Securing Outsourced Storages in Clouds

Gowsalya. K *, Sumathi R.
Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

Article Info
Article history:
Received 2 February 2015
Received in revised form
20 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords
River Ramganga,
TDS,
EC,
Discrete Meyer Wavelet

Abstract

With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. However, public auditing for such shared data - while preserving identity privacy - remains to be an open challenge. The traditional approach developed a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. This audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. This method based on probabilistic query and periodic verification for improving the performance of audit services. The audit service is performed by TPA monitoring. Sometimes the TPA may have chances to hide anomaly details to cloud users. To overcome this drawback, we propose dynamic audit service in the cloud. By this method we can dynamically audit the anomaly and send intimation to cloud user. So that we can secure the cloud storage data

1. Introduction

The cloud storage service (CSS) relieves the burden for storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to the clients because their data or archives are stored in an uncertain storage pool outside the enterprises. These security risks come from the following reasons: First, the cloud infrastructures are much more powerful and reliable than personal computing devices, but they are still susceptible to internal threats (e.g., via virtual machine) and external threats (e.g., via system holes) that can damage data integrity; second, for the benefits of possession, there exist various motivations for cloud service providers (CSP) to behave unfaithfully toward the cloud users; furthermore, disputes occasionally suffer from the lack of trust on CSP because the data change may not be timely known by the cloud users, even if these disputes may result from the users' own improper operations. Therefore, it is necessary for CSP to offer an efficient audit service to check the integrity and availability of stored data.

2. Existing System

We believe that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. So existing work introduced a dynamic audit service for integrity verification of untrusted and outsourced storages. Constructed on interactive proof system (IPS) with the zero knowledge property, our audit service can provide public auditability without downloading raw data and protect privacy of the data. It also developed an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof-of-concept prototype is also implemented to evaluate the feasibility and viability of our approaches. The experimental results not only validate the effectiveness of our approaches, but also show that our system does not create any significant computation cost and require less extra storage for integrity verification. This method also has one drawback that is named as TPA monitoring.

Corresponding Author,
E-mail address: kgowsalyait@gmail.com

2.1 Disadvantages

- It requires external TPA monitoring
- No Secure

3. Proposed System

To create a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. We propose dynamic audit service with Efficient SHA-2 Algorithm. In this method user sent query request to server and that server matches the user query and keyword if it is match, user can proceed the process otherwise, the user is automatically/dynamically marked as untrusted and sends intimation about anomaly detection to cloud user by server. So it's able to verify the integrity of shared data for a group of users without retrieving the entire data — while the identity of the signer on each block in shared data is kept private from the TPA.

3.1 Advantages

- No need Extra TPA
- Secure and Effective

4. Modules

- Authentication
- Cloud Storage
- Auditing
- Secure Notification
- Performance & Evaluation

4.1 Authentication

Authorization is the process of giving user permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, time access, maintain history, and so forth). Assuming that someone has

logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten.

4.2 Cloud Storage

We utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique; we can upload and download and view our data into and from the cloud for privacy, to achieve a public auditing system for cloud data storage security while keeping all above requirements in mind.

4.2.1 Authenticable Ring Signatures

We introduce a new ring signature scheme, which is suitable for public auditing. We intend to utilize ring signatures to hide the identity of the signer on each block, so that private and sensitive information of the group is not disclosed to the TPA.

4.3 Auditing

With the establishment of auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

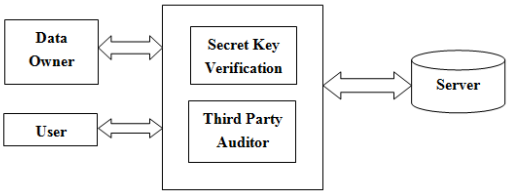
4.4 Secure Notification

Detection and notification refers to automatic detection of changes made to User pages and notification to interested users by Cloud Server or other means. Whereas search engines are designed to find User pages, detection and notification systems are designed to monitor changes to User pages. Efficient and effective change detection and notification is hampered by the fact that most servers do accurately track content changes through Modified.

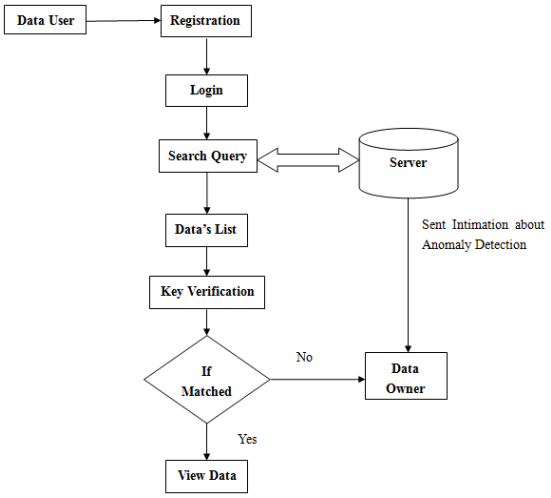
4.5 Performance and Evaluation

To detect anomalies in a low-overhead and timely manner, we attempt to optimize the audit performance from two aspects: Performance evaluation of probabilistic queries and scheduling of periodic verification. Our basic idea is to maintain a tradeoff between overhead and accuracy, which helps us improve the performance of audit systems.

5. Architecture Diagram



6. User Process



7. Conclusion

In this paper, we created a new privacy preserving public auditing mechanism for shared data in an untrusted cloud and we proposed a dynamic audit service with Efficient SHA-2 Algorithm. By this method we can dynamically audit the anomaly and send intimation to cloud user. So that we can secure the cloud storage data.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, A View of Cloud Computing, Communications of the ACM, 53(4), 2010, 50–58

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, Provable Data Possession at Untrusted Stores, in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, 598–610

[3] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, 525–533

[4] R. L. Rivest, A. Shamir, Y. Tauman, How to Leak a Secret, in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer- Verlag, 2001, 552–565

[5] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and Verifiably Encrypted Signatures from

Bilinear Maps, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Springer-Verlag, 2003, 416–432

[6] H. Shacham, B. Waters, Compact Proofs of Retrievability," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Springer-Verlag, 2008, 90–107

[7] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, S. S.Yau, Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, 1550–1557

[8] S. Yu, C. Wang, K. Ren, W. Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, 534–542

[9] D. Boneh, B. Lynn, H. Shacham, Short Signature from the Weil Pairing," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, 514–532

[10] D. Boneh D. M. Freeman, Homomorphic Signatures for Polynomial Functions, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2011, 149–168