IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"CLOUD DATA SECURITY" USING DATA INTEGRITY AUDITING SCHEMES WITH BIOMETRIC DATA UTILIZATION

Amrapali G Gund, PG student

Computer Science & Engg Department, N.B.Navale Sinhagad College of Engineering University

Abstract: Cloud is a service model to provide facility to user for store data in the cloud for avoids the expenditure of local data storage and maintenance. So many data integrity auditing scheme have been proposed for ensure the integrity of the data stored in the cloud. In the existing system the process of data integrity auditing scheme users requires the private key to generate data authentication. For storing the private key user will require hardware token (e.g. USB token, sensor card) and memorize a password for activate this private key. If this hardware token is lost or this password is forgotten most of the current data integrity auditing schemes would be unable to work. To solve this problem we proposed a new paradigm called data integrity auditing without private key storage and design such a scheme.

In the proposed system to use biometric data (e.g. iris scan, fingerprint) as the users fuzzy private key to avoid using the hardware token, to confirm the identity of the users we can utilize a linear sketch with coding and error correction process .in addition we can design a new signature scheme which not only supports blockless verifiability but also compatible with the linear sketch. The proof of safety and performance analysis show that our proposed scheme achieves security and efficiency.

Index Terms - **Cloud storage, Data integrity auditing, Data security, Biometric data**

I.INTRODUCTION

CLOUD storage can provide powerful and on-demand data storage services for users. By using the cloud service, users can outsource their data to the cloud without wasting substantial maintenance expenditure of hardware and software, which brings great benefits to users. However, once the users upload their data to the cloud, they will lose the physical control of their data since they no longer keep their data in local. Thus, the integrity of the cloud data is hard to be guaranteed, due to the inevitable hardware/software failure sand human errors in the cloud. Many data integrity auditing schemes have been proposed to allow either the data owner or the Third Party Auditor (TPA)to check whether the data stored in the cloud is intact or not. A feasible method is to use biometric data, such as finger-print and iris scan , 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 within evitable noise each time and cannot be reproduced precisely 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. 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.

.

II.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.

A.**PROPOSED SYSTEM ARCHITECTURE**

fig.1 system model of our data integrity auditing

The system model shown in Fig. 1 consists of users, clouds, and TPAs. The cloud has a lot of storage space accessible for customers to store their data in. There are a lot of files that need to be uploaded to the cloud by the end user. TPAs are public verifiers that are entrusted with assuring the integrity of data that is stored in a cloud service. During the registration procedure for the cloud storage service, the user's biometric data (such as a fingerprint) is collected. A biometric key generated from previously acquired data is used to generate a random signing key before data is uploaded to the cloud for safekeeping and access by authorized users. The owner of the data then generates data block authenticators using his signing key. They are uploaded to the cloud and deleted from local storage after he completes this step. For data integrity audits, the TPA employs challenge-response protocols to verify that the cloud is protecting the integrity of its users' personal information.

B. Design Goals

To enable data integrity auditing without private key storage for secure cloud storage, our scheme should achieve the following goals:

1) Auditing correctness: to ensure that when the cloud properly stores users' data, the proof it generates can passthe verification of the TPA.
2) Auditing soundness: to assure that if the cloud does not possess users' intact data, it cannot pass the verification of the TPA.
3) Auditing without private key storage: to allow the user to utilize biometric data as fuzzy private key to accomplish data integrity auditing without private key storage.

III. BACKGROUND

A. 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 Mode
- Service Models

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)

IV.ALGORITHM

A fuzzy signature scheme which is associated with a fuzzy key setting FKS = ((d, Y), γ, ε, Ω, θ) includes the following four algorithms:

a) Setup: The fuzzy key setting description FKS and a security parameter k are entered into the setup procedure (k defines the threshold value ε of FKS), and a public parameter pp is generated.

b) KeyGen: The public parameter pp and biometric data are inputs to the algorithm that generates the key y ∈ Y, verifies the key and produces a new one vk

c) SigGen: Biometric data and a public parameter pp are used as inputs to the signature creation method. y 0 ∈ Y and a data block mi , and generates the signature σi of mi

d) Verify: The method requires a public parameter pp, a verification key vk, a data block mi, and the signature as input σi of mi , and returns 1 or 0 to prove the signature σi is valid or not.

V.PRELIMINARIES

A. Fuzzy Signature

The concept of fuzzy signature was proposed in [37]. It usesbiometric data as private key, such as iris scan and fingerprint,to generate the signature. The biometric data **y** is a feature vector [38] which is defined as an n-dimensional vector in ourscheme.

Fig. 2 presents the architecture of fuzzy signature. In a fuzzy signature scheme, the key generation algorithm KeyGen takes the biometric data **y** as input, and generates a verification key vk. The signature generation algorithm SigGen takes as input the biometric data $\mathbf{y}'$ and a data block m_i, and generates the signature σ_i of m_i. The verification algorithm Verify takes as input the verification key vk, the data block m_i and the signature σ_i, and verifies whether the signature σ_i is valid or not. If the biometric data $\mathbf{y}'$ is sufficiently close to the biometric data **y**, it means that $\mathbf{y}'$ and **y** are extracted from the same user. Thus, the signature σ_i is valid; otherwise, it isinvalid

1 FORMALIZATION OF FUZZY KEY SETTING

In a typical biometric authentication scheme [39], bio- metric data $\mathbf{y} = (y_1, ..., y_n) \in \mathbf{Y}$ (**Y** is the metric space including all possible biometric data **y**) is extracted from a user in the phase of registration. In the phase of authen-tication, biometric data $\mathbf{y}' = (y_1', ..., y_n')$ **Y** is extracted from a user. If $\mathbf{y}'$ is sufficiently close to **y**, we can conclude that the user who generated the biometric data $\mathbf{y}'$ and the user who generated the biometric data **y** are the same user;otherwise, they are different users.

2 DEFINITION OF FUZZY SIGNATURE

A fuzzy signature scheme which is associated with a fuzzy key setting FKS = ((d, **Y**), γ, ε, Ω, θ) includes the following four algorithms:

a) Setup: The setup algorithm takes as input the description of the fuzzy key setting FKS and a security parameter k (kdetermines the threshold value ε of FKS), and generatesa public parameter pp.

b) KeyGen: The key generation algorithm takes as inputthe public parameter pp and biometric data **y** **Y**, and generates a verification key vk.

c) SigGen: The signature generation algorithm takes as input a public parameter pp, biometric data $\mathbf{y}'$ **Y** and adata block m_i, and generates the signature σ_i of m_i.

d) V erify: The verification algorithm takes as input a public parameter pp, a verification key vk, a data block m_i andthe signature σ_i of m_i, and returns 1 or 0 to prove thesignature σ_i is valid or not.

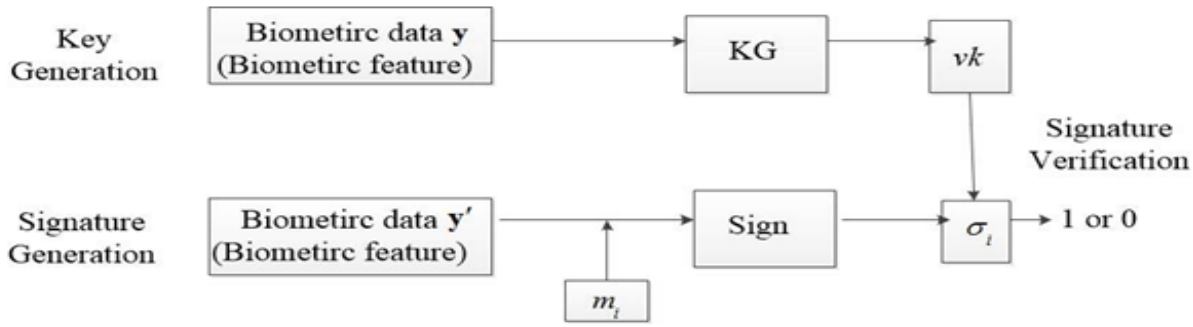

Fig. 2. The architecture of fuzzy signature

B. Linear sketch

Let FKS = ((d, **Y**), γ, ε, Ω, θ) be a fuzzy key setting defined previously. We design a linear sketch scheme whichis used to code and correct the error. This scheme is similarto the one-time pad encryption scheme. In a one-time pad encryption scheme, a plaintext m's ciphertext c with a key skis calculated as c = m + sk. The one-time pad encryption scheme satisfied the following property. For two ciphertextsc = m + sk and c′ = m′ + sk with the same key sk, the "difference" m = m m′ of plaintexts can be computed by comparing c and c′. In the designed linear sketch scheme,we make use of the above one-time pad encryption's property. Thus, the process of coding in the linear sketch scheme can be viewed as the process of one-way encryption in the one-time pad encryption scheme, which is used to code the biometric data with a random value. And the process of correcting error in the linear sketch scheme can be viewed as the process of finding the "difference" in the one-time pad encryption scheme, which is used to compute the "difference" of two random values.

VI . COMPARATIVE STUDY

An allotted computing activity is to deal with capacity challenges of particular types, and moderate distributed computing merchants provide different storerooms to accommodate this need. Indeed, it is an enormous challenge to place oneself on such an enormous stage as that which scales with the World Wide Web. For the purpose of determining the requirements for these storage spaces, we appear to be in agreement with the capabilities provided by Amazon Web Services Microsoft Windows Azure and Google's App Engine thus as much in imitation of draw the potential requirements of large informational collections as like specific illustrations, then desire as it would run about so an in. Table 1 shows a variety of possible combinations offered by the three retailers.

Storage Type	Amazon Web Services	Windows Azure	Google AppEngine
Unstructured	Yes	Yes	Yes
Structured	Yes	Yes	Yes
Message Queue	Yes	Yes	Yes
Block Devices	Yes	Yes	No
RDBMS	Yes	Yes	No

Table 1: Comparative Study Storage Types

IV. RESULTS AND DISCUSSION

It is possible for a user to access the operations of Cloud, Data Owner and TPA. It's possible to search for and download data The Upload File with Blocks, the View All Upload File with Blocks, the Data Integrity Audit, and the Transactions pages are all available to anyone who have access to the data. Actions may be retrieved on the cloud. Individuals can be seen and authorized. The file's owners may see and authenticate

each and every block and transaction. The option to see all defendants is available. Access and Analyze Time Delay and Throughput Information.

FIG.1 HOME PAGE

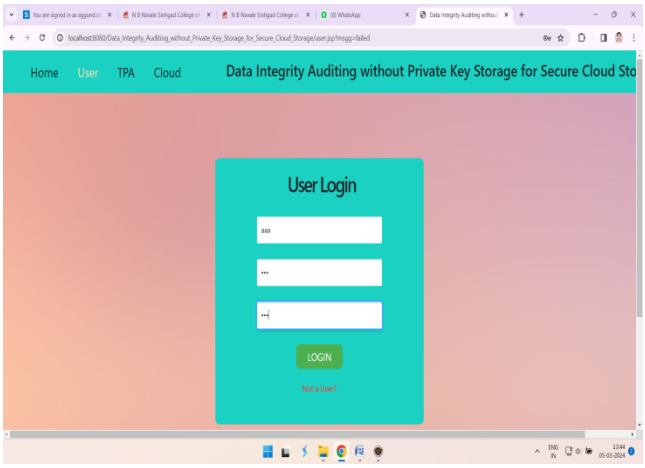

FIG.2 LOGIN PAGE

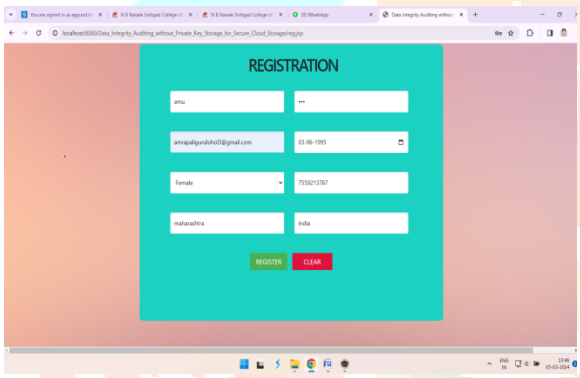

FIG.2 REGISTRATION PAGE

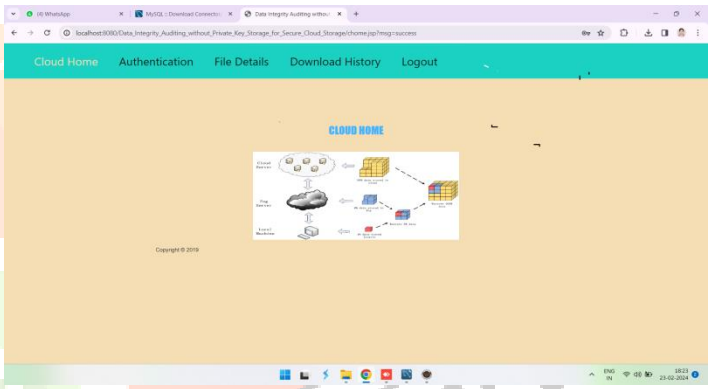

FIG.4 CLOUD PAGE

CONCLUSION

In this paper, 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 proofand 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 Transactions on 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," 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 Cryptography
and Network Security, 2012, pp. 507–525.

[8] B. Wang, H. Li, and M. Li, "Privacy-preserving public auditing 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.