Study of Security Problem in Cloud

Deepali Pande[#1], Prof. Vivek Jog[*2]

[#]SKNOCE, , Computer Engineering, University of Pune
Address Including Country Name

***Abstract*— The cloud computing has revolutionized the world in terms of services provided by it. But there are security problems of this cloud structure. This paper focuses on the security problems in cloud and various security measures taken to solve security problems. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud system.**

***Keywords*— Cloud Computing, Data integrity, TPA**

I. INTRODUCTION

Cloud computing is emerging field because of its performance, high availability, cost effectiveness and many others. Cloud computing now a days is a hot issue in industry as well as in academic with the rapid development of hardware and software. The cloud computing is the result of many factors such as technological advances in computer, communication technology and business technology. It has changed the next generation architecture of IT enterprise. The cloud system can be shared between large numbers of users. The users can access their data from anywhere. Cloud resources are provided as a service or on need basis i.e we can say that it provides on demand self service. It is characterized by broad network access. The resource can be the computing storage and other specification service. The majority of cloud computing infrastructure currently consists of reliable services delivered through data center that are build on servers with different levels of virtualization technologies. Due lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing.

In this paper we will discuss the various techniques used for providing security to cloud computing through various ways. The cloud appears as a single point of access for all computing needs of consumers

II. II PURPOSE OF STUDY

Cloud security Problem:

The cloud system is working with internet and the security problem which are related with internet is also be applicable to cloud system. The general security problems like virus attack, hacking is also applicable to cloud computing. The hackers and malicious users may attack cloud system and steal sensitive data stored on cloud system. But many companies fear to do this because of the problem of data leakage.

From 3D Cloud Security

Here we focus on the problem of data leakage and proposes a framework works in two phases. First phase which is known as Data classification is done by client before storing the data. During this phase the data is to be categorized on the basis of CIA (Confidentiality, Integrity, and Availability). The client who wants to send the data for storage needs to give the value of C (confidentiality), I (integrity), A (Availability). The value of C is based on level of secrecy at each junction of data processing and prevents unauthorized disclosure, value of I based on how much assurance of accuracy is provided, reliability of information and unauthorized modification is required, and value of A is based on how frequently it is accessible. With the help of proposed formula, the priority rating is calculated. Accordingly data having the higher rating is considered to be critical and 3D security is recommended on that data. After completion of first phase the data which is received by cloud provider for storage, uses 3Dimentional technique for accessibility. The sensitive proved data will send for storage to cloud provider. According to the concept of 3D user who wants to access the data

need to be authenticated, to avoid impersonation and data leakage. Now there is third entity who is either company's (whose data is stored) employee or customer who want to access, they need to register first and then before every access to data, his/her identity is authenticated for authorization.

Data Integrity in Cloud

Cloud storage allows client to store data in storage network. So it is necessary to ensure data integrity and and availability on a long term basis. There are following types of protocol used to check data integrity.

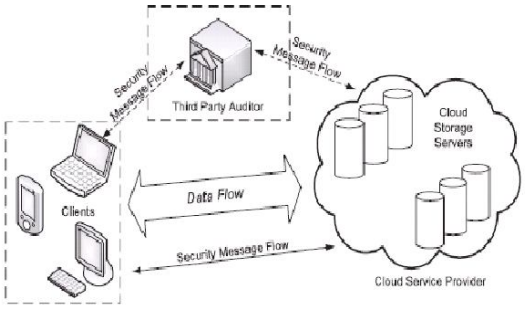

Fig 1 Cloud data storage architecture

Principles of data integrity checking protocol:

Remote data possession checking protocol is having following requirement.

In this case it is not necessary for verifier to keep an entire copy of files which he wanted to check. The protocol must be secure even if prover is malicious. The protocol must be efficient in terms of computation. In addition to this a protocol must consists of

Privacy : To perform tasks on cloud without hampering its privacy.

Lightweight : To allow checking to be performed with minimum storage , lower communication cost and less computation overhead.

Dependability.

There are two types of verification tag based vs. data replication based verification. In case of tag based verification the supplementary information is the main source of data verification.

Using Encryption Algorithm to Enhance Security in Cloud.

The main concept of cloud computing comes with the concept such as IaaS (Infrastructure as aService), PaaS (Platform as a Service) , SaaS(Software as a Service) and in all *aaS (Everything as a Service) that is why it can be called as service oriented architecture.

Cloud storage can deploy allocate and reallocate resources dynamically. Cloud computing is basically broken down into three parts application, storage and connection. It provides software data access, and storage resources which do not require cloud to know location and detail of the computing resources. It provides everything to the user but there is nothing like authentication or checking who is accessing what. So the main issue is security. However the security aspect of each user is different in terns of use. To solve the problem of data security various encryption algorithms are proposed like : AES, DES, RSA and blowfish. These algorithms are reliable as it do not require any third party to encrtpt data on client side. In this user is also authenticated using password and each and every data in cloud will go through encryption framework. It is secure as encryption keys are generated but never stored on cloud in any form.

Third Party Auditing for Secure d

Data Storage in Cloud through Digital Signature using RSA

In this method we use RSA algorithm for encryption and decryption which uses digital signature process for the message authentication. In this case there is third party auditor, cloud storage server and the user. The RSA algorithm helps TPA and user to generate their own public and private keys. Both of them follows the principle of RSA for generating public and private keys.

It selects two prime numbers p1 and q1 and perform operations as follows.

$N1 = p1 * q1$

$fn1=(p1-1)(q1-1)$

then any public key is selected and private key for TPA is generated Similarly user selects two relative prime numbers and generate private and public key for himself.

In this way the generated public key set is get exchanged between user and TPA. Data is signed with users private key and the data is encrypted with TPA's private key. The same package is send to cloud and TPA. The TPA will now decrypt the data with his private key. Same process is carried out in the cloud by TPA to verify the correctness of data. Efficient data security using third party auditor

Dynamic data auditing for outsourced data in cloud

In this we propose a dynamic audit service for verifying the integrity of an untrusted and outsourced storage.

III. Conclusion

This paper illustrates the cloud concept , cloud capabilities and various problems associated with cloud security and data. This paper also discusses several security methods for securing data in cloud storage. We have discussed several algorithms and other techniques for the security in cloud. Third party auditor is considered to be better method as compared to all other methods. So we need to work more in this direction.

IV. References

[1] Amazon Web Services, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.

[2] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007.

[3] M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009.

[4] A.A. Yavuz and P. Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009. [5] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[6] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm), pp. 1-10, 2008.

[7] C.C. Erway, A. Kupcu C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security, pp. 213-222, 2009.

[8] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology Advances in Cryptology (ASIACRYPT '08), J. Pieprzyk, ed., pp. 90-107, 2008.

[9] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H.Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A Study of User-Friendly Hash Comparison Schemes," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114, 2009.

[10] A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.

[11] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 756-758, 2010.

[12] M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. 33rd Int'l Conf. Very Large Databases (VLDB), pp. 782-793, 2007.