International Journal of Knowledge, Innovation and Entrepreneurship
Volume 2 No. 2, 2014, pp. 6—13

Security Management in Cloud Computing to Secure Cloud from Data Loss

ASMA SATTAR, FARIA NAZIR,
FAIZA KIANI & MUHAMMAD FAHAD KHAN
University of Engineering and Technology Taxila, Pakistan

Received 7 May 2014; received in revised form 1 December 2014; accepted 31 December 2014

ABSTRACT Cloud computing is growing rapidly in IT industry providing a set of services to customers that can be accessed remotely. Cloud computing technology has many advantages as well as challenges—one is a concern by organizations about putting their data in the cloud. This paper highlights a number of cloud computing security issues and proposes a model designed to make the cloud more secure. A security layer is also introduced to handle clients' mission-critical data—which, in cloud computing, is designed to manage, store, analyze and share complex amount of data more securely.

Keywords: Cloud Computing, Cloud Security Issues, Data Encryption, Risk Management

Introduction

The next generation in computation is cloud computation. Cloud computing enables individuals and organisations across the globe to access digital information on the cloud. Cloud computing is based on the internet. Clouds are actually clusters of computer servers that are used to store and transmit data. The servers in question are huge and have ability to store large amount of data. These servers can be housed anywhere in the world. Cloud computing is a technology which allows on-demand, and appropriate network access to a shared group of configurable computing resources. These resources can be networks, storage, servers, services and applications that can be quickly provisioned and then released with minimum effort by management or through interaction of the service provider. Cloud computing delivers calculation, software, access of data and the storage facilities that do not involve end-user information about the physical locality or configuration of system that provides the services. People can connect to the cloud through the internet for a variety of purposes such as performing computing tasks and running different applications.

Typical cloud computing suppliers provide common business requests and applications online that are retrieved from another web software or web browser while the data and software are stored on the servers. Cloud computing is a system in which all the capabilities that are related to the IT are provided in form of "service" that enable the user to access these services with the use of the internet (i.e. cloud). This process does not require any expertise, knowledge or control over technological infrastructure that are actually supporting them (Mirzaei, 2008). The principle behind the cloud is that any device or computer linked to the internet is linked to the same group of computing power, services, applications and files. The users can access and store private files such as pictures, music, bookmarks and videos or play games or use applications of productivity on a remote server instead of physically carrying a storage device such as a thumb drive or DVD. These files can also be made public (depending on the security level of the file) that can be searched by anyone. Many users of the internet are likely to be using a method of cloud computing without realizing it or recognizing such method. Example include users of web-based emails like Yahoo, Hotmail, Gmail, or client-owned emails such as Evolution, Outlook, Mozilla Thunderbird or Backup that are linked to the cloud email server. Similarly, the use of desktop applications to connect to cloud email is still regarded as a cloud application.

Cloud computing has a number of characteristics. It provides shared infrastructure. It is a virtualized software model which enables sharing of storage memory, services and networking facilities to the users. In cloud computing the services are offered on demands based of requirements and automated. These services can be easily accessed through internet using different type of portable and non-portable devices like mobiles, laptops and PCs. It provides only those services to user which is required to them and they pay only for those services. Cloud computing has both benefits and challenges (see for example Mirzaei, 2008); this paper sought to propose solutions to some of these challenges.

Literature Review

A number of studies have been conducted and reported in literature on cloud computing and related issues of security (see for example Ogigau-Neamtiu, 2012; Hamlen et el., 2010;

Chaitanya et el., 2011). Cloud Computing platform is a system of providing intensely scalable and the virtualized resources, software, hardware and bandwidth to consumers on their demand. As the data grew in cloud, the need for security and protection of those data becomes critical. However, the advent of cloud computing has enable consumers to save cost of software licenses, system maintenance and hardware deployment. Cloud computing has also present users with security issues to deal with.

Ogigau-Neamtiu's (2012) paper on cloud computing relates to cloud security and the risks of using cloud services. He highlighted the risks of moving mission-critical data to the cloud focusing in particular on the issues of security, operability, misunderstanding responsibilities and lack of standards. Similalry, Hamlen et el.,'s (2010) paper relates to cloud security. Hamlen et el. proposed two-layered security framework—data layer and storage layer—to resolve those security issues. Chaitanya et el.'s (2011) discourse on cloud computing concerned security problems often encountered by organisations adopting the cloud computing. He also set out steps which, to some extent, might be taken to resolve those security issues. In his paper, Rashmi et el., (2013) provides an empirical analysis of existing status of security challenges in cloud computing—including traditional issues like availability, authentication, authorization and cloud specific security issues relating to digital information and internet security. Onwubiko (2010) discussed cloud computing security risks including disaster recovery, data location, privacy, control, legal, trust, business continuity and security attacks and threats. He proposed cloud computing information asset and framework to help cloud users not only to choose the cloud services, but also have an understanding of the risks to and threats of using cloud.

Kresimir and Zeljko (2010) has discussed the high level security issues such as payment, data integrity and the privacy of critical information in cloud computing infrastructure, while Grobauer et el. (2010) explored the vulnerabilities of security that residing in cloud computing platform. Similarly, Hashizume et el.'s (2013) examines the vulnerabilities and threats in cloud computing and the relationship between the vulnerabilities, threats and countermeasures. Chen and Zhao (2012) examines privacy protection and data security in cloud computing and offer a number of 'solutions' crucial to addressing the problem. He argued that private data must be identified and isolated from non-private data. Jamil and Zaki (2011) highlighted four security problems of cloud—including Browser Security, XML Signature Element Wrapping, Flooding Attacks and Malware Injection Attack on cloud—as well as offer possible measures to overcome the problems. The Cloud Computing Use Case Discussion Group[1] has examined a number of cloud computing scenarios, issues and requirements—including the analyses of cases from the perspective of customer, security engineers and developers (see Cloud Computing Use Case Discussion Group, 2010). Similarly, ENSIA (2009) investigated the security risk parameter of adopting cloud computing and susceptibilities that lead to these risks in cloud computing.

Cloud Computing

Cloud computing is new general purpose technology that has huge economic benefits. It provides and delivers efficiency to public sector services such as health and social care, education among others. Cloud delivers computing resources as a service to the users. Computing facilities are provided on demand thereby remove the need for organisations to acquire

and install own cloud-based computing resources. The technology facilitates the sharing of data with different organisations which is managed by third party vendor. This technology allows more efficient computing because of centralized storage servers, effective memory management, networking and support for multiple application on a variety of platforms.

Service Models

In Cloud Computing, service delivery includes different service models. These layers or service models are accomplished by the layer of end user that encapsulates the perspective of end user on cloud services. The following are the three service models provided in cloud computing:

Software-as-a-Service (SaaS)

SaaS provides the complete applications to the end user of cloud. It is mostly accessed through a service oriented architectures and web portal that are based on the web service technologies. Applications such CRM or word processors and application services such as calendar or schedule execute in "cloud" through the internet interconnectivity for data propagation. User must provide the details of bank account or credit card to allow the payments to be billed for the use of services. The application layer services can be understood as an addition of the Application Service Provider (ASP) model. Here, an application is maintained, run and supported by an application service vendor. The main dissimilarities among the services on ASP model and the application layer are the dynamic procurement, application encapsulation as a service, and payment by the consumption units (i.e. Pay-as-you-go).

Platform-as-a-Service (PaaS)

PaaS is actually a computing platform that allows the formation of web applications easily without purchasing the whole software. Pass is similar to the SaaS except that in SAAS software is *produced* while PaaS platform is *provided*. PaaS provide the services to develop the application which can be tested and deployed. It provides the users with interface based on web that contains tools to develop, modify and test different user consequences. PaaS also provide support for effective collaboration between the team by providing requisite communication tools. It also handles the billing mechanism. Multiple users can use the same platform for creating the applications. PaaS is best suited when there are multiple persons working on the same project or another party wants to interact with the development team. PaaS is not used in situations where application have to be portable and where exclusive languages affect the development process and where performance of application needs to be customized.

Infrastructure-as-a-Service (IAAS)

In cloud computing, Infrastructure as a Service (IAAS) is a way of delivering storage, networks, servers and operating systems on demand. Instead of purchasing software, servers, space on datacenters, clients buy resources as a outsource service. IaaS is a rapidly developing field. IaaS provider is responsible for providing hardware to the clients and performs maintenance to guarantee that server runs correctly all time. Examples of IaaS providers include Amazon EC2, Profit Bricks or Rackspace Cloud. Clients pay for the virtual servers

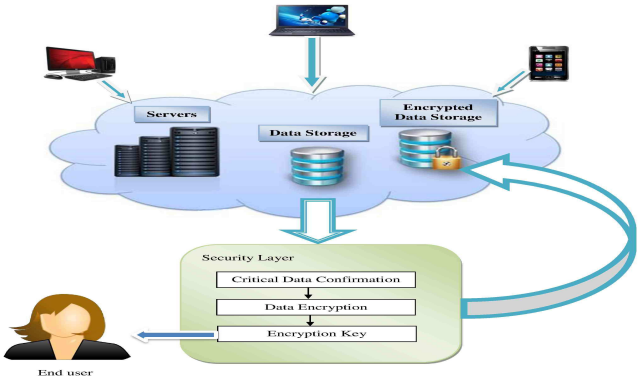
provided by these three providers for rent. IaaS provides a lot of advantages for multiple situations where scalability is beneficial.

Security issue in Cloud Computing

Security is regarded as a critical feature in everyday computing and this is not different in cloud computing, due to the sensitivity of data that are stored in the cloud. The main challenge in cloud computing therefore is how to address concerns about privacy and security of businesses that are thinking about adopting cloud computing. For example, one serious concern is the leakage of enterprise data outside the business firewall. Various malicious attacks on and hacking to cloud infrastructure often disturb clients' operations even if only one website is attacked. Many organizations do not feel comfortable in storing their valuable data and applications on off-site data centers mainly because of security concerns.

In 2008, Gartner (2008), in a seminal work, identified some issues related to security that should be identified and addressed by organizations before deciding whether or not to adopt the cloud computing model. Organization should spend time to know the cloud computing service providers and how these providers are regulated before outsourcing. Another issue highlighted in Gartner (2008) is that a client might never know in which country or jurisdiction their data is located. Another issue relates to data segregation—i.e. the assignment of encrypted information of multiple companies on the same hard disk. It should be necessary to have mechanism in place to separate such encrypted data. Other issues raised by Gartner (2008) include the recovery of data in case of disaster or a sudden data loss of losing data, necessary investigation support in case of any suspicious activities from the side of the provider side and the long term viability of the project should the current provider be taken over by another firm. This paper sought to address some of these issues.

Proposed Model



Methodology

To increase traffic in cloud platform and to encourage businesses and organizations to adopt cloud computing, it is essential to make cloud computing reliable in terms of security. In this research work, a database named *Encrypted Data Storage* is introduced in cloud. There are other components in cloud – i.e. servers, data storage database and applications. Encrypted data storage is a type of storage where only critical data is placed. Cloud computing is conceptualised as pay-as-you-go model. This means to make the data more secure, organizations have to pay for usage, and any data 'non -critical' is placed in data storage. To avoid the problem of data loss [from storage database] due to hacking or attacks, *encrypted data storage* database is introduced to store the client's encrypted data. A security layer is also introduced when the users request to share their data on cloud. In the security layer, the user is asked for critical data confirmation which s/he wants to store in encrypted form, in separate encrypted data storage, to make the data more secure. When the user confirms the critical data, this data is transformed into encrypted data. An encrypted key is generated and send to the user; and this encrypted data is moved to *encrypted data storage*. The user can access his/her encrypted data anytime by using assigned encrypted key.

It is important to know that the model presented in this paper only encrypts most critical data. It is therefore possible that not all data are encrypted – to save time, effort and resources. Issue regarding to privilege access can be solved initially in the contract by specifying exactly that who is the owner of data is when it is thrown on the internet. In this way client and provider both know who can access what. Provider must tell client about the country and jurisdiction where data is located. Encryption of data is not required generally when data is transmitted inside the organization. If data is transmitted across boundaries of enterprise, data integrity and security are necessary to prevent access by unauthorized user. The security and integrity of data can be achieved by encryption. The model [encrypted key] proposed in this paper might help to address some of the issues relating to data segregation.

Conclusion

Cloud computing technology provides benefits to individuals and businesses alike. The technology enables access to personal files and data from anywhere via the internet. Despite of the benefits of cloud computing, there remain some challenges. Security is a major issue in cloud computing which needs to be addressed to make cloud computing more reliable. The model proposed in this paper sought to address the need to encrypt data so as to make it more secure as well as store the data in question in a separate Encrypted data storage database. An additional security layer is introduced in the model which not only encrypts enterprise data but also assign a key against encrypted data to prevent unauthorized access as well as minimize hacking or malicious attacks.

Correspondence

Asma Sattar
University of Engineering and Technology Taxila, Pakistan
Mailing address: #390-A Gulistan Colony
No.2 Millat chowk sheikhupura Road Faisalabad
Email: asma_uett@yahoo.com

Faria Nazir
University of Engineering and Technology Taxila, Pakistan
Mailing address: # CB 1674, Siddique-e-Akbar Street
Zeeshan Colony Rwp
Email: faria.nazir@yahoo.com

Faiza Kiani
University of Engineering and Technology Taxila, Pakistan
Mailing address: # N/322, st # 7,Waris Khan Murree Road Rwp
Email: faiza5550@yahoo.com

Note1

Cloud Computing Use Case Discussion Group (Miha Ahronovitz, Dustin Amrhein, Patrick Anderson, Andrew de Andrade, Joe Armstrong, Ezhil Arasan B, James Bartlett, Richard Bruklis, Ken Cameron, Mark Carlson, Reuven Cohen, Tim M. Crawford, Vikas Deolaliker, Pete Downing, Andrew Easton, Rodrigo Flores, Gaston Fourcade, Thomas Freund, Tom Hanan, Valery Herrington, Babak Hosseinzadeh, Steve Hughes, William Jay Huie, Nguyen Quang Hung, Pam Isom, Shobha Rani J, Sam Johnston, Ravi Kulkarni, Anil Kunjunny, Edmond Lau, Thomas Lukasik, Bob Marcus, Gary Mazzaferro, Craig McClanahan, Meredith Medley, Walt Melo, Andres Monroy-Hernandez, Ayman Nassar, Dirk Nicol, Lisa Noon, Santosh Padhy, Gilad Parann-Nissany, Greg Pfister, Thomas Plunkett, Ling Qian, Balu Ramachandran, Jason Reed, German Retana, Bhaskar Prasad Rimal, Dave Russell, Matt F. Rutkowski, Clark Sanford, Krishna Sankar, Alfonso Olias Sanz, Mark B. Sigler, Wil Sinclair, Erik Sliman, Patrick Stingley, Phillip Straton, Robert Syputa, Robert J. Taylor, Doug Tidwell, Kris Walker, Kurt Williams, John M Willis, Yutaka Sasaki, Michael Vesace, Eric Windisch, Pavan Yara and Fred Zapper). "Cloud Computing Use Cases Version 3.0," 2010.

References

Grobauer, B., Walloschek, T. and Stöcker, E. (2010) "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, Vol. 99.

Onwubiko, C. (2010) "Security Issues to Cloud Computing ", in Cloud Computing: Principles, Systems & Application, (Eds) Nick Antonopoulos and Lee Gilam, Springer-Verlag, August, 2010.

Jamil, D. and Zaki, H. (2011) "Security Issues in Cloud Computing and Countermeasures", International Journal of Engineering Science and Technology, Vol.3, No.4.

Chen, D. and Zhao, H. "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651, Hangzhou, China, March 2012.

ENISA (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment; [online] accessed: Jul. 10, 2010.

Ogigau-Neamtiu, F. (2013) "Cloud Computing Security Issues", Journal of Defense Resources Management,3(2), 141- 148.

Hashizume, K, Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B. (2013) "An Analysis of security issue for cloud Computing" , Journal *of Internet Services and Applications*, online: http://www.jisajournal.com/content/4/1/5.

Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, B. (2010) "Security Issues for cloud computing", International *Journal of Information Security and Privacy*, 4(2), 39-51, April-June 2010.

Chaitanya.Y. K., Shankar.Y. B., Krishna.V. K.R., Rao, S. (2011) "Study of Security issues in Cloud Computing", *International Journal of Computer Science and Technology*, Vol. 2, No.3, September 2011.

Morsy. M.A., Grundy, J. and Müller, I. (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC.

Kresimir, P. and Zeljko, H. (2010) "Cloud computing security issues and challenges," In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349.

Rashmi, R., Sahoo, G. and Mehfuz, S. (2013)"Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing, Vol.3, No.4, August 2013

Gartner (2008) "Assessing the Security Risks of Cloud Computing", 3 June 2008, online: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing.