International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 3(D); March 2018; Page No. 10718-10720
DOI: http://dx.doi.org/10.24327/ijcar.2018.10720.1830

Research Article

PRIVACY PRESERVING PUBLIC AUDITING FOR SHARED DATA IN DISTRIBUTED ENVIRONMENT

Kousalya R., Akshaya Devi S., Sangeetha S and Smitha P.S[AP]

Velammal Engineering College, Anna University, Chennai, India

A R T I C L E I N F O

Article History:

Received 4th December, 2017
Received in revised form 8st
January, 2018 Accepted 12th February, 2018
Published online 28th March, 2018

A B S T R A C T

In distributed environment where group of systems connected over a network and the individual computers were physically distributed within some geographical area where the users can form a group for uploading or viewing the files. They may face some security breaches at the storage servers and while sharing the files. As with physical security, the motivators for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, others are activists or criminals looking for financial gain. Even while storing those files in server the attacks may happen. So the files must be protected by using some encryption algorithm and digital signature schemes. In this system Advanced Encryption Standard (AES) algorithm for encrypting and ring signature has been used. If an unauthorized user tries to access or modify those stored files in server, they can be traced and blocked using their IP address.

To ensure the correctness of data, we consider the task of allowing a Third Party Auditor (TPA), to verify the integrity of the data stored in the server, the auditing process should bring in no new vulnerabilities towards user data privacy, so the TPA can only view the hash values of those stored files. They cannot demand for the local copy of the file for auditing. This system uses methods like AES algorithm, Ring Signature are for securing data. Thus our protocol is much more efficient than a recent preserving public auditing protocol.

INTRODUCTION

In distributed environment where data is being centralized or outsourced to the users and it provides many advantages but it also brings security threats towards users outsourced data. As users cannot stay on-line burden of the users and to audit the data frequently, introduces Third Party Auditor (TPA) to audit the user outsourced data when needed.

This project discusses about the methods used to publicly audit the uploaded files in the distributed environment. And also to provide security to those file, they are encrypted using Advanced Encryption Standard (AES) encryption and Ring Signature. Third party auditor is used for auditing but TPA should not gain knowledge about user data. And for that many methods are introduced to protect the data being viewed by the TPA and makes auditing more secure. Secure Hash Algorithm (SHA-256) has been used to generate the hash values this value can only be viewed by the TPA. They cannot view the entire or the partial file while auditing. TPA only can audit the file cannot view the users data.

Corresponding author:* **Kousalya R
Velammal Engineering College, Anna University, Chennai, India

TPA can even drop the modified files in addition to this trace-ability has also been introduced to find the unauthorized users. Apart from the Introduction there are Sections,

Section2 covers Existing System
Section3 covers Proposed system
Section4 covers System Architecture
Section5 covers Breaking down the Proposed System
Section6 covers Conclusion
Section7 covers Future work
Section8 covers References.

Existing System

Traditional data integrity checking methods are no longer suitable for the distributed storage environment, since it is impractical for users to download the whole data for integrity checking. In 2007, Ateniese *et al*. [2] proposal two integrity checking protocols in the "Provable Data Possession (PDP) " model which are based on RSA cyptosystems and homomorphic linear authenticators. The protocols are probabilistic, namely only checking some random sampled file blocks, the data corruption will be detected with a high probability. Besides, the improved protocol [2] also enables public auditability, which allows anyone, not just the data owner, to check the data integrity. Another approach to check the integrity of the outsourced data is called "Compact Proofs

of Retrievability" which is proposed ny B.Waters *et al*. [4]. It was also shown by Ateniese *et al*.[2] that those schemes can be used to construct leakage-resilient identification (ID) protocols in the bounded retrieval models. Other similar work can be found in [3], [5].

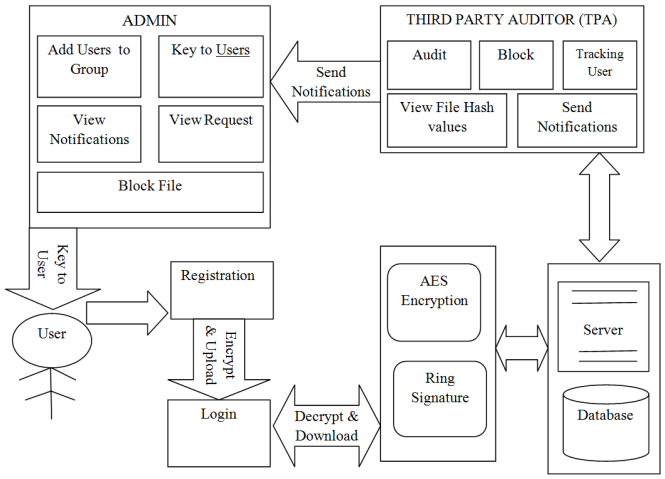
Proposed System

The proposed system contains Admin, User, Third Party Auditor (TPA). The user can register and upload the new files or download the existing files. The TPA audits the files and identifies the unauthorized users by modified hash values, then the TPA sends notification to admin about the unauthorized users. The TPA only can audit file cannot view the users data. The admin can block and unblock the users.

Advantages of Proposed System

- The user finds that their key has been mishandled user can send a request to admin for a new key.
- The users can be tracked so that one who modifies the files can be identified.
- The unauthorized users are identified by TPA, then he will send a notification to the admin so that admin can block them using their IP address.

System Architecture



Breaking Down the Proposed System

- User
- Admin
- Third Party Auditor (TPA)

User

The user can upload the file which will be stored in the server and it can also be shared with the other users in the group. While uploading files will be encrypted using AES encryption and Ring Signature for data security. The other users can even download the file but they can't modify the data without the data owner's permission. The users in the group can view the file using the random key provided to them. Incase of any misuses of users random key they can change their key by sending a request to the admin. By sending the request to TPA they can check the data integrity of the files by auditing.

Admin

Admin is one who assists the group of users. Admin will add users to group and he generates the random key to the users in the group. When unauthorized users accesses the files stored in the server, he receives the notification from the TPA. Admin also has the encrypted copy of all files stored on the storage server.

Third Party Auditor (TPA)

TPA will audit the user file stored in the server. While auditing the stored files TPA should not view the user data so the files hash values are given to him. Hash values for files are generated using SHA-256. By comparing the hash values TPA will come to a conclusion that the files have been modified or not. If the files gets modified he will drop or block the modified files. He can trace the users by which he knows whether the file is being modified by the authorized owner of the file or by the unauthorized users. If any unauthorized users tries to modify or access the stored files then he will send a notification to the Admin.

CONCLUSION

This system allows users to share their files in a secured way in the group. For secure sharing files are encrypted using Advanced Encryption System (AES) and for data privacy users data's are protected using Ring Signature. Admin will add the registered user to the group and will generate Random Key for each and every users in the group. All the keys generated by admin will be unique. Using that key users can view, decrypt and download their from the group.

In the existing system even if the users key is misused user cannot change the key. But in the proposed system, if the user finds that their key has been mishandled user can send a request to the admin for a key. In order to maintain the data integrity, the files stored in the server can be audited by the TPA. Here TPA will have the hash values of file using that TPA will audit the files, whether the files stored in the server are modified intentionally or unintentionally by the users or unauthorized users. In the existing system if the TPA finds the modified file, but he cannot block that file. But in the proposed system TPA can block the modified file, so that other users in the group cannot view the modified file. Here the user can be tracked so that one who modifies the files can be identified. And if they are an unauthorized user TPA will send a notification to the admin so that admin can block them using their IP Address.

Future Work

In future the TPA can audit multiple files simultaneously. And then auditing can be in the form of Batching Auditing. Efficiency of the auditing can be increased by using Bi-linear Aggregate Algorithm it can be achieved. In the proposed system the files which got modified can be blocked, but in future those files can be retrieved using some techniques.

References

1. Jiangtao Li, Lei Zhang, Joseph K. Liu, Haifeng Qian, and Zheming Dong. Privacy-preserving public auditing protocol for low performance end devices in cloud. *IEEE Transactions on Information Forensics and security, 2016.*
2. G.Ateniese, R.D.Pietro, L.V.Mancini, and G.Tsudik. Public auditing for shared data with efficient user revocation in the cloud. *4th International Conference Secure and Privacy in Communication Network, pages 110, 2008.*

3. Mehul A. Shah, Ram Swaminathan, and Mary Baker. Privacy-preserving audit and extraction of digital contents. *The Third Information Systems International Conference.*
4. H. Shachum and B. Waters. Compact proofs of retrievability. *Proceeding in, ASIACRYPT vol. 350, 2008.*
5. Lanxiang Chen. Using algebraic signatures to check data possession in cloud storage. *Vol. 29, pages 1709-1715, 2013.*

How to cite this article:

Kousalya R *et al* (2018) 'Privacy Preserving Public Auditing for Shared Data in Distributed Environment', *International Journal of Current Advanced Research,* 07(3), pp. 10718-10720. DOI: http://dx.doi.org/10.24327/ijcar.2018.10720.1830

****