isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Apr,2023,ISSN_NO: 2321-3337

DATA INTEGRITY AUDITING WITHOUT PRIVATE KEY STORAGE FOR SECURE CLOUD STORAGE

Deva.H[1], Dinesh Babu.S[2], Pavan Kumar.B[3], Malathi.S[4]

UG Scholar[1 2 3] –Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, India.

Assistant Professor[4] - Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, India

devab7183@gmail.com, umameenaselvam8172@gmail.com, pavanjanakib@gmail.com, malathi.s@grt.edu.in

Abstract **-** Utilizing distributed storage administrations, clients can store their information in the cloud to maintain a strategic distance from the consumption of nearby information stockpiling also, support. To guarantee the honesty of the information put away in the cloud, numerous information uprightness evaluating plans have been proposed. In most, if not all, of the current plans, a client needs to utilize his private key to create the information authenticators for understanding the information honesty inspecting. Therefore, the client needs to have an equipment token (for example USB token, shrewd card) to store his private key and remember a secret phrase to actuate this private key. On the off chance that this equipment token is lost or this secret phrase is overlooked, the majority of the current information honesty inspecting plans would be not able work. So as to defeat this issue, we propose another worldview called information uprightness examining without private key stockpiling and structure such a plan. In this plan, we use biometric information (for example iris check, unique mark) as the client's fluffy private key to abstain from utilizing the equipment token. In the interim, the plan can in any case adequately complete the information honesty auditing. We use a straight sketch with coding and blunder remedy procedures to affirm the personality of the client. What's more, we structure another mark plot which supports blockless undeniable nature, yet in addition is perfect with the straight sketch. The security evidence and the execution examination demonstrate that our proposed plan accomplishes alluring security and productivity.

1. INTRODUCTION

In cloud data integrity auditing schemes, the data owner firstly needs to provide security key for file before uploading them to the cloud. This key is useful for the cloud audit while updating files in it. These signatures are used to prove that the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner upload these data blocks along with their corresponding signatures to the cloud. By compressing the files in the cloud will improve the storage efficiency. With the help of compressed files stored in the cloud improves the efficiency. This method can ensure the sensitive information in hiding since only the data owner can decrypt this file. Every companies and individuals using the cloud to store the data. Cloud storage files will be deleted with some human errors and robots as a fault. To prevent from this kind of improper access we are using key generating center, to assign key for the security purpose. Every files has it is own integrity with the maximum data storage. Eligible category will be uploaded by the verifier. When a user wants to view and to download the files they have to get a permission from the owner. Check the data integrity in the cloud while uploading files. Files in the cloud will be not be shared if the users are untrustworthy. Every file in the cloud with the explosive growth of data, will be stored in order to present from the hackers. Cloud data integrity checking is the essential feature to develop cloud data sharing.

2. BACKGROUD

2.1 OVER VIEW OF CLOUD COMPUTING

Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

- Deployment Models
- Service Models

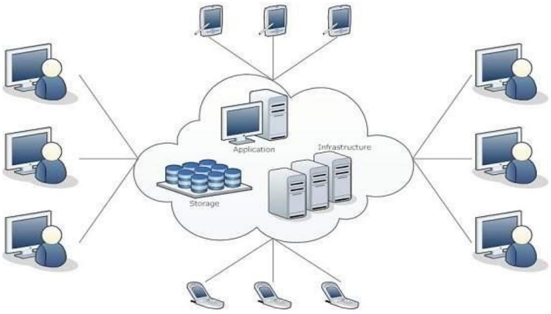


Fig2.1:Cloud Computing

Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.

Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

2.2 MICRO SOFT SQL SERVER

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet).

Microsoft markets at least a dozen different editions of Microsoft SQL Server, aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users.

Fig 2.2:Sql Server SQL Server Components

SQL Server works in client-server architecture, hence it supports two types of components − (a) Workstation and (b) Server.

- **Workstation components** are installed in every device/SQL Server operator's machine. These are just interfaces to interact with Server components. Example: SSMS, SSCM, Profiler, BIDS, SQLEM etc.

- **Server components** are installed in centralized server. These are services. Example: SQL Server, SQL Server Agent, SSIS, SSAS, SSRS, SQL browser, SQL Server full text search etc.

3. RELATED WORK

3.1 SECURELY OUTSOURCING ANALYSIS

Securely outsourcing data analysis to third-party service providers has recently grown rapidly, especially with the increasing popularity of cloud technology. For this purpose, provably secure outsourcing has attracted significant attention during past decade. For instance, Sion et al. define the requirements to build a secure outsourcing mechanism. Zhou et al. [5] propose a secure key management scheme which ensures that the source of the data can be securely accessed by different parties under different requirements. Alternatively, oblivious random access memory (ORAM) [6] aims to hide the access patterns of the users, which has been well developed on different topics [10], [7], [8], [4]. In addition, Franz et al. [10] propose a method which can make the data owner delegate rights to new clients for accessing to the outsourced data via a curious server based on ORAM. Stefanov et al. [1] propose a simple ORAM protocol with a small amount of client storage, which is formally proven to require small bandwidth and overheads.

3.2 PROPERTY PRESERVING ENCRYPTION SCHEMES

Broadly, various encryption schemes have been proposed to protect the data in different security levels, including fully homomorphic encryption (FHE) [7], [1], functional encryption [5], [3], searchable symmetric encryption [4], [6] and oblivious RAM (ORAM) [1], [4]. Moreover, there are a number of property preserving encryption schemes based on the CryptDB [6], such as order preserving encryption [1], [2] and deterministic encryption [9]. CryptoPAn [10] was proposed by Xu et al. to ensure the prefix preserving property on IP addresses from the cryptographic view. Kerschbaum [7] proposes a new order preserving encryption scheme which can hide the frequency pattern of plaintexts via randomizing the ciphertexts to mitigate frequency analysis.

3.3 INFERENCE ATTACKS

Brekne et al. [10] presents the attacks via frequency analysis to compromise IP addresses under two prefix preserving anonymization schemes. There are several works which focus on the practical attacks to the encrypted data [4], [5], [9], [6]. Naveed et al. [9] present a series of inference attacks on the property preserving encrypted database and implement the attacks on the medical databases to show the effectiveness of the attacks. Recently, Kellaris et al. [5] develop a generic reconstruction attacks on the range queries in the outsourced databases where the access patterns and communication volume are leaked.

4. PROPOSED SYSTEM

We design a practical data integrity auditing scheme without private key storage for secure cloud storage. In our scheme, two fuzzy private keys (biometric data) are extracted from the user in the phase of registration and the phase of signature generation. We respectively use these two fuzzy private keys to generate two linear sketches that contain coding and error correction processes. In order to confirm the user's identity, we compare these two fuzzy private keys by removing the "noise" from two sketches. If the two biometric data are sufficiently close, we can confirm that they are extracted from the same user; otherwise, from different users. How to design a signature satisfying both the compatibility with the linear sketch and the block less verifiability is a key challenge for realizing data integrity auditing without private key storage. In order to overcome this challenge, we design a new signature scheme named as MBLSS by modifying the BLS short signature based on the idea of fuzzy signature. We give the security analysis and justify the performance via concrete implementations. The results show that the proposed scheme is secure and efficient.

5. ARCHITECTURE DIAGRAM

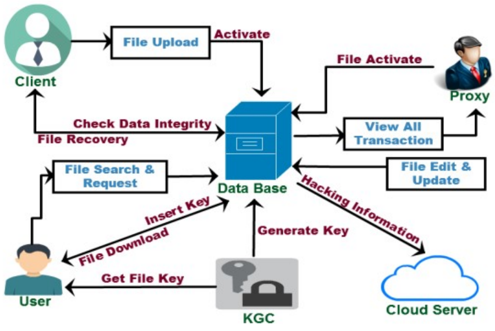


Fig5.1: Architecture Diagram

6. MODULES

6.1 FILE UPLOADING AND ACTIVATION

The data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in many cloud storage applications

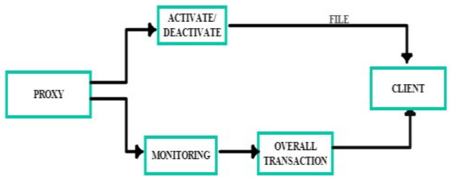


Fig6.1: File Uploading And Activation

6.2 DATA INTEGRITY AUDITING

Data integrity auditing scheme that realizes data sharing with sensitive information hiding. However, the data stored in the cloud might be corrupted or lost. Data integrity auditing on the condition that the sensitive information of shared data is protected.

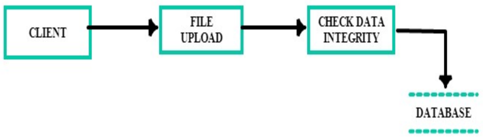


Fig6.2: Data Integrity Auditing

6.3 SENSITIVE INFORMATION SHARING

Sensitive information hiding to ensure that the personal sensitive information of the file is not exposed to the hacker, and all of the sensitive information of the file is not exposed to the cloud and the shared users. This method not only realizes the remote data integrity auditing, but also supports the data sharing on the condition that sensitive information is protected in cloud storage.

6.4 GENERATING KEY SIGNATURE

A potential method of solving this problem is to encrypt the whole shared file before sending it to the cloud, and then generate the signatures used to verify the integrity of this encrypted file, finally upload this encrypted file and its corresponding signatures to the cloud. This method can realize the sensitive information hiding since only the data owner can decrypt this file.

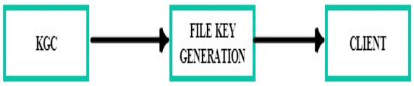


Fig6.3: Generating Key Signature

6.5 FILE SECURITY AND RECOVERY

If a file has been partially overwritten or otherwise compromised, the chances of any usable recovery are low, even with the best recovery software in the existing system. In our proposed work, we can easily recover the file while deleted files are inaccessible and are in danger of being overwritten, they can often be recovered.

7. EXPERIMENTAL RESULTS

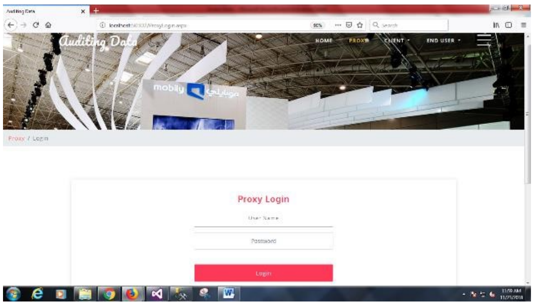


Fig 7.1: Proxy Login

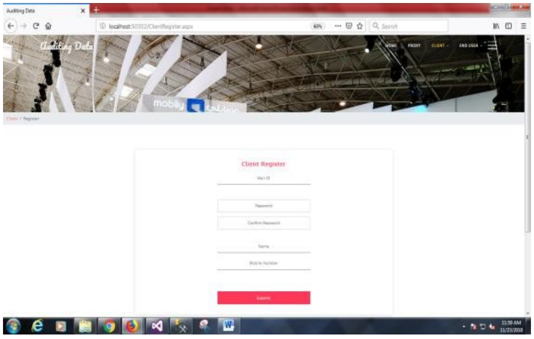


Fig 7.2: Client Register

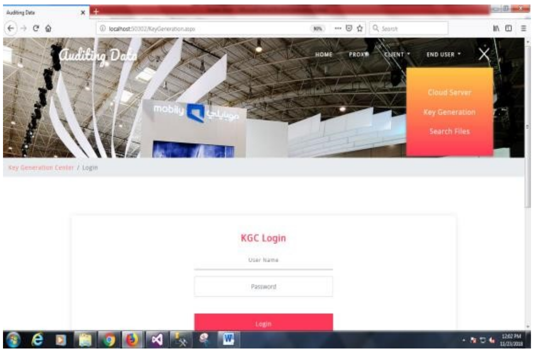
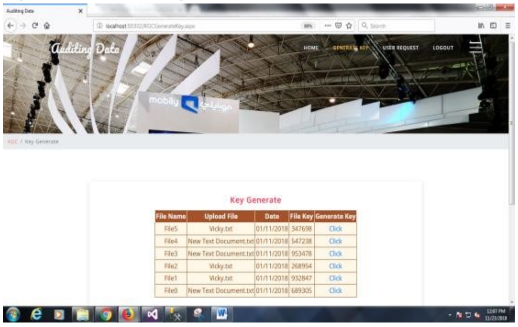


Fig 7.3: KGC Login



Key Generate

File Name	Upload File	Date	File Key	Generate Key
File5	Vicky.txt	01/11/2018	347698	Click
File4	New Text Document.txt	01/11/2018	547238	Click
File3	New Text Document.txt	01/11/2018	953478	Click
File2	Vicky.txt	01/11/2018	268954	Click
File1	Vicky.txt	01/11/2018	932847	Click
File0	New Text Document.txt	01/11/2018	689305	Click

Fig 7.4: Key Generate

8. CONCLUSION

We investigate how to utilize fluffy private key to acknowledge information honesty inspecting without putting away private key. We propose the principal handy information respectability evaluating plan without private key stockpiling for secure distributed storage. In the proposed plot, we use biometric information (for example unique mark, iris filter) as client's fluffy private key to accomplish information trustworthiness inspecting without private key stockpiling. Moreover, we structure a mark plan supporting block less certainty and the similarity with the direct sketch. The formal security confirmation what's more, the presentation investigation demonstrate that our proposed plan is provably secure and productive.

9. 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, Jan 2020.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2021, pp. 598–609.

[3] A. Juels and B. S. Kaliski, “Pors: Proofs of retrievability for large files,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2019, pp. 584–597.

[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2019.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2019.

[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. 2020.

[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, “Symmetric-key based proofs of retrievability supporting public verification,” in Computer Security – ESORICS 2021. Cham: Springer International Publishing, 2015, pp. 203–223.

[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, “Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,” Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2019.

[9] J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2019.

[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2020, pp. 1–10.