Public Auditing for the Shared data in the Cloud

Meera Chheda
Final Year Computer Department, Pune University
Dr. D.Y. Patil College Of Engineering, India
meerachheda8@gmail.com

Anmol Achhra
Final Year Computer Department, Pune University
Dr. D.Y. Patil College Of Engineering, India
anmolachhra@gmail.com

Priyanka Vaswani3
Final Year Computer Department, Pune University
Dr. D.Y. Patil College Of Engineering, India
priyanka22vaswani@gmail.com

Rajeshwari Agale
Final Year Computer Department, Pune University
Dr. D.Y. Patil College Of Engineering, India
rajeshwariagale04@gmail.com

Vidya Bhise
Final Year Computer Department, Pune University
Dr. D.Y. Patil College Of Engineering, India
vidya7986@gmail.com

Abstract - With data storage and sharing services in the cloud, users can easily modify and share data. The main aim of this study is to check the integrity of the user in order to prevent data being attacked by unauthorized user. In this paper we propose method to eliminate the Third Party Auditor from cloud computing which mainly checks the integrity of user by ensuring whether the user is authorized or not. In this paper we include the new concept of dynamic encryption. In dynamic encryption the encryption algorithm type is decided dynamically depending upon the type of data as well as the size of data.

1. INTRODUCTION

The cloud computing is the concept of delivery of computing as a service rather than product, the computer resources, software and information shared instead of other devices.

In the idea of cloud computing the user of cloud outsources its data on to the cloud, and then the third party auditor is going to check authorization of that user to access the cloud [2]. In cloud if it is found that the unauthorized user is trying to access data of any other authorized user then the third party comes in picture, the third party comes in picture, the third party auditor gives the notification to the authorized user that some unauthorized user is trying to access its private data [5]. The concept of cloud computing represents a shift in thought, in that end users need not know the details of a specific technology. The service is fully managed by the provider. This on demand service can be provided at cloud service providers are making a substantial effort to secure their systems, in order to minimize the threats of insider attacks, and reinforce the confidence of customers. In the cloud scenario if third party auditor itself get hacked then the authorized will not receive any notification of unauthorized access of its data. So in the propose method the service will eliminates the third party auditor.

2. RELATED WORK

Cloud Computing could be defined as utilizing the internet to provide technology enabled services to people and organizations [1].The advantages for using cloud computing are Reducing capital expenditure, operational risk, complexity, maintenance and increase scalability. They propose diffie-hellman key exchange blended with advance encryption standard algorithm and digital signature but in future they faced the problem that if key in transmission is hacked then diffie-hellman key exchange is useless [4].

Traditional cryptographic technologies for data integrity and availability, based on hash functions and signatures schemes [7],[8],[9],cannot work on the outsourced data without a local copy of data. In addition , it is not a practical solution for data validation by downloading them due to the expensive communication especially for large size files. Moreover the ability to audit the correctness in a cloud

environment can be formidable and expensive for cloud users. Therefore it is crucial to realize public auditability for CSS, so that data owners may resort to a TPA who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics.

To implement public auditability, the notions of proof of retrievability (POR) [7] and PDP [9] have been proposed by some researches. These approaches were based on a probabilistic proof technique for a storage provider to proof that client's data remain intact. For ease of use, some POR/PDP schemes work on a publicly verifiable way, so that anyone can use the verification protocol to prove the availability of stored data. Hence, they help accommodate the requirements from public auditability. POR/PDP schemes evolved around an untrusted storage offer a publicly accessible remote interface to check the tremendous amount of data.

In this scheme an outsourced file is directly split into *n* blocks, and then each block generates a verification tag. Therefore, it is inefficient to build an audit system based on this scheme. To address such a problem, we introduce a fragment technique to improve system performance and reduce the extra storage.

Some researchers have suggested that user data stored on a Service-provider's equipment must be encrypted [11]. Encrypting data prior to storage is a common method of data protection, and service providers may be able to build firewalls to ensure that the decryption keys associated with encrypted user data are not disclosed to outsiders [12]. However, if the decryption key and the encrypted data are held by the same service provider, it raises the possibility that high-level administrators within the service provider would have access to both the decryption key and the encrypted data, thus presenting a risk for the unauthorized disclosure of the user data.

Existing methods for protecting data stored in cloud environment are user authentication, building secure channel for transmission of data. For this procedure they use various Cryptographic as well as Security based algorithm such as AES (Advance Encryption Standard), DES (Data Encryption Algorithm), Triple DES, RSA algorithm with digital signature [13].

Another major concern is the security issue of dynamic data operations for public auditing services. In clouds one of the core design principles is to provide dynamic scalability for various applications. This means that remotely stored data might be not accessed by the clients but also dynamically updated by them, for instance, through block operations such as modification, deletion and insertion. However , this operations may raise security issues in most of the existing schemes, example ,the forgery of the verification metadata generated by DOs and the leakage of the user secret key. Hence it is crucial to develop a more efficient and secure mechanism for dynamic audit services, in which a potential adversary's advantage through dynamic data operations should be prohibited.

In our proposed model some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

We propose a model which separates Encryption-Decryption service from the actual cloud storage. Because of this the data and decryption key will be at different storage area so the attacker will get either encrypted data or decryption key. This tends to provide extra level of security. In their proposed model the Encryption-Decryption service will only encrypt the data and this encrypted data is send to cloud storage and then original data is deleted from Encryption-Decryption service.

The algorithms used in existing systems are RC4, RC5, AES that resulted with many drawbacks. To overcome these drawbacks we are using RC6 for encryption and decryption and SPEKE for key generation.

3. EXISTING SYSTEM

In the existing system the main role of authentication of user is done by TPA, the TPA verifies the user whether it is valid user or not [3]. If the user is not authorized then the TPA notify to the user that his data is used by some unauthorized person. But if the TPA itself get hacked then the user will not get an notification mail from TPA. Authentication and verification is done at TPA level and not at admin level. In existing system, the clients store the data in server. That server is untrustworthy and after the third party auditor can audit the client files. Existing protocols can support both features (Data Dynamics and Public Verifiability) with the help of a third party auditor. Remote data integrity checking is a crucial technology in cloud computing.

In existing cloud system, there are no of threats occurred and they are as follow:

1) Abuse and Nefarious use of cloud.
2) Insecure Interfaces and APIs.
3) Malicious Insider.
4) Shared Technology Issues.
5) Data Loss and Leakage.
6) Account or Service Hijacking.

4. PROBLEM DEFINITION

Current working scenario involves paper based work for Data analysis and verification. Data Storage is one way to mitigate the privacy concern. Unauthorized users can leak or misuse the data, this problem still remains due to the paper based work**.** To overcome the disadvantages of the existing protocols, in this paper we are coming with a model of service which will replace TPA by Data Auditing service in the cloud scenario .

5. SYSTEM ARCHITECTURE

We adapt to support public verifiability, without help of a third party auditor. The protocol does not leak any private information to third party verifiers.

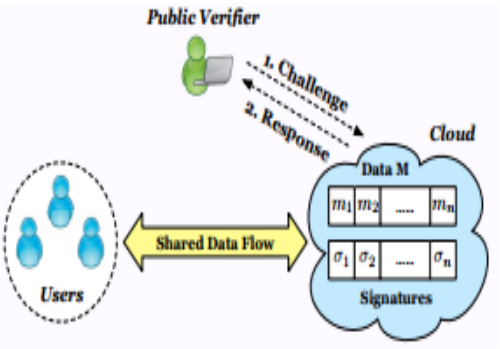

Figure 5.1.System Architecture

5.1. Service model:

We propose a service model in the following way:

Step 1: As emphasized [15], for security reasons, it is necessary for the cloud service providers to storage data and keys separately on different servers inside the cloud in practice. Therefore, in our mechanism, we assume the Encrypted data and key are stored separately on different storage media.

Step 2: Before decrypting the data the user have to enter OTP which is sent on his mail and combination of OTP, key and encrypted data are used to generate original data.

Step 3: For accessing the data the user is restricted in read only mode and for insert, modify and delete the notification is sent to admin.

Step 4: After encryption or decryption the original data is deleted from the Encryption and Decryption services.

Step 5: For securing the Account and Service Hijacking, we are replacing the TPA. The work of TPA will be done by data auditing service.

5.2. Data Auditing Mechanism:

1) Initialization - Data owner sends encrypted data and verification tags to server.
2) Challenge - Auditor sends Challenge to the cloud server.
3) Proof - Server responses with Proof.
4) Verification - Auditor verifies correctness of the Proof.

6. SUMMARY

In this paper, we examine the threats in cloud system and with our proposed service we are eliminating these threats. We presented our security solution for privacy- preserving cloud services. In addition, fair revocation process for all users. Users use secure devices during the authentication process. Use of data auditor prevents data leakage.

7. REFERENCES

[1] B. Wang, B. Li, and H. Li, "*Public Auditing for Shared Data with Efficient User Revoation in the Cloud*," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "*A View of Cloud Computing*," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "*Provable Data Possession at Untrusted Stores, in the Proceedings of ACM CCS 2007, 2007, pp*. 598–610.

[4] H. Shacham and B. Waters, "*Compact Proofs of Retrievability*," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "*Ensuring Data Storage Security in Cloud Computing*," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.
[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "*Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,*" in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "*Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing*," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.
[8] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "*Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds*," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.
[9] *C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.*
[10] "*A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability*": http://www.ieeexplore.org/A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability
[11] "*Business Model for Cloud Computing Based Separate Encryption and Decryption Service IEEE* ": http://www.ieeexplore.org/ business Model for Cloud Computing Based Separate Encryption and Decryption Service IEEE.
[12] "Privacy-Preserving Public Auditing for Secure Cloud Storage" http://www.ieeexplore.org/ Privacy-Preserving Public Auditing for Secure Cloud Storage.
[13] P. Mell, T. Grance ,"Draft NIST working definition of cloud computing", [Online]Available: http://www.csrc.nist. gov/groups/SNS/cloud-computing/index.html. [14] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz,A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica,M. Zaharia,"Above the clouds: A berkeley view of cloud computing", University of California, Berkeley, Tech. Rep.UCB-EECS-2009-28, Feb 2009.
[15] M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos, "*Hourglass schemes: how to prove that cloud*
files are encrypted," in the Proceedings of ACM CCS 2012, 2012, pp.265–280.
[16] X. Liu, Y. Zhang, B. Wang, and J. Yan, "*Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud*," IEEE Transactions on Parallel and Distributed Systems (TPDS), vol. 24,no. 6, pp. 1182–1191, 2013.