Enabling Authorized Encrypted Search for Secure Cloud Computing

S.Jagadesan[1], S.Jagan[2], N.K.Madhinilavan[3], K.Naveenkumar[4], Ms K.Karthika[5] ,

UG Students [1,2,3,4], Assistant Professor[5],

Department Of Information Technology[1,2,3,4,5],

Adhiyamaan College Of Engineering(Autonomous), Hosur, Tamilnadu, India.

ABSTRACT:

Utilizing distributed storage administrations, clients can store their information in the cloud to maintain a strategic distance from the use of nearby information stockpiling furthermore, support. To guarantee the honesty of the information put away in the cloud, numerous information respectability examining plans have been proposed. In most, if not all, of the current plans, a client needs to utilize his private key to produce the information authenticators for understanding the information respectability examining. In this way, the client needs to have an equipment token (for example USB token, keen card) to store his private key and retain a secret key to enact this private key. On the off chance that this equipment token is lost or this secret key is overlooked, the vast majority of the current information honesty reviewing plans would be not able to work.

So as to defeat this issue, we propose another worldview called information honesty inspecting without private key stockpiling and structure such a plan In this scheme, we use biometric data as the user's fuzzy private key to avoid using the hardware token. Meanwhile, the scheme can still effectively complete the data integrity auditing.

1. INTRODUCTION:

Numerous information respectability examining plans have been proposed topermit either the information proprietor or the Third Party Auditorto check whether the information put away in the cloud is unblemished or not.

These plans centre around various parts of information trustworthiness evaluating, for example, information dynamic activity the protection security of information and client personality's key presentation flexibility the disentanglement of endorsement the board furthermore, security saving authenticators and so forth. In the above information respectability examining plans, the client needs to produce authenticators for information obstructs with his private key. It implies that the client needs to store and deal with his private key in a safe way.

The data sharing is used widely in cloud storage scenarios. To protect the identity privacy of user. Based on the identity-based setting, we constructed a cloud storage auditing scheme for shared data supporting real efficient user revocation. To realize the data sharing with sensitive information hiding and designed an identity-based cloud storage auditing scheme for shared data. However, all of existing remote data integrity auditing schemes do not take the problem of private key storage into account. In this paper, we explore how to achieve data integrity auditing scheme without private key storage for secure cloud storage.

To help client communications including information alteration, inclusion and cancellation. We developed a powerful information honesty inspecting plan by abusing the record hash tables additionally considered the issue of information elements in information respectability examining and structured an information uprightness evaluating plan supporting information dynamic activities dependent on the Divide and Conquer Table. In open information respectability evaluating, the TPA may determine the substance of client's information by testing similar information hinders on various occasions. To secure the information protection, Wang abused the arbitrary concealing method to build the primary open information respectability inspecting plan supporting security saving. Li et proposed an information honesty inspecting plan which jam information security from the TPA. Yu proposed a distributed storage inspecting plan with flawless information security protecting by utilizing zero-information evidence. To assuage the client's calculation weight of authenticator age, Guan developed an information uprightness reviewing plan utilizing vagary muddling system, which decreases the overhead for creating information authenticators.

2. LITERATURE SURVEY:

1. TITLE: RESEARCH IN CLOUD SECURITY: PROBLEMS AND PROSPECTS

Author: VAISHALI SINGH

ABSTRACT:

Distributed computing keeps on being bragged as a significant leap forward in IT the board. With the fast development just as request of Cloud registering, the significant concern is on its security and protection, which is controlled by the strategies, controls and advances expected to ensure the information, applications, and the related framework of Cloud figuring. These difficulties force a few new research inquiries to the examination network to guarantee legitimate security of the IT foundation. The objective of this undertaking is to give the ongoing headways and an expansive diagram of the current writing covering different components of the Cloud security. The paper additionally remembers different headings for future research for Cloud security dependent on the related distributed work and industry patterns.

2TITLE: Dynamic and Public Auditing with Fair Arbitration for Cloud Data

Author: SAJJA SUNEEL

ABSTRACT:

Storage outsourcing turned into a rising trend with the advent of the cloud computing, advancing the secure remote data auditing to be the future research area. Other than this research considers the problem of data dynamics support, public verifiability and dispute arbitration simultaneously. The information elements issue in reviewing is understood by introducing a list switcher to save a mapping between square files and label files and destroy the aloof result of square files in the label calculation without acquiring a lot of overhead. We give decency assurance and question discretion in our plan, which guarantees that both the information proprietor and the cloud can't get rowdy in the reviewing procedure or, more than likely it is simple for an outsider judge to discover the swindling party. The system is connecting by executing the information progressively and sensible caution on social events later on.

3.TITLE: Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds

Author: Yan Zhu

ABSTRACT:

In this project, we propose a dynamic audit service for verifying the integrity of untrusted and outsourced storage. Our audit service, constructed based on the techniques, fragment structure, random sampling and index-hash table, can support provable updates to outsourced data, and timely abnormal detection. In addition, we propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. Our experimental results not only validate the effectiveness of our approaches, but also show our audit system has a lower computation overhead, as well as a shorter extra storage for audit metadata.

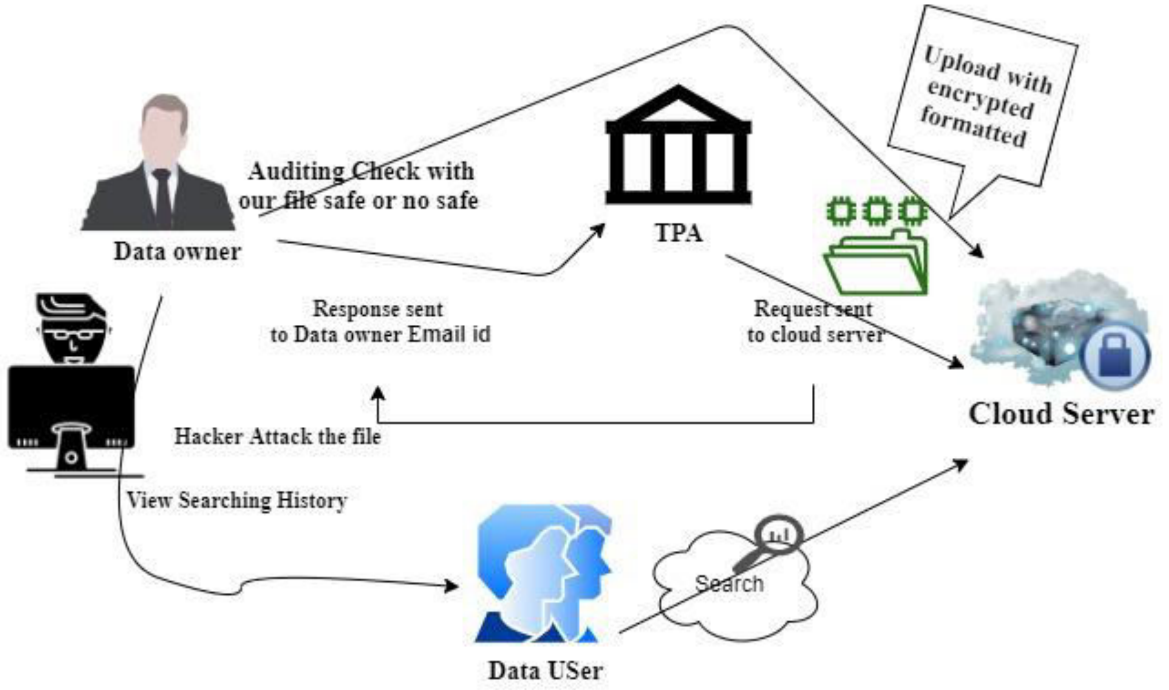
3. EXISTING SYSTEM:

Existing system isin order to verify the integrity of the data stored in the cloud many remote data integrity auditing schemes has been proposed. To reduce the computation burden on the user side, a Third-Party Authority. is introduced to periodically verify the integrity of the cloud data on behalf of user. In order to protect the data is privacy. The problem of verifying is if an un-trusted server stores a client's data. We introduced a model for provable data possession, in which it is desirable to minimize the file block accesses, the computation on the server, and the client server communication.

4. PROPOSED SYSTEM:

In this project we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. Our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. The proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.An identity-based data integrity auditing scheme for secure cloud storage, which is supports data sharing with sensitive information hiding. In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed.

5. SYSTEM ARCHITECTURE:


Upload with encrypted formatted
Auditing Check with our file safe or no safe
Data owner
TPA
Response sent to Data owner Email id
Request sent to cloud server
Cloud Server
Hacker Attack the file
View Searching History
Search
Data USer

6. MODULE DESCRIPTION:

In this project we have 5 modules,

6.1. **Data Owner (n- number of data owners)**

→**Register:**Data owner have to register first.

→**Login:**The Data owners has to Login into the account after successful Login.-→**Upload Files:**Upload the files to the cloud by using Homomorphic Algorithm. At the time of file uploading automatically file public key was generated by using fuzzy logic.

→**View all Files:**View all uploaded files by them

→**Auditing Files:**Sends the auditing request (check our file is safe or not) to the TPA.

→**Logout:**The Data owner can Logout.

6.2. Data User (n- number of data users)

→**Register:**User have to register our details with bio-metric (fingerprint) technique.

→**Login:**In user login module have 3-steps verifications

1) The 1st step is only authorized users can able to login our account.

2) The 2nd step is user have to enter our username and password.

3) The 3rd step is user can get the OTP to our registered mail and 3-step is bio-metric verification.

→**Search Files:** Search the files by keyword and k value..

- User can get the top-k files
- Send the file private key request to TPA.

→**Download Files:**Using file private key user can download the files in decrypted format.

→**Logout:** The Data user can Logout

6.3. TPA(Trust Party Authorized)

→Login: The TPA Login with username and Password.

→ Send key to the users

→ Sends the file private key to user's registered mail id.

→ Forward auditing request to cloud server

→Logout

6.4. Attacker

→ **Login:** The acttacker logins into the Websites.

→**Attack Files:** Attack the files uploaded by the data owner.

→**Logout**

6.5. Cloud Server

→**Login:** Only Authorized users Can Login to the Cloud Sever and cloud accept the new user for login.

→**View Auditing Request:** Check the file is safe are not .and send the status to the file's owner mail.

→**View Attacked Files**: View all attacked files and View all uploaded Files and view all registered owners and users.

→**Result:** View the result in graph format.

1. File request based

2. Total Number of Files Uploaded in the Cloud (count of individual Files)

→**Logout:**

7.CONCLUSION:

In this project, we explore how to employ fuzzy private key to realize data integrity auditing without storing private key. propose the first practical data integrity auditing scheme without private key storage for secure cloud storage. In the proposed scheme, we utilize biometric data (e.g. fingerprint, iris scan) as user's fuzzy private key to achieve data integrity auditing without private key storage. In addition, we design a signature scheme supporting block less verifiability and the compatibility with the linear sketch. The formal security proof and the performance analysis show that our proposed scheme is provably secure and efficient.

8. REFERENCE:

[1] H. Dewan and R. C. Hansdah, "A survey of cloud storage facilities," in 2011 IEEE World Congress on Services, July 2011, pp. 224–231.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.

[3] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, March 2015.

[4] N. Garg and S. Bawa, "Rits-mht: Relative indexed and time stamped merkle hash tree based data auditing protocol for cloud computing," Journal of Network & Computer Applications, vol. 84, pp. 1–13, 2017.

[5] H. Jin, H. Jiang, and K. Zhou, "Dynamic and public auditing with fair arbitration for cloud data," IEEE Transactions on Cloud Computing, vol. 13, no. 9, pp. 1–14, 2014.

[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.

[7] B. Wang, B. Li, and H. Li, "Knox: privacy-preserving auditing for shared data with large groups in the cloud," in International Conference on Applied Cryptography and Network Security, 2012, pp. 507–525.