Vol.4,No.1, July, 2015
186 - 189,ISSN:0975-5446 [VNSGU JOURNAL OF SCIENCE AND TECHNOLOGY]

Loss of Control over Data in Cloud Computing

KAPADIA Gayatri S.
Assistant Professor
Master of Computer Application Department
Sarvajanik College of Engineering & Technology
Surat, Gujarat, India.
gayatri.kapadia@scet.ac.in

GULATI Ravi M.
Associate Professor
Department of Computer Science
Veer Narmad South Gujarat University,
Surat, Gujarat, India.
rmgulati@gmail.com

Abstract

In information technology area, today's most up-to-date standard is Cloud Computing which provides various services like centralized data storage (without bothering about actual storage locations) and online access to available computer resources or services. As an organization we can use services provided by Cloud Computing to develop our infrastructure. One of the services provided by cloud computing is Storage. We can hand over our data to the third party service providers who will look after storage and management of our data; we do not worry about it. And yet security of these data is the biggest issue for us as data travel across the internet to all over world and we have control on neither physical infrastructure nor entry/exit outlet points. Our data can be misused, trapped, theft or deleted. This paper presents some of issues dealing with loss of control over data and recommendations - few of which are discussed by authors [2] [3] [6] [8].

Keywords*:* Control over Data, Categorization of Data,

1. Introduction

Moving to the cloud does not exactly mean we are expanding our infrastructure. It is unsafe to outsource critical data to the cloud because we do not know which boundaries of different countries or regions are crossed by our data? Once the data are handed over to the third-party, we feel free that nothing can go wrong. But actually we have given direct control over data and we cannot revert this. And it is really scary to loss control over data. So, let's understand some issues regarding controlling the data on the cloud and recommendations.

2. Concern and Recommendations

Almost every area of Information and Communication (ICT) is affected by Cloud Computing. There are two major issues exist with security and privacy aspects of Cloud Computing [1]:

1. Loss of control over data and
2. Dependence on Cloud Computing Provider (CP)

This paper presents various issues related with the first major issue and their recommendations.

1. Loss of Control over data:

Service user (SU) does not know where exactly its data is stored and processed in the cloud. [2]

Issue: As data are free to cross international borders over the internet and this can expose to further security. [2] The substance of data security and privacy safety in cloud is similar to that of conventional data security and privacy protection. It is also implicated in every stage of the data life cycle. [4] Is there any way to keep track of which are different ways crossed by our data over internet, so that we can prevent our data from unauthorized access? The answer is no – practically it leads to wastage of time and resources.

Recommendation: The transparency should be existed between CP and SU with regard to the processing and storage of data. For example, the physical location of data storage. Make SU know about it. Thus the trust between CP and SU can be strengthened.

Issue: Most of Cloud Computing providers are used to perform data mining techniques to analyze user data. This is a very sensitive function because users are often storing and processing sensitive data when using Cloud Computing services. For example, for social media applications that supports users to share much of their private details like photos. [1]

Recommendation: The Cloud Computing providers should ensure data confidentiality, integrity, and authentication control. Categorize user data, split data into chunks and provide these chunks to the proper cloud providers. This approach consists of categorization, fragmentation and distribution of data. The categorization of data is done according to mining sensitivity. Distribution restricts an attacker from having access to a sufficient number of chunks of data and thus prevents successful extraction of valuable information via mining. [3]

Issue: Data Segregation is the separation of data of one consumer to the data of another consumer. (See Figure) 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.

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 [5]. 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. [6]

Recommendation: You should ensure that the data leak prevention (DLP) measures are takes place in the infrastructure of the cloud service provider. [6]

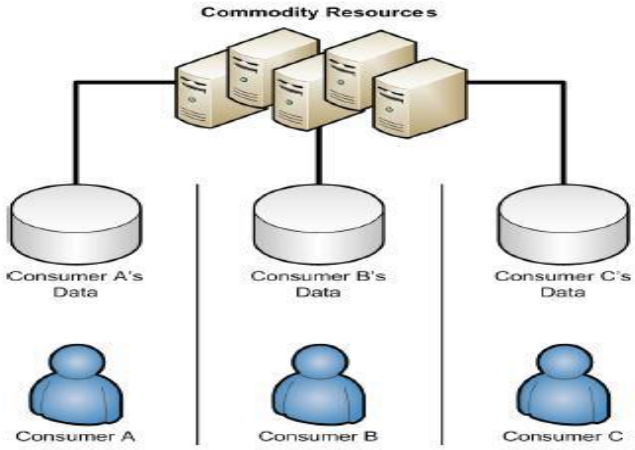

Figure Data Segregation across multiple customer data stores [5]

Issue: Accountability – even though cloud services are difficult to trace for accountability purposes, in some cases this is a mandatory application requirement. [2]

Accountability [7] is the obligation to act as a responsible for preserving the personal information of others and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that personal information.

Recommendation: The system should not interfere with cloud and cloud application actions, but collect data and snapshots to enforce accountability policies. [2]

We can develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user can retrieve the logs as needed. [8]

3. Technical Aspect

We have seen issues dealing with loss of control over data and recommendations. Now, let us understand how to achieve control over data technically, we can design various types of controls for data input, processing and output. [10]

Table: Controls for providing control over data in cloud computing.

Controls	**Description**
Validation Controls	By placing validations on Input, we can ensure that inputs of data to an application or a system are accurate and inclusive.
Access Controls	Provide authentication for accessing data, verify whether the user is authorized user or not. Only authorized user can access the sensitive and/or encrypted data.
Backup and Recovery Controls	To keep up logical and physical control over data backup and recovery, use some data backup and recovery mechanisms which not only ensure that nobody can directly access data but also ensure that data is deleted permanently from all duplicate storages.
Auditing Controls	Periodically maintain proper logs of data. So that its owner or stakeholders access and used these data logs for auditing purpose.

File Controls	Ensure that data are manipulated correctly in structured as well as unstructured files.
Output Conciliation Controls	Ensure that data are put to rights from input to output.

4. Conclusion

It is more and more important to protect people's privacy on the Internet, against unwanted and unauthorized disclosure of their confidential data. Right through this paper, the authors have systematically studied and review the security issues with loss of control over data in cloud computing. We speak up for solutions to deal with these issues in the cloud. Cloud computing introduces the business environment where users can cooperate directly with the virtualized resources and safe the cost for the consumers. It has model to protect its data for the business users. An organization used private clouds within its organization to prevent from loss of data.

References

[1] Marko Holbl "Cloud Computing Security and Privacy Issues" Council of European Professional Informatics Societies (CEPIS) Newsletter Version V17/15/3/2011 p.p. 1, 2.

[2] Lombardi F, Di Pietro R. "Secure virtualization for cloud computing" J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.06.008 p.p. 3.

[3] Uppunuthula Venkateshwarlu, Puppala Priyanka "Survey on Secure Data Mining in Cloud Computing"International Journal of Advanced Research in Computer Science & Technology ISSN : 2347 – 8446 Vol. 2, Issue 2, Ver. 1 (April - June 2014) p. p. 4

[4] Dr.P.K.Rai, R.K.Bunkar, Vivekananda Mishra " Data Security and Privacy Protection Issues in Cloud Computing" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IX (Feb. 2014), pp 41

[5] Figure "Data Segregation across multiple customer data stores. Retrieved from http://www.geotrust.com/geocenter/resources/gt/iDefense_Cloud_Computing_TRP_20090501-1.pdf pp 18

[6] Kiranjot Kaur, Sheveta Vashisht "Data Separation Issues in Cloud Computing" International Journal for Advance Research in Engineering and Technology ISSN 2320-6802 Vol. 1, Issue X, Nov.2013 pp 28

[7] S. Pearson, "Towards Accountability in the Cloud ," IEEE Internet Computing, Vol. 15, Issue 4 pp. 64-69, Jul-Aug 2011 DOI:10.1109/MIC.2011.98

[8] C. Madhuri, 2 A. Krishna chaitanya "Cloud Information Accountability Frameworks for Data Sharing in Cloud" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 13, Issue 2 (Jul. - Aug. 2013), PP 93

[9] "How to Control Data in Cloud Computing", Access from http://www.dummies.com/how-to/content/how-to-control-data-in-cloud-computing.html