INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Data Separation Issues in Cloud Computing

Kiranjot Kaur[1], Sheveta Vashisht[2]

[1] Department of Computer Sciences and Engineering, Lovely Professional University,
Phagwara, Punjab, India- 144411
kiranjot70@gmail.com

[2] Department of Computer Sciences and Engineering, Lovely Professional University,
Phagwara, Punjab, India- 144411
sheveta.16856@lpu.co.in

Abstract*: Cloud Computing is a term for delivering hosted services over the internet. It follows a pay-as-you-go paradigm. Cloud Computing is an emergency paradigm for large scale infrastructures. It has the advantages of reducing cost by sharing computing and storage resources, decrease in cost of electricity, network bandwidth, and operations. 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 security, reliability, confidentiality, and availability of the data. The paper describes the major issues in data separation and method by which we can separate the data.*

Keywords: *Cloud computing, Data storage, Data separation, Reliability, and Security.*

1. INTRODUCTION

Cloud Computing refers to the delivery of applications as services over the internet. It also includes the hardware and the system software in the data centers which provide those services [1], [4]. It increases the utilization of the resources. So users just need to pay to the cloud service provider. It follows pay-as-you-go paradigm. Organizations are moving to Cloud to eliminate the need of CAPEX model and just use OPEX model [4]. It provides shared resources in terms of computation and storage. These shared resources are the only way to gain the economies of scale that result in lower costs. So security of these shared resources is the most challenging task in cloud computing. For security reasons, it is important to note that as an organization moves to the cloud, it loses operational flexibilities and direct control over security. IaaS customers have greater control over its configurations, actions and security than as SaaS customers. The cloud service provider is responsible for providing nearly everything, making it easy for organizations to switch to this new business model. To provide integrity, confidentiality, 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.

There are numbers of challenges are as follows:-

- Governance, management and updating the data.
- Management of software services.
- Monitoring of products and processes.
- Reliability and availability of systems and infrastructures.

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

The rest of the paper is organized as follows: Section II describes the security challenges. Section III describes issues due to which we need to separate the data. Section IV describes the issues in separating the data. Section V represents methods for data separation. In the last section, conclusion and future work is presented.

2. SECURITY CHALLENGES

2.1 Secure Data Transfer

Whenever we have to access any service in the cloud, we need to use internet. There are more changes of eavesdropping, modification or stealing of the data over the internet by an attacker. This means data may be hacked in between. So for security purposes 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. Always use standard protocols such as IPSec (Internet Protocol security) for authentication purpose [2].

2.2 Secure Software Interfaces

Set of software interfaces or APIs are exposed by the cloud service providers to the customers to interact with the services in the cloud. These software interfaces or APIs provides the security and availability of the cloud services [2], [9]. The Cloud Security Alliance (CSA) recommends that you must use secure software interfaces, or APIs to interact with cloud services because weak set of software

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

interfaces or APIs may cause security issues such as confidentiality, integrity, availability, and accountability.

2.3 Secure Stored Data

Many organizations use cloud computing to store their data on the storage arrays of cloud provider. Make sure that your 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 your data will not be misused [2]. Also ask to the cloud service providers that how they can provide security to your data not only when it is transmitted but also when it is on their server and accessed by any cloud service.

2.4 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 [2], [7]. 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.

2.5 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 [2]. 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 [7].

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 [7].

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 [5]. 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 [11].

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 datacenters. 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 [3].

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

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

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 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.

4.3 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.

4.4 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.

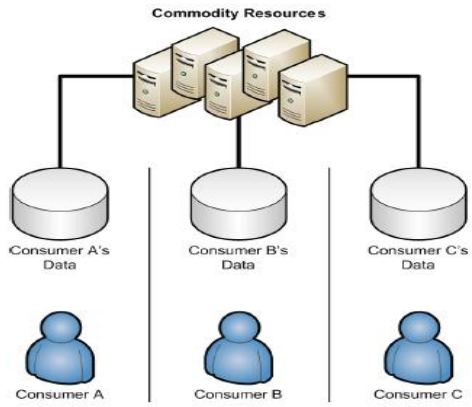

Figure 1: Data Segregation across multiple customer data stores [6]

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 [8]. 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 Encryption

The best way is encrypting your data before sending it to service provider. Firstly data is encrypted by user with any cryptographic algorithm and then it is transferred to the infrastructure of Service Provider through internet (see Figure 2). It is a complex algorithm which is used to encode the information programs like PGP or Truecrypt can encrypt the file so that only those with a password can access it.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

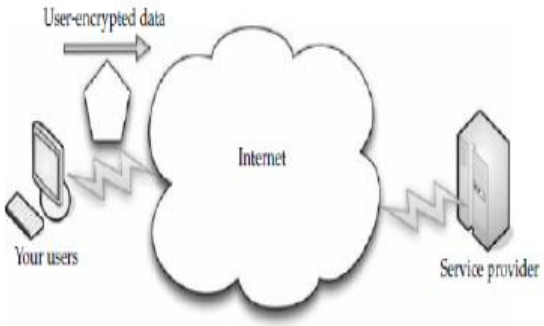

Figure 2: Encrypt your data before it sent to the service provider [10]

5.3 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. X.509 certificates, one-time passwords, and device fingerprinting are the user authentication methods.

5.4 Authorization Practices

It describes which user has which privileges and what a user is allowed to do. It is the next step after authentication. Authentication can be determined based on user identity and/or by user role. Many corporations have multiple levels of authorization.

5.5 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]

6. CONCLUSION

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

REFERENCES

[1] **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.**

[2] **J. Beckham, "Top 5 Security Risks of Cloud Computing," cisco.com, May 3, 2011. [Online]. Available: blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing/**

[3] **T. Mather, "Cloud Computing Risks and How to Manage them," search security. Tech target.com, June, 2010. [Online]. Available: http://searchsecurity.techtarget.com/magazine Content/Cloud-computing-risks-and-how-to-manage-them**

[4] **F. P. Miller, "Cloud computing," wikipedia.com, para. 2, June, 2013. [Online]. Available:http://en.wikipedia.org/wiki/Cloud_computing#Software_as_a_service_.28SaaS.29.**

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

[6] **Figure 1. Data Segregation across multiple customer data stores. Reprinted from *Cloud Computing*, iDefence Security Intelligence. Retrieved from http://www.geotrust.com/geocenter/resources/gt/iDefense_Cloud_Computing_TRP_20090501-1.pdf. Copyright 2009 by VeriSign. Reprinted with permission.**

[7] **J. Bui, "Data Security in the Cloud," castelain.com.au, May 17, 2010. [Online]. Available: http://www.castelain.com.au/blog/data-security-in-the-cloud**

[8] **The VeriSign, iDefense Security Intelligence Team. "Cloud computing," geotrust.com, May 1, 2009. [Online]. Available: http://www.geotrust.com/geocenter/resources/gt/iDefense_Cloud_Computing_TRP_20090501-1.pdf**

[9] **R. Los, D. Gray, D. Shackleford, and B. Sullivan, "Cloud Computing Top Threats in 2013," cloudsecurityalliance.org, Feb, 2013. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf**

[10] **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. Reprinted with permission.**

[11] **N. Carr, "Crash: Amazon's utility goes down," roughtype.com, Feb 15, 2008. [Online]. Available: http://www.roughtype.com/?p=1067**

[12] **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.**