SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY

Full Length Article

ENABLING USER REVOCATION IN IDENTITY BASED CLOUD STORAGE AUDITING USING VISUAL CRYPTOGRAPHY

[a] D. Lavanya , [b] S. Pavithra, [b] V. Preetha, [b] K. Vinethkumar

[a] Assistant Professor(Sr.Gr),Department of Computer Science and Engineering, Vellalar college of Engineering and Technology, Erode, Tamilnadu, India

[b] Student, Department of Computer Science and Engineering, Vellalar college of Engineering and Technology, Erode, Tamilnadu, India

* Corresponding Author

(D. Lavanya)

ABSTRACT: Cloud computing is concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage is managed. In this paper, we focus on designing a cloud storage system for robustness, confidentiality, and functionality. A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. It is very robust because the message can be retrieved as long as one storage server survives. Another way is to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message, each of its codeword symbols is stored in a different storage server.

1 Introduction

The data storage and sharing services provided by the cloud, people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing would like to utilize cloud data for particular purposes (TPA) who is able to provide verification services on data integrity to users. Most of the previous works focus on auditing the integrity of personal data. Different from these works, several recent works focus on how to preserve identity

SYSTEM ANALYSIS:

Existing System:

Although the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting data dynamics has not been fully addressed. How to achieve secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task. In Existing the document or file which is being stored by client in the cloud computing means that was stored entirely due to this someone can able to hack that so, hacker can able to see all the information’s of the uploaded file.

DISADVANTAGE:

Especially to support block insertion, which is missing in most existing schemes. Authentication was provided only at the time of upload not at the time of download. For auditing in existing scheme we are using private auditing due to this we don’t need to appoint a person to verify that.

PROPOSED SYSTEM:

Here we are providing better security in owner's upload side as well as on the download side. For better security client splitting that single file into nine different blocks and providing a unique identification number for each block. Using Honor Algorithm we are converting a block tag into secret value using ASCII value.

Client: An entity, which has large data files to be stored in the cloud computing and relies on the cloud computing for data maintenance and computation, During login for a client here an OTP was generated and that was sent to the registered mail id using that OTP only a client can login.

Trusted Party Auditor (TPA): We are using a public auditing in proposed an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud computing storage services on behalf of the clients upon request. For better security we are using an AES algorithm 128 bit to provide security. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file.

In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

ADVANTAGE:

1) We motivate the public auditing system of data storage security in Cloud computing, and dynamic data operations, especially to support block insertion, which is missing in most existing schemes.

2) We extend our scheme to support scalable and efficient public auditing in Cloud computing. In particular, our scheme achieves auditing tasks from different users can be performed simultaneously by the TPA.

3) Spitted into blocks and it is uploaded in the cloud computing for better security.

4) We prove the security of our proposed construction and justify the performance of our scheme through concrete implementation and comparisons.

MODULES DESCRIPTION :

1. User interface

2. Mail alert process

3. File Retrieval and Error Recovery and Batch Auditing for Multi-client Data

4. Verification phase

5. Trusted Party Auditing

CONCLUSION :

Assumptions and without random oracles, and with short group signatures. Even less ambitious would be an efficient scheme that supports some subset of these properties (e.g., a fully dynamic scheme with a group manager) but meets the strongest definitions of security, as the only schemes we have seen that come close to achieving this level of edibility provide only CPA-style anonymity. we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner.

REFERENCES :

[1] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[2] B. Wang, B. Li, and H. Li, “Privacy-Preserving Public Auditing for Shared Data in the Cloud,” In Proc. of IEEE Cloud 2012, pp. 295-302, 2012.

[3] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,” In Proc. of International Conference on Applied Cryptography and Network Security, pp. 507-525, 2012.

[4] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao. “Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability,” Journal of Systems and Software, vol. 113, pp. 130-139, 2016.

[5] B. Wang, B. Li, and H. Li, “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, 2015.