RESEARCH ARTICLE OPEN ACCESS

Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud

Ms. Priya Kharmate, Prof. Ranjeetsingh Suryawanshi
Department of Computer engineering
Trinity College of Engineering and Research, Pune
Maharashtra – India

ABSTRACT

The cloud security is one of the important role in cloud, here we can preserve our data into cloud storage. The security issues are the major thing in cloud but Cloud service is necessary. Here we can overcome the security issues in our project. In existing they are using a remote verification technique to audit by the third party or private auditing. In this technique the data owners need to be online to manage that auditing. In our system we are using the own auditing based on the token generation. Using this token generation technique compare the token values from original tokens we can find out the changes about the file. Users can login into their account then they upload our files. The files will be stored into the cloud storage. In our system we provide the two tier security for our uploaded files. The files does not stored directly it will be converted into the files, it will be stored into three different cloud server locations. The original file content split into three parts and it will be store into each files. Not only stored also the content will be encrypted in the cloud server. If anyone try to hack at the cloud end is not possible to break the two tier block. They need first decrypt the files and also combine the splited files from three different locations. This is not possible by anyone. Anyone can download the files from the server with file owner permission. At the time of download key generated (code based key generation) and it will send to the file owner. We can download the file need to use the key for verification and some other users want to download file owner permission is necessary.

Keywords: - Cloud storage, public audit, privacy preserving, Data integrity, Third Party Auditor (TPA).

I. INTRODUCTION

The development of cloud computing environment [1] is encouraging many organizations to migrate their IT infrastructure to function completely or partially in the cloud. Also computing has changed itself from being a product to a service that can be delivered to the consumers over internet through large scale data centres.

In cloud storage the prime burden is data privacy resulting some hesitation in the mind of individual or enterprisers. This burden can minimized by enabling public auditability for cloud storage so that users have alternative to check the integrity of outsourced data through third party auditor (TPA). Third Party Auditor is kind of examiner. There are two categories for auditing data stored on cloud server: private auditability and public auditability. While private auditability can achieve higher scheme efficiency, public auditability allows everyone, not just the client, to verify the cloud server for the correctness of data storage without demanding the local copy of data and resulting into minimize communication and computation overhead as compared to the traditional data auditing approaches. [2]

Therefore to ensure the data security and to save the user's computation resource, it is of critical importance to enable public auditability for cloud data storage so that user may resort to Third party auditor (TPA) and based on audit report which could help users to evaluate the risk of their subscribed cloud data service.

Also the economies of scale in auditing Cloud data can be achieved by eliminating the direct involvement of the client. The user can determine the risk involved in storing his data on cloud server after examining the audit report, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will facilitate data owner to make sure that his data are secure in the cloud and management of data will be easy to data owner.

II. LITERATURE REVIEW

The concept of remote data checking to ensure data integrity was introduced in [3] [4] Further it gave rise to the frameworks like provable data possession (PDP), proof of retrievability (POR), by Ateniese et al. [5] and Juels et al. [6] which are used by TPA for ensuring possession of data files on untrusted storages. Also each of these frameworks meets user needs and give examples associated with some of these techniques which are usable. Then this paper also mentions some issues in other research in this domain, based on the survey conduct. At the end, paper concludes a promising future of this area of research by M.S.Shashidhara.[9]

The creator Reza Curtmola and Osama Khan they shows that Using MR-PDP to store t replicas is computationally much more efficient than using a single-replica PDP scheme to store t separate, unrelated files (e.g., by encrypting each file separately prior to storing it). Another advantage of MR-PDP is that it can generate further replicas on demand, at little expense, when some of the existing replicas fail.[10]

The public auditability, scheme reveals the linear combination of sampled blocks exposed to external auditor. ZHANG Wei describe a new method, called the bit split–bit combination data privacy protection program [7], for the privacy protection of data that does not depend on the performance of encryption keys. In this method, the original data are broken up through BS and uploaded to multiple cloud storages after the completion of the split to achieve data privacy protection for users. When users want to access the original data, they can download the split data from the different cloud storages and access the data after the appropriate BC process is completed. The use of the BSBC [7] data privacy protection technology can protect the privacy of user data without the management of encryption keys and can significantly shorten the time required for data privacy protection.

In a subsequent work, M.S.Shashidhara propose methods related to the security and privacy capabilities in cloud paradigm especially data storage in multi cloud environment. [9]

In multi cloud architectures different methods include, resource replication, split application system [7] into tiers based on PIR methods, split both application logic and data into segments which allows categorizing the schemes and analyze them according to their security benefits.

Further Alexandru Butoi proposed the protocol based on a secret sharing scheme in which data is split in optimal chunks, each chunk carrying a minimum informational content relative to the entire informational content of the data set. The file chunks are stored in multiple cloud storage volumes in a way that minimizes the probability for an insider or an attacker to reconstruct the original data set.[12]

All the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, however none of them meet all the requirements for privacy preserving public auditing in cloud computing. The Data robustness and respectability is a main factor for storage systems. In absence of personality protection, where the clients are unaware with inspector of the information over globally scattered datacentres. To resolve this concern identified with clients character, information respectability and clients accessibility [15] the improved model is proposed with the features like correctness, efficient user revocation and public auditing which reviews the information trustworthiness of shared information and preserve security with clients repudiation.

III. EXISTING SYSTEM

To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Here third party public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model. Moreover, we design a novel public verifiable authenticator [9], which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code- based cloud storage.

Disadvantage of Existing System:

a. The cryptographic techniques for the purpose of data security protection cannot be directly user's control.
b. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.
c. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.
d. This is not just a third party data warehouse. The data stored in the cloud may be often updated by the users.

IV. PROPOSED SYSTEM

We propose the system with an effective and flexible distributed scheme with data in the cloud. Here we are using the erasure code technique for distribute the data to cloud locations and access the data from cloud. User can register and login into their account. They have a option to store, share and access the data from cloud storage. Here we are using the two tier security scheme for storing data into the cloud. The first tier security is your data or file splited into multiple parts and it will store into different cloud server locations. Each and every file generates the token for auditing. Then second tier security is each and every splited file will encrypt before store into different locations. The shared users can edit the file in the cloud with file owner's permission. That file eligible of own public auditing. Then user can have to login and access the own files or some other files. User first can search and download the files, at the time of download user should use the security key. If authentication success it will be decrypt and combine to get the original data from cloud.

The cloud data storage service involving three different entities, as illustrated in the cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage To fully ensure the data integrity and save the cloud users computation resources as well as online burden, it is of critical importance to enable public Auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and even serve for independent arbitration purposes. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud.

V. SYSTEM ARCHITECTURE

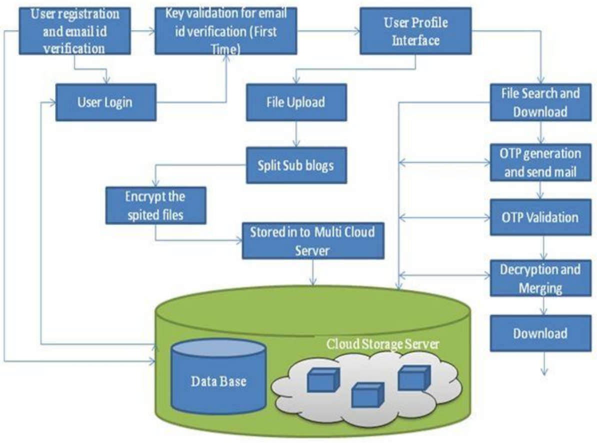

Fig.1: System Architecture Design

In this Application we need to register the Registration form and if valid user, we can able to enter our application. Here, user profile having two different interfaces. One is File upload and another one is File download. if user upload the files, the file automatically, splitted into three parts and it will be stored encrypted format in three different locations. Here AES algorithm used for file encryption. After completing this process, if user want to download a file, that time also user need to login our application. If valid user, they have privilege to access our application. Now file will be searching, entered file name available in server means, it will go for download page. You're going to click download button, our application required the secret key for download the file. Without secret key we can't able to download. The secret key will be automatically generated and send to the corresponding file owner mail id. If owner share the key to user, that user can able to download file. Our file stored in encrypted format, it will be decrypted using AES algorithm while user entered secret key thenafter that file will be downloaded. Normally, no one can access the server, if hacker hack our file means, he didn't get a full original file. Because it's split & stored in different locations. In this system having token generation, in the sense, some user downloads the file, he edited the original content means, easily we can find out.

VI. MODULE DESCRIPTION

1. User interface:

In our Secure System we have a user friendly user interface to interact with our System. Every Act dual role as a data owner and data consumer while uploading file they are the owner of that file if they search other's file than they are the consumer.

Users can create the account them self for that we have new pages, in that page we will get the details from the user and we generate the account for the user's. We have authentication system; we only allow authorized users to access our System.

In our System we providing the easy file searching user's don't want to keep remember all uploaded file's exact name, for that we have given the keywords while uploading the files it will help to search the file easily.

2. Secret key generation:

Firstly the secret key will be generated as the initial step while uploading the file, every which is uploaded, will have unique secret key. This key will be taken as an identification of every file. The secret key which we are using is a three digit number we will make it use for both uploading and downloading. If the user want download some file and if he gives the download request the secret key of that file will be sent to the file owner of the file maybe he can share it.

3. File uploading process:

To provide data robustness while storing data over storage servers one way is to replicate a message such that each storage server stores a message. The other way is to encode a message of k symbols into a code word of n symbols by erasure coding. Each of its single word symbols is stored in a different storage server. A storage servers to a secure code error of the word symbol. As long as the number of servers is under the tolerance static value of the code, the message can easily recovered from the code word symbols stored in the available storage servers by the decoding process.

4. Mail alert process:

The uploading and downloading process of the user is first get the secret key in the corresponding user email id and then apply the secret key to encrypted data to send the server storage and decrypts it by using his secret key to download the corresponding data file in the server storage system's the secret key conversion using the Share KeyGen (SKA, t, m). it's distribute the the secret key of a user to a set of key servers.

5. File Downloading process:

File downloading process is to get the corresponding secret key to the corresponding file to the user mail id and then decrypt the file data. The file downloading process re-encryption key to storage servers such that storage servers perform the re-Encryption Operation. The length of forwarded message and the computation of re-encryption is taken care of by storage servers. Proxy re-encryption methods alternatively reduce the overhead of the data forwarding function in a secure storage system.

VII. CONCLUSION

In this paper, we propose an privacy-preserving public auditing scheme for data storage security in cloud computing. We exploit the homomorphic linear authenticator and accidental masking to agreement that the TPA would not learn any familiarity about the data satisfied stored on the cloud wine waiter during the able auditing process, 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 outflow. Considering TPA may alongside handle many audit sessions from diverse users for their outsourced data files.

ACKNOWLEDMENT

We would like to thank IJCST for giving such wonderful platform for the PG students to publish their research work. Also would like to thanks to our guide & respected teachers for their constant support and motivation for us. Our sincere thanks to TRINITY COLLEGE OF ENGINEERING AND RESEARCH, PUNE for providing a strong platform to develop our skill and capabilities.

REFERENCES

[1] 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," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010

[2] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf.Cloud Computing, pp. 295-302, 2012

[3] Y. Deswarte, J.-J. Quisquater, and A. Sa¨ıdane, “Remote integrity checking,” in Integrity and Internal Control in Information Systems VI.Springer, 2004, pp. 1–11.

[4] D. L. Gazzoni Filho and P. S. L. M. Barreto, “Demonstrating data possession and uncheatable data transfer.” IACR Cryptology ePrint Archive, vol. 2006, p. 150, 2006.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedingsof the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07. New York, NY, USA: ACM, 2007, pp. 598–609.

[6] Juels and B. S. Kaliski Jr, “Pors: Proofs of retrievability for large files,” in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[7] ZHANG Wei and SUN Xinwei, “Data Privacy Protection Using Multiple Cloud Storages”. International Conference on Mechatronic Sciences, Electrical Engineering and Computer (MEC) Dec 20-22, 2013 pp 1768 - 1772.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010.

[9] M.S.Shashidhara and Jaini.C.P, “Privacy Preserving Third Party Auditing In Multi Cloud Storage Environment” Proc.IEEE Conf. Conference on Cloud Computing for Emerging Markets 2014 (CCEM ’14), pp. 90-99, 2014.

[10] Reza Curtmola and Osama Khan, “ MR – PDP : Multiple-Replica Provable Data Possession,” Comm. ACM, vol. 14, no. 1, 2011.

[11] 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. 598-610, 2007.

[12] Alexandru Butoi, Nicolae Tomai, “Secret sharing scheme for data confidentiality preserving in a public-private hybrid cloud storage approach,” Proc. ACM 7th International Conference on Utility and Cloud Computing (UCC’14), pp: 992-997, 2014.

[13] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,” Proc. 14th European Conf. Research in Computer Security (ESORICS’09), pp. 355-370, 2009.

[14] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS’09), pp. 1-9, 2009.

[15] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote Data Checking for Network Coding-Based Distributed Storage Systems,” Proc. ACM Workshop Cloud Computing Security Workshop (CCSW’10), pp. 31-42, 2010.