RUN TIME PUBLIC AUDITING IN CLOUD COMPUTING USING PROTOCOL BLOCKER FOR PRIVACY

[1]DHANASHRI PATIL, [2]BABITA BHAGAT

Student, M.E. [1]Comp. Department of Computer Engineering, Pillai's HOC college of Engineering and Technology, Rasayani
[2]Guide, Department of Computer Engineering, Pillai's HOC College and Technology, Rasayani
E-mail: [1]patildhanu1990@gmail.com, [2]babitas12@gmail.com

Abstract-Cloud Computing is huge computing utility, where user can remotely store their data into cloud and enjoy high the on-demand high quality cloud application and services without burden of local hardware and software management and also decreases the maintenance load of users by providing low cost scalability. In the corporate world there are large number of client who accessing their data and modifying data. User can access data, use the data and store that data. Cloud computing moves the application software and databases to the centralized large data centers, where the management of data and services may not be fully dependable. To manage this data we use TPA (third party auditor) it will check reliability of data but it increases the data integrity risk .In this paper, we propose a secure cloud storage system for privacy preserving public auditing.

Keywords-Data Storage, Privacy Preserving, Public auditing, TPA, Cloud Computing

I. INTRODUCTION

Cloud computing is computing resources to provide service through internet. cloud computing provide various service models as Platform as a Service (PaaS) is developer can design ,build and test application that run on cloud providers infrastructure example: Google application engine ,Software as a Service(SaaS),is company host their data in cloud and user can access through internet example: Gmail, Facebook. Infrastructure as a Service (IaaS) is provides basic services .cloud computing has four models public cloud services are available over a network that is open for public use. Private cloud Microsoft, Google, Amazon is Public cloud. Hybrid cloud is the combination of cloud deployment models each cloud is individually managed while application and data would be allowed to move across the hybrid. Community cloud shares infrastructure between several organizations from specific community. The main goal of cloud computing is data being centralized outsourced to the cloud.both the individuals and IT enterprises, strong data remotely to the cloud .the major benefits of storing data on cloud is relief of the burden for storage management. In cloud data is stored in centralized form and managing this data and providing security is difficult task.TPA can read the content of data owner hence can modify. Third party auditing is play important role for the storage auditing in cloud computing.

The following two fundamental requirements to securely introduce an effective third party auditor (TPA)

- TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user.
- The third party auditing process should bring in no new vulnerabilities towards user data privacy.

In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. To support multiple auditing user tasks, we explore the technique of bilinear aggregate signature to extend our main result into a multi-user, where TPA can perform multiple auditing tasks simultaneously. Security and performance analysis shows the proposed schemes are provably secure and highly efficient.

Here by following the aspects and we are using automatic blocker to the cloud environment, which particularly blocks the auditing protocols from unauthorized access from the external user for privacy preserving for data security in cloud computing.

II.THE BASIC SCHEME

A. Cloud Model

In the below figure we prepared model in which client, cloud service provider (CSP)/cloud server and TPA .cloud user is who stores large amount of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that will be manage by cloud service provider. Third party auditor will do theauditing on users request for storage correctness and integrity.

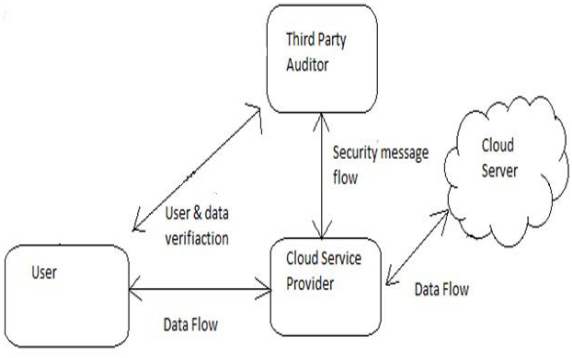

Fig1: The architecture of cloud data storage

The proposed system specifies that user can access the data on cloud without worrying about the integrity of the data .hence TPA checks the integrity of data and storage correctness.

In the cloud data is store in centralized form. Data management and providing security is a difficult task. in cloud computing TPA can read the owner data hence they can change the owner data easily hence reliability is increased but integrity is not achieved.

TPA always checks the integrity of data and TPA itself leaks the information of user'sdata. Hence the new concept auditing with zero knowledge privacy where TPA will audit users data without seeing any data.

B. Roll of Third Party Auditing

External audit party is called TPA.TPA helps the user to audit the data.TPA should audit the data from the cloud, not ask for a copy.

- Public Auditing is done.
- Privacy is preserved as attributes of file are used for comparing original file and changed file.
- Batch Auditing for multiple owners is done
- TPA discards the changed files from cloud server.
- Mail is sent by TPA to data owner regarding changed file.
- It is a light weight process as downloading of file is not needed to check its integrity.

C. Limitation of Existing System

- Infrastructure of cloud computing is very powerfull and large but still they are facing problem of internal and external threats.
- Cloud service provider behave unfaithfully towards the user regarding their outsource data.
- Encryption is not fully solve the problem of security so unauthorised leakage still remains possible.

III. PROPOSED MODEL

A. Design Goals of Cloud Computing

- *Publicauditability:*It allows TPA to audit user's data without retrieving the copy of data.
- *Batch auditing:*It supports batch auditing where multiple users request for data auditing will be handled simultaneously.
- *Storage Correctness:* To ensure that there do not exist cheating on cloud server.
- *Privacy preserving*:It provides security and increase performance and TPA can't read the users data during auditing phase.
- *Light Weight:* To allow TPA to perform auditing with minimum communication and computation overhead.

B. Privacy Preserving Public Auditing Proposed Scheme

For achieving privacy preserving public auditing we first propose homomorphic linear authenticator with random masking .Public auditing allows TPA to do auditing without requesting for local copy of the data.TPA can audit the data and cloud data privacy is maintained.

TPA checks the integrity of outsource data stored on cloud without accessing the content. Existing research work of proofof Retrievability(POR) technique does not consider data privacy problem. It uses RSA based HA for auditing the cloud data and randomly sampling few blocks of files.POR allows user to retrieve files without any data loss. It uses spot checking and error correcting codes .

C. Algorithms

- *KeyGen:* Its key generation algorithm that is run by user to setup scheme.
- *SignGen:*It is run by cloud user andused by user to generate verification metadata which consist information that used for auditing
- *GenProof :* It is used by cloud server to generate a proof of data storage correctness.
- *VerifyProof :* It is run by TPA to audit the proof from cloud server.

D. Properties of Proposed System

- Uses the One Time Password Verification scheme.
- TPA audits the data to check its integrity.
- Privacy of data is maintained from Third Party Auditor.
- File attributes are used for comparing original file and changed file.
- Batch Auditing is done by TPA.
- Supports Data Dynamics.
- Overwriting of original file is allowed.
- Implementation on real cloud.

IV. WORKING OF PROJECT

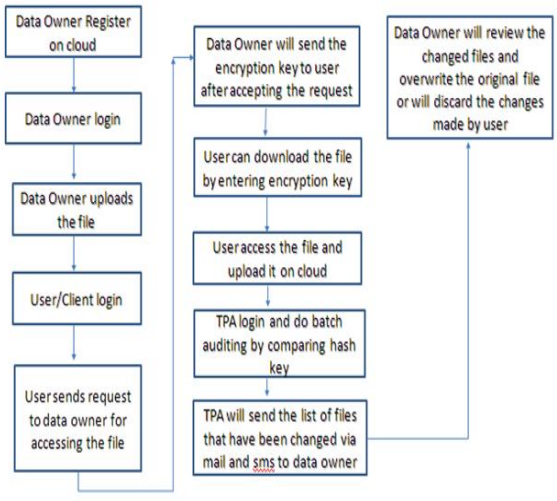

Fig2:Block Diagram

Dataowner first done registration on the cloud. then dataowner login is done. dataowner upload the file on the cloud. User/client also done with there login. user send the request to data owner for accessing the file. dataowner sent the encryption ley to user after accepting the request. user can download the file by entering the encryption key. user then access the file and upload it on the cloud.TPA do the login and do the batch auditing by comparing hash key.TPA will send the list of files that have been changed via mail and sms to dataowner. dataowner will review the changed files and overwrite the original file or will discard the changed made by user.

A. Use of Rijndael Algorithm

Best combination of security, performance, efficiency, ease of implementation and flexibility.high speed and versatility across a variety of platforms. Run efficiently on large computers, desktops and small devices like smart cards. It allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits. Rijndael is simple to implement and uses very little system memory. It i a practically crack-proof algorithm. Brute force attacks against Rijndael have proven ineffective to date.

B. Steps of Rijndael Algorithm

Step 1: ByteSub Transformation

Step 2: ShiftRow Transformation

Step 3: MixColumn Transformation

Step 4: Round Key Addition

CONCLUSION

In this paper, we propose a privacy preserving public auditing for storage data security purpose.To protect the data from unauthorized access and to ensure that data is intact, TPA model proposed a scheme, which solve the problem of integrity, unauthorized access, privacy and consistency. This model presents a network in which cloud architecture, users and TPA are shown and then how file is retrieved. This scheme utilizes Rijndael Algorithm to create an encryption key that user gets while requesting to data owner for file accessing. This scheme uses SHA-512 algorithm for generating hash key that TPA uses for checking data integrity.

C. Flow of file access

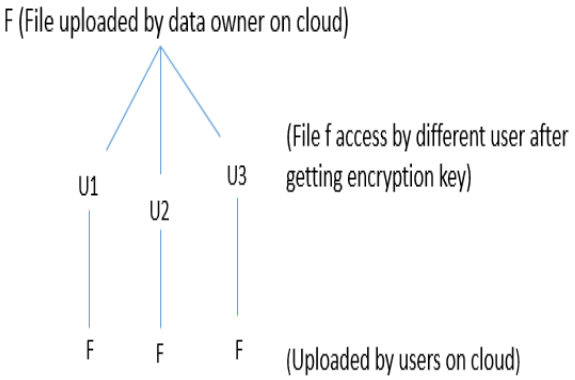

Fig.3 Flow of file access

- TPA do auditing, discard unchanged files, and send warning to user regarding changed files.
- Data owner will check all the changed files and replace the original file with the file with valid data.

REFERRENCES

[1]. K.Kiran Kumar, K.Padmaja, P.Radha Krishna,Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing, IEEE 2012 Transactions on CloudComputing, Volume: PP,Issue:99

[2]. A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations, International Journal of Cryptology Research 1(2): 215-223 (2012) 35

[3]. Privacy-Preserving Public Auditing for Secure Cloud Storage, Cong Wang, Member,IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member,IEEE, and Wenjing Lou.

[4]. Eficient integrity checking technique for securing client data in cloud computing , Dalia Attas and Omar Batra IJECS-IJENS Vol: 11 No: 05 43

[5]. "Cloud Data Security and Integrity Using Third Party Auditor", International Conference on Research and Scientific Innovation ICRSI-2013.

★★★