Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

ROBUST DATA INTEGRITY CHECKS IN CLOUD SYSTEMS USING IDENTITY FUZZING

1. Ramesh kothapali, Assistant professor, Department of CSE Aditya University, rameshk@adityauniversity.in

2. Santhi Babu Mamidi, Assistant Professor, Department of Computers and Applications K B N College (Autonomous), Kothapet, Vijayawada, saani009@gmai.com

ABSTRACT

Ensuring data integrity remains a critical concern in cloud storage systems. To validate the correctness of outsourced data without retrieving it entirely, data auditing protocols have become an essential solution. However, most existing frameworks struggle with complex key management. This project introduces an innovative approach called Fuzzy Identity-Based Data Auditing, aiming to simplify key handling while maintaining strong data verification capabilities.

In this method, a user's identity is represented through a set of descriptive features, such as biometrics, forming a "fuzzy" identity that allows for a certain level of variation or error. We propose a secure system model where a private key linked to one identity can successfully validate a response generated by a similar identity, provided they meet a predefined closeness threshold. This adds an error-tolerant dimension to data verification.

Our solution is supported by a concrete protocol built on foundational cryptographic assumptions, including the Computational Diffie-Hellman and Discrete Logarithm assumptions, under a selective identity-based security model. Additionally, we have implemented a functional prototype of this system to demonstrate its real-world viability and effectiveness in simplifying cloud data integrity checks.

INTRODUCTION

The era of Big Data has revolutionized how information is generated, stored, and processed. With more than 2.5 quintillion bytes of data produced daily, traditional storage systems struggle to handle the volume, variety, and velocity of data. Cloud storage, particularly under the Infrastructure-as-a-Service (IaaS) model, has emerged as a scalable solution, offering

benefits such as global access, elasticity, and reduced management overhead.

However, the outsourcing of data to third-party cloud servers introduces critical security and trust issues, especially concerning data integrity. Data owners lose physical control over their files, raising the risk of accidental corruption or intentional deletion by cloud providers. This necessitates remote data integrity checking (RDIC) solutions that can verify the correctness of stored data without retrieving the entire dataset.

Existing auditing protocols based on Public Key Infrastructure (PKI) and identity-based cryptography simplify certificate management but face limitations like identity ambiguity, certificate revocation complexity, and susceptibility to forgery. These schemes typically rely on "what you have" (certificates) and "what you know" (identity strings).

In contrast, fuzzy identity-based cryptography introduces a new dimension—"what you are"—by integrating biometric attributes. Biometric-based schemes provide error-tolerant, secure, and user-friendly authentication, reducing dependency on strict identity matching. Despite their potential, such methods have not yet been fully applied to cloud data integrity auditing, primarily due to challenges in tolerating identity errors while maintaining provable security guarantees.

This gap in current research presents an opportunity to develop fuzzy identity-based data auditing protocols, which could enhance usability and security in cloud environments by enabling secure verification even when minor mismatches occur in biometric data.

LITERATURE SURVEY

M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap," NIST Cloud Computing Standards Roadmap Working Group, SP 500-291 v1.0, NIST, Jul, 2011. The NIST Cloud Computing Standards Roadmap Working Group has surveyed the existing standards landscape for security, portability, and interoperability standards/ models/ studies/ use cases, etc., relevant to cloud computing. Using this available information, current standards, standards gaps, and standardization priorities are identified in this document. The NIST Definition of Cloud Computing identified

cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. 2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech. Rep. CLOUD COMPUTING, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about overprovisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000..

EXISTING SYSTEM

The existing cloud data integrity auditing protocols face several challenges, particularly in key management. Traditional designs often rely on complex cryptographic key infrastructures that are difficult to manage securely and efficiently.

Key Limitations of the Existing System:

Complex Key Management: Traditional PKI-based systems require certificate generation, renewal, and revocation.

High Computational Overhead: Maintaining and verifying keys increases system complexity.

Dependence on Trusted Certificate Authorities: These can be single points of failure or bottlenecks.

No Support for Biometric Identity: Existing protocols do not utilize unique, user-friendly biometric identities.

Limited Flexibility: Lack of support for error-tolerant identity matching (e.g., fuzzy identity).

PROPOSED SYSTEM

To overcome the limitations of existing systems, we propose a Fuzzy Identity-Based Data Auditing Protocol, which introduces biometric identity (e.g., fingerprint or iris scan) into cloud data auditing.

Highlights of the Proposed Protocol:

implified Key Management:

Uses fuzzy identity instead of traditional public/private keys.

Biometric-Based Authentication:

Leverages unique user biometrics for secure identity verification.

Error-Tolerant Identity Matching:

Supports fuzzy identity to allow slight variations in biometric input.

Practical Implementation:

Prototype implementation confirms the protocol is feasible and efficient.

Security-Proven:

The protocol's security is demonstrated in the selective-ID model.

RELATED WORK

1. Remote Data Integrity Checking

- Introduced by Deswarte et al.
- Involves three entities: data owner, clou d server, and Third Party Auditor Allo ws verification of data without downloa ding it.

2. Provable Data Possession (PDP)

- Proposed by Ateniese et al.
- Uses Homomorphic Verifiable Tags (H VT) based on RSA.
- Efficient in reducing communication ov erhead between server and TPA

3. Proof of Retrievability (PoR)

- Proposed by Shacham and Waters.
- Based on short signature algorithms.
- Ensures both data integrity and retrieva bility with high security.

4. Enhanced RDIC Schemes

- Support for dynamic data operations (u pdate, delete, append).
- Enable privacy-preserving verification without revealing data.
- Allow public auditing by third parties f or transparency.

5. Public Key Infrastructure (PKI)-Base d Protocols

- Use public/private key pairs and digital certificates.
- Limitations include:

Complex certificate generation and revocat ion.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

High computational overhead.

Dependence on trusted Certificate Authorit ies (CAs).

6. Identity-Based Cryptography (IBC)

- Proposed by Shamir to simplify PKI.
- User identity (e.g., email, name) acts as the public key.
- Benefits:

No need for digital certificates.

Easy key management.

7. Fuzzy Identity-Based Cryptography

- Extends IBC by allowing slight var iations in identity (error-tolerance).
- Ideal for biometric identities (finge rprint, iris, face).
- Biometrics are:

  Unique and difficult to forge.

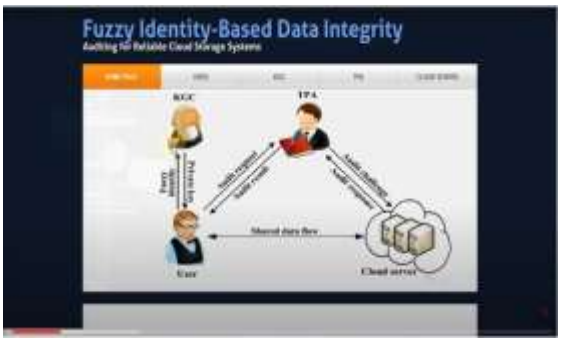
  Portable and always available (can not be lost or forgotten).

- Challenge:

  No existing fuzzy identity-based int egrity auditing protocols for cloud s torage.

  Difficult to design efficient error-to lerant yet secure auditing mechanis ms.

SAMPLE RESULTS



CONCLUSION

Cloud storage services have become an

integral part of modern information technology, offering scalable and efficient data management solutions. However, ensuring the integrity and security of data outsourced to the cloud remains a major concern. In this paper, we introduced the first fuzzy identity-based data integrity auditing protocol, which significantly enhances traditional remote data integrity checking mechanisms. The proposed system simplifies complex key management processes by leveraging biometric-based fuzzy identities, thereby eliminating the need for exact identity matching and reducing administrative overhead. We presented a detailed system architecture and security model for this innovative approach and proved its security in the selective-ID model. A prototype implementation of the protocol was developed, demonstrating the practical feasibility of the solution in real-world scenarios. This advancement not only improves data integrity verification in cloud environments but also offers a more user-friendly and secure identity management system. Future work will focus on deploying the protocol in large-scale cloud platforms, optimizing its performance, and extending its capabilities to support multi-user environments and dynamic data updates.

REFERENCES

[1] M. Hogan, F. Liu, A. Sokol and J. Tong, "NIST Cloud Computing Standards Roadmap," NIST Cloud Computing Standards Roadmap Working Group, SP 500-291-v1.0, NIST, Jul, 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing, University of California, Berkeley, Tech. Rep.

[3] Y. Deswarte, J. J. Quisquater and A. Saidane. "Remote integrity checking". Integrity and Internal Control in Information Systems VI. Springer US, pp.1-11, 2004.

[4] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson and D. X. Song, "Provable data possession at untrusted stores," in Proc. of ACM Conference on Computer and Communications Security, pp.598-609, 2007.

[5] G. Ateniese, S. Kamara and J. Katz. "Proofs of storage from homomorphic identification protocols". Proc. of ASIACRYPT, pp.319-333, 2009.

[6] R. L. Rivest, A. Shamir and L. Adleman. "A method for obtaining digital

signatures and public-key cryptosystems". Communications of the ACM, 21(2), pp.120-126, 1978.

[7] H. Shacham and B.Waters, "Compact proofs of retrievability," Proc. of Cryptology ASIACRYPT, 5350, pp.90-107, 2008. [8] D. Boneh , B. Lynn, and H. Shacham, "Short signatures from the weil pairing", In Proc. of Asiacrypt 2001, pp.514-532, 2001.