Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Run Time Public Auditing in Cloud Computing using Protocol Blocker for Privacy Preservation

Ms. Dhanashri Patil,
PG Student,
Department of Computer Engineering,
Pillai's HOC college of Engineering and Technology,
Rasayani, Raigad, India

Prof. Babita Bhagat
Department of Computer Engineering,
Pillai's HOC college of Engineering and Technology,
Rasayani, Raigad, India

***Abstract* - Cloud Computing is huge computing, it is the internet based computing, where all users can remotely store their data into the cloud so as to enjoy the latest and high quality applications and services. In outsourcing data, users can be relieved from the burden of local maintenance and data storage .Thus, enabling public auditability for cloud data storage security is of difficult, so that users can resort to an external audit party to check the integrity of outsourced data when needed. The management of data, services may not be fully dependable when cloud moves the application software and databases to the centralized data centers and those data center is large. In this we propose a privacy-preserving public auditing for cloud data storage. To enable the TPA to perform audits for multiple users simultaneously and efficiently. And also doing batch auditing for multiple users' data.**

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

I. INTRODUCTION

Cloud computing is a computing resource which provides service through internet. Cloud computing provides various service models such as Platform as a Service (PaaS) where developer can design, build and test application that run on cloud providers infrastructure.[1] 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 providing basic services. Cloud computing has four models first is public cloud services are available over a network that is open for public use. Microsoft, Google, Amazon is Public cloud. A cloud that is used exclusively by one organization is called private cloud. Hybrid cloud is the combination of cloud deployment models where an 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. The individuals and IT enterprises, strong data remotely to the cloud. The major benefits of storing data on the cloud are relief of the burden for storage management. In cloud data is stored in centralized form and managing this data and providing security is a difficult task. The Third Party Auditor can read the content of the data owner, hence can modify. Third party auditing is playing an important role for the storage auditing in cloud computing.

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

- TPA introduces no additional on-line burden to the cloud user.
- Cloud data storage efficiently audit by TPA.
- The third party auditing process should bring in no new vulnerabilities towards user data privacy.

II. LITERATURE SURVEY

Shah et al., proposes allowing a TPA to keep online storage by first encrypting the data, then they will send the number of symmetric key hashes over the encrypted data to the auditor. The auditors check the integrity of data. This situation work with all encrypted files and suffer from the auditor usage, when key hashes are used they may bring online burden to the user.

Ateniese et al., proposes the public auditability in their defined Provable Data Possession (PDP) model for making sure that controlled of data by untrusted storages. Previously authors have implemented the RSA based algorithm, this scheme utilizes homorphic authenticators for auditing the outsource data. Though, the public auditability demands the linear combination of sampled blocks and these blocks exposed to the external auditor. Privacy is not preserved in this protocol. So therefore, leaks user data information to the auditor.

Juels et al., described Proof of Retrievability (PoR) model, where error correcting and spot checking is used to make sure that both possession and retrievability of data files. An audit challenge that a user can perform public auditability is not supported. For public PoRs they describe a Merkle-tree construction and this technique works with encryption process. Shacham, et al.[5], proposes full proofs of security to improve and form secure blind signatures, i.e. BLS can build homomorphic authenticators. But this approach does not support privacy-preserving so for the same situation.

Ateniese et al.[6], proposes a partially dynamic version of the PDP. This model uses symmetric key cryptography. In a distributed scenario, this supports partial dynamic data storage. The data correctness and bugs can be determined by challenge-response protocol. In a subsequent work, PDP

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

model proposes the combination of BLS based homomorphic authenticator and Merkle tree to support both public auditing and data dynamics.

III. THE BASIC SCHEME

A. *Cloud Model*

In the below figure we prepared model in which client, a 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 managed by the cloud service provider. TPA will do the auditing on users request for storage integrity and correctness .

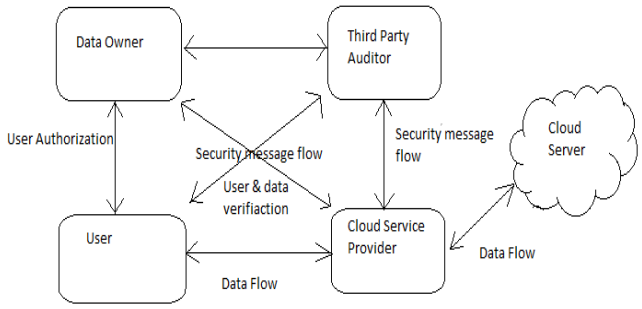

Fig 1. The architecture of cloud data storage

This system specifies that user can access the data on a cloud without worrying about the integrity of the data. Hence TPA checks the integrity of data and storage correctness. In the cloud data is stored in centralized form. It is very difficult to provide security and managing data. In cloud computing TPA can read the users' data, hence they can change the users' data easily, hence reliability is increased but integrity is not achieved.

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

B. *Role of Third Party Auditing*

The external audit party is called TPA.TPA helps the user to edit 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 the file are used for comparing original file and changed file.
- For multiple owners batch auditing is done.
- The changed files always TPA discards from cloud server.
- It is a lightweight process as downloading of file is not needed to check its integrity.

IV. PROPOSED MODEL

A. *Design Goals of Cloud Computing*

- Public auditability: It allows TPA to audit user's data without retrieving the copy of the data. [1]
- Batch auditing: 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 servers.
- Privacy preserving: It provides security and increase performance and TPA can't read the users' data during the auditing phase.
- Light Weight: To allow TPA to perform auditing with minimum communication and computation overhead.

B. *Algorithms*

Keygen: Its key generation algorithm that is run by user to setup scheme.

SignGen: It is used by the user to generate verification metadata which consist information that used for auditing.it is run by cloud user.

GenProof: To generate a proof of data storage correctness.it is used by a cloud server

VerifyProof: It is run by the TPA to audit the proof from cloud server. [1]

C. *Properties of Proposed System*

- One Time Password Verification scheme.
- TPA audits the data to check its integrity.
- Using Third Party Auditor privacy of data is maintained.
- 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 of real cloud.
- Relief of the burden for storage management.
- Block unauthorized user access.
- Protecting data privacy
- Storage security of their data

V. WORKING OF PROJECT

Step 1: Cloud owner first do registration on the cloud. After login OTP generated that OTP will send to owners mail or phone. Entering the OTP number owner will do login and upload the file to the cloud. When file uploaded successfully that time hash value generated using SHA-512 algorithm.

Step 2: Cloud user/client also do registration and after entering the OTP they will do their login. Searching the owners file user will download file but he will not get access to download file, so user will send request to data owner for file authorization.

Step 3: Cloud owner accepting the users request or block the user its totally depends on owner. After accepting the request owner sends the encryption key to the users mail or sms.

Encryption key will be generated by using Rijndael algorithm for more security.

Step 4: Entering the encryption key user can download the owners file and making changes in that file again user upload the file to the cloud. After uploading file hash value will be generated.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Step 5: TPA do login and do batch auditing by comparing original file and changed file hash value if the hash value getting same then file is not tampered otherwise it is tempered by User.

Step 6: Admin do login and will send the list of files that have been changed via mail and SMS to the data owner.

Step 7: Data owner will review the changed files and overwrite the original file or will discard the changed made by user.

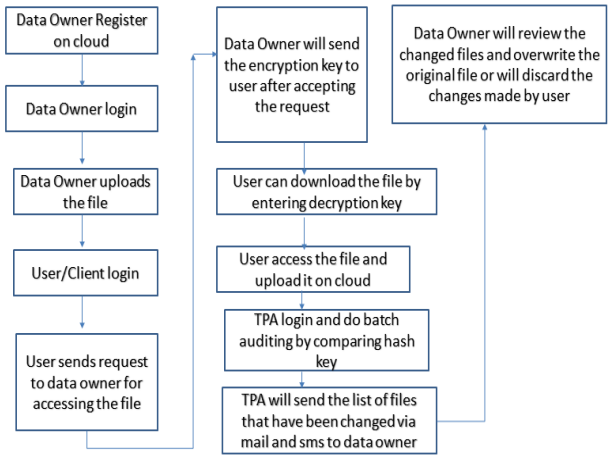

Fig 2. Block Diagram

VI. USE OF RIJANDAEL ALGO

Rijndael encryption algorithm is proposes new encryption technique for encryption and decryption purpose.It is advanced AES algorithm is use to encrypt sensitive information.it is symmetric key encryption algorithm to be used to encrypt sensitive information.it is 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. 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. [7]

VII. RESULT

Owner done with their login

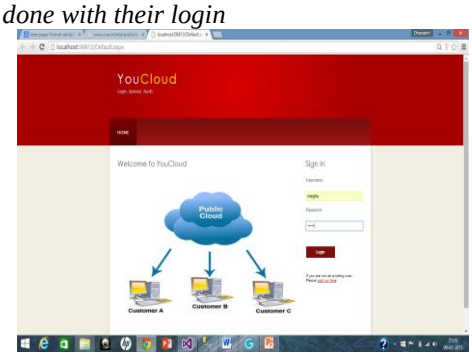

Fig:2 Login form of owner

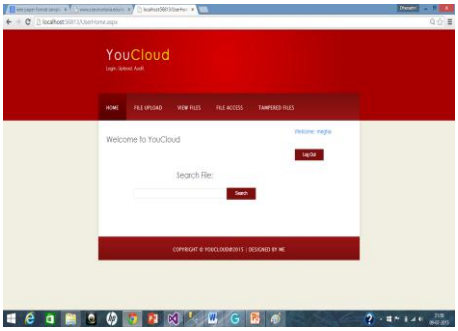

Fig:3 Login form of user

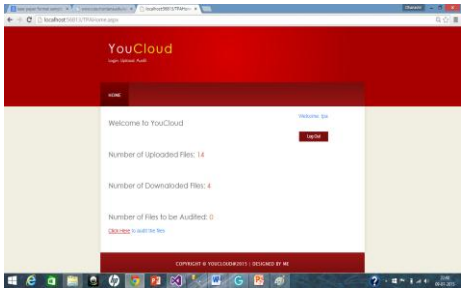

Fig: 4 TPA login

VIII. CONCLUSION

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

IX. REFERENCES

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

[2] Shingare Vidya Marshal “Secure Audit Service by Using TPA for Data Integrity in Cloud System” International Jproposednal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-4, September

[3] Cong Wang, Student Member, IEEE, Qian Wang, “Toward Secure and Dependable Storage Services in Cloud Computing” IEEE transactions on services computing, vol. 5, no. 2, April-June 2012

[4] Yan Zhu, Member, IEEE, Gail-Joon Ahn “Dynamic Audit Services for Outsproposedced Storages in Clouds” IEEE transactions on services computing, vol. 6, no. 2, April-June 2013

[5] Rakhi Bhardwaj, Vikas Maral “ Dynamic Data Storage Auditing Services in Cloud Computing” International Jproposednal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

[6] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing” IEEE transactions on parallel and distributed systems, vol. 24, no. 9, September 2013.

[7] Federal Information Processing Standards Publication, “Advance Encryption Standard“26 November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf