ELSEVIER
Available online at www.sciencedirect.com
SciVerse ScienceDirect
Procedia - Social and Behavioral Sciences 73 (2013) 30 – 34
Procedia
Social and Behavioral Sciences

The 2nd International Conference on Integrated Information

The Roles of Security and Trust: Comparing Cloud Computing and Banking

Ranjit Bose*, Xin (Robert) Luo, Yuan Liu

University of New Mexico, Anderson School of Management, Albuquerque, NM 87131, USA

Abstract

The evolution of information technology (IT) – related to Web, servers and data – and their capabilities have brought cloud computing to the forefront. While cloud computing in recent years has energized the information systems professional community, it has now embarked on information systems research arena as a prevalent topic for integrated information and systems. Organizations of all sizes are keen on understanding this intriguing yet potentially risky IT artifact as they see it to be a game changer in terms of the way their current and future computing needs could potentially be met. However, they also are skeptical and concerned about the security, trust and privacy issues related to its adoption. In this study we identify the roles of security and trust in cloud computing environments from the perspective of organizations who would entrust their private information to the cloud computing providers. We compare cloud computing and banking since to both security and trust is of vital importance for their service users and providers. For any new technology such as cloud computing trust is not easily established, it gradually builds based on providers' reputation for good performance and security, earning users' trust over time. The clients must trust the cloud providers just like they would be willing to trust banks to put their money into them. Similarly, the cloud providers must demonstrate that they are reliable and trustworthy. Therefore for widespread adoption of cloud computing, we contend that customers should be able to store their data in the cloud with same confidence as they store their money and other valuables in the banks today. To help study and address the roles of security and trust further, we provide technological, regulatory, and behavioral recommendations for consideration.

Keywords: Cloud computing; Information security; Information privacy; Users' trust

* Corresponding author. Tel.: 15052777097; fax: 15052777108.
E-mail address: bose@mgt.unm.edu

1877-0428 © 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of The 2nd International Conference on Integrated Information
doi:10.1016/j.sbspro.2013.02.015

1. Introduction

The evolution of information technology (IT) – related to Web, servers and data – and their capabilities have brought cloud computing to the forefront [1]. The distinguishing characteristics of cloud computing are: it is sold on demand; the service is managed by the provider; user can determine the amount of service they take; and users can log on to the network from any computer in the world. The benefits of cloud computing to the users are: it provides access to a huge range of applications without having to download or install anything; applications can be accessed from any computer, anywhere in the world; they can avoid expenditure on hardware and software, only using what they need. Subscribing companies can therefore share resources in one place; their consumption can be billed as a utility with minimal upfront costs; and scalability can be provided via on-demand resources.

While cloud computing is the current wave in computing, there are many concerns about its security and the trust by its users [2, 3]. An analogy could be made with the banking services from its advent to where it is now in terms of its popularity and maturity. It is also understood that for cloud to become as popular as banking, it has to be managed and governed through technology, people and regulations.

2. Cloud Computing and Banking

Security, privacy and trust play a paramount and central role in both cloud computing and banking services. To some extent, cloud security is similar to security controls in online banking systems. They both need to incorporate technological means, such as firewalls, intrusion detection/prevention systems, anti-virus, authentication, authorization and encryption, etc., to authenticate business information in different settings.

To a great extent, cloud computing is similar to banking systems. There was a time when money and other valuable tangible assets were retained in secret places because people did not trust banks for depositing their wealth. The two-way trust-winning process took almost half a century to build the users' trust towards the bank. Nowadays banks are often seen as the most secure institutions in the world because people entrust banks with their money. We contend cloud computing will also evolve in a similar manner in the sense of trust establishment. Before the advent of cloud computing, clients had to store their valuable data on their own terminals and they were frequently unable to access their data on demand. Today, cloud providers store data more securely than clients did individually, just like banks store money more securely than customers themselves can. Additionally, both cloud and bank provide access to data and services to their clients around the clock.

People today hardly keep a large amount of cash with them; they carry plastic cards and transact digitally to minimize loss. As banks are effectively doing business despite frauds, thefts and malpractices, cloud computing should similarly evolve and develop counter forces to thrive in spite of its security threats. With sufficient trust built with the service providers, customers can store data in the clouds with the same confidence as they keep money and other valuable assets in the banks today.

A commonality between cloud and banking services is that they both deal with digital assets. A digital asset is any item of text or media that has been formatted into a binary source that includes the right to use it. A digital file without the right to use it is not an asset. Digital assets are categorized in three major groups which may be defined as textual content (digital assets), images (media assets) and multimedia (media assets) [4]. Therefore, management of these digital assets in an environment that is secured and trustworthy is critical in the effectiveness of both cloud and banking services. Digital asset management would therefore involve the management, organization, and distribution of digital assets from a central repository or asset warehouse. Administrators of digital asset management system would need to have varying degrees of control over assets, permissions and workflows. Management of assets would then involve regulating the influx of new digital assets, assigning and editing metadata associated with each asset, and associating the assets to groups of users with role-based permissions. Each user or group of users would have different degrees of access to different assets. Metadata is the embedded descriptive information that stays with the asset. It is what allows assets to be catalogued, searched for and retrieved for its permitted use(s). Therefore, just like in banking, the development and effective administration of digital assets is critical for cloud service providers.

The challenges of trusting cloud computing don't reside entirely in the technology itself. The bank is trustful not only because of its safety, but also of its assurance. Users can easily deposit, access, transfer, and withdraw their money on demand. Even if the bank encountered threats, users are guaranteed to receive their money back. Comparatively, we currently trust cloud less because it is yet to provide users with sufficient security and assurance. For instance, user lacks controllability of their data, they do not know the exact location where their data currently resides; furthermore, unclear security assurances are primary reasons for this mistrust. To gain consumers' trust, cloud providers must offer better transparency and more consumer control of data and processes.

As most of the cloud services are executed on virtual machines, the service providers should focus on securing a holistic virtual environment and maintaining several different layers of protection to boost customers' trust in cloud computing. The most crucial security and trust issues fall under such categories as: access control, confidentiality, integrity, reliability, availability, recoverability, accountability, and long-term viability [5].

2.1. Critical security thinking

Bank security systems are comprised of several levels and components, including physical security (e.g. vault security, lockers, safe deposit boxes), transaction security (e.g. ATMs, surveillance camera, audio system), and electronic security (e.g. alarm system, CCTV/DVR systems, monitor service). These systems in combination with other state-of-the-art technologies are in place to help prevent potential fraud and protect the customers' assets.

Cloud services on the other hand are provided in an open virtual environment, which helps make it a lucrative target for hackers [6]. Hackers can exploit software back-loops to steal valuable data. For enterprises, customers' data is their most valuable asset and the quality of the security provided to protect the asset directly relates to their operation and reputation in the public. Thus it is critical to be proactive in security thinking so that additional security measures can be planned and designed into the new cloud software and systems to prevent failure instead of dealing with post-failure remedies. It is therefore crucial to recognize the possible threats and to establish security processes to protect services and hosting platforms from attacks. This critical security thinking anchored with the use of technology and strategy would help make cloud computing more trustworthy, analogous to the transformations banks went through over the years.

2.2. Access control and availability

Organizations cannot afford to divulge their sensitive data, such as personnel or financial to unauthorized parties. As mentioned in digital asset management above, cloud service providers should exert robust access controls over clients' resources. The process of access control usually includes authorization and authentication. Due to increased number of entities and access points in cloud environment, authentication and authorization are increasingly crucial to safeguard clients' resources. There are many access controls in bank security systems, for example a PIN on an ATM system only allows authorized users access to their money for withdrawal from the ATM terminal. An access mechanism for online banking combing with log in password, security questions, and security image can provide strict access control. For most of the banks, even the manager won't be able to open the door of vault by himself. Instead there needs to be two people physically present to open the door. We believe that similar two-key behavioural and technological mechanism can be applied to the cloud service as well.

Availability means service resources and data storage within a cloud is made accessible and usable on demand by an authorized entity. The availability of cloud computing, to some extent, is similar to water, gas or electric utility. It is important that providers supply resources, software, information, high network reliability on demand via the Internet. Customers, who have subscribed to cloud services, are entitled to receive services anytime and from anywhere. In the same vein, bank customers' money can be accessible from ATMs, telephone call-centers, and internet browsers, virtually from anywhere in the world at any time. Additionally, cloud customers need greater accessibility to their data by a variety of different computing methods and devices.

2.3. Confidentiality and privacy

Confidentiality and privacy are vital requirements that must be guaranteed by cloud service providers to their customers since their sensitive data is outsourced to the cloud. Swiss bank, for example, over the years has gained respect and reputation for the protection of customers' privacy, which makes them attract and retain the confidence of worldwide customers; similarly, cloud computing providers need to ensure that their data privacy property must appeal to existing and prospective clients. Organization's data are highly valuable assets; data breach may lead to severe consequences. The responsibility of privacy control is shared by both providers and customers.

2.4. Long-term viability and regulation

Before an organization and/or its individual users transfer their informational resources into the clouds, the provider's longevity and viability is yet another crucial factor to account for. Like other business settings such as banking, consequence may become serious if a service contract comes to an end abruptly as a result of insolvency of a provider. Without a business continuity strategy, customers will be reluctant to migrate to cloud computing. Similar to banking institution's bankruptcy where customers are guaranteed to retrieve their money, cloud computing will eventually and inevitably have to cope with the long-term viability issue. Regulatory efforts are needed to play an important role in alleviating the potential perilous aftermath.

Regardless of cultural and political governance, regulations all across the world assume vital importance in creating a trusted legal and secured framework for banking, such as FDIC's general deposit insurance rules and newly mandated FFIEC regulations over online banking security. Compared to banking, there are less regulations and standards relating to the cloud computing segment. Many regulations, such as the Federal Rules of Civil Procedure, the Electronic Communications Privacy Act, US Federal Information Security Management Act, the Gramm-Leach-Bliley Act, the European Union Data Protection Directive, and so on, haven't been updated yet to address the comparatively unique problems of a cloud computing domain. In particular, a lack of common security standards makes service providers resort to existing standards (e.g. ISO 27001) which were not purposefully established for cloud computing.

To promote cloud security and comply with industrial standards, concerted efforts are expected to be exerted on creating regulatory standards of cloud computing. While the US National Institute of Standards and Technology (NIST) has created a cloud computing security group, other organizations such as ISO, the Cloud Security Alliance, and CloudAudit are also working to set up regulatory standards of cloud computing. Ultimately the cloud computing industry will reach agreements on critical issues including standards, interoperability and third-party support programs, etc. In turn, businesses must be able to witness cloud service providers meet regulatory requirements before moving their organizations to the clouds.

3. Conclusions

Security of cloud-based applications and data needs planning and resources. Cloud providers have security advantages because they can spread their security costs across multiple customers therefore they can have more money available to invest in different security solutions. For example, they can hire a team of security patch installation specialists to cut down on vulnerability period. They are also better positioned to recruit and hire trained system specialists.

As organizations move their IT solution to cloud, their IT managers must not relinquish oversight and responsibility for performance and data management. Based on the service-level agreement with the cloud provider, the managers should monitor key system operations to ensure that the levels of service are being effectively met. Additionally organizations must create policies, procedures, and controls that not only ensure strategic alignment, but also provide confidence in the accuracy and security of the cloud-based solutions.

Modern virtualization technologies are helping many businesses to dramatically improve their storage utilization, service delivery, resource efficiency, and space utilization. While cloud computing provides a virtual business environment to firms through a suite of integrated applications and tools that support their specific and major capabilities and needs, this capability enables users and the usage of every information service within an organization to be tracked. The ability to verify the history, location, or application of an item through recorded documentation (traceability) is crucial for ensuring that companies comply with internal and external constraints.

References

[1] Iyer, B. & Henderson, J.C. (2010). Preparing for the future: understanding the seven capabilities of cloud computing. MIS Quarterly Executive, 9, 117-131.

[2] Heiser, J. & Nicolett, M. (2008). Assessing the security risks of cloud computing, Gartner.

[3] Cass, S. (2009). Cloud computing, just another online fad – or the biggest revolution since the Internet? Technology Review, 112, 53-63.

[4] van Niekerk, A.J. (2006). The strategic management of media assets: a methodological approach, Allied Academies.

[5] Lombardi, F. & Pietro, R.D. (2011). Secure virtualization for cloud computing. Journal of Network and Computer Application, 34, 1113-1122.

[6] Coleman, N. (2011). Securing the cloud: questions and answers, retrieved May 14, 2012 from http://www.wired.com/cloudline/2011/10/525/.