International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 8, August - 2014

A System of Privacy Preserving Public Auditing for Secure Cloud Storage System

Miss. Pratiksha Meshram
Student
Computer Science and Engineering
TGPCET
Nagpur, India

Prof. Roshani Talmale
Assistant Professor
Computer Science and Engineering
TGPCET
Nagpur, India

Prof. G. Rajesh babu
Assistant Professor
Computer Science and Engineering
TGPCET
Nagpur, India

***Abstract* — The Cloud computing is the internet based computing it enables sharing of services. It allows user to use application without installation of any application and user can access their personal files and application at any computer with internet or intranet access. In recent time number of user are using clouds for storing their data on cloud. It is beneficial for user because it allows user to store data and user can access it anytime and anywhere. Cloud computing is the technology for next generation information and software enabled work that is capable of changing software working environment. Cloud computing is the connection of nodes here nodes are computers connecting with each other for sharing information. The cloud is a platform where data owner remotely store their data in cloud storage. The main goal of cloud computing concept is to protect and secure the data which come under the property of users. The security of cloud computing environment is exclusive research area which requires further development from both research and academic communities. In the corporate world there are a huge number of cloud users which is storing data on cloud, accessing the data and modifying the data. In the cloud, services and application move to centralized huge data center and services and management of this data may not be trustworthy, into cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. As users are placing their data in cloud so correctness of data and security is the prime concern. Cloud data security is a major concern for the cloud user while using the cloud services provided by the service provider. To ensure correctness of data here we propose the task of allowing a third party auditor. On behalf of cloud user request to verify the integrity of data stored in the cloud is done by TPA .The advantage of TPA is that there is no additional online burden to user.In this paper we propose a secure cloud storage system supporting a privacy preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently with AES and BLOWFISH Encryption Algorithm. This shows the proposed scheme is highly efficient and data modification attack, and even server colluding attacks. Resulted encrypted method is secure and easy to use.**

Keywords— Cloud computing, privacy-preserving public auditing, Data integrity, Third Party Auditor (TPA).

1. INTRODUCTION

The evolution of computers made the life of people easier. They were using computers for storing data. They started to find ways to make the data accessible to other. By using floppy, writable disks data transferred from one computer to another computer. But all these devices were expensive during their time. The data is very much private on personal devices like PC, laptops, mobile phones etc .Hence to share data with other was considered to be expensive. As computing become more advanced the devices become cheaper. In recent years a new term evolved call"cloud"which is provided by different provider. It is latest efforts in delivering computing resources. It is gaining popularity in the IT industry. Cloud is nothing but facility or service of different components like storage software, platform, and hardware etc.It is gaining importance because user will be free from maintenance perspective on an investment of some money for the use of these services provided by cloud service providers.

As such services provided by cloud service provider to cloud user, naturally the providers must have and rather can have access to resources which are used by the user. Among the reasons these access are greatly required are for maintenance perspective. As numbers of users are using such service provided by cloud service provider then the infrastructure ought to capable enough to support them and these resources ought to be shared between numbers of users. Data synchronization between number of users, service availability, and availability of data via any devices which includes browser facility make cloud more attractive. Since the info gets shared or stored in provider's area, the user gets worried about privacy of its data, though there are certain agreements and SLA which are agreed by both cloud provider and cloud user. Although user have a platform to generally share the information or store the information ,the expense of securing his/her data or in a nutshell making its data private gets costlier. The cloud term is useful not only for the single user but also for organization. With organization as a consumer the concern of data security becomes multifold. Consider the example of a small scale business that has different departments for example HR/Finance etc.We will focus on Finance department because finance details of any company or organization is

considered to be more sensitive and must be confidential. Therefore if small scale company thinks of using the cloud services like storage. Storing all finance related information in cloud storage makes it prone to leakage of sensitive information by unauthorized users. Therefore securing this information is important before it gets uploaded to the cloud storage and just in case the data stored in cloud storage gets tempered there should be a method required to verify the integrity of the data stored in cloud. Simply speaking the user must have the ability to store the data securely, verify the integrity of the data stored in cloud.

2. OBJECTIVES

Our objective is as follows:

1) To construct the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., in our scheme an external auditor audit users outsourced data in the cloud without learning knowledge on the data content.
2) To construct the user application which would encrypt the users data before uploading data on cloud and decrypting data while after downloading from cloud.

Our scheme supports scalable and efficient public auditing in cloud computing .The TPA will be able properly audit integrity of the data.

3. SYSTEM ARCHITECTURE

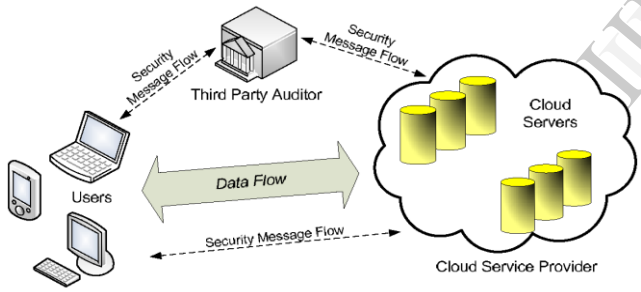

Fig. 1: The architecture of cloud data storage service

4. EXISTING SYSTEM

The cloud data storage service consists of three different entities.

Cloud user (U): who has large amount of data files to be stored in the cloud.

Cloud server (CS): It is place where cloud user stores data which is managed by cloud service provider (CSP) .

Third party auditor (TPA): who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Here cloud service provider is different administrative entity. User losses control over data after storing data on untrusted server. Though infrastructure of cloud storage is more powerful than the personal computer, they are still facing problem of internal attack and external attack. Sometime cloud service provider hides the data corruption so it is important to check data integrity regularly.

Disadvantages of existing system:

1) Cloud storage system provides storage to store important data .But it does not give any guarantee about data security. Because users data are not encrypted on some open source cloud storage systems. Therefore the cloud service providers can easily access the user file. Here privacy is not preserved.

2) TPA demands retrieval of user data, for its integrity verification. Downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. And because of downloading all data it does not support data privacy.

5. PROPOSED SYSTEM

The main goal of proposed system is to provide more security to user's data stored in cloud i.e. provide Confidentiality, integrity, and availability of data stored on cloud. As user's data stored on cloud, Users have to perform storage correctness checks whether his data is as it is or not. In our scheme TPA who has expertise and capabilities will periodically check the integrity of data stored on cloud on behalf of user request.

To enable privacy-preserving public auditing for cloud data storage, our protocol design should achieve the following security and performance guarantees. Public audit ability allows TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. Storage correctness to ensure that user's data is intact on cloud. Privacy-preserving to ensure that the TPA cannot derive users sensitive data from the information collected during the auditing process. Here we provide a scheme which checks data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. It is important to note that in our proposed system proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

In our proposed system user will first encrypt data and then that encrypted data will store on cloud. For encrypting data we are using Hybrid algorithm. Hybrid algorithm is consist of two algorithms AES and BLOWFISH.As these are powerful algorithm hence it provide more security to users data. User files are encrypted in cloud storage hence confidentiality of data is maintained and user's data privacy is preserved in cloud storage system. For storage correctness we need to check integrity of data periodically. Hence we are using SHA-1 algorithm for checking integrity of data. In the proposed design there is encryption/decryption is done by user itself and a hash service data integrity verification is provided by third party auditor. In the proposed system the encryption/decryption will be done by user itself and hashing of data is done by the Third party auditor. The system provides the data storage for each client is done in the databases .The security is provided to data by encryption/decryption process on client side. The third party auditor which is used for computing hash of data store only hash of data along with it. The encrypted data is kept in cloud

storage. The division of responsibility has big effect as there is no burden on single user because hashing is done by the third party auditor.

Advantages of proposed system:

1) We are providing security to user's data storing on cloud by encrypting it with hybrid algorithm. Hence it is protected from any unauthorized access or modification.

2) We provide a privacy-preserving auditing protocol for Security of data in Cloud storage. Our scheme enables an external auditor to audit user's cloud data without learning the data content. There exists no way for TPA to derive users' data content from the information collected during the auditing process. Therefore data privacy is preserved against Third party auditor.

3) As auditing is done by TPA there is no burden on user about integrity verification.

Algorithm Selection

In this section we discuss some of the advantages of selection of particular algorithms.

1 Selection of AES

Broadly speaking the encryption/decryption can be done via symmetric key or asymmetric key. In symmetric algorithms, both parties share the secret key for both encryption/decryption, and from privacy perceptive it is important that this key is not compromised, because cascading data will then be compromised. Symmetric encryption/decryption requires less power for computation. On the other hand asymmetric algorithms use pairs of keys, of which one key is used for encryption while other key is used for decryption. Generally the private key is kept secret and generally held with the owner of data or trusted 3rd party for the data, while the public key can be distributed to others for

Encryption. The secret key can't be obtained from the public key. In our case since the encryption/decryption is performed on user side, symmetric key is used.

2 Selection of Blowfish

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher. It is suitable for applications where the Key does not change often, like a communications link or an automatic file encryptor.

3 Selection of SHA-1

A hash function maps the variable length input to fixed length output. By comparing the hash values for two inputs we can get two answers. First two inputs are not same or second two outputs are definitely same. Hashing is used for authentication, integrity checking, performance improvement, error checking, and encryption. In our paper we are using SHA-1 Algorithm for performing hashing task.SHA stands for "Secure Hash Algorithm". It is a hashing algorithm designed by the United States National Security Agency .again it is published by NIST.It is a cryptographic hash function technique where hash of data is computed. As compared to SHA-0, SHA-1 is widely used because it corrects errors in SHA hash specification, which led to weakness. SHA-1is used to hash a message, M, having a length of l bits, the algorithm use first message schedule of eighty 32-bit words, second five working variables of 32 bits each, and a hash value of five 32-bit words. The final result of SHA-1 is a 160 bit message digests**.**

6. WORKING METHODOLOGY

System Architecture Preserving Storage Data on Cloud using AES, Blowfish, SHA-1 Algorithm.

1. In our proposed methodology user store data to cloud. At the time of sending data to cloud it get encrypted by cryptographic algorithms.
2. That encrypted data transfer to the TPA.
3. TPA generates hash of that encrypted data.
4. That generated hash is stored along with TPA.
5. Then that encrypted data TPA will send to cloud.
6. When user wants to check integrity of data then user will send request to the TPA.
7. TPA forward that request to the cloud.
8. Cloud will generate the hash of requested file and send that generated hash to the TPA.
9. TPA fetches stored hash of that requested file and performs comparison in newly generated hash and stored hash.
10. If both the hash are equal then TPA transfer acknowledgement to the user. If both are equal then acknowledgement will be that stored data is as it is. If data get corrupted by cloud then acknowledgement will be that your data is corrupted.
11. Similarly, when user want to download data from cloud then user send request to the TPA to download data from cloud.TPA will transfer request to the cloud. Cloud accepts that request and send data to the user.

7. ENSURING DATA SECURITY WITH ENCRYPTION AND AUDITING

Figure 2:To upload file on cloud

User has to browse the file and click on Update. user have to select file and click on update after clicking on update button user have to fill details regarding that file .Then that file get encrypted on user machine then that file first get transfer to TPA .then on TPA machine there is generation of hash of users encrypted data.TPA store that hash of encrypted

data on its machine and that encrypted file get transfer to cloud storage.

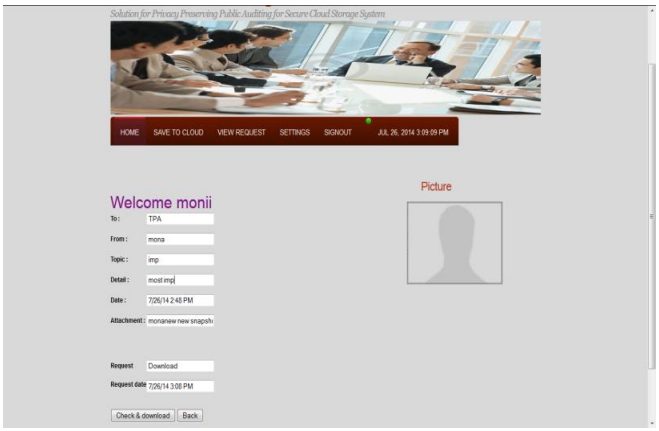

Figure 3: Viewed request send by one user to TPA

When TPA click on one of file then there display file along with all the details of that file. As shown in figure TPA view request of one of user Mona to check download of file. When TPA view request of the user then there two types of request can be send by user to TPA.one request is of checking integrity of stored data on cloud and another request is of downloading file from cloud storage. when there is request of downloading file from cloud storage then that request get transfer directly to the cloud storage and then CSP will transfer that requested file to the TPA. And from TPA to user. When user request to TPA for checking integrity of file then there TPA will check the integrity.TPA will receive request of check the integrity and forward it to CSP.Now CSP will generate the hash of stored data and transfer it to TPA.Now TPA will compare the new hash and old hash of file and then if both the hash are equal then TPA send acknowledgement to the user that users file is secured on cloud storage.

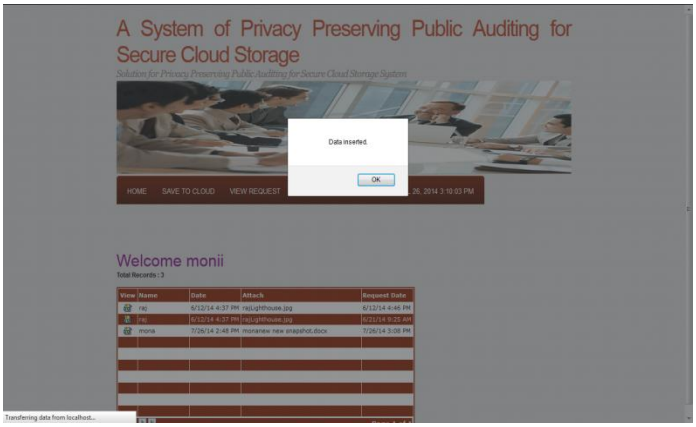

Figure 4: Request forward by TPA

When TPA click on Check & download then that request forward by TPA to CSP.TPA login to the system. After authentication that TPA can use his/her account. When user send data to cloud then that data get transfer to TPA.TPA then click on “save to cloud”. When TPA click on “save to cloud “then the hash get computed of that particular file and that data file transfer to cloud.TPA application is used for computation of hash of file which is transferred by user, Then that TPA generated hash will be saved by TPA itself and that encrypted file is transferred to cloud. When TPA click on “view request “then there display all users request. Then that request transfer by TPA to cloud. If the request is of download then it will get transfer to cloud. Cloud accepts that request and sends that requested file to user. If the request is of checking integrity then it transfers by TPA to cloud. Cloud then generates Hash of requested file and transfer to TPA.Then TPA will compare both the new and old hash and send acknowledgement to user.

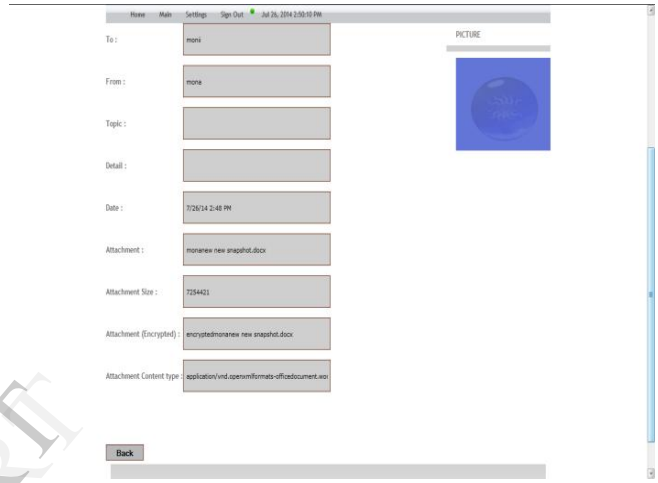

Figure 5: Data file viewed by CSP

It is showing data of stored file of one of cloud user. The working of cloud is to store data. It is managed by CSP.When user upload data on cloud then CSP receives it and then it stored in cloud. When there is request send by TPA to check integrity of particular file of one of cloud user. Then CSP generate hash of that file and forward that hash to the TPA.When user wants to download file then user send that request to the TPA .TPA forward that request to cloud then cloud transfer that file to user.

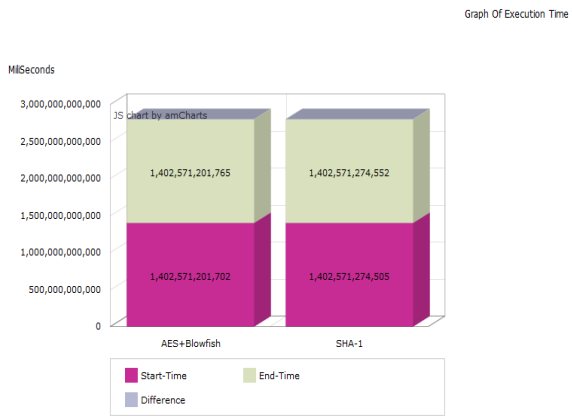

Figure 6: Execution time required for each algorithm

This is the execution time required for algorithm while performing encryption and generating hash. It is stored along with admin.It will generate the time required for encryption /decryption of each file in millisecond. Again it will calculate time for generation of hash of encrypted file. This chart saved along with Admin.

8. ENCRYPTED FILE STORED ON CLOUD

Let's use now discuss the example of data upload on cloud. The file is exactly stored in encrypted format. Figure shows the encrypted file which was stored by a user.

Figure 7: Encrypted file stored cloud

The above figure showing users file stored on cloud is in encrypted format. Secondly the hash of data is stored along with TPA.

9. CONCLUSION

A system of privacy preserving public auditing provides security to data stored in cloud storage. The cloud storage is advantageous than earlier traditional storage system. In cloud storage requirement is to provide security to data stored on cloud. Our system uses encryption of data before storing it on cloud. Therefore data will be secured on cloud storage. The cloud user can check integrity of their data stored on cloud server using TPA.TPA will immediately intimate to the client of file and so security and data integrity is secured properly.TPA would not learn any knowledge about the data content stored on the cloud server during auditing which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task but also alleviates the users fear of their outsourced data leakage. Cloud data security is an important aspect for the cloud user while using cloud services.TPA is used to ensure security and integrity of data stored on cloud. As user is encrypting data before storing it on cloud server, it ensures that it cannot be accessed by any unauthorized user. The task of allowing a third party auditor ,on behalf of the cloud user to verify integrity of the data stored in the cloud relief user from burden of auditing task resulted method is secure .

REFERENCES

[1]CongWang; Chow,S.S.M.; QianWang; KuiRen ;WenjingLou "Privacy preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers 2013.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[3] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Proc. ACM Workshop Cloud Computing Security ,2009.

[4] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents,"Cryptology ePrint Archive, Report 2008/186, 2008.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Theory and Application of Cryptology and Information Security: Advances in Cryptology Dec. 2008.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[7] XU Chun-xiang, HE Xiao-hu, Daniel Abraha, "Cryptanalysis of auditing protocol proposed by Wang et al. for data storage security in cloud computing", http://eprint.iacr.org/2012/115.pdf,and cryptologyeprintarchieve: Listing for 2012 .

[8] Z.Hao,S.Zhong and N.Yu,"A Privacy Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability",IEEE transaction Knowledge and Data Engineering,2011.

[9] Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A.Deshmukh, "Investigation of TPA (Third Party AuditorRole) for Cloud Data Security", International Journal of Scientific and Engineering Research, vo. 4,no. 2,ISSn 2229-5518, Feb 2013.

[10] B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 6602 3127,2011.

11. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009.

[12] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[13] William Stallings, "Cryptography and Network Security", 2009.

[14] IK.Meenakshi, IIVicto Sudha George IStudent (M.Tech), "Cloud Server Storage Security Using TPA"International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014).

[15] Ranchal, R., B. Bhargava, L. Ben and L. Lilien "Protection of identity information in cloud computing without trusted third party" Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems, Oct. 31 Nov. -03, IEEE Xplore Press, Indian, pp: 368-372. DOI: 10.1109/SRDS.2010.57.

[16] Hao, Z., Zhong, S., & Yu, N. "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability" Knowledge and Data Engineering, IEEE Transactions on, 2011.

[17] Gohel, M., & Gohil, B "A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage" 2012.

[18] Jayalatchumy, D., Ramkumar, P., & Kadhirvelu, D."Preserving Privacy through Data Control in a Cloud Computing Architecture Using Discretion Algorithm" In Emerging Trends in Engineering and Technology (ICETET), November 2010, pp. 456-461 .

[19] Yang, K., & Jia, X. "Data storage auditing service in cloud computing: challenges, methods and opportunities". World Wide Web, 15(4), 2012,409-428.

[20] A. Kupcu ,C. Erway, , C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS'09. Chicago, IL, USA: ACM, 2009.