Computers in Human Behavior 58 (2016) 150–157

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Full length article

Understanding and predicting students' intention to use mobile cloud storage services

Ibrahim Arpaci

Gaziosmanpasa University, Department of Computer Education and Instructional Technology, Tokat, Turkey

ARTICLE INFO

Article history:
Received 2 May 2015
Received in revised form
23 December 2015
Accepted 28 December 2015
Available online xxx

Keywords:
Mobile cloud computing
Cloud storage
Ubiquity
Trust

ABSTRACT

The challenges of mobile devices such as limited bandwidth, computing, and storage have led manufacturers and service providers to develop new value-added mobile services. To address these limitations, mobile cloud computing, which offers on-demand services including platforms, infrastructure, and software have been developed. This study attempts to build a significantly improved research framework based on the Technology Acceptance Model in order to identify factors that affect students' attitudes toward and intentions in using mobile cloud storage services. A structural equation model was used to assess the proposed model based on the data collected from 262 undergraduate students. Results show that perceived usefulness, subjective norm, and trust have a significantly positive effect on the attitude, which in turn is a significant predictor of behavioral intentions. The research model, which explains 82% of the variance in attitudes toward using mobile cloud storage services has a strong predictive power. The findings have both theoretical and practical implications for academics, managers, and educational institutions.

1. Introduction

Cloud computing is a specialized distributed computing paradigm that offers dynamically scalable computing resources, such as computational power, storage, or business applications provisioned as a service over the Internet (Stanoevska-Slabeva, Wozniak, & Ristol, 2010). Similar to the Internet's layered architecture, cloud computing has hardware, software, virtualization, and management layers. The hardware and software layers, which include hard drives, processors, network devices, the operating systems are responsible for storage and processing. The virtualization layer, which separates the logical from the physical layer, is used to provide the essential cloud characteristics of location independence, resource pooling, and rapid elasticity. Differing from the traditional client–server network topology cloud computing is able to offer robustness and alleviate traffic congestion. Thus, the management layer is able to monitor traffic and implement security mechanisms throughout the cloud (Zissis & Lekkas, 2012).

Cloud computing provides services at three different levels including Infrastructure as a Service (IaaS), Platform as Service (PaaS), and Software as Service (SaaS). IaaS offers users with the capability to control the underlying cloud infrastructure, including operating systems, network, servers, storage, and applications. Whereas, PaaS offers users with the capability to deploy applications produced using programming languages and tools supported by service providers on the cloud infrastructure. However, SaaS provides users with the capability to use applications provided by cloud service providers on the cloud infrastructure. The users do not manage the underlying cloud infrastructure or application capabilities (Shon, Cho, Han, & Choi, 2014).

Deployment models offered by cloud providers have different levels of security. In private and community cloud, the cloud infrastructure is managed by the organization or a third party, and may exist on premise or off premise. However, in public cloud the infrastructure is made available to the general public. In hybrid cloud, the cloud infrastructure is a composition of two or more deployment models that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (Mell & Grance, 2009).

Cloud computing has a number of unique characteristics including the flexibility of capabilities, the scalability of infrastructure, broad network access, location independence, reliability, the economies of scale, cost effectiveness, and sustainability (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009; Shon et al., 2014). However, it has a number of challenges such as data

E-mail address: ibrahim.arpaci@gop.edu.tr.

http://dx.doi.org/10.1016/j.chb.2015.12.067
0747-5632/

recovery, confidentiality, privacy, integrity, availability, reliability, and security (Fernando, Loke, & Rahayu, 2013; Kim & Park, 2013; Wang & Dey, 2013). These risks are similar to mobile cloud computing, which inherits the challenges and advantages of mobile devices. On the other hand, most of the challenges of mobile devices such as limited bandwidth, computing, and storage can be addressed by mobile cloud computing services (Dinh, Lee, Niyato, & Wang, 2013).

In this paper, mobile cloud computing refers to an infrastructure in which different mobile devices (i.e. smartphones, tablets, and laptops) can access various computing resources anytime and anywhere. One of the key functionalities of mobile cloud computing is providing users data storage services on the cloud where they can backup, revise, access, or share files over their mobile devices. Some popular examples of mobile cloud storage services are Dropbox, iCloud, SkyDrive, and Google Drive. These services can operate across different platforms including Android, iOS, and Blackberry and enable users synchronize their application data such as photos, videos, music, calendars, documents, and files.

Mobile device ownership has recently experienced substantial growth and thus the user acceptance of mobile cloud services has emerged as a significant research domain. Among others, mobile cloud storage services are the most closely related to students' needs as they provide them to store, share, and effectively manage their files and documents. To this end, the present study aims to identify the key factors affecting students' attitudes toward and intentions in using mobile cloud storage services. The major contribution of this paper is to identify new factors as well as to develop an integrated model to investigate the factors affecting the decision to introduce cloud computing services in the educational settings.

2. Literature review

Cloud computing has been a frequent theme of recent research (Alamri et al., 2014; Jou & Wang, 2013; Lin, Wen, Jou, & Wu, 2014; Navimipour, Rahmani, Navin, & Hosseinzadeh, 2015; Park & Ryoo, 2013; Stantchev, Colomo-Palacios, Soto-Acosta, & Misra, 2014; Zhang, Ma, Wu, Ordonez de Pablos, & Wang, 2014). For example, Shin (2015) investigated the factors that influence potential user adoption of cloud computing. His results show that user intentions and behaviors are largely influenced by the perceived values of cloud services, which include access, availability, security, and reliability. In another study, Paquette, Jaeger, and Wilson (2010) identified possible risks associated with the governmental use of cloud computing such as the reliability of the cloud, the continuity of the services, security to prevent unauthorized access, safety mechanisms, data confidentiality and privacy, and the location of legal jurisdiction.

Yang, Sun, Zhang, and Wang (2015) investigated the factors that influence organizational readiness to adopt SaaS. Their results suggest that organizational users need to get prepared from technological, organizational, and environmental aspects for the adoption of SaaS. In a similar study, Gupta, Seetharaman, and Raj (2013) focused on the adoption of cloud computing by small and medium enterprises (SMEs). Their results suggest that the ease of use, convenience, security, privacy, and cost reduction are the main factors influencing cloud usage by businesses. Moreover, their results indicate that SMEs do not want to use cloud services for sharing data and collaborating with their stakeholders as they do not trust these services.

Rong, Nguyen, and Jaatun (2013) reported some important security challenges in cloud computing, including resource location, interoperability and free data movement among clouds, security, identity management and privacy, authentication and trust, system monitoring and logs, and multi-tenancy issues. Moreover, they suggested some possible solutions for these challenges such as service level agreements for security and holistic mechanisms for ensuring accountability in the cloud. In another study, Marston, Li, Bandyopadhyay, Zhang, and Ghalsasi (2011) identified the strengths (i.e., lowering costs, immediate access to resources, and scalability), weaknesses (i.e., the quality of service, data location, and availability), opportunities (i.e., the effective use of information technology and mashups), and threats (i.e., the lack of standards, security, performance, and reliability) of cloud computing from a business perspective.

González-Martínez, Bote-Lorenzo, Gómez-Sánchez, and Cano-Parra (2015) suggested the benefits of cloud computing for educational institutions such as the availability of online applications to support education, the flexible creation of learning environments, support for mobile learning, computing-intensive support for teaching, learning and evaluation, the scalability of learning systems and applications, and cost savings. Moreover, they reported several risks of cloud computing for educational institutions such as the lack of interoperability, performance, reliability, security, privacy, licensing, and price models. In another study, Duranti and Rogers (2012) identified some concerns violating the trust in cloud computing such as availability, the location of legal jurisdiction, data location, trade secrets, and data protection. Shin (2013) investigated the acceptance of cloud computing services by government agencies based on the Technology Acceptance Model. The results show that the usefulness and ease of use are the significant antecedents of cloud computing. In another study, Sultan (2010) focused on the green credentials of cloud computing and reported that the cost advantages of cloud computing include using less power and thereby reducing carbon footprint.

Most studies reviewed here focus on the adoption to and use of cloud computing services by organizations. However, there is limited number of studies that investigate the determinants of cloud computing services adoption in educational settings. To fill up this gap, the present study aims to identify the key factors affecting students' attitudes toward and intentions in using mobile cloud storage services.

3. Research model and hypotheses

The present study proposes a research framework based on the Technology Acceptance Model (TAM), which is one of the most widely used adoption models in predicting user acceptance of new technologies and systems. The TAM uses Fishbein and Ajzen's Theory of Reasoned Action (TRA) as a theoretical basis. The TRA posits that the adoption behavior is predicted by behavioral intentions, which are also predicted by attitudes toward the behavior and subjective norms with respect to the behavior (Fishbein & Ajzen, 1975). However, the TAM posits that two particular beliefs, the perceived usefulness and perceived ease of use, are the main determinants of attitudes toward using a new technology.

In order to improve the prediction power of the TAM, this study extended the TAM by adding perceived ubiquity, subjective norm, perceived security, perceived privacy, and trust. More importantly, these external factors were considered significant in predicting the adoption of mobile cloud storage services. Fig. 1 presents the research model to be empirically tested in this study. The model suggests that behavioral intentions to use mobile cloud storage services are predicted by the attitude and subjective norm towards the behavior, while the attitude is predicted by perceived usefulness, trust, and subjective norm. Furthermore, perceived usefulness is predicted by the perceived ease of use and perceived ubiquity, while trust is predicted by perceived security and perceived