ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Review Article*
www.ijptonline.com

A METHODICAL STORAGE SECURITY DESIGN WITH SELF AUDITING IN CLOUD

[1*]Pritam Debnath,[2] S.Jagadeesan
[1]PG student, CSE department, SRM University, Kattankulathur.
[2]Assistant Professor, CSE department, SRM University, Kattankulathur.
Email:pritamvtu@gmail.com

Received on 18-01-2017 *Accepted on: 12-03-2017*

Abstract:

To have a cloud which provides secured data storage is really a tough task and a big challenge. Nowadays number of cloud users have increased, all want their data which is stored is cloud to be secured. So the cloud security has become a major challenge in this modern era. When we focus we find out that overall completeness, accuracy and consistency of the data are the huge area of concern in having secured cloud storage. So in our system we proposed a self auditing scheme, using which the users himself can audit his data which is stored in cloud. A token 1 will be generated once the file owner upload files to cloud, once the file is shared by owner and gets edited by the shared users token two will be generated. This token 2 will equate with the token 1, if there is a mismatch, a notification will be sent to the file owner asking for its approval. Once approved by file owner the data will be stored permanently in the cloud. For storing the data in cloud we use double tier security process, using which the file uploaded is splitted into different parts and gets encrypted before it gets stored in different server location. While downloading, the file gets decrypted and a secret key is generated and send to file owners. With the file owner consent which is using the secret key the file can be downloaded.

Keywords: Data storage, cloud security, self auditing, audit, token, secret key.

1. Introduction

As the concern arises among the cloud users over the protection and privacy of their data stored in cloud [6], it has become really important to focus on these matters seriously. In our paper we used the secured erasure code, this is a double tier security process, at first the data will get splitted into different parts and get stored in different locations and secondly, before storing the splitted data which is stored in the cloud gets encrypted. AES (Advanced Encryption Standard) algorithm is used for the encryption method. Now if any users who are not authorized try to access the

valuable data of the file owner which is stored in cloud becomes really a tough job almost a impossible task, as the files are splitted and stored in different location with a encrypted format [22]. Remote Data Checking (RDC) is a tool that allows the users to check whether their outsourced data is kept unimpaired or is damaged and act as a repair tool[19]. The internal security threads can be handled by introducing HAIL (High-Availability and Integrity Layer) [18].

2. Problem Statement

Using the third party auditing scheme the important information of the file owner had to be given to the third party for the auditing purpose. So there is a chance that the important information gets mishandled and gets used in a wrong way without the knowledge of the file owner. And the cryptographic process used for the protection of the valuable data does not match with the users expectation when it comes to protections of their data, as the data are not splitted and stored in different location. It becomes quite easy for the unauthorized users to access the data.

3. Related Work

Z. Fu, X. Sun, Q. Liu, L.Zhou, J. Shu in 2015 have proposed an efficacious method to secure the seclusion of the data. They designed variable searchable encryption process. This consists of both multi-keyword ranked search and parallel search. Two secure searchable encryption scheme is used in order to face different privacy requirements [1] .Y. Ren, J. Shen, J. Wang, J. Han, S. Lee in 2015 proposed a strong evident of provable data possession, which uses the Diffie-Hellman shared key to construct the homomorphism authenticator [2].Many authors have proposed a secured distributed storage scheme which supports security saving open inspecting. They spoke about the TPA (Third Party Auditing) which perform surveys for different users [7,8,10,13,17]. Authors have published a paper on Proxy provable data possession (PPDP) [16]. H. Wang in 2013 have proposed a greatly methodical PPDP protocol which is reliable. It is completely based upon the bilinier pairing [4]. Ateniese, R.DiPietro, L. V. Mancini, G.Tsudik in 2008 have proposed a model for safe PDP framework which is developed by using the the symmetric key cryptography. Here it does require any of the encryption process [5]. M. B. Jayalekshmi, S. H. Krishnaveni in 2015 gave an overview of the security related issues on cloud data storage. They also gave information about the encryption process and about the auditing [6]. Alexandru Butoi, Nicolae Tomai in 2014 had proposed a protocol which deals in secretly sharing of the data which splits in optimal chunks. Each chunk has a minimum information content to the whole informational content of data set [9]. Juels and B. S. Kaliski Jr in 2007 defined the proof of retrievability. The POR enables a archive to produce a proof that the verifier

can retrieve a target file that the archive retains.The goal of a POR is to accomplish the checks without downloading the files by the users themselves [11]. S.Suganya,P.Damodharan in 2013 proposed a dispersed storage scheme with auditing mechanism which assures the accuracy and consistancy of the data. It uses the homo-morphic token and distributed erasure coded data[12]. Authors also have proposed a model which allows a client that stores treplicas of a file in a storage system[14]. ZHANG Wei, SUN Xinwei described the bit split bit combination data privacy protection program .Here the data are broken into different parts and uploaded into different position in the cloud servers [20]. The authors also have proposed a scheme to improve the service quality the cloud provider which uses the hybrid approaches for analyzing the task scheduling [23].

4. Existing System

Remote data integrity is checked by the users who store their data in cloud with the help of the internet. The user is not allowed to store his data in the cloud, if he is suspected of being a fraud or have done any another commercial crime, at that time he will give his proxy to upload the data in cloud and process them. Here for the security purpose they have proposed proxy oriented data uploading and remote data integrity checking (ID-PUIC) process in public key cryptography. This ID-PUIC scheme was proposed using the computational Diffie Hellman.

Disadvantages of Existing System:

1. The valuable information has to given to the third party for processing the data.
2. The data is not splitted and stored in different location so unauthorized access to the data becomes quite easy.

5. Proposed System

In our system we proposed for a self auditing scheme. Using this scheme the file owner can easily audit his data by self without giving the valuable information to the third party. Here two token are generated, the first token is generated once the file is uploaded by the file owner in cloud. Another token gets generated once the file uploaded gets edited by another user with whom the file owner has shared the file. Once the file is edited by the shared users both the tokens gets compared and if there is a mismatch in the token a notification message goes to the file owner asking for his approval. Once it gets approved by the file owner the edited file gets permanently stored in the cloud. If the file owner does not give his approval the edited file does not get saved. The token is generated using the random ASCII values of the characters present in the file.

The double tier security process is used for the storing the uploaded files in cloud [22]. The file gets splitted into many parts and is encrypted and then gets stored into different locations. A secret key is generated and send to the file owner which is used for the downloading process as a authentication. Only after the file owners consent the file can be downloaded using the secret key.

Advantages of Proposed System:

1. We use self auditing, the valuable information need not to be given to the third party.
2. The uploaded data gets splitted and is stored into different location after encryption so access to the data by any unauthorized users becomes really tough almost impossible.
3. secret key is generated and sent to the file owner using which the file can be downloaded

The proposed model of this project is as shown in the figure 1 which consists of three main phases as follows,

- User Interface
- Secret Key Generation
- File Uploading Process
- File Sharing Process
- File Auditing Process
- Mail Alert Process
- File Downloading Process

A. System Architecture

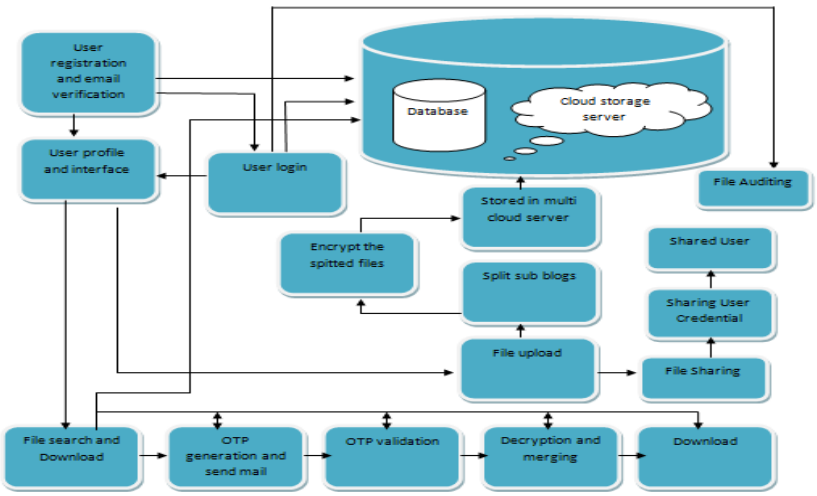

Fig.1 System Architecture Design.

B. User Interface: Here a user friendly interface is build so that the interaction becomes easy. Easy Searching facility to the file which is uploaded in cloud in provided. While uploading the file the user will be asked to provide a keyword for the file, this keyword can be later used in searching the file instead of giving the whole file name.

C. Secret Key Generation: A secret key is generated and send to the file owner which is used for the downloading process as a authentication. Only after the file owners consent the file can be downloaded using the secret key.

D. File Uploading Process:

The file uploaded is splitted into different parts and gets encrypted before it gets stored in different server location. Now if any users who are not authorized try to access the valuable data of the file owned which is stored in cloud becomes really a tough job almost a impossible task, as the files are splitted and stored in different location with a encrypted format.

E. File Sharing:

In our application we can share a file to a registered user by providing basic credentials, with the sharing option it is necessary to provide authority to the shared user whether to view or edit the file. A user can view the shared file within the application without downloading it and the same is possible with the edit option.

F. File Auditing:

Auditing is the process of checking the file whether the original contents of the file is changed. This module provides the file owner auditing, this we achieve by generating tokens. The tokens are generated with the ASCII values of the characters in the file and these characters are stored in the DB while uploading the file. If a shared user edit's the file and saves it, again a new token will be generated and stored in the DB. Both the tokens gets compared and if there is a mismatch in the token a notification message goes to the file owner asking for his approval. Once it gets approved by the file owner the edited file gets permanently stored in the cloud.

G. Mail Alert Process: The secret key which is generated is send to the file owner mail, using the mail alert process.This secret key need to be provided to download the files which is stored in cloud. It utilizes the Share Key Gen (SKA, t, m). This calculation shares the unknown key SKA of a user to an arrangement of key servers.

H. File Downloading Process:

The splitted file which is encrypted and stored into different location gets decrypted and form the original file. Then only after applying the secret key, the original file can be downloaded from the cloud.

6. Algorithms

SECURE ERASURE CODING

Start;

→own and pwd; Based: = the privileges based upon the basic methodology in the cloud computing field.

ownname =own && pwd=password

Then

→ If(xkey==cfile)

Files upload j;

j→split1,split2,split3;

→Encryption & decryption with AES

e→encyp1, encyp2, encyp3

d→decyp1, decyp2, decyp3

file downloading fd;

serfile from db & server

if(fd==serfile)

xkey→send to file owner mailed (otp).

Add orgnl data→(split1+split2+split3)

Download the file.

→Else

Cancel the file;

End;

7. Mathematical Model

1. Initialize Tokens
    (a) At={}
    (b) Ot={}
2. Files which is uploaded to Cloud

F = {}

3. Process encryption module

   En=fp,uid_otn

   Where fp Ɛ F

   uid_otn Ɛ OT

4. Decryption module D=Fc,uid_otn

   Where Fc Ɛ En

5. Encrypted files which is obtained from the equation

   $S(En)=\sum_{n+1}^{fn} fp\text{^}uid\_OT$

   Total no. of files in a set F={} is n, the file of the plain text is fp and user Authorization token is uid_OT

6. The Original files which is obtained from the equation is

   $S(Dn)=\sum_{n+1}^{fn} fp\text{^}uid\_OT$

Total no. of files in a set F= {} is n, the file of the cipher text is fc and Authorization token is uid_OT.

8. Advanced Encryption Standard (AES)

Description

It is a web tool used for the encryption and decryption of the text using AES encryption algorithm. AES is actually designed to be efficient in software as well as hardware. The lengths of the key here is 128, 192, and 256 bits. AES execute all its computation on bytes rather than bits. Hence, AES serves the 128 bits of a plaintext block the same as 16 bytes[15]. The Advanced Encryption Standard (AES) is a symmetric block cipher which is used to protect the important information. It can be implemented in software as well as the hardware for the encryption purpose. AES has three blocks of ciphers, AES-128, AES-192 and AES-256[21].

The Features of AES

Symmetric blocks of cipher.

Block length is 128 bits.

The key length are 128, 192, 256 bits.

It is faster than Triple-DES.

9. Conclusion

We have already gone through about the existing technique which was used for secure storage of the files in the cloud. The techniques which we proposed here to secure the data are Advanced Encryption Standard (AES) which is used to encrypt the data and Secure Erasure Coding (SEC) for splitting the file. Finally, we achieve the security to the files which will be saved in the Cloud.

Reference

1. Z. Fu, X. Sun, Q. Liu, L.Zhou, J. Shu. Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Transactions on Communications. 2015; vol. E98.B, no. 1, pp.190-200.
2. Y. Ren, J. Shen, J. Wang, J. Han, S. Lee. Mutual verifiable provable data auditing in public cloud storage. Journal of Internet Technology. 2015; vol. 16, no. 2, pp. 317-323.
3. H. Wang. Proxy provable data possession in public clouds. IEEE Transactions on Services Computing. 2013; vol. 6, no. 4, pp. 551-559.
4. G.Ateniese, R.DiPietro, L. V. Mancini, G.Tsudik. Scalable and efficient provable data possession. SecureComm 2008.
5. M. B. Jayalekshmi, S. H. Krishnaveni. A Study of data storage security issues in cloud computing. Indian Journal of Science & Technology. 2015; vol 8, no.24, pp.2-4
6. 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.
7. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf.Cloud Computing, pp. 295-302, 2012.
8. M.S.Shashi Dhara, "Privacy Preserving Third Party Auditing In Multi Cloud Storage Environment.", IEEE International Conference on Cloud Computing in Emerging Markets (CCEM),pp.1-6,2014.
9. Alexandru Butoi, Nicolae Tomai, "Secret sharing scheme for data confidentiality preserving in a public-private hybrid cloud storage approach." IEEE/ACM International Conference on Utility and Cloud Computing Pages 992-997, 2014.

10. Dr.J.Suganthi, Ananthi J Archana, "Privacy preservation and public Auditing for cloud data using ass ",International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS),pp.1-6,2015.
11. A. 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.
12. S.Suganya, P.Damodharan, "Enhancing Security for storage services in cloud computing", International Conference on Current Trends in Engineering and Technology (ICCTET),pp.396-398,2013.
13. 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.
14. Reza Curtmola and Osama Khan, "MR-PDP: Multiple-Replica Provable Data Possession," Comm. ACM, vol. 14, no. 1, 2011.
15. Poonam.M.Pardeshi,Deepali Borade, "Enhancing Data Dynamics and Storage Security for Cloud Computing using Merkle Hash Tree and AES Algorithms",International Journal of Computer Applications; Vol. 98, p1, Jul 2014.
16. Megha Patil,Prof.G.R.Rao, "Integrity Verification in Multi-Cloud Storage Using Cooperative Provable DataPossession", IEEE Transactions on Parallel and Distributed Systems, Volume:23, Issue: 12, pp. 2231 -2244, Feb 2012.
17. Syam Kumar P,Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", International Journal of Computer Science Issues (IJCSI); Vol. 8 Issue 6, p261, Nov2011.
18. D.Bowers, Ari Juels, Alina Opera "HAIL: A High- Availability and Integrity Layer for Cloud Storage", ACM conference on Computer and communications security,pp.187-198,2009.
19. 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
20. 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.
21. P. Anitha, V.Palanisamy. Data protection algorithm using AES. international journal of current research. 2011; vol. 3, issue, 6, pp.291-294.

22. P. Debnath, S. Jagadeesan, "A Survey on a Reliable Method to Achieve Cohesion and Possession of the Data in Cloud", International Journal of Pharmacy & Technology, 2016: vol. 8, no. 4, pp. 5251-5256.

23. S. Nair, P. Akilandeswari, "Analysis of Task Scheduling for Private and Public Cloud in Real Time Environment," International Journal of Pharmacy & Technology, 2016: vol. 8, no. 4, pp. 5198-5204.

Corresponding Author:

Pritam Debnath*,

Email:pritamvtu@gmail.com