Journal of Network and Computer Applications 61 (2016) 59–80

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Authentication in mobile cloud computing: A survey

Mojtaba Alizadeh [a,b], Saeid Abolfazli [c,*], Mazdak Zamani [d], Sabariah Baharun [b], Kouichi Sakurai [a]

[a] Department of Informatics, Graduate School and Faculty of Information Science, Kyushu University, Fukuoka, Japan
[b] Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi, Malaysia
[c] YTL Communications and Xchanging, Malaysia
[d] Department of Computer Science, Kean University, NJ, USA

ARTICLE INFO

Article history:
Received 29 March 2015
Received in revised form
21 September 2015
Accepted 18 October 2015
Available online 6 November 2015

Keywords:
Cloud computing
Mobile cloud computing
Security
Authentication

ABSTRACT

Mobile cloud computing (MCC) is the state-of-the-art mobile distributed computing model that incorporates multitude of heterogeneous cloud-based resources to augment computational capabilities of the plethora of resource-constraint mobile devices. In MCC, execution time and energy consumption are significantly improved by transferring execution of resource-intensive tasks such as image processing, 3D rendering, and voice recognition from the hosting mobile to the cloud-based resources. However, accessing and exploiting remote cloud-based resources is associated with numerous security and privacy implications, including user authentication and authorization. User authentication in MCC is a critical requirement in securing cloud-based computations and communications. Despite its critical role, there is a gap for a comprehensive study of the authentication approaches in MCC which can provide a deep insight into the state-of-the-art research. This paper presents a comprehensive study of authentication methods in MCC to describe MCC authentication and compare it with that of cloud computing. The taxonomy of the state-of-the-art authentication methods is devised and the most credible efforts are critically reviewed. Moreover, we present a comparison of the state-of-the-art MCC authentication methods considering five evaluation metrics. The results suggest the need for futuristic authentication methods that are designed based on capabilities and limitations of MCC environment. Finally, the design factors deemed could lead to effective authentication mechanisms are presented, and open challenges are highlighted based on the weaknesses and strengths of existing authentication methods.

Contents

* Corresponding author.
E-mail addresses: amojtaba2@live.utm.my, 9IE14015W@s.kyushu-u.ac.jp (M. Alizadeh), abolfazli@ieee.org (S. Abolfazli), mzamani@kean.edu (M. Zamani), sabariahb@utm.my (S. Baharun), sakurai@csce.kyushu-u.ac.jp (K. Sakurai).

http://dx.doi.org/10.1016/j.jnca.2015.10.005
1084-8045/

1. Introduction and motivation

The mobile cloud computing (MCC) is “a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or the Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle.” (Sanaei et al., 2013). MCC incorporates cloud computing, mobile computing, and wireless networking and aims to provide cloud-based services to the mobile consumers (Abolfazli et al., 2014a; Fernando et al., 2013). In MCC, execution time and energy consumption are significantly improved by transferring execution of resource-intensive application from the hosting mobile to the cloud-based resources.Therefore, once MCC is fully deployed, the mobile devices do not require high resources, such as central processing unit (CPU), random access memory (RAM), storage, and particularly battery, because the entire data or complex computing are manipulated in the remote cloud-based resources (Ko et al., 2012; Abolfazli et al., 2012; Liu et al., 2015). MCC has emerged as a subset of cloud computing to enable intensive on-demand elastic computing and storage on the go to the potential mobile users. Mobile devices, particularly tablet personal computers, smart phones, and PDAs are becoming an integral part of today's lifestyle as they are convenient and effective communication endpoint. The swift development of mobile computing has become a forceful pattern in IT technology's development in commerce and related fields. According to Cisco visual networking index statistics (Cisco, 2014), the usage of smartphone and global mobile data traffic grew 50 and 81 percent in 2013, respectively. Nevertheless, performance and functionality of mobile devices are hindered by several limitations, particularly computing and storage resources (i.e., CPU, RAM), wireless communication throughput, battery life, local data safety, communication security, and mobility impeding development of the quality of service (Abolfazli et al., 2014a). The idea of remote computing and the process of augmenting mobile devices using remote cloud-based computing and storage resources is envisioned to overcome the inherent challenges and shortcomings in mobile computing (Aminzadeh et al., 2015). This is carried out by utilizing other resource providers besides the mobile device to host the delivery of resource-intensive mobile applications (Dinh et al., 2013; Alizadeh et al., 2013a,b).

Although MCC is proven to be advantageous in augmenting computational capabilities of mobile devices and conserving their native resources, leveraging remote resources introduces several challenges, including reliability, security, trust, and privacy (Khalil et al., 2014; Xuanxia et al., 2014; Khan et al., 2013a; Sood, 2012). Successful diffusion of cloud computing technology with mobile devices incites users desires for efficient and also secure service delivery. Furthermore, in MCC environment, typical mobile devices communicate through the combination of heterogeneous wireless networks, which is more energy-intensive compared to wired communication. Hence, reducing mobile devices' resource consumption is an important and critical problem in delivering sustainable and long-lasting on-demand services to the end-users (Shon et al., 2014). Although mobile devices' resource poverty can be alleviated by cloud computing and cloud-based augmentation techniques (Abolfazli et al., 2014a), inadequate security management inhibits development and successful deployment of cloud-connected security-sensitive applications in broad areas, including health-care, financial services, and e-government services.

Researchers in several efforts (Yang et al., 2014; Li and Li, 2014; Si et al., 2014; Xia et al., 2014; Sookhak et al., 2014; Kaewpuang et al., 2013; Rahimi et al., 2013; Yang et al., 2013; Ma and Wang, 2012; Satyanarayanan et al., 2009; Ra et al., 2011) have studied varied aspects of MCC, including task outsourcing, heterogeneity, virtualization, energy saving, and remote auditing, aiming to enhance the MCCs performance and efficiency. However, security (as another crucial aspect of MCC), particularly authentication is overlooked. The security challenges in MCC are twofold, namely cloud security and mobile network security because of the co-existence of cloud computing and mobile computing in MCC (Peng et al., 2014; Morrow, 2011; Zissis and Lekkas, 2012; Dijiang et al., 2011). One of the most important security issues for MCC users is authentication and authorization (Esposito and Ciampi, 2015; Yu and Wen, 2012; Riley et al., 2011). As an example, a lost or stolen mobile device could be abused to access a host and download sensitive data from the cloud, if a mobile user is registered with a particular cloud service provider, both mobile device and cloud server should authenticate each other in order to secure the communication when the mobile user accesses the cloud from different locations using heterogeneous networks and various mobile devices (Clarke et al., 2002).

Several studies (Xu et al., 2013; Wang et al., 2013; Noureddine and Bashroush, 2013; Ghazizadeh et al., 2014; Singh and Singh, 2012; Guo et al., 2012; Dinesha and Agrawal, 2012; Li et al., 2013; Zhi-Hua et al., 2012; Zhang et al., 2012; Yongqing and Xiang, 2012; Yassin et al., 2012; Wang and Jia, 2012; Sang-Ho et al., 2012; Ahn et al., 2011) have been conducted to propose suitable authentication schemes in cloud computing. However, authentication in MCC, as one of the most crucial security countermeasures, has not been studied yet. Moreover,