Novel Method to Achieve Data Integrity Auditing In Cloud Server

MANDELA MANJU #1, B.SURYANARAYANA MURTHY #2

#1 MSC Student, Master of Computer Science,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

#2 Associate Professor, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract

In current day’s cloud computing has become one of the fascinating domains which are used by almost all MNC and IT companies. Using cloud storage services, users can store their data in the cloud to avoid the expenditure of local data storage and maintenance. To ensure the integrity of the data stored in the cloud, many data integrity auditing schemes have been proposed. In most, if not all, of the existing schemes, a user needs to employ his private key to generate the data authenticators for realizing the data integrity auditing. They require a physical device to authenticate the identity by using third party devices like smart card or some token generators. If this token generator or smart card is lost or this password is forgotten, most of the current data integrity auditing schemes would be unable to work. In order to overcome this problem, we propose a new paradigm called data integrity auditing without private key storage and design such a scheme. In this scheme, we use biometric data (e.g. iris scan, fingerprint) as the user’s fuzzy private key to avoid using the hardware token. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

1. INTRODUCTION

CLOUD storage can provide powerful and on-demand data storage services for users [1]. By using the cloud service, users can outsource their data to the cloud without wasting substantial maintenance expenditure of 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.

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.

PROBLEM STATEMENT

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.

PURPOSE

The contribution of this paper can be summarize 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 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.

OBJECTIVE

We propose a new paradigm called data integrity auditing without private key storage and design such a scheme. In this scheme, we use biometric data (e.g. iris scan, fingerprint) as the user’s fuzzy private key to avoid using the hardware token. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

The main scope for designing this current application is to overcome the problem which is faced in current networks .In present days there was no security for the data which is stored in the cloud server,
because the data is not encrypted by strong means of encryption and there is no facility to block the un-
authorized data access.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing
the tool, it is necessary to determine the time factor, economy and company strength. Once these things
are satisfied, ten next steps are to determine which operating system and language used for developing the
tool. Once the programmers start building the tool, the programmers need lot of external support. This
support obtained from senior programmers, from book or from websites. Before building the system the
above consideration r taken into for developing the proposed system.

1) Public Key Encryption with Keyword Search.

We study the problem of searching on data that is encrypted using a public key system. Consider
user Bob who sends email to user Alice encrypted under Alice’s public key. An email gateway wants to
test whether the email contains the keyword “urgent” so that it could route the email accordingly. Alice,
on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and
construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test
whether the word “urgent” is a keyword in the email without learning anything else about the email. We
refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a
mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism
Alice can send the mail server a key that will enable the server to identify all messages containing some
specific keyword, but learn nothing else. We define the concept of public key encryption with keyword
search and give several constructions.

2) VABKS: Verifiable Attribute-Based Keyword Search Over Outsourced Encrypted Data.


It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be
fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as:
How should a data owner grant search capabilities to the data users? How can the authorized data users
search over a data owner’s outsourced encrypted data? How can the data users be assured that the cloud
faithfully executed the search operations on their behalf? Motivated by these questions, we propose a
novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution
allows a data user, whose credentials satisfy a data owner’s access control policy, to (i) search over the
data owner’s outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii)
verify whether the cloud has faithfully executed the search operations. We formally define the security
requirements of VA B K S and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

3) Fuzzy identity-based encryption.

**Author:** A. Sahai and B. Waters.

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as a set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω₀, if and only if the identities ω and ω₀ are close to each other as measured by the “set overlap” distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term “attribute-based encryption”. In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

3. EXISTING SYSTEM

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like key generation and maintenance of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In the existing clouds there is no security for the sensitive data which is uploaded into the cloud server.

**LIMITATION OF EXISTING SYSTEM**

The following are the main limitations of the existing system. They are as follows:

1) In the existing clouds there is no method like revocation identification in the cloud server.
2) All the data is accessed by centralized server and hence if the hacker or intruder hack the centralized location, then he/she can access or modify any users data that is available in the server.
3) The traditional account/password-based authentication is not privacy preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems.
4. PROPOSED SYSTEM

We propose a new paradigm called data integrity auditing without private key storage and design such a scheme. In this scheme, we use biometric data (e.g. iris scan, fingerprint) as the user’s fuzzy private key to avoid using the hardware token. The security proof and the performance analysis show that our proposed scheme achieves desirable security and efficiency.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system, they are as follows:
1) The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.
2) The performance comparisons indicate that the proposed protocol has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes JSP, HTML and Java Beans and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

1) Data Owner
2) Cloud Server
3) TPA
4) Data User

Now let us discuss about each and every module in detail

5.1 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.

5.2 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
5.3 TPA

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

5.4 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.

6. RESULTS (OUTPUT SCREENS)

1 Home Page

![Home Page screenshot](image)

Explanation:

The home page mainly contains the following links like Data owner, Cloud server, TPA and the End users. All are connected within the same main page.
2) CLOUD SERVER LOGIN

Explanation:
Here the storage server or admin is one who can enter with a valid user name and password and they can verify the following details as follows.
3) Cloud server can view the list of all files that are uploaded in the storage server

4) Cloud server can view Set of all users transactions
5) Cloud Server can view all the attacker details

6) Cloud Server can view Time Delay Result
7) Cloud Server can view the Throughput Details

![Graph showing throughput details](image1.png)

8) User Login

![Login page with options](image2.png)

Cloud storage, Data integrity auditing, Data security, Biometric data

In this scheme, we use biometric data (e.g., iris scans, fingerprints) as the second factor to provide security. Additionally, this scheme can still effectively complete the data integrity auditing. The scheme also includes a biometric search system that can help users recognize and correct information in real-time.

Welcome Manjunath
9) User Can upload a file

10) User can View all the File Blocks
7. CONCLUSION

In this proposed work, 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.

8. REFERENCES


