Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.9, 2018

Enhancement Data Security in Cloud Computing: Issues and Challenges

Obed Jatau Wycliff[1] Abdulrahman Saidu[2]
1. Information & Communication Technology Unit, Federal Polytechnic Bali, Taraba State
2. Department computer Science, Federal Polytechnic Bali, Taraba State

Abstract
Cloud Computing can save an organization's time and money but trusting the system is very much important because the real asset of any organization is the data which they share in the cloud to use the needed service by putting it directly in the relational database. No organization can transfer its data or information to a third party until a bridge of trust is built. This paper provides a concise and all roun 小 d analysis on data security and privacy protection issues associated with computing across all stages of data life cycle. It argues that, in contrast to the traditional solution where unauthorized third party can access organizational data illegally which raises a serious concern since data is scattered at different places all over the globe. The security concerns of users need to be addressed to make cloud environment safe and trustworthy. Every cloud provider solves this by encrypting data using encryption algorithm which is inadequate. The paper concludes by recommending that in addition to the traditional methods, the security of cloud computing can also be enhanced through authentication using thumb print, face, voice and image identification.
Keywords: Cloud computing, Information Technology, Data Integrity, Authentication, Security and Challenges.

Introduction

Cloud computing is a type of computing that relies on sharing computing resources rather than having local services on personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for *the internet*. So the phrase *Cloud* means a type of internet based computing, where different services, storages and applications are delivered to an organization's computers and devices through the internet. Thus, Cloud Computing means storing and accessing data and programs over the internet instead of computer's hard drive. It can also be seen as the hardware and software resources in the data centers that provide diverse services over the network or internet to address the user requirements (Leavitt, 2009).

A lot of research has been done on the potentials of cloud and the services that cloud computing can and could offer. In essence though, these services can be categorise into four main sections: Storage as a Service (StaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Cloud offers a storage space that is enormous, seemingly endless, and growing every day. Storage as a service (StaaS) enables cloud applications to scale beyond their limited servers. Cloud storage systems are expected to meet several laborious equipment for maintaining users' data and information, including high availability, reliability, performance, replication and data consistency. In addition to those services, consumers are also relieved of their responsibility to own and maintain their own computer storage as cloud vendors offer them the choice of storing their information in the cloud which is accessible whenever they want.

Cloud computing offers a prominent service for data known as cloud storage, but data security has always remained a major issue in IT and in cloud, it is particularly of serious concern since data are scattered at different places all over the globe. It can equally save an organization's time and money but trusting the system is very much important because the real asset of any organization is the data which they share in the cloud to use the needed services by putting it directly in the relational database through an application. But the security concerns of users must be addressed to make cloud environment trustworthy. In cloud computing a trustworthy environment is a basic prerequisite to win confidence of a user to adopt such technology. Data protection and security are the two main foremost factors for gaining user's trust and making the cloud successful. From the perspective of data security, which has always been an important aspect of quality of service, cloud computing inevitably poses new challenging security threats for number of reasons; Data stored on cloud servers is not completely secure from infection. While popular cloud services such as Google Docs are equipped with virus scanning software, there is still the possibility of an internal or external attack affecting your data; The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification; appending, reordering, etc. this post another challenge in cloud computing; In cloud computing there are three primary users that manage database i.e. User, Cloud Service provider (CSP) and Third Party Auditor (TPA), each of this need an independent authentication to access the database. This is another issue in cloud computing that need security. Albeit the above challenges, this paper attempts to discuss how the security of cloud computing can further be enhanced to make it safe and trustworthy.

DEFINITION OF KEY TERMINOLOGIES

Cloud Computing Security (CCA): It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing
User*:* Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
Cloud service provider (CSP): Is one who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live cloud computing.
Third party Auditor (TPA): An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

BENEFITS OF CLOUD COMPUTING

Cloud computing plays an important role in the advancement of Information Technology (IT) hence, adding value to human life. Some of the advantages are enumerated below:

- It provide availability of a huge array of software applications, seemingly unlimited storage, has given access to lightning processing power and the ability to easily share information across the globe.
- Cloud computing allows consumers and corporate structure to use all the applications offered by the cloud without the extra effort of instillation and also offers access to their personal file from any computer anywhere at any time with internet access.
- It offers access to a large number of sophisticated supercomputer and their resultant processing power, connected as numerous locations around the world, thus offering speed in the tens of trillions of computations per second.
- It also promises tangible cost saving and speed to costumers.

Despite these advantages, the cloud is not completely safe or trustworthy since data of the users can be compromised or illegally accessed by an unauthorized third party. This paper attempts to proffer solution on how to enhance security in cloud computing to make it safer, trustworthy and reliable.

RELATED WORKS

Cloud computing is an informal expression used to describe different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. This means it refers to network-based services which appear to be provided by real server hardware, which in fact served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user - arguably, rather like a cloud (Carrol et al. 2012).

Cloud computing has emerged to become one of companies' greatest means of reviving and enhancing their business and IT infrastructure. Nevertheless, there are certain data security issues and challenges related to cloud computing. In everyday computing, security is one of the most acute aspects to be considered and it is no less important for cloud computing due to the sensitivity and significance of data stored in the cloud, (Al Zain et al. 2012). In cloud computing operations, there are issues of secure data transfer, secure software interfaces, secure stored data, and user access control and data separation, which are very important in ensuring the integrity of client data (Beckham, 2011).

Rewagad and Pawar (2013) maintains that in cloud computing, organizations can use services and data that can be stored at any location beyond their control, this facility has raised various security questions such as privacy, confidentiality, integrity etc, and it demands a trustworthy computing atmosphere where data confidentiality can be maintained. The authors have proposed a very good solution to the security questions raised by using three kinds of protection scheme. One is to use the Diffie-Hellman Algorithm to generate keys for the key exchange step. Next, digital image signature will be used for authentication; afterwards, the Advance Encryption Standard (AES) encryption algorithm will be used to encrypt or decrypt the user's data file.

In the cloud computing environment, data security issues can be divided into four types: safety problems caused by virtual technology; root authority of the data centre; data security and consistency; and problems prompted by new technology, (Han and Zhang, 2012). In order to overcome the outlined security issues the authors introduced new technology, which is the agent. According to them, at present, agent-oriented technology as a software system designed and developed by new methods is of widespread interest in academia and the business community. Its features are autonomy, responsiveness, initiative, social and others.

Likewise, data transmissions in networks are often intercepted, tampered with or replaced by hackers (Weihai, 2013). This author outlined that there is a guarantee of the security of data transmission on the network to HTTPS, or TCP/IP, which is coupled with modern cryptographic algorithms and network security equipment. Another problem mentioned is that data storage security is non-volatile or has a fast recovery after a loss. It was proposed that this security issue be taken into consideration by software engineers in the design stage of cloud storage services. Also, data redundancy, dynamic, and isolation should be included in the design. It was added that management needs to consider the replacement or deactivation of service providers because, once the

cooperation agreement expires, as the user may disable a service, it is uncertain what will happen to the data stored in the cloud or whether it will be returned to its owner. The solution he provided is to use the products of another service provider, who will then deal with seamless data panning. Furthermore, it was maintained that, in cloud computing infrastructure, the sharing of physical resources causes crises in data security and privacy, and one can no longer rely on a physical machine or network boundary. Moreover, users worry about the transparency of the data storage location. Therefore, it has been suggested that relevant laws and regulations be put in place as soon as possible and must be compatible with data between cloud computing service providers and client to ensure that seamlessly pan (faultless damage) data, and service providers should establish effective and efficient disaster recovery machinery to guarantee the accessibility of the data (*ibid*).

Similarly, one of the most important concerns about cloud data storage is data integrity verification and untrustworthy servers. Another big concern from the previous design of cloud computing is that of supporting dynamic data operation for cloud data storage, (Wang et al. 2011). In order to solve these problems, these authors have proposed cloud data storage architecture with three basic components; One of them is the client, an entity that has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; they can be either individual dual consumers or organizations. The second is Cloud Storage Server (CSS), an entity managed by the Cloud Service Provider (CSP). The third component is the third-party auditor, an entity with the expertise and capabilities that clients do not have, who is trusted to assess and expose the risks of the cloud storage service on behalf of the clients at their request.

The foregoing shows the important role that cloud computing plays in managing data across the world through computer networks by the service of the Internet. Effective and efficient management of data in the cloud has posed many security challenges that need to be addressed. However, various solutions have been proposed and some have been implemented. Nonetheless, there are some gaps that need to be filled in order to obtain a dynamic, functional and secure cloud computing atmosphere.

SECURITY ISSUES AND CHALLENGES

Companies and organization are rapidly moving unto cloud because they can now use the best resources available in the global market in the blink of an eye and thus reduce their operations cost drastically. But as more information is moved to the cloud, the security concern have started to develop. Some of the security challenges are classified below:

Defect of Trend

The IBM developed a fully homomorphic encryption scheme in June 2009. This scheme allows data to be processed without being decrypted. Roy I and Ramadan HE applied Decentralized Information Flow Control (DIFC) and differential privacy protection technology into data generation and calculation stages in cloud and put forth a privacy protection system called *airavat*. This system can prevent privacy leakage without authorization in Map-Reduce computing process. A key problem for data encryption solutions is key management. On one hand, the users have not enough expertise to manage their keys. On the other hand, the cloud service providers need to maintain a large number of user keys. The organization for the Advancement of Structured Information Standards (OASIS) key Management Interoperability Protocols (KMIP) is trying to solve such issues.(OASIS, NY). About data integrity verification, because of data communication, transfer fees and time cost, the user cannot first download data to verify its correctness and then upload the data. And as the data is dynamic in cloud storage, traditional data integrity solutions are no longer suitable. NEC Labs Provable Data Integrity (PDI) solution can support public data integrity verification, (Zeng K, 2008). Also, Cong Wang et al(2009: 1-9) proposed a mathematical way to verify the integrity of the data dynamically stored in the cloud. In the data storage and use stages, Mowbray proposed a client-based privacy management tool. It provides a user centric trust model to help users to control the storage and use of their sensitive information in the cloud. Munts-Mulero discussed the problems that existing privacy protection technologies (such as K anonymous, Graph Anonymization, and data pre-processing methods) faced when applied to large data and analyzed current solutions. The challenge of data privacy is sharing data while protecting personal privacy information. In a related development, Randike Ganjanayake proposed a privacy protection framework based on Information Accountability (IA) components. The IA agent can identify the users who are accessing information and the types of information they use. When inappropriate misuse is detected, the agents defines a set of method to hold the users accountable for misuse, (Randike Gajanayake, et al, September 2006).

Data Integrity

- Data breaching is the biggest security issue. A capable hacker can easily intrude in to a client side application and get into the client's confidential data.
- Inefficient and flawed APIs (Access Point Infrastructures) and interfaces become easy targets.IT companies that provide cloud services allow third party companies to modify the APIs and introduce their own functionality which in turns allows these companies to understand the inner working of the cloud.
- Denial of service (DoS) is also a major threat wherein the user is granted partial or no access to his/her data.

Companies now use cloud 24/7 and DoS can cause huge increase in cost both for the user and service provider.

- Connection eavesdropping means that a hacker can scan your online activities and reproduce/replay a particular transmission to get into your private data. It can also lead the user to illegal or unwanted sites.
- Data loss is another issue. A malicious hacker can wipe the data or any natural/man-made disaster can destroy your data. In such cases having an offline copy is a big advantage. Carelessness of service provider can also lead to data loss.
- Compatibility between different cloud services is also an issue. If a user decides to move from one cloud to another the compatibility ensures that there is no loss of data.
- Cloud can also be used for wrong purposes i.e. cloud abuse. Due to the availability of latest technologies on the cloud it can be used for high end calculations which cannot be done on a standard computer.
- Insufficient understanding of cloud technologies can lead to unknown levels of risk. Companies move to cloud because it provides substantial reduction in cost but if transfer is done without proper background learning. The problem arise can be even greater.
- Inside theft in the form of a current or former employee, a contractor, etc who is able to use the data for harmful purposes.
- Safe storage of encryption keys is also a problem. Even if you are using encryption for enhanced security, safe keeping becomes an issue. Who should be the owner of the key? User seems to be the answer but how diligent and careful can he/she decide the security of the data.*(Notorious Nine, Cloud Security, Info World February 25, May 2013 accessed from http://www.infoworld.com)*
- Disaster and Data Breach: with the cloud security as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily unavailable due to a natural disaster are real concerns. Therefore, clients need to know how their data is being secured and what measure of the integrity and availability of data in case of natural disaster. Also, what is the measure if there breach agreement between the cloud and clients?

Minqui Zhou et al. (2010) and kresimir popovic et al. (2010) classify the various threats concerning cloud security in the following areas:

- **Access:** The aim of cloud services to provide information to the user from any place, at any time. As a web service cloud enables the user to access his/her data from anywhere and this is applicable to all the services being provided by it. The client should know where data is being stored. In a situation where the client ask the cloud service provider to delete his/her data. The data should be deleted. The cloud service provider should not withhold any information.
- **Control:** In a cloud, controlling the system and its use is important. The amount of data that is visible to any member of the service provider should be controlled. The visibility of the data defines the level of control.
- **Compliance:** Proper authorities need to define laws to govern the safekeeping of data in the cloud because cloud can cross multiple jurisdictions around the world. If a piece of data is stored in a different country and it contains sensitive data that is wanted by the authorities than the rules apply on data that data.
- **Data Integrity:** Data integrity in simple terms means that the data is preserved and no changes are made without the user's permission. In cloud, data integrity is a fundamental requirement.
- **Audit:** This means to keep a simple check on the activities happening on the cloud. The presence of an auditing mechanism can maintain a log, list of events, e.t.c. to help prevent breaches.
- **Privacy Breaches:** The cloud service provider should inform its user about any breach in security. The user has to the right to know what's happening in his/her space.
- **Confidentiality:** This ensures that the user's data is kept secret. Confidentiality is one aspect of cloud storage security that will raise questions in a common users mind. Cloud as such is a public network and is susceptible to more threats, thus, confidentiality is very important.

TECHNIQUES OF ENHANCING DATA IN CLOUD COMPUTING

The encryption algorithm is the most commonly used technique to protect data cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. According to key characteristics, modem cryptosystem can be classified into symmetric cryptosystem and asymmetric cryptosystem. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), 3DES and AES (Advanced Encryption Standard. For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret.

The cloud architecture deployed with samba storage uses operating system feature specifying permission

values for three attribute **(User/Owner, Group and Global)** and maps it to cryptographic application which performs cryptographic operations. Cryptographic application supports symmetric and asymmetric encryption algorithm to encrypt/decrypt data for uploading/downloading within cloud storage.

Users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case that user does not necessarily have the time, feasibility or resources to monitor their data, they can make or delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

Data Protection: Securing your data both at rest and in transit: Implementing a cloud computing strategies means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount important. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encrypted keys.

Contingency Planning: cloud providers necessary measures for internal external backup in case of natural disasters. Additionally, companies should also have contingency plans in place in the event their cloud provider fails or goes bankrupt

User Authentication: limiting access to data and monitoring who accesses the data: Data resting in the cloud needs to be accessible only by those who authorized to do so. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. To achieve this, various steps of authentication are provided in terms of communication among Client machine with cryptographic module and server storage.

CONCLUSION

The authors were able to examine and revealed the security issues and challenges that generally affect the integrity of data in cloud computing. They also outlined possible techniques that will assist enhancement of data reliability in cloud computing environment. In addition, the authors suggested good ways of collaboration between cloud computing providers and clients.

RECOMMENDATION

In this digital age of globalization, the role that cloud computing plays in managing data across the world through computer networks by the service of the Internet which in turn has improved research and development, commerce and industry, corporate governance, health and related issues cannot be taken with levity. Thus, effective and efficient management of data in cloud computing becomes not only important but necessary. Therefore, many security challenges posed and need be addressed. Despite the fact that various solutions have been proposed and some have been implemented (as discussed), there still remain some gaps that need to be filled in order to obtain a dynamic, functional and secure cloud computing atmosphere.

In view of the above, the following techniques/algorithm were suggested that will provide secure atmosphere:

- Username and password allocated to user for access to server storage
- Verification and validation are performed by matching details stored in server storage
- After user authentication storage is allocated for uploading and downloading
- Cryptographic application based on AES and ECC with SHA used for encryption/decryption operation on data.
- The user should be provided with storage space and decides to upload data using encryption application or directly on storage.
- Data downloaded from storage space and decrypted using key stored in user's mail server
- After upload and download user logout from server storage
- Storage loaded to server and connection terminated.

In addition, the use of thump print, face, voice and image identification should be adopted for user authentication.

REFERENCE

Al Zain, M., Soh, B., & Pardede, E. (2012). A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. IEEE.

Beckham, J. (2011), 'The Top 5 Security Risks of Cloud Computing' available at: http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing/ (accessed 17/09/2013).

Chander etal.(2013) *International Journal of Advanced Research in Computer Science and Software Engineering* Vol 3(5) May -2013, pp. 570-575

Han, D. and Zhang, F. (2012), Applying Agents to the Data Security in Cloud Computing. International Conference on Computer Science and Information Processing (CSIP). IEEExplore Pp. 1126 – 1127

kresimir popovic and Zeljko Hocenski (2010) Cloud Computing Security and Challenges in MPRO

Mariana Carroll, Paula Kotzé, Alta van der Merwe (2012). "Securing Virtual and Cloud Environments". In I. Ivanov et al. Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy. Springer Science+Business Media.doi:10.1007/978-1-4614-2326-3.

Minqui Zhou, Rong Zhang, etal . (2010) " Security and Privacy in Cloud Computing: A Survey" In *Sixth International Comference on Semantics, Knowledge and Grids.*

No author stated, (NY) Notorious Nine, Cloud Security, Info World February 25, May 2013 [Online] *http://www.infoworld.com*

Rewagad, P. and Pawar, Y. (2003), Using Digital Signature with Differ Hellman Key Exchange and AES Encryption Algorithm to Enhance Data security in Cloud Computing. International Conference on Communication System and Network Technologies IEEExplore Pp. 437 - 438

Veeraju Gampala, Srilaskhmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography" vol. 2 Issues 3, July, 2012.

Weihai, P.R. (2013), Data Security in Cloud Computing. The 8th International Conference on Computer Science and Education (ICCSE) IEEExplor. Pp. 811- 813 Columbo, Sri Lanka

Wang, Q., Wang, C., Ren, K., Lou, W. and Li, J. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing IEEE Transactions on Parallel and Distributed System Vol. 22, No. 5, Pp. 848 – 849.