International Journal of Computer Applications (0975 – 8887)
Volume 114 – No. 11, March 2015

A Concern towards Data Security in Cloud Computing

Maninder Singh Bajwa
Department of Computer Science and Engineering
Global Institute of management & Emerging
Technologies, Amritsar, India

Himani
Assistant Professor
Department of Computer Science and Engineering
Global Institute of management & Emerging
Technologies, Amritsar, India

ABSTRACT

Cloud computing is one of the emerging innovative trend of IT technology today. This trend has got remarkable advancement in computing world. Although cloud is boon to computing world but its adoption in IT sector is lack behind due to many issues. In this paper we focus on most prevailing issues related to data security of cloud. The main objective is related to data security which may include the concepts like confidentiality, integrity, data leakage, availability, data access.

Index Terms:

Cloud Computing, Data Security issues.

1. INTRODUCTION

Cloud computing technology is one of the latest trends now days, as it provides services according to the user requirements or on-demand-services. Cloud computing delivers four types of basic deployment models: Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud and three delivery models: SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service). Cloud computing comes with many benefits like Flexibility, increases collaboration, reduces cost and may more. In spite of these benefits, organisations are lacking behind in affiliation of cloud due to several issues.

Data security is one of the major concerns today due to which the organisations not fully take up this technology. The users do not know where the data is being residing after uploading to cloud and even they do not know who is handling their data. Hence the concerns come into mind that whether their data is confidential. Integrity of the data is lost if the alteration is done by any unauthorized person. If the data is not highly available when the user wants to access the data then it may lead to degradation to the business. In this paper we consider those challenges that the users have to deal when they use cloud computing.

2. RELATED WORK

Many research work has been carried out related to data security in cloud computing. Tao Jiang et.al [12] provides an efficient public integrity auditing scheme with user revocation placed on vector commitment and verifier local revocation group signature. In this technique public auditing is done to check the integrity of dynamic data. Rashmi, et.al [10] proposed a Secure Data Sharing in Clouds (SeDaSC) methodology. This methodology uses single encryption key to encrypt files and generates two share keys; one for user and other for trusted third party. Dharmendra S. Raghuwanshi et .al [5] proposed data security architecture which involves encryption and verification services both at file and storage level. This technique ensures the data security and privacy. Cindhamani et.al [3] proposed a trust management framework in which they use 128 bit encryption and RSA algorithm for data security, Trusted Party Auditor for data integrity. Taeho Jung et.al [11] is presents a Semianonymous privilege control scheme. In this model they use AnonyControl and AnonyControl-F to control the privilege access and identity privacy. Ayad F. Barsoum et.al [2] proposed a map-based provable multicopy dynamic data possession (MB-PMDDP) scheme which provides a satisfactory guarantee that the CSP stores all that copies agreed upon the service agreement.

3. SECURITY ISSUES IN CLOUD ENVIRONMENT

Data security is the one of the major challenge in cloud computing as because the users do not know where the data is saved and who handles that data. Some of the challenges are listed below:

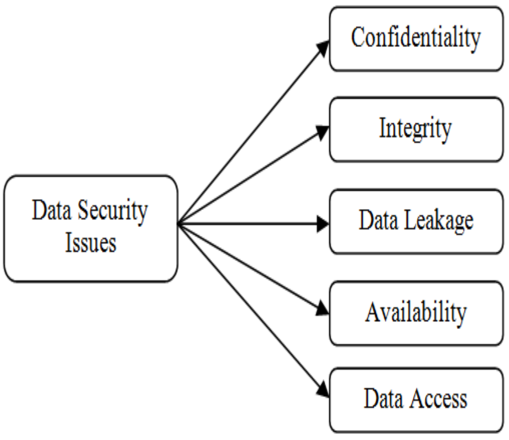

Figure1: Data Security Issues

3.1 Confidentiality

Confidentiality refers to the prevention of the information from the unauthorized access. The information being stored or shared over the cloud is accessed through the internet connection. There are various types of services that the cloud computing provides today like data storage sites, music sites, video sites, tax preparation sites, online banking record websites, live streaming sites and many more. The users can take any service and their records may be stored with single service provider or with multiple service providers. Whenever the information is shared over the cloud whether that information is shared by individual, organisation, government or any other entity then the question of privacy, confidentiality arises.

3.2 Integrity

Integrity refers to the prevention of intentional or unintentional alteration of the information. Integrity should only be maintained when authorized users can get the data access. Public integrity auditing is done to check the integrity of the data and it is done with the group user revocation i.e. based on vector commitment and verifier-local revocation group signature [12]. In order to check the integrity of the data the backup of original data is compared with the present data of the cloud, so the data is properly maintained or backup by the data owner or by third party for the auditing of the cloud data.

3.3 Data Leakage

The data that is gained by any unauthorized person when user/owner sends or receives the data that transits over network is referring as a data leakage. The important step that must be carried by data owner/user is to backup the data because in this way they save ourselves from the financial loss. As the data can be deleted or modified any time by the intruders or even by the users too, if the data is not backed up then this will lead to data loss [8]. More over the preventions can be taken in order to prevent from data leakage; some of the techniques are encryption, implementing strong API security measures, analyzing data protection and so on.

3.4 Availability

Availability refers to ensure that the data provided by the cloud service providers are available to all users. Availability is ensured when the resources and data are reliable and timely accessed by the users. The availability is one of the big concerns of the cloud service providers, if at any reason the cloud service is disrupted then it may affect the customers. For instance, some of the disruption of cloud services are Amazon cloud service in the year 2011, Google cloud failure and took down a number of websites [10]. The method that is used to increase the availability of the data is to clean up the datacenters, which host cloud environments as because of large amounts of useless and redundant data is present over there [1].

3.5 Data Access

While accessing the data, the data access is the main issue related to security policies provided to the users. Some of the employees are not given access to certain amount of data due to security policy consideration. Integrity and data confidentiality should be maintained only when authorized users can obtain the data access. Small organisations typically use cloud services such as data access for their business processes which may be provided by different providers. These organizations may have its own security policies based on which employee can have access to a particular amount of data. To avoid intrusion of data by unauthorized users, security policies are stick to cloud. As the multiple organizations are deploying their business processes within a single cloud environment, so the model must be able to provide organizational boundary within that cloud [10]. Forward and backward access control can be used to control that which employee can get access and which not [9].

4. CURRENT SECURITY SOLUTIONS

A lot of research has been done in the field of data security in cloud computing. Several organisations and groups are developing the standards for cloud computing and are interested in developing security solutions. Some of the solutions are:

Table1: Security areas and Solutions

S.No.	Security Areas	Existing Solutions
1	Confidentiality	• Hybrid Multilevel Encryption and Verification [5] • Attribute based Proxy Re-Encryption [11]
2	Integrity	• Public Integrity Auditing [12] • Hash based message authentication code
3	Data Leakage	• Encryption
4	Availability	• map-based provable multicopy dynamic data possession (MB-PMDDP) [2]
5	Data Access	• Access Control List [9] • Data Access Management [4]

5. CONCLUSION

Cloud computing is on demand technology, in which services are delivered from one side and acquired from another. In this paper the main area of concern is difficulties that cloud computing facet today. Generous research has been taken place but the problems are not clear up completely. There are some questions which are unanswered such as "Is data at cloud?" is in secure hands. Due to the data security reasons many of the individuals/organisations do not accept this technology wholly. Hence, there is need to develop those technologies that will fix up the problems. In future the methodology can be proposed to resolve the security related issues. Therefore, there is need to endeavor on numerous security mechanisms that has been mentioned, in order to cater translucent services that can be trusted by all users.

6. REFERENCES

[1] Aws Naser Jaber, Mazlina Binti Abdul Majid, Mohamad Fadli Bin Zolkipli and Nusrat Ullah Khan, "A Study in Data Security in Cloud Computing", 2014 IEEE.

[2] Ayad F. Barsoum et al "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015

[3] Cindhamani.J et al "An enhanced data security and trust management enabled framework for cloud computing systems", 5th ICCCNT – 2014.

[4] Cristina Basescu et al, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies". IEEE 2011 INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION NETWORKING AND APPLICATIONS, ROME.

[5] Dharmendra S. Raghuwanshi et. al "MS2: Practical Data Privacy and Security Framework for Data at Rest in Cloud", 2014 IEEE.

[6] Jeong-Min Do et.al, "Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments". 1ST IEEE ACIS/JNU INT. CONFERENCE ON COMPUTERS, NETWORKS, SYSTEMS, AND INDUSTRIAL ENGINEERING (CNSI 2011), KOREA.

[7] Jingwei Li et.al. “Secure Auditing and Deduplicating Data in Cloud”, 2015 IEEE TRANSACTIONS ON COMPUTERS.

[8] Louai A. Maghrabi, “The Threats of Data Security over the Cloud as * Perceived by Experts and University Students”, 2014 IEEE.

[9] Mazhar Ali et al “SeDaSC: Secure Data Sharing in Clouds”, IEEE SYSTEMS JOURNAL 2015.

[10] Rashmi, Dr.G.Sahoo and Dr.S.Mehfuz, “Securing Software as a Service Model of Cloud Computing: Issues and Solutions”, INTERNATIONAL JOURNAL ON CLOUD COMPUTING: SERVICES AND ARCHITECTURE (IJCCSA), VOL.3, NO.4, August 2013.

[11] Taeho Jung et. al “Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.

[12] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma, “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation,” IEEE 2015.