International Journal of Engineering Research and General Science Volume 3, Issue 6, November-December, 2015
ISSN 2091-2730

IMPLEMENTATION CONCEPT FOR ADVANCED CLIENT REPUDIATION DIVERGE AUDITOR IN PUBLIC CLOUD

[1]Ms.Nita R. Mhaske, [2]Prof. S.M.Rokade
[1]student , Master of Engineering, Dept. of Computer Engineering Sir Visvesvaraya Institute of Technology, Chincholi, Sinner
nita.mhaske90@gmail.com,9960530968
[2]Head Of Department of Computer Engineering, Sir Visvesvaraya Institute of Technology, Chincholi, Sinner ,
,smrokade@yahoo.com

Abstract— Cloud provides data storage and sharing services and people works together as a group. After creating the group, member of a group able to access, modify and shares latest updated data with the rest of the group members. To sure the integrity, group member need to upload the data with their sign. After modification user have to upload data with his own private key. If user is repudiated from group then data signed by repudiated user are signed by existing users. In this, proposed an auditing mechanism for integrity of shared data with efficient user repudiation. Existing user resign the data during user repudiation without downloading data .

Keywords—Diverge auditing , shared data, user repudiation, cloud computing.

INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. There are various essential characteristics of cloud such as on demand self service, broad network access , resource pooling ,rapid elasticity etc. There are three different service platform IaaS, PaaS, SaaS. Also there different deployment model like private cloud, public cloud, hybrid cloud. In this system we use IaaS platform with public cloud .Public cloud service provider like Amazon AWS. and operate the infrastructure at their data center and access is generally via the Internet. AWS offer direct connect services called "AWS Direct Connect".

As Cloud provides data storage and sharing services and people works together as a group. After creating the group ,member of a group able to access, modify and shares latest updated data with the rest of the group members. cloud providers provides secure and reliable environment to the users, still there may be problem with integrity of the data due to repudiation of user. Previously after repudiation of user any of the existing user download all the data , verity it and again upload all the data ,but it having communication overhead and time. In this system original user of the group resign the data with his private key due to this data in cloud remain safe. As a result, the efficiency of user repudiation can be significantly improved, and computation and communication resources of existing users can be easily saved.

RELATED WORK

Cong wang, Qian wang, Kui Pen, W. Lou proposed an distributed scheme for data with explicit dynamic operation .It also ensure users data securely stored in cloud. This system is efficient against Byzantine failure, malicious data attack etc. User can perform operation for checking storage correctness perform operation for checking and dynamic operation. Mostly focus on data checking and dynamic operation .

Cong wang, Qian Wang, Kui Ren, w. lou proposed system consist, as there are burden on user if we stored data locally. So that it uses the functionality of cloud data can stored remotely and user can access data as on demand. It uses TPA to audit the data on demand.In this , they utilized the public key based homomorphic authenticator with random mask technique to achieve privacy preserving auditing system for the data security purpose. In this most focus on security of data with public key..G.Ateniese ,R.Burns, R.curtmola proposed mechanism ,that allowed the client who stored the data at an untrusted server to verify that the server possesses the original data without retrieving it. They allow to verify data possession without having access to the actual data file.

C.Wang, Q.Wang, K.Ren proposed mechanism focusing on cloud data storage security which effect on quality of service, supports secure and efficient dynamics operations on data blocks including data update,delete and append. H.Shacham & B.Waters proposed two proofs for retrievability schemes for full proofs of security against arbitrary adversaries in the strongest scheme which is

Juels and Kaliski and secondly scheme with private verifiability. B.Wang, B.Li, H.Li, F.Li proposed first certificateless diverge auditing mechanism for verifying data integrity in the untrusted cloud is based on CDH assumption and DL assumption. .H.Wang proposed system for proxy provable data possession for the purpose when the client cannot perform the remote data possession checking. System was based on bilinear pairing technique.

SYSTEM DESIGN

In system design basic Block diagram includes three entities: the cloud, the public verifier, and two or many users (who share data as a group). The cloud offers data storage and sharing services to the group. The public verifier, such as a client who would like to utilize cloud data for particular purposes or a third-party auditor (TPA) who can provide verification services on data integrity, aims to check the integrity of shared data via a challenge-and response protocol with the cloud. In the group, there is one original user and a number of group users. The original user is the original owner of data. This original user creates and shares data with other users in the group through the cloud. Both the original user and group users are able to access, download and modify shared data. A user in the group can modify a block in shared data by performing an insert, delete or update operation on the block.

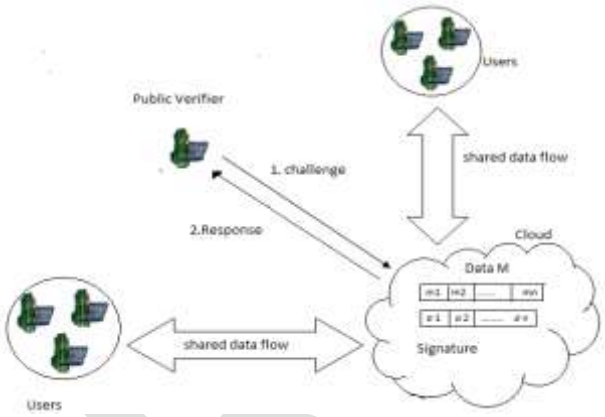

Figure 1: block diagram of proposed system

This system is divided into different modules as shown in figure 2. System consist of different moduls: controller, storage service, trusted third party auditor, security service, data re-signature service, most important entity is user. User get interface with system though web server and web application. Any web browser work on HTTP. User send and gain reply though HTTP. The component which handle this is called web server. Web application is intermediate between web server and controller.

All the services are executed though controller. Which operation executed first it is decided by controller (i.e. registration of user, upload, download). Storage service handle all database related operation (i.e. insertion, deletion, modification). Security to the data is provided through security service such as encryption and decryption of data If user want to check the data integrity periodically and whenever he want it done though third party auditor. Similarly not only user but also group admin and super admin can audit the data. Auditing done as challenge and email obtain from third party auditor taken as response. All members in the cloud and cloud computing environment should be trusted by each other and the members that have communication should be trusted by each other. Trust is major concern of the consumers and providers of service that participate in a cloud computing.

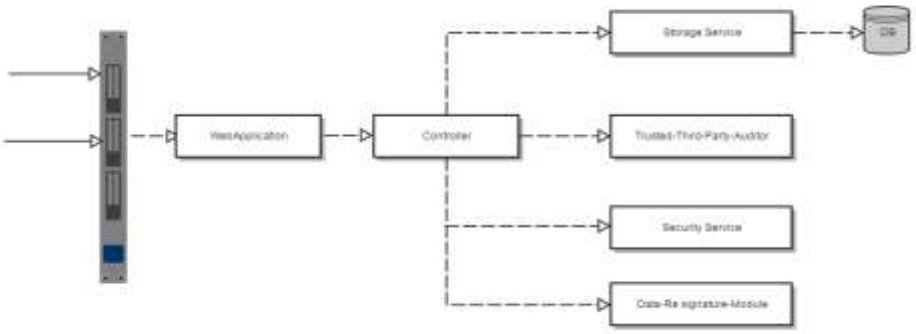

Figure 2:Modular system of proposed system

Design objective of the system are

- Integrity: The public verifier can be check the correctness i.e. integrity of shared data.
- secure user repudiation: after repudiating the user block signed by him are efficiently resigned by existing user.
- divergence: auditing the integrity of shared data without downloading all the data even if some data signed by cloud.
- Scalability: we add any number of user in the group as we can maintain our system properly.

For security purpose i.e. for encryption and decryption we used AES algorithm. Pseudo code for AES algorithm is as follows:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
    begin
        byte state[4,Nb]
        state = in
        AddRoundKey(state, w[0, Nb-1])
        for round = 1 step 1 to Nr-1
            SubBytes(state)
            ShiftRows(state)
            MixColumns(state)
            AddRoundKey(state,
        w[round*Nb, (round+1)*Nb-1])
        end for
        SubBytes(state)
        ShiftRows(state)
        AddRoundKey(state, w[Nr*Nb,
    (Nr+1)*Nb-1])
    End
```

Figure 3: AES algorithm

EXPERIMENTAL RESULT

Now we go for what exactly we done in the system is

1. User registration into the system

In this system we create number of group when user want to enter into the system he have to registered in to the system. At the time of registration he has to choice in which group he want to go and has to follow terms and condition.

2.User Task

After getting entry into the system user can perform various task with his private key such as upload data delete and modified the data .He give challenge as audit the system though perform audit tab provided to user by admin. Auditing report to the user as response to the user from TPA.

3.Admin task

As admin can perform all the operation user can perform with additional rights. He handle all group information, which user stay in the group. When user not follow terms and condition then admin has right to repudiate the user. All the file on account of repudiated user are get on admin account , due that integrity of that get maintain and this is done with reassignment report.

4.Auditing task

When user and admin asked for auditing then TPA will mail the report to the user who done the request. Auditing help us to maintain the integrity. In auditing report it consist server communication time and total time required for auditing.auditing time is nothing but time to response by TPA.server comunicationtime is input request comes what time and response in what time , the difference between this two .


Result :- Success

Audit Report

sendEmail

Go To Main Home Page

Number Of Record	Server Communication Time	Auditing Time
2	1010 (milisecond)	60 (milisecond)

Conclusions

In this system user can perform dynamic operation such as insert, delete, modify data. Admin of the group as rights to repudiate the user from the system. with this system we achieve efficient user repudiation so that integrity and security of data maintain

ACKNOWLEDGMENT

It is a great pleasure to acknowledge those who extended their support, and contributed time and psychic energy for this projectwork.At the outset, I would like to thank my Project guide Prof. S.M.Rokade, who served as sounding board for both contents and programming work. His valuable and skillful guidance, assessment and suggestions from time to time improved the quality of work in all respects. I am also thankful to Prof. S.M. Rokade, Head of Computer Engineering Department for his timely guidance, inspiration and administrative support without which my work would not have been completed. I am also thankful to the all staff members of Computer Engineering Department and Librarian, SVIT Chincholi, Nasik. Also I would like to thank my colleagues and friends who helped me directly and indirectly to complete this Project work. Lastly my special thanks to my family members for their support and co-operation during this Project work.

REFERENCES:

[1]. B. Wang, B. Li, Member, H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud " in the Proceedings of IEEE INFOCOM 2014, 2014
[2]. 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.
[3]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, an M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.
[4]. 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.
[5]. H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springe Verlag,2008,pp. 90–107.
[6]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEEIWQoS 2009, 2009, pp. 1–9.
[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]. H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.
[9]. B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, 2012, pp. 295–302.
[10]. B. Wang, S. S. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in Proceedings of IEEE ICDCS 2013, 2013.
[11]. B.Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," in Proceedings of IEEE CNS 2013, 2013, pp. 276–284.