the physical infrastructure is owned and managed by a group of organizations; (c) private clouds in which the infrastructure is owned and managed by a specific organization or company; and (d) hybrid clouds which include combinations of the previous three models [3].

Recent statistics [4] showed that most organizations that adopted Cloud Computing are running IaaS applications and over a public Cloud infrastructure. These organizations have witnessed a remarkable growth in Cloud benefits during the previous years in a variety of categories, including higher availability, geographic reach, cost savings, and business continuity. These statistics also showed that security concerns are one of the main factors slowing down the Cloud adoption, especially for healthcare companies and businesses that deal with sensitive and confidential information. Although organizations can take advantage of many security benefits provided by the Cloud, compared to traditional on-premises technologies, the Cloud presents many specific features that introduce new vulnerabilities and security challenges. Besides its very large scale, resources in the Cloud are completely distributed, heterogeneous and virtualized. Thus, traditional security mechanisms in their current form, involving identity management, authentication, authorization, and infrastructure security, are no longer efficient to ensure the protection for clouds. The Cloud may present different risks to an organization compared to traditional IT solutions, which makes moving critical applications and sensitive data to public Cloud environments a great concern for corporations [1].

To reduce these concerns and entice companies to take advantage of the many benefits of Cloud Computing technologies, CSPs should be able to assess their security levels through contin-

* Corresponding author.
E-mail addresses: talal.halabi@polymtl.ca (T. Halabi), martine.bellaiche@polymtl.ca (M. Bellaiche).

http://dx.doi.org/10.1016/j.jisa.2017.01.007
2214-2126/

uous self-evaluation. Evaluation of Cloud security services should be based on standard vocabularies and effective metrics, which are missing in today's clouds. Evaluating Cloud security services will also allow the providers to situate themselves within the Cloud market and help them determine the price of their services based on their security level. We propose through this research, a methodology to quantify and evaluate the Cloud security services. The contribution of this work is twofold:

- First, we identify the Cloud security services provided on each layer of the Cloud architecture and we develop a set of measurable security metrics using the Goal-Question-Metric (GQM) method in order to evaluate these services and quantify their performance.
- Second, we propose a methodology for relative evaluation of CSP's security services based on objective weighting of metrics which facilitates automation.

The remainder of this paper is organized as follows. Section 2 discusses the literature review related to Cloud security challenges and existing Cloud security evaluation approaches. Sections 3 and 4 define the Cloud security aspects and services respectively. In Section 5, the set of Cloud security evaluation metrics is developed. Section 6 describes the proposed Cloud security evaluation methodology. In Section 7, the proposed methodology is applied through a case study scenario. Finally, Section 8 concludes the paper.

2. Literature review

In this section, the recent research that tackled Cloud Computing security challenges, issues, and existing and emerging solutions is presented. Then, the recent work related to the evaluation of Cloud security is surveyed.

2.1. Cloud Computing security challenges

Many recent papers address the security challenges in the Cloud. The Cloud Security Alliance (CSA) [5] specified the top threats to Cloud Computing security as: abuse and nefarious use, insecure interfaces and APIs, malicious insiders, shared technology, data loss or leakage, account or service hijacking, and unknown risk profiles [6]. It also developed security guidance for critical areas of focus in Cloud Computing including Cloud architecture, governance, and operation [7]. The guide describes best practices and recommended security solutions in the domains of data security, virtualization, encryption and key management, identity and access management, and incident response.

Subashini and Kavitha [8] identified the security issues that emerged due to different service delivery models in a Cloud system. They categorized Cloud security problems into four fundamental categories: data storage security, data transmission security, application security, and security related to third party resources. In their survey, they provided a detailed description of security issues in SaaS Cloud models, and considered data security, network security, service availability, and identity management as essential elements for secure SaaS applications.

Gonzalez et al. [9] presented a three-dimensions Cloud security taxonomy by arranging Cloud risks and vulnerabilities into hierarchical categories. The architecture dimension comprises the issues related to network security, interfaces and virtualization; the compliance dimension deals with required responsibilities toward CSPs; and the privacy dimension is based on data security and legal issues.

Khalil et al. [3] conducted a survey on the current Cloud security issues and state-of-the-art security solutions. They divided Cloud security into five categories: security standards, network, access control, Cloud infrastructure, and data, and discussed the security issues for each category, in addition to the relationships between them. They also described known attacks against clouds in terms of causing vulnerabilities, provoked incidents, and related consequences, and provided a comparative analysis of the solutions and countermeasures.

Bhadauria and Sanyal [10] discussed the threats to security in Cloud Computing on the basic level, network level, and application level. They mentioned three different threats to basic security, namely: SQL injection attacks, Cross Site Scripting (XSS) attacks, and Man in the Middle attacks (MITM). They also described the threats to network level security, such as DNS attacks, sniffer attacks, issues of reused IP addresses, and BGP prefix hijacking. Finally, they described threats to application level security, such as security of Hypervisor, Denial of Service attacks, and other threats related to security of web applications.

Sen [11] identified the threats to different Cloud security aspects. He discussed internal/external attacks and data leakage as threats to confidentiality, user access and data segregation and quality as threats to integrity, and denial of service, change management, physical disruption, and inefficient backup procedures as threats to availability.

Xiao and Xiao [12] described in detail the vulnerabilities and threats related to Cloud security, in addition to existing defense strategies, in the context of five different Cloud security attributes, namely: confidentiality, integrity, availability, accountability, and privacy. They identified Cloud vulnerabilities as: VM co-residence, loss of physical control, bandwidth under-provisioning, and Cloud pricing model, and related it to three essential Cloud characteristics: outsourcing of data, multi-tenancy, and massive data and intense computation.

2.2. Cloud security evaluation

Cloud security evaluation is a challenging area in the research on Cloud Computing. Although present security standards can help CSPs in implementing their security systems, more efforts are needed for Cloud security standardization. NIST [13,14] and CSA [5] are investing much efforts in this area. CSA CRC [19] and CCM [20] projects are good examples of such work. The main motivation of our work in this paper is the lack of standard Cloud security evaluation metrics that can be used in assessing CSP's security levels in an efficient manner. The metrics developed here can also be defined and described using the model proposed by NIST in [14] for the Cloud Computing service metrics description. Many authors have been trying to develop standard methodologies to evaluate the performance of security services in Cloud Computing. We review here some of the work conducted in this area.

The Service Measurement Index (SMI) [15] is in continued development to provide valid measures that help in evaluating and comparing Cloud services but no quantitative security evaluation metrics have been developed yet. Da Silva et al. [16,17] proposed a Cloud management methodology as well as an approach to Security Service Level Agreement (Sec-SLA) based on a security metrics hierarchy that describes the security level in a Cloud computing environment. However, they did not consider all critical security aspects and services in the Cloud. In [18], the same authors use the proposed system of metrics to evaluate the Return On Security Investment (ROSI) in the Cloud.

Ristov et al. [21] defined a methodology to quantify the ISO 27001:2005 requirements [22] grouped into control objectives, based on which they compared on premise and Cloud environments. They concluded that the existing general purpose security standards do not cover all Cloud security challenges, and proposed a new ISO 27001:2005 control objective, called Virtualization Man-

Please cite this article as: T. Halabi, M. Bellaiche, Towards quantification and evaluation of security of Cloud Service Providers, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.007