ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Cloud Computing: Data Separation Issues

Mrs. Seema Singh Solanki
Assistant Professor,
Department of Computer Sciences and Engineering,
Everest College of Engineering, Aurangabad.

Shaikh Nabeel
ME-I year,
Department of Computer Sciences and Engineering,
Everest College of Engineering, Aurangabad.

Abstract:

Cloud Computing is a new way of computing where dynamically scalable and often virtualized resources are provided as services over the internet. With Cloud Computing Technology, the end users share a number of devices, i.e PCs, laptops, smart phones, storage, program and application development platforms over the internet, through services that are accessible by cloud computing service providers.

It offers many benefits, but still there are many critical issues in Data Storage. One of the issues is Data Separation. The data is stored in same space from different organizations as they share resources to reduce the cost. There may be possibilities of mixing the data of many organizations which cause many problems. So there we need to separate the data to provide reliability, confidentiality, security, and availability of the data. This reseach paper illustrates the issues in data separation and method by which data can be separated.

Keywords:

Cloud computing, Data separation, Reliability and Security, Authentication, Encryption, Data storage.

1. INTRODUCTION:

Cloud computing is a paradigm shift in which computing is moved away from PC and even the individual enterprise application server to a 'cloud' of computers. A cloud is a virtualized server pool which can provide the different computing resources of their clients.

The Cloud allows users to use and share a mass of software and hardware as well as data resource regarding their applications and services[1].

The concept of data computing system such as Client/ Server and distributed system to cloud computing were the advantages which include reducing costs, automation promotion, more flexibility, integrating data and security[2].

Moving the data to the cloud depends on the security objectives of a firm, cloud computing should be approached carefully with special consideration of the sensitivity of data that the firm is planning to move beyond their firewall.

The less control you have for your data on cloud means more you have to trust the providers' security policies. So security of these shared resources is the most challenging task in cloud environment.

For security purposes, it is important to note that as a firm moves to the cloud, it loses operational flexibilities and direct control over security. IaaS customers have greater control over its configurations, security and actions than as SaaS customers.

The cloud service provider is responsible for providing nearly everything, making it easy for a firm to switch to this new business model.

To provide confidentiality, integrity, availability, and trust in the cloud, they need to separate the data. If you want to store the data on the cloud, make sure that you secure the data by encrypt it and then transmit it with technologies like SSL.

In this research paper, we discuss on what are the security issues in the cloud computing, why there is a need to separate the data, what are issues faced by cloud service provider after data separation and how they can separate the data.

2. CHALLENGES IN SECURITY :

2.1 Secure Data Transfer :

To access any service in the cloud, requires internet. There are always chances of modification or stealing of the data over the internet by an intruder. So for security purposes always make sure your data is always travelling on a secure channel. Use "https" in the URL to connect your browser to the cloud. Data must be encrypted before sending to the cloud. Use standard protocols such as IPSec (Internet Protocol security) for authentication purpose [6].

2.2 Secure Software Interfaces :

Set of software interfaces are exposed by the cloud service providers to the customers to interact with the services in the cloud. These software interfaces provides the availability and security of the cloud services [6,13]. The Cloud Security Alliance (CSA) recommends that you must use secure software interfaces to interact with cloud services because weak set of software interfaces may cause security issues such as confidentiality, integrity, availability, and accountability.

2.3 User Access Control :

Data stored on the cloud provider's server can be accessed and managed by persons those are not privileged to users such as employees of cloud service provider's company and we don't have personal control over those people [6,11]. They can misuse the data. Consider carefully the sensitivity of the data that we are allowing into the cloud. Ask to the cloud service provider about those people who manage you data.

2.4 Secure Stored Data :

Many firms uses cloud computing to store their data on the storage blocks of cloud provider. The firm should make sure that data should be securely encrypted when it is on the provider's servers and while it is in use by the cloud service so that data will not be misused [6]. Also ask to the cloud service providers that how they can provide security to the data not only when it is transmitted but also when it is on their server and accessed by any other cloud service.

2.5 Data Separation :

All the resources are shared in the cloud computing so every service shares resources such as space on the provider's servers and other parts of the provider's infrastructure. Hypervisor is used to create virtual containers on the provider's hardware for each of its users [6]. But still there is lack of security of data of the customers. Data is stored in a shared environment where one customer's data is stored alongside another customer's data.

2.6 Data Protection:

Data can be stored at any geographical location in cloud computing. In cloud computing service contract, customer is not guaranteed that their data is always stored within a specified region and it will not transfer outside a specified region. Users need to be aware that local laws may apply to data held on servers within the cloud. Customer should enquire the details of data protection laws in the relevant jurisdictions [11].

2.7 Data Recovery :

Many unexpected problems can occur in cloud computing. A customer should aware that what plan will be place by cloud service provider to recover your data in event of a disaster and how long it will take to recover the data [11].

3. ISSUES DUE TO WHICH WE NEED TO SEPARATE THE DATA:

3.1 Loss of Sensitive Information:

In cloud computing all the resources are shared. To reduce the cost, data from different customers are stored in one container. If there is aggregation of data done by service provider then data of different organizations can mix or may loss. For example, In 2007 Microsoft and Yahoo! released some search data to the US Department of Justice as part of a child pornography case. In 2006, AOL released search terms of 650,000 users to researchers on the public web pages. In 2007, the British government even misplaced 25 million taxpayer records [9].

If your data was innocently mixed with this data then you were wrongly pulled into an investigation. So that's why we need to separate the data.

3.2 Outages :

As discussed above without data separation, there may be loss of data. Client applications will go offline. Clients will not be able to access their data. So clients might leave the company which provides the cloud service. For example, in February 2008, Amazon Simple Storage Service(S3) had a massive outage which in turns had an impact on a lot of web services. Numerous clients were not able to access their data. Amazon reports that they have resolved the problem and performance is returning to normal levels for all Amazon Web Services that were impacted [9].

3.3 Theft:

As storage providers put everything in one container, so your company's data could be stored next to your competitor's data. The risk of stolen your information is real. Your data could be stolen or viewed by those people who don't have permissions to see your data. These people may be hackers or employees of the cloud service provider's company. Risk of stealing your data is increases as the data go outside your data centers. So ensure that cloud service provider must take guarantee of your data in the security point of view.

3.4 Trusted Boundaries are Unclear:

Information security practitioners in traditional organizational IT know their trusted boundaries very well. In cloud, security of information is the responsibility of cloud service provider but mostly it is not clearly mention in the cloud provider's Service Level Agreement (SLA) and those changes in the responsibilities may vary from provider to provider.

Due to this, one organization may or may not access the data of another organization. It could cause misuse of that data. There should be trusted boundaries made by cloud service provider for the security of your data. Data can be accessed within the trusted boundaries. An organization can't access the data of another organization [7].

3.5 Insecurity in Logical Data Separation:

Earlier organizations used their own data centers to store their data and it was physically separated from the data of another organization. This mechanism provides security to the data. Even in the private cloud, dedicated servers are provided to the organization to run their applications and store their data.

But in public cloud all the resources are shared by multiple organizations and data of many organizations are placed in these shared resources and also under the control of cloud service provider. There is logical isolation between the data of each and every client but still risk of stolen your information is real.

3.6 Less Reliability :

Data from many organizations is just logically separated from each other. It can be mixed. If your data is not secure or may be accessed by another person then you never prefer to store your data. A disgruntled employee could alter or destroy the data using his or her own access credentials. If cloud storage system is not reliable, no one wants to save the data on an unreliable system.

3.7 Lack of Availability:

As we know that without data separation, one organization can access the data of another organization. It is also possible that data may misuse or even loss. You can't compromise your data only to reduce the cost. Organizations always need their data to run their businesses so we need to separate the data for high availability.

4. ISSUES AFTER SEPARATING THE DATA:

4.1 Cost :

Data can be separated either physically or logically to provide security. To provide physical separation of data, cloud service provider need to purchase storage arrays. There is high cost in separating the data in the cloud because service provider has to do encryption and decryption techniques, separate backups for data of an organization to provide security.

4.2 Secure Technology :

SSL is the standard security technology for establishing an encrypted link between a web server and browser. It ensures that data passed between the browser and the web server stays private. Data of an organization must be transferred using SSL.

4.3 Cloud Storage :

Cloud storage systems utilize hundreds of data servers. All the data should be redundant, without it cloud storage systems could not assure clients that they could access their information at any given time. So there is need of more storage arrays just for storing Backup data.

4.4 Data Mobility :

When data mobility is at a high level then the risks and issues increases especially when the data is transferred to another country. After separating the data of one organization from the data of another organization we can say that it is stored secure but you must ensure that provider take care the security of your data even when it is transferring from one place to another.

4.5 Different Levels of Security :

In the cloud computing, without adequate security controls can place the IT infrastructure at risk. After separating the data we can provide different levels of security of data for different customers as pay-per-use on-demand computing. But monitoring all these things is difficult task.

5. METHODS FOR SEPARATING THE DATA :

5.1 Data Segregation :

Data segregation is the separation of data of one customer to the data of another customer (see Figure 1). Consumer A, Consumer B, and Consumer C shares the same commodity resources but due to segregation they have their own data separate from each other.

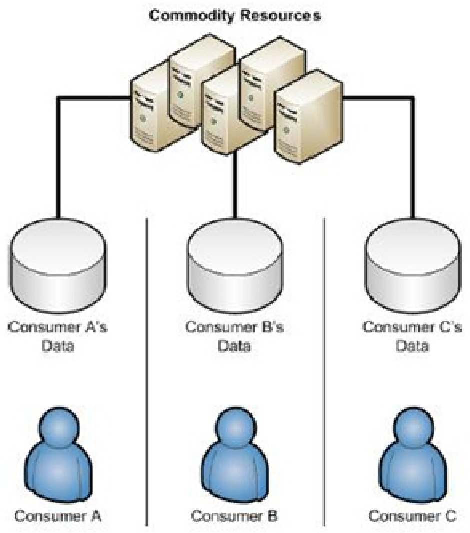

Figure 1: Data Segregation across multiple customer data stores [8]

In the cloud environment, the resources are shared by multiple customers this means the data for multiple customers may be stored or processed on the same physical computers [12]. It is difficult to ensure data segregation in cloud computing. If data segregation solution will fail at some point then one customer can access the data of another customer. You should ensure that the data leak prevention (DLP) measures are takes place in the infrastructure of the cloud service provider.

5.2 Data Fragmentation:

It is the process when piece of data is broken into multiple pieces. Files are fragmented and encrypted before leaving the system. We can provide security and confidentiality of data using fragmentation in cloud computing environment. [12].

5.3 Masking and Encryption:

Procedures related to encryption are popular from ancient era to keep the data secure. A lot of work had been doing in this issue, from Cesar encryption method which already decode in a twinkling of an eye to the most modern of them which takes a million years to reveal. It can also be noted to the cases such as data such as data encryption in network space (input and output data of database which exchange based on encryption standards such as RC4, DES, AES and also SSL techniques), data masking (when we want to transmit sensitive data from an environment which created to the other one to improve applications, test and data analyses) [20], export encryption (in most database server , the possibility of data input and output as encrypted is provided which can be used in credit cards) and back up encryption (not only the data must be encrypted during usage but also when backing up in external storage of media , they must be encrypted) [17, 18, 19].

5.4 Authentication Process :

It is the process in which a user needs to enter the user name and password into the system for the user identity validation. So that only authenticated user can access authorized data. One-time passwords, X.509 certificates and device fingerprinting are the user authentication methods.

5.5 Monitoring:

Monitoring is one of the main involved parts of the data base server. This service provides the possibility of monitoring of the related applications and interactions on data base effectively [20]. It can be noted to the main parts of monitoring such as database auditing (which usually include auditing records such as auditing procedures, users actions, time and date),

fine grained auditing (this technique was introduced by Oracle9i for the first time and provide auditing based on security), audit consolidation, reporting and alerts (considering authentication, priorities, the possibility of access to data auditing, reports and messages will be available) and secure configuration scanning [17, 18, 19].

5.6 User management:

In this part, it can be noted to the security items such as choosing secure password (choose passwords by considering related issues such as compound using of characters), centralized user management, strong authentication, proxy authentication and secure configuration basics which each of the above-mentioned can increase the level of security and its sub-groups [17, 18, 19].

5.7 Access Control:

Access control is one of the important issues related to the security in different cases which include subjects such as privileged user controls, controlling database, when, where, who and how to access data and related applications to database, determining row and column level security, multi-level security and data classifications which can do changes based on cloud environment needs and optimized use of previous achievement [17, 18, 19].

6. CONCLUSION :

Cloud computing is a latest trend to access the shared resources. It helps to reduce management responsibilities, reduce cost and increase efficiency of a firm. Advantages are many but there are also challenges. Challenges relate to loss of sensitive information, price, reliability, outages, data mobility etc. This research paper focuses on and discusses the data separation issues, security issues, and methods by which we can separate the data for security purpose, availability and cost.

7. REFERENCES:

[1] J. Che, Y. Duan, T. Zhang, J. Fan," Study on the security models and strategies of cloud computing", Procedia Engineering, Vol. 23, pp586-593, 2011.

[2]S. Marston, Z. Li, S. Bandyopadhyay , J. Zhang , A. Ghalsasi, "Cloud computing — The business perspective", Decision Support Systems,vol. 51, pp176-189, 2010.

[3]N. Sultan, "Cloud computing for education: A newdawn", International Journal of Information Management , vol. 30, pp109 – 116, .2010.

[4]F..S. Gharehchopogh, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy", International Journal of Scientific & Technology Research (IJSTR), ISSN 2277-8616, Vol. 1, Issue. 6, pp 49- 54 , 2012.

[5]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A.Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud Computing," Communications of the ACM, LIII (4), pp.50-58, April, 2010.

[6] J. Beckham, "Top 5 Security Risks of Cloud Computing," cisco.com, May 3, 2011.

[7] T. Mather, "Cloud Computing Risks and How to Manage them," search security. Tech target.com, June, 2010.

[8]F. P. Miller, "Cloud computing," wikipedia.com, para. 2, June, 2013.

[9]A. T. Velte, T. J. Velte, and R. Elsenpeter, Cloud Computing-A Practical Approach, The McGraw-Hill Companies, New York, 2010.

[10]Figure 1. Data Segregation across multiple customer data stores. Reprinted from Cloud Computing, iDefence Security Intelligence.

[11]J. Bui, "Data Security in the Cloud," castelain.com.au, May 17, 2010.

[12]The VeriSign, iDefense Security Intelligence Team. "Cloud computing," geotrust.com, May 1,2009.

[13]R. Los, D. Gray, D. Shackleford, and B. Sullivan, "Cloud Computing Top Threats in 2013," cloudsecurityalliance.org, Feb, 2013.

[14] Figure 2. Encrypt your data before it send to the service provider. Reprinted from Cloud Computing: A Practical Approach (p. 32), by A.T. Velte, T.J. Velte, and R. Elsenpeter, 2010,New York: Mc. Graw Hill. Copyright 2010 by the McGraw-Hill Companies.

[15]N. Carr, "Crash: Amazon's utility goes down," roughtype.com, Feb 15, 2008.

[16]H. Aleksandar, S. Islam, P. Kieseberg, S.Rennert, E. R. Weippl, "Data confidentiality using fragmentation in cloud computing," International Journal of Pervasive Computing and Communications, IX (1), pp. 37 – 51, 2013.

[17] P. Huey, "Oracle Database Security Guide 11g Release 1 (11.1)",p.374,October 2007.

[18]Sideris Courseware Corp ,"Oracle Database 11g R2: Encryption & Advanced Data Security",P.322,May 9, 2011.

[19]Osborne/McGraw-Hill ,"Oracle Security Handbook : Implement a Sound Security Plan in Your Oracle Environment",p.624, August 2001.

[20] S. Fogel, J. Stern, C. McGregor , "Oracle Database 2 Day DBA 11g Release 1 (11.1)",p.274, February 2012.