ISSN: 2366-1313

Data Integrity Auditing without Private Key Storage using Biometric image for Secure Cloud

DHANDAMUDI HAPPY BALA SOWRI [1], Dr SIKHAKOLLI GOPI KRISHNA[2]

[1]Assistant professor, [2] Professor

CSE Department, Sri *Mittapalli College* of *Engineering*, *Guntur*, *Andhra Pradesh*-522233

Abstract: By using cloud storage providers, the user can secure his information from losing while it's not being used and can stick the customers' information into the cloud. This data has to be edited to prevent breaching of the security by having an auditing system in place before putting the details in a cloud. In current work, we need users to use a private key to build authenticators that can be used while doing data integrity auditing. The consumer must carry around a hardware token (e.g. USB token, intelligent card) so that it can be used to store its private key (as well as password) and be used to unlock the key. One type of protection we currently have is that if a hardware token is missing or a password is missed, much of the present data integrity check mechanisms cannot work. In our proposed work, we are using a new model named non-private key storage data integrity audit. When we use biometric scans (e.g. iris scanner, fingerprint) on our hardware token, we convert the user's blurred private key back into the hardware token. A machine scanning the data integrity is also an effective method of data integrity auditing. Only the owner and the recipient may be allowed by the administrator to sign in to the system. There is a distance that is set between the user's fingerprint and the login, and then he / she can recover the link. As protection and efficiency needs, the security evidence and performance review demonstrates that the effective framework we have included is a final end.

I.INTRODUCTION

CLOUD storage can provide powerful and on-demand data storage services for users [1]. By using the cloud service, users can

ISSN: 2366-1313

outsource their data to the cloud without wasting substantial maintenance expenditure on hardware and in practical scenarios, which is not user-friendly. In addition, the hardware token that contains the private key might be lost. Once the password is forgotten or the hardware token is lost, the user would no longer be able to generate the authenticator for any new data block. The data integrity auditing will not be functioning as usual.

Therefore, it is very interesting and appealing to find a method to realize data integrity auditing without storing the private key. A feasible method is to use biometric data, such as fingerprint and iris scan [16, 17], as the private key. Biometric data, as a part of human body, can uniquely link the individual and the private key. Unfortunately, biometric data is measured with inevitable noise each time and cannot be reproduced precisely [18] since some factors can affect the change of biometric data. For example, the finger of each person will generate a different fingerprint image every time due to pressure, moisture, presentation angle, dirt, different sensors, and so on. Therefore, the biometric data cannot be used directly as the private key to generate authenticators in data integrity auditing. Contribution.

The contribution of this paper can be summarized as follows: We initiate the first study on how to employ biometric data as fuzzy private key to perform data integrity auditing, and propose a new paradigm called data integrity auditing without private key storage. In such a

ISSN: 2366-1313

scheme, a user utilizes biometric data as his fuzzy private key for confirming his identity. The data integrity auditing can be performed under the condition that there is not any hardware token for storing the private key. We further formalize the definition of data integrity auditing scheme without private key storage for secure cloud storage. 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

II. LITERATURE SURVEY

RESEARCH IN CLOUD SECURITY: PROBLEMS AND PROSPECTS, "VAISHALI SINGH"

Cloud computing continues to be boasted as a major breakthrough in IT management. With the rapid growth as well as demand of Cloud computing, the major concern is on its security and privacy, which is determined by the policies, controls and technologies needed to protect the data, applications, and the related infrastructure of Cloud computing. These challenges impose several new research questions to the research community to ensure proper security of the IT infrastructure. The goal of this project is to provide the recent advancements and a broad overview of the existing literature covering various dimensions of the Cloud security. The paper also includes various directions for future research in Cloud security based on the related published work and industry trends. This may be very useful, particularly for the entry level researchers, who wish to conduct the research in these related areas.

Dynamic and Public Auditing with Fair Arbitration for Cloud Data , "SAJJA SUNEEL"

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 data dynamics problem in auditing is solved by presenting an index switcher to preserve a mapping between block indices and tag indices and eradicate the passive outcome of block indices in the tag computation without incurring much overhead. We provide fairness guarantee and dispute arbitration in our scheme, which ensures that both the data owner and the cloud cannot misbehave in the auditing process or else it is easy for a third-party arbitrator to find out the cheating party. The

ISSN: 2366-1313

framework is reaching out by executing the data dynamically and reasonable discretion on gatherings in the future.

III. SYSTEM ANALYSIS

EXISTINGSYSTEM

- Ateniese et al. [19] firstly proposed the notion of Provable Data Possession (PDP). They employed the random sample technique and homomorphic linear authenticators to design a PDP scheme, which allows an auditor to verify the integrity of cloud data without downloading the whole data from the cloud. Juels and Kaliski [20] proposed the concept of Proof of Retrievability (PoR). In the proposed scheme, the errorcorrecting codes and the spot-checking technique are utilized to ensure the retrievability and the integrity of the data stored in the cloud. Shacham and Waters [21] constructed two PoR schemes with private verifiability and public verifiability by using pseudorandom function and BLS signature.
- To support user-interactions, including data modification, insertion and deletion, Zhu et al. [22] constructed a dynamic data integrity auditing scheme by exploiting the index hash tables. Sookhak et al. [23] also considered the problem of data dynamics in data integrity auditing and designed a data integrity auditing scheme supporting data dynamic operations based on the Divide and Conquer Table. In public data integrity auditing, the TPA might derive the contents of user's data by challenging the same data blocks multiple times. To protect the data privacy, Wang et al. [24] exploited the random masking technique to construct the first public data integrity auditing scheme supporting privacy preserving.
- Li et al. [25] proposed a data integrity auditing scheme which preserves data privacy from the TPA. Yu et al. [26] proposed a cloud storage auditing scheme with perfect data privacy preserving by making use of zero-knowledge proof. To relieve the user's computation burden of authenticator generation, Guan et al. [27] constructed a data integrity auditing scheme using indistinguishability obfuscation technique, which reduces the overhead for generating data authenticators. Li et al. [28] proposed a data integrity auditing scheme which contains a cloud storage server and a cloud audit server. In this scheme, the cloud audit server helps user to generate data authenticators before uploading data to the cloud storage server. Shen et al. [29] designed a light-weight data integrity auditing scheme, which introduced a Third Party Medium to generate authenticators and verify data integrity on behalf of users.
- The data sharing is used widely in cloud storage scenarios. To protect the identity privacy of user, Wang et al. [30] proposed a shared data integrity auditing scheme based on the ring signature. Yang et al. [31] designed a remote data integrity auditing scheme for shared data, which supports both the identity privacy and the identity traceability. By using the homomorphic verifiable group signature, Fu et al. [32] proposed a privacy-aware remote

ISSN: 2366-1313

data integrity auditing scheme for shared data.

- In order to achieve efficient user revocation, Wang et al. [33] designed a shared data integrity auditing scheme supporting user revocation by making use of the proxy re-signature. Based on the identity-based setting, Zhang et al.
  [34] constructed a cloud storage auditing scheme for shared data supporting real efficient user revocation. To realize the data sharing with sensitive information hiding, Shen et al. [35] designed an identity-based cloud storage auditing scheme for shared data.

Disadvantages

- In the existing work, there are no accurate data integrity proof results.
- The system's security is very less due to lack of BLS Short Signature for data blocks.

PROPOSED SYSTEM

- The system designs 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 blockless 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.

Advantages

- An affective technique to ensure that when the cloud properly stores users' data, the proof it generates can pass the verification of the TPA.
- An efficient technique to assure that if the cloud does not possess users' intact data, it cannot pass the verification of the TPA.
- Secure and efficient techniques to allow the user to utilize biometric data as fuzzy private key to accomplish data integrity auditing without private key storage.

IV. MODULES DESCRIPTION DATA OWNER

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Upload File with Blocks, View All Upload File with Blocks, Perform Data Integrity Auditing, View Transactions.

ISSN: 2366-1313

CLOUD SERVER

In this module the cloud will authorize both the owner and the user and also performs the following operations such as View and Authorize Users, View and Authorize Owners, View All File's Blocks, View All Transactions, View All Attackers, View Time Delay Results, View Throughput Results

TPA

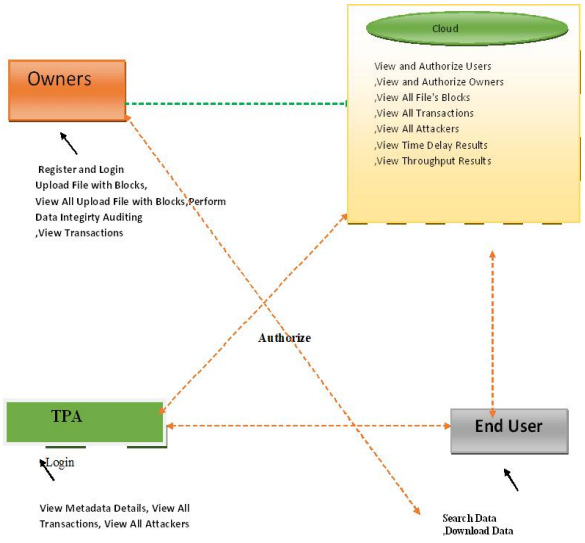
In this module, the TPA performs the following operations such as View Metadata Details, View All Transactions, View All Attackers

DATA USER

In this module, the user has to register to cloud and log in and performs the following operations such as Search Data, Download Data.

SYSTEM DESIGN

Architecture Diagram



V. CONCLUSIONS

In this thesis, we explore how to employ fuzzy private key to realize data integrity auditing without storing private key. We 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.

REFERENCES

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

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

[3] A. F. Barsoum and M. A. Hasan, "Provable multicopydynamic 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 andtime stamped merkle hash tree based data auditingprotocol for cloud computing," Journal of Network &Computer Applications, vol. 84, pp. 1–13, 2017.

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

[6] S. G. Worku, C. Xu, J. Zhao, and X.He, "Secure andefficient privacy-preserving public auditing scheme forcloud storage,"

ISSN: 2366-1313

Comput.Electr. Eng., vol. 40, no. 5, pp.1703–1713, Jul. 2014.
[7] B. Wang, B. Li, and H. Li, "Knox: privacy-preservingauditing for shared data with large groups in the cloud,"in International Conference on Applied Cryptographyand Network Security, 2012, pp. 507–525.
[8] B. Wang, H. Li, and M. Li, "Privacy-preserving publicauditing for shared cloud data supporting groupdynamics," in 2013 IEEE International Conference onCommunications (ICC), June 2013, pp. 1946–1950.
[9] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enablingcloud storage auditing with key-exposure resistance,"IEEE Transactions on Information Forensics and Security,vol. 10, no. 6, pp. 1167–1179, 2015.
[10] J. Yu, K. Ren, and C. Wang, "Enabling cloud storageauditing with verifiable outsourcing of key updates,"IEEE Transactions on Information Forensics and Security,vol. 11, no. 6, pp. 1362–1375, June 2016.
[11] J. Yu and H. Wang, "Strong key-exposure resilient auditingfor secure cloud storage," IEEE Transactions onInformation Forensics and Security, vol. 12, no. 8, pp.1931–1940, Aug 2017.