Information Sciences 305 (2015) 357–383

Contents lists available at ScienceDirect

Information Sciences

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

Security in cloud computing: Opportunities and challenges

Mazhar Ali [a,c,*], Samee U. Khan [a], Athanasios V. Vasilakos [b]

[a] North Dakota State University, USA
[b] Kuwait University, Kuwait
[c] COMSATS Institute of Information Technology, Abbottabad, Pakistan

ARTICLE INFO

Article history:
Received 5 September 2014
Received in revised form 28 January 2015
Accepted 29 January 2015
Available online 7 February 2015

Keywords:
Cloud computing
Multi-tenancy
Security
Virtualization
Web services

ABSTRACT

The cloud computing exhibits, remarkable potential to provide cost effective, easy to manage, elastic, and powerful resources on the fly, over the Internet. The cloud computing, upsurges the capabilities of the hardware resources by optimal and shared utilization. The above mentioned features encourage the organizations and individual users to shift their applications and services to the cloud. Even the critical infrastructure, for example, power generation and distribution plants are being migrated to the cloud computing paradigm. However, the services provided by third-party cloud service providers entail additional security threats. The migration of user's assets (data, applications, etc.) outside the administrative control in a shared environment where numerous users are collocated escalates the security concerns. This survey details the security issues that arise due to the very nature of cloud computing. Moreover, the survey presents the recent solutions presented in the literature to counter the security issues. Furthermore, a brief view of security vulnerabilities in the mobile cloud computing are also highlighted. In the end, the discussion on the open issues and future research directions is also presented.

1. Introduction

Since its inception, the cloud computing paradigm has gained the widespread popularity in the industry and academia [88]. The economical, scalable, expedient, ubiquitous, and on-demand access to shared resources are some of the characteristics of the cloud that have resulted in shifting the business processes to the cloud [25,2]. The cloud computing attracts the attention of research community due to its potential to provide tremendous benefits to the industry and the community [9,88]. The resources are provided to the users and released based on demands from the pool of shared resources [4]. The on-demand resource provisioning ensures the optimal resource allocation and is also cost effective [78]. The consumers (individuals and business organizations) no longer need to invest heavily in the information technology (IT) infrastructure [4]. Customers use resources provided by the cloud and pay according to the use. On the other hand, cloud providers can re-use resources as soon as they are released by a particular user resulting in improved resource utilization [78]. Ease of use is yet another advantage being offered by the cloud computing because it does not require the customers to possess extraordinary expertise pertaining to the cloud specific technologies [5]. The management of the technology and services has moved from user to the service provider's end [5].

* Corresponding author.
E-mail addresses: mazhar.ali@ndsu.edu (M. Ali), samee.khan@ndsu.edu (S.U. Khan), vasilako@cs.ku.edu.kw (A.V. Vasilakos).

http://dx.doi.org/10.1016/j.ins.2015.01.025
0020-0255/

The cloud computing provides virtualized resources to the customers using various technologies, for example, Web services, virtualization, and multi-tenancy. The cloud services are delivered to the customer through the Internet [25]. The Web applications are used to access and manage cloud resources that makes Web applications an important component of the cloud computing [70]. The customers' processes are executed in virtualized environment that in turn utilize the physical resources [35]. Multiple virtual processes of various users are allocated to same physical machines that are segregated logically. This gives rise to a multi-tenant environment in the cloud. Despite the provided advantages, the cloud computing is not exclusive of risks with security being the key risk [57].

Security is one of the biggest obstacles that hamper the widespread adoption of cloud computing [28]. Several business and research organization are reluctant in completely trusting the cloud computing to shift digital assets to the third-party service providers [57]. The conventional IT infrastructure keeps the digital assets in the administrative domain of the organizations. All of the processing, movement, and management of data/application are performed within the organizational administrative domain. On the other hand, organizations do not enjoy administrative control of cloud services and infrastructure [52]. The security measures taken by the cloud service providers (CSP) are generally transparent to the organizations. The presence of large numbers of users that are not related to the organizations, aggravate the concerns further [57]. The users might be trusted by the CSP but they may not be of trust to each other. The aforementioned reasons keep the customers under uncertainties about their digital assets located at the cloud resulting in reluctance to adopt cloud computing [57].

There are various studies in the literature discussing the security issues of the cloud computing. The authors in [85,101] presented reviews on the security issues of the cloud computing. However, the aforesaid studies are limited to the discussion of security issues only and the security solutions are not discussed. Ref. [71] reviewed the security issues at different levels of cloud computing. The security solutions have also been presented in [71]. However, the future discussion has not been discussed comprehensively and overview of the cloud technology is missing. The authors in [1] presented a comprehensive study of privacy preservation in the cloud with focus only on e-health clouds. Moreover, the study in [1] is limited in scope to the privacy only. Ref. [121] reviewed the security and privacy challenges in the cloud computing and discussed the defense strategies for the existing vulnerabilities. However, the discussion of the security issues in [121] was centered on confidentiality, integrity, availability, accountability, and privacy-preservability with little discussion on the technologies causing the vulnerability origination. The authors in [74] elaborated the security issues in the cloud along with the approaches that can be employed to tackle the vulnerabilities. Nevertheless, the discussion on future research directions is lacking in the survey. Likewise, the work in [39] detailed the security issues in the cloud computing in depth with brief discussion on current and latest security solutions. The work in [18] surveyed the popular security models of cloud computing, such as cube model, multi-tenancy model, and risk assessment model. Moreover, the authors of [18] have discussed the security risks of cloud computing. However, the risks are discussed from the perspective of different stack holders, like customers, government, and service providers. Security issues from the technological and operational point of view were not in the scope of the aforesaid study. Similarly, the strategies to relieve the security issues are discussed in terms of "what" components and processes should be secured and evaluated. "How" the security objectives are achieved in current research is not elaborated. Similarly, the article [104] describes the security issues in cloud computing and associated security solutions. However, the discussion is more focused on the privacy part of cloud security. Moreover, there is no discussion on future research directions. Our survey differs significantly from the aforesaid surveys in terms of its extensiveness, comprehensive discussion on security issues in cloud computing, and emphasizes on latest security solutions presented in the literature. We also provide the tabulated comparisons of the presented techniques. Moreover, we briefly discuss the security issues pertaining to mobile cloud computing and generic strategies that can lead to solutions. The contributions of this survey with respect to the aforesaid surveys are presented in Table 1. The "✓" and "✗" denote whether the domain specified in the column has been discussed in the survey or not.

The remainder of the paper is organized as follows. Section 2 provides the architectural framework of the cloud computing. The security issues in the cloud computing paradigm are detailed in Section 3 whereas the existing solutions in the contemporary literature are presented in Section 4. Section 5 highlights the security concerns in the mobile cloud computing (MCC). Section 6 discusses the techniques and open issues and Section 7 concludes the survey.

Table 1
Contributions of this study with respect to the discussed surveys.

Work	Cloud overview	Security issues	Counter measures	Open issues
[85]	✓	✓	✗	✗
[101]	✓	✓	✗	✗
[71]	✗	✓	✓	✗
[1]	✗	Privacy only	✓	✓
[121]	✓	✓	✓	Privacy only
[74]	✗	✓	✓	✗
[39]	✗	✓	✓	✗
[18]	✗	✓	✓	✗
This survey	✓	✓	✓	✓