ISSN:0975-9646

Dandawate Vrushali Vilas et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6514-6516

Study of Different Security Issues in Cloud Storage

Dandawate Vrushali Vilas
Information Technology Department
SGGS IE&T
Vishnupuri, Nanded

Dr. Ravindra C. Thool
Information Technology Department
SGGS IE&T
Vishnupuri, Nanded

***Abstract*— Cloud computing is a model that provides on-demand services to its clients. Data storage is among one of the primary services provided by cloud computing. Cloud service provider hosts the data of data owner on their server and user can access their data from these servers. As data owners and servers are different identities and also data being stored on network, the paradigm of data storage brings up many security challenges. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper we will study different techniques that are used to secure data storage on cloud.**

***Keywords*— cloud computing, data storage, cloud storage server.**

I. INTRODUCTION

Cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. We can say cloud computing is a term for anything that involves delivering services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-service (IaaS), Platform-as-a-Service (PaaS) and software-as-a-Service (SaaS). Cloud computing has long list of advantages in IT enterprise such as: on-demand service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage based pricing, ultra large scale, virtualization, high reliability, versatility, high extendibility, extremely inexpensive. Cloud computing is also referred to as utility computing or on demand computing. In this cloud computing model, it allows a user to pay for only as much utility as is used, and provide the data as and when needed. Because this pay as you use model resembles the way electricity, fuel and water are consumed.

II. CLOUD STORAGE

Cloud storage is one of the primary use of cloud computing. We can define cloud storage as storage of the data online in the cloud. Basically a cloud storage system can be considered as a distributed data centers which typically use cloud computing technologies and offers some kind of interface for storing and accessing data. When storing data on cloud, the user sees a virtual server that is; it appears as if the data is stored in a particular place with specific name. But that place does not exist in reality. It is just a pseudonym used to reference virtual space carved out of the cloud. In reality, the user's data could be stored on any one or more of computers used to create the cloud. With the cloud storage, data is stored on multiple third party servers, rather than on the dedicated servers used in traditional networked data storage. Storing the data at different location may increase the availability of the data.

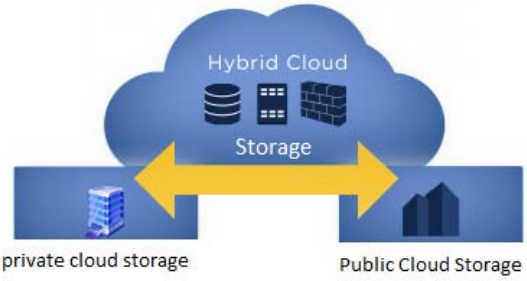

Figure 1 Types of Cloud Storage

There are four main types of cloud storage:

Personal Cloud Storage: It is also known as mobile cloud storage. In this type storage, individual's data is stored in the cloud, and he/she may access the data from anywhere.

Public Cloud Storage: Public cloud storage is where the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data center. The cloud storage provider fully manages the enterprise's public cloud storage.

Private Cloud Storage: it is a form of cloud storage where the enterprise and cloud storage provider are integrated in the enterprise's data center. In private cloud storage, the storage provider has infrastructure in the enterprise's data center that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

Hybrid cloud storage: It is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

As we know cloud services are based on pay as you use basis, user can buy the storage space according to his needs, store data in cloud and he does not have to worry about purchasing, maintaining and managing expensive hardware. Also user does not even have to maintain local copies of data. User-friendly, easily accessible and money-saving ways of storing and automatically backing up stored data are available on-demand on the Internet. So in case of natural disaster backup of data is safe at remote location saving the cost for disaster recovery measures. Accessibility

of files at any time from any place given the internet is possible in cloud.

To summarize, outsourcing data into the cloud brings many benefits such as relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data.

The data is of great value and its irrecoverable loss or damage could be a total disaster for its owner. Since users stored their data in the cloud, it means that they will lose the control of them and more and more worries come out about the data security. Data security is an important aspect of quality of service. Cloud computing inevitably poses new challenging security threats for number of reasons:

Firstly, traditional cryptographic measures for securing the data cannot be directly adopted due to the users' loss control of data under Cloud Computing. Also user may store various kinds of data on storage servers, so continuous assurance of the data safety and integrity becomes challenging task.

Secondly, Cloud Computing is not just a third party data warehouse. User may want to update the data frequently including insertion, deletion, modification, appending etc. Ensuring storage correctness under dynamic data update is therefore very important.

Thirdly, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats.

The main challenge of cloud storage is guaranteeing control, and the necessary integrity and confidentiality of all stored data. Also cloud faces challenges such as Security and privacy, lack of standards, continuously evolving, compliance concerns, data recovery and availability, management capabilities etc. There are some more concerns such as follows:

When data is distributed it is stored at more than one location, increasing the risk of unauthorized physical access to the data. The number of people with access to the data could be compromised. By sharing storage and networks with many other users/customers it is possible for other customers to access your data. Sometimes because of some erroneous action, faulty equipment, a bug and sometimes because of criminal intent.

III. Related Work

A This section will discuss different security techniques that are proposed by different authors for cloud storage security. Each of the technique has its merits and demerits.

1. User Authenticator Scheme

In this paper [1], author has introduced an approach which combines encryption mechanism along with the data integrity check mechanism. Author has used homomorphic authenticator technique as they are unforgeable metadata generated from individual data blocks. This scheme combines verification protocol along with the auditability. One of the main advantages of this scheme is that it uses much less time than third party auditor.

2. Secure Storage and Access of Data

In this paper [2], authors have proposed an approach which will encrypt the data at the client side using secret key before sending to the cloud storage and decrypted using same key after receiving data from cloud. Secret key is always with data owner and need not be communicated over network so there is no fear for leakage of data and client is assured of data security. Author have divided data into two sections private and shared data section according to which users are allowed to access the data. This increases performance during storage and accessing of data. One to many, many to many communication is not possible since only members of group are allowed to access data over shared section.

3. Two way Handshake Based on Token Management

This [3] paper proposes a distributed scheme with explicit dynamic data support to ensure correctness of users' data in the cloud. This scheme uses erasure correcting code. This scheme also uses homomorphic token with distributed verification of erasure coded data. This method helps deriving a challenge-response protocol for verifying correctness of storage and also identifies misbehaving server. This method introduces procedure for file retrieval and error recovery based on erasure correcting code. In this method file is divided into m number of pieces and they are stored at n different location. Whenever user needs file it is reconstructed from any of the (m+k) parity vectors. This method is used to achieve storage correctness assurance. It reduces storage and communication overhead as compared to traditional replication based file distribution technique.

4. Digital Signature with Diffie-Hellman and AES Encryption

When users stores data on cloud they lose control over it. Data being inside cloud user fears modification of his data by server itself. So author has proposed a three way technique in [4] which will assure user that his/her data is stored in trusted environment. Two different kinds of servers also maintained one for encryption purpose other for storage. In this method client server exchanges the keys using Diffie-Hellman. Server authenticates client using digital signature. And then AES is used to encrypt the data file.

5. Digital Signature with RSA

In this paper [5], authors have proposed digital signature scheme with RSA algorithm to ensure security of the data in cloud. In this scheme requested document is applied with some hash function which is then encrypted using secret key. Result of which is digital signature. It is then applied with RSA to provide security as RSA is the only asymmetric key algorithm used for private/public key generation and encryption

6. Data sharing : Third Party Auditor

This paper [6] has proposed a decentralized information accountability framework and object centered approach. Third party auditor between cloud service provider (CSP)

and data owner reduces the burden of data owner to audit the data. In the framework proposed by author set policies are defined for user when accessing the data. This framework uses JAR programmable capability. This capability can create both dynamic and traveling object. When user tries to access data an authentication and automated logging control to JARs is triggered.

7. Ensuring Data Storage Security in Cloud Computing

In this paper [7], authors have proposed an effective and flexible distributed scheme with explicit dynamic data support including block update, delete, and append. Erasure-correcting code in the file distribution preparation provides redundancy parity vectors and guarantees the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, this scheme has achieved the integration of storage correctness insurance and data error localization that means, whenever data corruption is detected during the storage correctness verification across the distributed servers, the scheme almost guarantee the simultaneous identification of the misbehaving server(s). Scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

IV. CONCLUSIONS

The In both larger and smaller scale organizations cloud computing environment is being used because of large advantages of cloud computing. The cloud computing has different security issues, one can say that concern about data security is the worth mentioning disadvantage of cloud computing.

In this paper we have studied about cloud storage, its merits and security issues that come along with it. Later we have discussed different existing techniques described in various papers for securing the data on cloud and provide assurance to data integrity.

REFERENCES

[1] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, “Data Confidentiality and Integrity Verification usingUser Authenticator scheme in cloud”, Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, “Secure Storage and Access of Data in Cloud Computing”, 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade, “Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management”, 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms.Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing”, 2013 International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[6] Vanitha, R.Raju, “Data Sharing: Efficient Distributed Accountability in Cloud Using Third Party Auditor”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-5, April 2013

[7] Cong Wang, Qian Wang, and Kui Ren,Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing", 17th International Workshop on IW Quality of Service (IWQoS), 13-15 July 2009.S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.