IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 1, Feb - March, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Two Tier Security Scheme For Store Share And Audit Our Data Into Cloud

M.Pavithra[1], D.Sivaranjani[2], Mr.B.Ravikumar[3]

[1,2]B.E IV Year CSE Dept,GKM College of Engineering & Technology, Chennai,Tamilnadu,India.

[3]Assistant Professor- CSE Dept,GKM College of Engineering & Technology, Chennai,Tamilnadu,India.

ABSTRACT
The important role in cloud is cloud security, here we overcome security issues in our project. In our system we are using own auditing based on token generation. The token values are compared with original tokens to find out changes about the file. Users can login into their account then they upload their files. The files will be stored into the cloud storage with two tier security . The original file content split into three parts and it will be stored into three different cloud server locations, after getting encrypted. Now hacking is not possible against two tier block. They need first to decrypt the files and combine the splitted files.we can download files from the server with file owner permission. At the time of downloading, key generated will be sending to file owner. After getting key from file owner, we can download file with verification process.

Keywords: *Two tier security, Token generation, cloud server, file owner permission.*

1 INTRODUCTION

Cloud computing is a technology that provides the best service for storage. Cloud storage allows the user to move data from their local systems to the Cloud.The cloud which contains data is seen as valuable to few people with malicious target. cloud storage is easy to come by different services with a free space to just for signing up but those services are looking at the files upload and most importantly with services encrypt personal data. Although security in the cloud is generally good,the hacker's don't have definite target that they can attack there still are some serious security concerns.for instance,the interconnectedness of server in the cloud may lead to a situation in which hacker breaches one system and they can make their own way into other linked systems.

This paper is mainly concentrates on the security issues. Here we are using the own auditing with the help of token generation. Using this token generation technique , we can find out the changes about the file by comparing the token values. Users can login into their account and get secret key from key server to upload their files. Then the files will be stored into the cloud storage. we provide the two tier security for uploaded files. The original file can be stored into three different cloud server location ,by splitting into three parts with encryption.In cloud server tokens can be generated for each splitted file and it can be stored into database. If someone try to hack at the cloud server is impossible to break the two tier block. They need first decrypt the files and also combine the splitted files from three different locations. This is not possible by anyone.User which have access privilege from file owner can able to view the file. At the time of download randomly key generated (code based key generation) will send to the file owner. User can download and update the file by using randomly generated key from the file owner.After auditing the files with tokens,an alert message will be send to the file owner,to upload the files into cloud.

1.1 Two Tier Security

A Two Tier security technique is an interface runs on a client and datastructure gets stored on a server .Separating these components into different location represent a two tier security scheme.

1.2 Token Generation

Token Generation allows for secure transmision of files which can stored in cloud.whenever the changes are made in the files,tokens are compared with the original token and an alert message is send to file owner.

1.3 Cloud Server

A Cloud server is a logical server that is built ,hosted and delivered through a cloud computing platform over the internet.Cloud server possess and exhibit similar capabilities and functionality to a typical server but are accessed remotely from a cloud service provider.

1.4 File Owner Permission

The user gets access priviledge to view the file from file owner.And also User needs permission to update and download a file.

2 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, 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.

2.1 Algorithm

The data owner maintains this procedure to initialize the auditing scheme.

KeyGen(1 κ) → (pk, sk): This polynomial-time algorithm is run by the data owner to initialize its public and secret parameters by taking a security parameter κ as input.

Degelation(sk) → (x): This algorithm represents the interaction between the data owner and proxy. The data owner delivers partial secret key x to the proxy through a secure approach.

SigAndBlockGen(sk, F) → (,, t): This polynomial time algorithm is run by the data owner and takes the secret parameter sk and the original file F as input, and then outputs a coded block set , an authenticator set and a file tag t.

2.2 Disadvantages

1 The cryptographic techniques for the purpose of data security protection cannot be directly user's control.

2 Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.

3 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.

4 This is not just a third party data warehouse. The data stored in the cloud may be often updated by the users.

3 MODULE DESCRIPTION FOR PROPOSED SYSTEM

3.1 User Interface

At any time user can use them.For example , the email service is the most popular one. Cloud Computing is a concept that treats the resources as a unified entity on the internet.Users just use services without being concerned about how computation is done and storage is managed.In this paper, we focus on designing for robustness,confidentiality, and functionality in a cloud storage system.A cloud storage system is considered entry level creation for user interface in this module.

3.2 Secret Key Generation

The data forwarding phase, user forwards his encrypted message with an identifier ID stored in storage servers to user such that can decrypt the forwarded message by using his secret key. the secret keys of target users, and the shared keys stored in key servers.

3.3 File Uploading Process

Storing data over storage servers ,one way to provide data robustness is to replicate a message such that each storage server stores a message.The other way is by erasure coding to encode a message of k symbols into a codeword of n symbols .Storing of these codeword is takes place in a different storage server. A storage server corresponds to an erasure error of the codeword symbol.As long as the number of servers is under the tolerance threshold of the erasure code,the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process.

3.4 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 Key Gen(SKA, t, m). This algorithm shares the secret key SKA of a user to a set of key servers.

3.5 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. In a secure storage system ,Proxy re-encryption Schemes reduce the overhead of the data Forwarding function significantly .

4 SYSTEM ARCHITECTURE

In this Application we need to register the Registration form and if valid user, we can able to enter our application. Here, user profile consists of 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 for file encryption ,AES algorithm is used . 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.

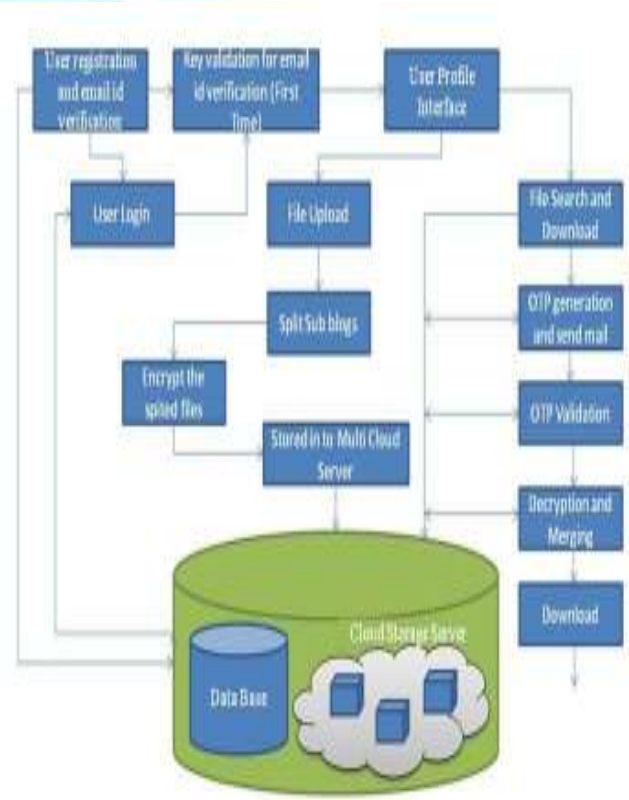

Fig.1: System Architecture Design

5 SECURE ERASURE CODE ALGORITHM

1 Storing data in a third party's cloud system causes serious concern over data confidentiality.

2 Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.

3 A threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated.

4 The distributed storage system not only supports secure and robust data storage and retrieval, but also without retrieving the data back ,lets a user forward his data in the storage servers to another user .

5 The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages.

6 It's stored the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server.

6 ADVANTAGES

1 Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.

2 Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.

3 Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

7 CONCLUSION

In this paper, we have implemented the privacy preserving public auditing for data storage security in cloud computing. We have overcome third party auditor for auditing purposes. Here we store , share and audit our data into cloud in an efficient manner. So data leakage can be avoided from it. We have used secure erasure code algorithm for own auditing, it provides more security to the outsourced data.

ACKNOWLEDMENT

We would like to thank IJREAT for giving such wonderful platform for the UG students to publish their paper. Also would like to thanks to our Professor Mr.B.Ravikumar for his constant support and motivation for us. Our sincere thanks to GKM COLLEGE OF ENGINEERING AND TECHNOLOGY,CHENNAI for providing a strong platform to develop our skill and capabilities.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian ,Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage
Information Forensics and Security, IEEE Transactions on (Volume:10 , Issue: 7)

[2] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee,D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences,University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.

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

[4] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009,pp. 187–198.

[5] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010, pp. 31–42.

[6] Syam Kumar P, Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing," in International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[7] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage," Computers & Electrical Engineering, 2013.

[8] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 43–54.

[9] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in Theory of Cryptography. Springer, 2009, pp. 109–127