# Monitoring Data Consistency in Trustworthy Cloud Memory Platforms Using Fuzzy Identities

**Mehaboob Basha,[1] SK Naseer Ahmed [2], Ch Subhash [3], V Venkata Sahithi [4], T Sai Siddhardha[5]**
[1] Associate Professor, Department of Computer Science and Engineering
[2,3,4,5] Student, Department of Computer Science and Engineering
[1,2,3,4,5]QIS College of Engineering & Technology

## Abstract

Data integrity has been recognised as an important aspect of secure cloud storage. An auditor may quickly and easily verify the correctness of the outsourced data without having to download the data itself, thanks to data auditing protocols. Existing designs of data auditing methods provide a significant research challenge due to the complexity in key management. The purpose of this study is to tackle the intricate Fuzzy identity-based auditing is introduced, solving a significant management difficulty in cloud data integrity verification, and is the first method of its kind. To be more precise, we introduce the foundational concept of fuzzy identity-based data auditing, in which the identity of a user is conceptualised as a collection of descriptors. For this novel primitive, we formally define both the system and security models. Using biometrics as the fuzzy identity, we then demonstrate a practical implementation of an auditing system based on fuzzy identities. To provide error-tolerance, the new protocol associates a private key with one identity and uses that identity to validate the accuracy of a response created with another identity, provided both identities are sufficiently similar. With the use of the computational Diffie-Hellman assumption and the discrete logarithm assumption from the selective-ID security model, we demonstrate the safety of our protocol. At last, we create a working prototype of the protocol to show how our plan might work in practise.

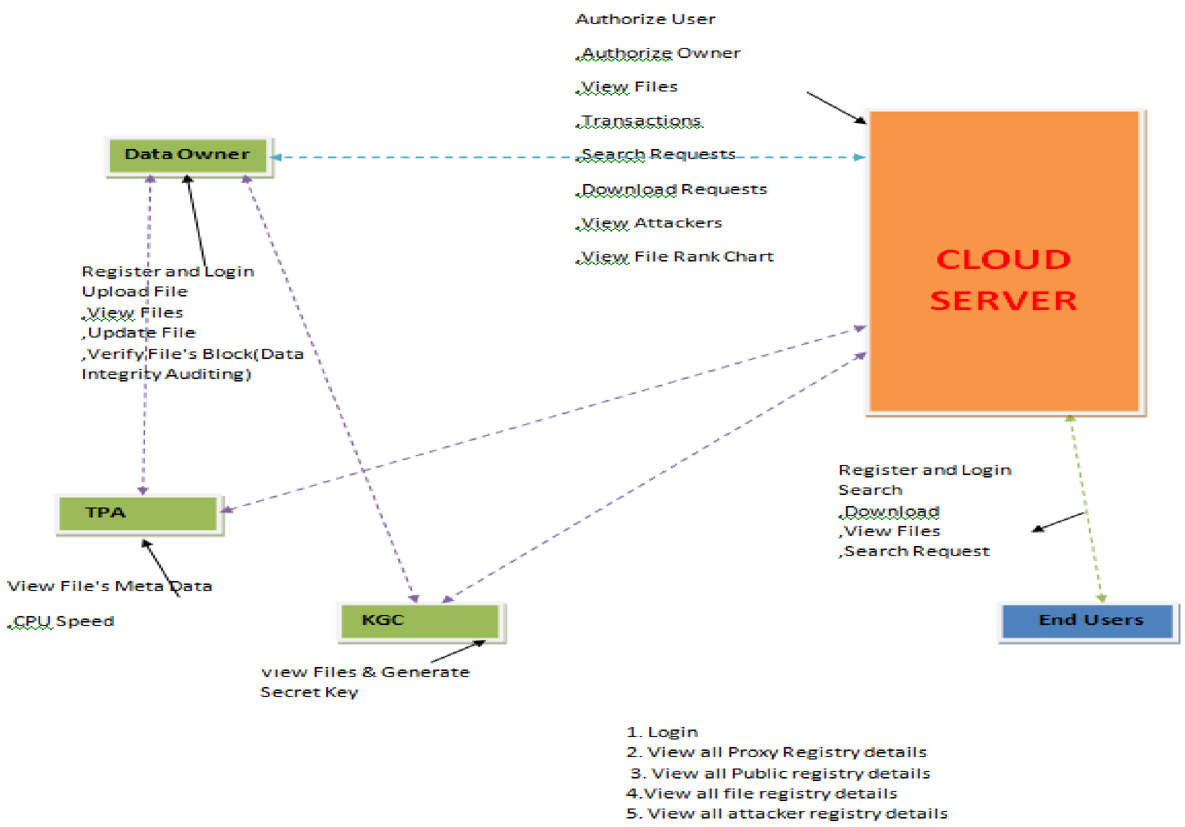
## 1. INTRODUCTION

When data owners outsource their data to the cloud, they often lose physical control of their data and may not even know where their data are really kept or who has the authorization to gain access to their data, which presents a number of security problems. Thus, after users have uploaded their data to the cloud, the servers in question decide what happens to it. In spite of the greatest efforts of the cloud servers to prevent accidental data loss, there is always a chance that some information might be lost. That's hardly a big surprise. One, data is vulnerable to corruption in the event of a temporary failure of the cloud server or the storage media (such as RAM). In addition, users' information may be destroyed if cloud providers delete it to create room for more profitable files.

43% of respondents to a survey2 said they had lost outsourced data and had to restore it from backups. One of the major worries about cloud storage is the possibility of data loss, which occurs regularly in practise. For instance, many customers' data was irretrievably lost when the Amazon cloud service crashed.

It was noted that "the data loss was relatively minimal compared to the overall data saved, but anybody who operates a web site will quickly grasp how horrifying the idea of data loss is." As a result, businesses which outsource their data need to know that it will remain secure. They are concerned about the reliability of the cloud storage facilities where their data may be kept. As a result, keeping data intact in the cloud is crucial for safe and dependable cloud storage.

There has been a rise in the use of fuzzy theory and methods based on fuzzy identities [22], [23], [24] in a wide variety of contexts [25], [26], [27]. Biometrics, a common kind of ambiguous identification, are based on who you are. Biometric passports and mobile devices like Apple ios and Samsung phones are only two examples of the many real-world uses of biometric-based schemes [28], [29]. These schemes work by using a user's unique physiological or behavioural characteristics to verify the user's identity. It's hardly unexpected, considering the advantages provided by biometric-based methods. There is no way to lose or forget a biometric identity, and it may be used everywhere. We find that there are no published fuzzy identity-based data integrity auditing standards for cloud storage services, despite the fact that such protocols would be useful. This might be because it is difficult to design error-tolerant auditing systems for data.



## 2. SYSTEM ANALYSIS

### Existing System

Existing designs of data auditing methods provide a significant research challenge due to the complexity in key management. To the best of our knowledge, this study is the first to provide fuzzy identity-based auditing as a means of addressing the difficult key management problem inherent in cloud data integrity verification.

## 3. PROPOSED SYSTEM

Key management in conventional remote data integrity checking methods is completely overhauled by the proposed protocol. We also proposed a concrete fuzzy identity based data integrity auditing protocol that takes biometric based identification as an input, and the corresponding system and security models for this basic. After establishing the protocol's safety in the selective-ID model. Proof of the proposal's feasibility is provided by the prototype implementation of the protocol. The next step is to put the suggested procedure into practise and assess its performance in the actual world.

A remote data integrity check (RDIC) is proposed, which involves the cloud server, the data owner, and an independent auditor (TPA). Cloud data integrity may be verified by the TPA or any interested party using a publically verifiable RDIC protocol without requiring the whole dataset to be retrieved from storage.

Proof of Retrievability (POR) is defined, and a concise signature algorithm-based construction is provided and proven secure in the random oracle model. Remote data integrity checking techniques have been suggested to meet a variety of practical needs, including dynamic operation, privacy preservation, and public auditing.

User's private identifier that may be used in place of a digital certificate. Many ID-based techniques (such as protocols for auditing data remotely) have been presented since then. Multiple ID-based remote data auditing systems have been developed, each treating identity data as a free-form string of characters. The latter consists of the user's name, IP address, and email address, which are needed to register for a private key from the private key generation centre that is unique to the user's identity.

## ALGORITHM

### RSA algorithm

RSA is a popular method for digital encryption and decryption on today's computers. It's a kind of cryptography that uses asymmetric keys. The two keys are dissimilar, or asymmetric. Since one of these keys may be shared publicly, this kind of encryption is also known by that name. The second key is secret and must not be shared.

**Deterministic Algorithm**:

Given a certain input, a deterministic algorithm will always generate the same result, with the underlying machine following the same set of predetermined steps.

**Polynomial Time Algorithm**:

An algorithm with polynomial time guarantees that it will complete within a certain number of steps, where the number of steps is a function of the problem's size. To learn more, check out computational temporal complexity. Data should be searched quickly so that process output may be provided.

## 4. IMPLEMENTATION

Data Owner

TPA Auditing.

Server.

User.

**Data Owner:**

Client wants to upload fresh files to the cloud, thus it must validate the cloud's encrypted secret key and get the genuine secret key. We demonstrate that the two processes occurred at distinct points in history. Only occur when a client has fresh files that need to be uploaded to the cloud. To add, the cloud can undertake all the legwork necessary to ensure that the encrypted secret key is valid.

By using TPA Auditing, data integrity in the cloud may be verified with little data retrieval. Because an HVT compiles the responses of all challenged blocks into a single value, it drastically cuts down on server-to-client data transfers. On behalf of the cloud user, the TPA verifies the authenticity of the cloud data.

When checking to see whether data are still in good shape, the TPA and cloud server will use a challenge response protocol. The TPA can now identify cloud-based file F corruption thanks to homomorphism and without incurring significant additional communication costs. The TPA takes a random sample from the blocks of the file M and uses it to create a challenge chal, which it then sends to the remote server. In the Response method, the server creates proof resp in response to a challenge by summing the authenticators for the challenged blocks. At last, the TPA checks the reply answer to make sure file F in the cloud is unharmed.

**Server:**

After data owners submit their files to the cloud, it is the cloud servers that decide what happens to them. Data loss events will occur regardless of how trustworthy a cloud service provider is (most have a strong interest in protecting their reputation and avoiding legal trouble). That's why it's crucial for cloud service providers to provide a rock-solid assurance of data accuracy and security before handing over sensitive information. As a result, keeping data intact in the cloud is crucial for safe and dependable cloud storage.

With an HVT, the server and TPA just have to exchange a single value instead of the individual responses from each block that was challenged. For the aforementioned methods, the data owner has a pair of public and private keys (pk and sk) that are used for different purposes. The sk is used to construct authenticators of blocks, while the pk is used to check the evidence that the cloud server has generated.

Finally, a challenge response protocol is used by both the TPA and the cloud server in order to conduct an audit of the data's integrity.

**TPA Auditing.**

The data is signed by a collective of users before being made public. Since this is the case, disagreements between the two sides are to be expected. Therefore, a neutral third-party arbiter for resolving auditing-related disputes is required for any credible auditing programme. By imposing various trust assumptions on the auditor (TPAU) and the arbitrator (TPAR), we expand the threat model in current public schemes. As the TPAU is primarily a delegated party to examine client data integrity, and as a possible disagreement may arise between the TPAU and the CSP, it is important that the arbitrator be an impartial third party who is distinct from the TPAU.

We find the TPAR to be forthright but inquisitive. It's likely to act ethically most of the time, but it may sometimes pry into auditing data out of pure curiosity, thus such data has to be protected from prying eyes. Also, although the topic of privacy is beyond the purview of this article, it is worth noting that our approach may leverage the random mask technique described for privacy preservation of auditing data, or the ring signatures in to safeguard the identityprivacy of signers for data shared among a group of users.

As a means of relieving the burden on their clientele, public auditing systems often include the use of a third-party auditor (TPA). However, such models often presume an honest owner versus an untrustworthy CSP, therefore the fairness issue is seldom discussed. To what degree might the CSP have faith in the auditing outcome, given that the TPA is acting on behalf of the owner? Imagine a scenario where the proprietor and the TPA plot against a trustworthy CSP for financial benefit. The usefulness and viability of auditing techniques is diminished by such models.

The task associated with updating secret keys is transferred to the TPA. In contrast, at the end of each period in scheme, it is up to the client to change the secret key. We evaluate the two approaches by looking at how long it takes for the client to get an updated key. The client's key update time is proportional to the node depth during the period in question. Subcontract auditing of cloud storage keys for increased key-exposure resistance.

An auditing technique for cloud storage that may be used to ensure the integrity of any outsourced changes. With this protocol, the client is not aware of when a new key is generated or distributed; instead, this task is outsourced to the TPA. As an added layer of security, the TPA only sees the encrypted client secret key, while the client may double-check the integrity of the TPA's encrypted secret keys before downloading them. We provide a formal verification of the scheme's security and a performance simulation.

**User:-**

One way to define identity is as a collection of characteristics. For this novel primitive, we formally define both the system and security models. Using biometrics as the fuzzy identity, we then demonstrate a practical implementation of an auditing system based on fuzzy identities.

Specifically, the new protocol binds with a private key to one identity, which may be used to check the validity of a response created with another identity, provided that the two identities are sufficiently close.

To generate more money, cloud storage providers may knowingly delete user data in order to free up space for other files. According to the results of a poll, 43% of respondents have experienced data loss while using an outsourcing service and had to rely on previous backups to restore their files. In truth, data loss is common, and it is widely recognised as one of the most significant security concerns associated with cloud storage.

Certification authority, is a combination of a central directory, a certificate management system, and an authentication authority. User's private identifier that may be used in place of a digital certificate. Many ID-based techniques (such as protocols for auditing data remotely) have been presented since then.

If the identification information is not carefully selected (for as by selecting a common name like "John Smith"), the user's identity may not be genuinely unique. Second, the private key generating centre requires "proof" from the user that he is entitled to the claimed identity. This "proof" might be in the form of a government-issued ID or other official document.

## 5. CONCLUSION

These days, the IT sector just wouldn't function without cloud storage services. The security of cloud-stored information is becoming more important as more people use this method of data management. In this study, we introduced the first auditing technique for data integrity that relies on fuzzy identities.

Compared to existing remote data integrity checking techniques, the suggested method significantly improves upon key management. We also provided a concrete fuzzy identity-based data integrity auditing protocol that takes biometric-based identities as input, as well as models for the underlying system and security of this basic. After that, we showed that the approach is safe in the selective-ID model. The prototypical realisation of the protocol proves the proposal's viability.

## REFERENCES

[1] M. Hogan, F. Liu, A. Sokol, and J. Tong, "NIST Cloud Computing Standards Roadmap," NIST Cloud Computing Standards Roadmap Working Group

[2] Above the clouds: A berkeley perspective on cloud computing, University of California, Berkeley,

[3] A. Saidane, Y. Deswarte, and J. J. Quisquater. Remote verification of data integrity. Information System Integrity

[4] Obtainable proof of data ownership in untrusted storage. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song.

[5] Proofs of Storage from Homomorphic Identification Protocols by G. Ateniese, S. Kamara, and J. Katz. 2009

[6] The work of Rivest, Shamir, and Adleman Digital signature and public-key cryptosystem acquisition technique.

[7] Compact demonstrations of retrievability, H. Shacham and B. Waters ASIACRYPT 2008 Proceedings,

[8] Short signatures from the weil pairing, D. Boneh, B. Lynn, and H. Shacham, Asiacrypt

[9] A. Kupcu, C. Papamanthou, and C. C. Erway Dynamic, verifiable data possession. Information and System Security

[10] Enabling public verifiability and data dynamics for storage security in cloud computing, by Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou

[11] "Improved security of a dynamic remote data possession verification protocol for cloud storage," authored by Y. Yu, J.B. Ni, M. H. Au, H.Y. Liu, H. Wang, and C.X. Xu, is referenced here

[12] Dynamic audit services for outsourced storages in Clouds," by Y. Zhu, G. J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. J. Hu

[13] Enhancing the privacy of a remote data integrity-checking system for secure cloud storage, Y. Yu, M.H. Au, Y. Mu, S.H. Tang, J. Ren, W. Susilo, and L.J. Dong

[14] privacy is essential for keeping their cloud-based data safe, as explained in by C. Wang, Q. Wang, K. Ren, and W. Lou.

[15] "Privacypreserving public auditing for safe cloud storage," by C. Wang, S. S.Chow, Q. Wang, K. Ren, and W. Lou

[16] "Comments on a Public Auditing Mechanism for Shared Cloud Data Service" by Y. Yu, J.B. Ni, M. H. Au, Y. Mu, B.Y. Wang, and H. Li.

[17] "Identity-based Cryptosystems and Signature Schemes," by A. Shamir

[18] A Privacy-Preserving Identity-Based Public Verification for Cloud Data Storage Security, J. N. Zhao, C. X. Xu, F. G. Li, and W. Z. Zhang,

[19]: "Provably Secure Identity Based Provable Data Possession" by Y. Yu, Y. F. Zhang, Y. Mu, W. Susilo, and H. Y. Liu. 2015,

[20] "Identity-Based Distributed Provable Data Possession in Multicloud Storage," by H. Q. Wang

[21] A.Sahai and B. Waters, "Fuzzy identity-based encryption").

[22] Fuzzy identity based signature with applications to biometric authentication.

[23] P. Yang, Z. Cao, and X. Dong. (2011), Computers and Electrical Engineering,

[24] "Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption." F. C. Guo, W. Susilo, and Y. Mu.

[25] Smart cloud storage service selection based on fuzzy logicc. Esposito, M. Ficco, F. Palmieri, and A. Castiglione. 2015, Theory of Evidence and Game Theory,

[26] Li, X.; Li, J.; Huang, F. Safe cloud storage with privacy-preserving fuzzy deduplication, Soft Computing,

[27] Self-adaptive trust management based on game theory in fuzzy large-scale networks. H. Fang, L. Xu, and X. Huang. Soft Computing, pp.1-15, 2015.

[28] Biometric recognition: Security and privacy considerations. P. Salil, S. Pankanti, and A. K. Jain. Chapter 2: "Security and Privacy

[29] Drs. A. K. Jain, A. Ross, and S. Prabhakar. "Principles of biometric identification: (2004),