International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Cloud-Based Data Encryption with Revocable Storage

1 PAMULURU VENKATESWARLU, 2 NIDAMANURI SRI HARSHA, 3 PAGIDI MANOJ KUMAR

4 MR.KANDEEBAN, 5 MR J.JAYAPRAKASH , 6 MRS.CHINCHU NAIR

1 2 3 Students,4 Professor,5 Professor,6 Assistant Professor

pamuluruvenkatesh123@gmail.com , sriharshanidamanuri@gmail.com , manojkumarreddy0045@gmail.com Dr. MGR

Educational and Research Institute , Maduravoyal , Chennai 600095 , TN

Strategic adoption of cloud computing enables enterprises to significantly curtail IT infrastructure costs by leveraging hardware and software resources more efficiently. This paradigm has empowered organizations to effectively utilize cloud storage for sharing data among personnel. Initially, storing shared data in encrypted form and securing it with access controls seems like an straightforward solution. However, the cloud, being a third-party entity, can introduce potential security vulnerabilities. Therefore, stringent encryption protocols and effective access controls become imperative to safeguard shared data stored in the cloud. Noteworthy is the fact that some personnel may be malicious, deviating from the expected information exchange mechanism. Current research explores solutions to mitigate the risks associated with legitimate data encryption and decryption. Unfortunately, existing literature fails to address the nefarious activities of malicious data publishers who compromise data integrity by sharing accessible encrypted texts. This ultimately compromises the intellectual property of organizations. Given these findings, it is pressing to establish a systematic approach for addressing the challenges originating from malicious data publishers in the cloud storage ecosystem. That inquiry becomes an elusive, albeit critical, research problem. Our research endeavors to tackle this very obstacle. To accomplish this, we design and present a novel conceptual framework - the Sanitizable Access Control System (SACS), tailor-made for highly secure cloud storage environments, inclusive of immunity to malicious data publishers. To facilitate this aim, we will delineate a perestroika hazard model, coupled with its cognate mathematical security rendition. Conversely, the actual architecture leverages the mathematical proof rooted in q-parallel bilinear Diffie-Hellman exponent. Through evaluation of our system's respective security, qualitative efficiency metrics and our comprehensive risk appraisal guarantee enhanced cloud storage functionalities that secure organizational resources.

Keywords: Blockchain, Cloud Storage, Sanitizable Access Control System (SACS), Data Encryption.

I. INTRODUCTION

With the growing reliance on Cloud Service Providers (CSPs) for data storage, concerns regarding information security have intensified. Data transfers within cloud infrastructures are vulnerable to malware, malicious actors, and potential data corruption. To maintain data integrity, frequent verification of stored records is essential. Currently, remote data validation in cloud environments is conducted through third-party auditors (TPAs) utilizing cryptographic techniques. TPAs also facilitate public auditing by offering superior computational and communication resources compared to traditional users.

Public auditing mechanisms empower TPAs to validate the accuracy of cloud-stored data without necessitating full data extraction from CSPs. However, a critical issue in many auditing frameworks is the lack of stringent measures to protect user data from unauthorized access by TPAs. Consequently, the confidentiality and integrity of sensitive user information can be compromised.

This study delves into cryptographic methodologies aimed at enhancing cloud data auditing while addressing prevalent privacy concerns. The literature presents multiple strategies for maintaining data integrity and confidentiality, categorized into various models such as static, dynamic, multi-tenant, and multi-user approaches. Our research systematically reviews and evaluates these methodologies, identifying their strengths and limitations to inform future advancements in cloud security. Although cloud security encompasses a broader spectrum of concerns, this study specifically highlights the importance of secure cloud data auditing.

II. LITERATURE SURVEY

A critical phase in software development is conducting a literature review, which helps determine key factors such as time investment, cost efficiency, and business sustainability before system expansion. Once these aspects are analyzed, the next step involves selecting a suitable operating system and programming language for implementation. Developers often require external resources, including books, online references, and expert guidance, to facilitate system design and development.

Evaluating project requirements is an essential aspect of software development, ensuring that key factors like infrastructure needs, human resources, and economic feasibility are addressed before system implementation. The subsequent step involves selecting appropriate technological components, such as software frameworks and tools, necessary for project execution.

One challenge in public-key encryption with keyword search (PEKS) is maintaining stability while minimizing false positives. Computational and statistical enhancements have been proposed to refine PEKS security, building upon earlier schemes like the Boneh et al. model. Additional improvements include adaptations such as anonymous identity-based encryption (IBE), hierarchical identity-based encryption (HIBE), and public-key encryption with ad hoc keyword searches.

Re-encryption techniques, such as atomic proxy re-encryption proposed by Blaze, Bleumer, and Strauss (BBS), allow intermediaries to convert encrypted data for different users without accessing the plaintext. While this technique offers efficiency, concerns regarding security vulnerabilities have hindered its widespread adoption. Recent advancements propose improved security models for proxy re-encryption, strengthening access control mechanisms in secure file systems.

PEKS-based encryption systems, as introduced by Boni, Di Crescenzo, Ostrovsky, and Persiano, enable searching encrypted data without compromising security. However, challenges such as secure channel deletion and keyword updates require further refinement. Enhancements to PEKS focus on eliminating secure channel dependencies and mitigating security risks associated with frequently used keywords.

Cloud computing facilitates global data accessibility but introduces security concerns, particularly in e-health applications where sensitive medical data is shared. Traditional encryption schemes demand high computational resources, making cloud-based cryptographic techniques essential for securing patient data. Recent research evaluates the Quinn scheme, analyzing its vulnerabilities related to data confidentiality.
Attribute-based encryption (ABE) offers a flexible access control mechanism but introduces computational overhead in key generation and decryption. To address this, new outsourced ABE frameworks delegate complex cryptographic operations to third-party services while maintaining security through rigorous verification methods.

Patient privacy remains a crucial concern in electronic medical record (EMR) systems, necessitating encryption and access control measures. Advanced cryptographic schemes empower patients to manage their encryption keys, safeguarding personal health data in case of security breaches. Effective solutions balance encryption with usability, ensuring seamless access to authorized healthcare providers.

In collaborative healthcare environments, secure data sharing is paramount. Implementing fine-grained access control with cross-domain authentication ensures that sensitive patient information is protected while facilitating seamless cooperation between medical entities.

With the growing adoption of cloud services, safeguarding outsourced data is a priority. Privacy-preserving search mechanisms, such as multi-keyword ranked search schemes (MRSE-HC), enhance encrypted data retrieval efficiency. Techniques like keyword clustering and bit vector-based indexing optimize search performance while ensuring confidentiality.

A novel CB-PHR model enhances secure cloud-based personal health record (PHR) management by integrating semi-trusted cloud service providers and multi-domain security controls. This approach streamlines access control and key management, improving usability and security for PHR users.

III. EXISTING SYSTEM

Modern encryption techniques, such as Attribute-Based Encryption (ABE), are widely used to protect cloud-stored data by ensuring that only authorized users with valid decryption keys can access the information. This approach enhances data security by encrypting content before storage. However, its effectiveness depends on the integrity of data publishers. In cases where malicious actors deliberately manipulate encryption keys or share sensitive data with unauthorized entities, existing ABE-based solutions fail to prevent data breaches.

Despite numerous security enhancements, current methodologies do not comprehensively address threats posed by malicious data publishers. This vulnerability raises concerns about data integrity and confidentiality, potentially leading to unauthorized access and intellectual property risks for organizations. Addressing these issues requires a more robust security framework that actively mitigates the risks associated with compromised encryption mechanisms.

REQUIREMENT ANALYSIS

Necessity & Feasibility Analysis of the Proposed System

To combat the limitations of traditional encryption models, we introduce the **Sanitizing Access Control System (SACS)**—a security-driven framework designed to prevent unauthorized access and mitigate risks posed by malicious data publishers. SACS builds upon ABE principles by incorporating an additional security layer that neutralizes compromised encryption attempts.

Key features of SACS include:

Enhanced Access Control – Ensures that only authorized recipients with valid decryption keys can access stored data.

Sanitization Mechanism – Transforms compromised ciphertexts into secure, non-decryptable formats, preventing unauthorized data retrieval.

Robust Security Architecture – Integrates cryptographic measures to detect and counteract malicious encryption activities.

Through this approach, SACS provides a highly secure environment for cloud data storage, ensuring that organizations can safeguard their intellectual assets against potential security threats. Additionally, the implementation of SACS enhances compliance with stringent data protection regulations, making it a viable solution for secure cloud storage.

IV. PROPOSED SYSTEM

Proposed System: Sanitizing Access Control System (SACS)

The primary objective of our approach is to ensure data confidentiality, even in scenarios where data publishers act maliciously or fail to comply with encryption protocols. To address this challenge, we propose the **Sanitizing Access Control System (SACS)**, a security mechanism designed to enhance cloud storage protection against unauthorized data access.

SACS extends existing security models by incorporating a sanitization feature that prevents malicious data publishers from generating ciphertexts that unauthorized users can decrypt. If a compromised encryption attempt occurs, the system converts the affected ciphertext into a format that only legitimate private key holders can decrypt, ensuring that unauthorized access is effectively mitigated.

The core components of SACS include:

1. **Data Publisher** – The entity responsible for encrypting and storing data in the cloud.
2. **Recipient** – The authorized entity that retrieves and decrypts stored data.
3. **Sanitizer** – A security module that ensures encrypted data remains inaccessible to unauthorized users by modifying compromised ciphertexts.
4. **Cloud Storage** – The platform where encrypted data is securely maintained.

Objectives of SACS

- **Streamlined Access Control** – Ensures that only entities with authorized private keys can access sensitive information.
- **Enhanced Data Security** – Prevents unauthorized decryption attempts by malicious actors.
- **Robust Encryption Model** – Implements cryptographic techniques to reinforce cloud security.

By integrating SACS into cloud storage frameworks, organizations can achieve a higher level of security and mitigate threats posed by malicious data publishers, reinforcing the confidentiality and integrity of sensitive data.

SYSTEM ARCHITECTURE:

The description of the overall features of the product is connected to the importance of the necessities and the expressed need for the acute degree of the device. Architectural layout involves describing and designing more than one net page and its relationships. The primary components of the software program are described, divided into processing modules and conceptual recording systems, and their interactions are described. The accompanying blocks are categorized via the proposed structure.

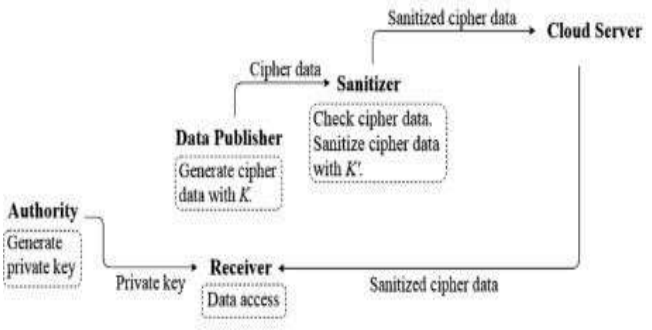

Fig 1: System Architecture

SELECTED METHODODLOGIES

SACS is built upon the principles of **Secure Attribute-Based Encryption (SABE)**, which enhances data protection by sanitizing ciphertext and preventing unauthorized access. SABE ensures that only authorized users possessing valid decryption keys can retrieve and interpret encrypted data.

The primary objective of SACS is to maintain data confidentiality, even in scenarios where data publishers attempt to bypass encryption protocols. By implementing advanced encryption techniques, SACS safeguards information from malicious entities, ensuring that encryption policies are strictly enforced throughout the system.

Blockchain:

Blockchain is a decentralized and immutable ledger system that facilitates the secure and transparent recording of transactions across a network. It can be used to track both tangible and intangible assets, such as real estate, vehicles, financial transactions, intellectual property, and patents. By leveraging blockchain, organizations can enhance efficiency, lower operational costs, and minimize risks associated with data tampering.

As a distributed ledger, blockchain ensures that all network participants have access to a single, consistent version of recorded transactions. This technology is particularly valuable for maintaining data integrity, as stored information cannot be altered without network consensus. Blockchain supports various applications beyond cryptocurrency, including supply chain management, financial transactions, identity verification, and smart contracts.
One of its core advantages is the elimination of intermediaries, thus enhancing trust and reducing reliance on third-party auditors. Since its introduction with Bitcoin in 2009, blockchain has evolved significantly, powering innovations in decentralized finance (DeFi), non-fungible tokens (NFTs), and automated contract execution. Its ability to provide secure, real-time verification of transactions makes it a critical component of modern digital infrastructure.

V. SYSTEM MODULES

The following modules are proposed to be introduced to the gadget:

1. Authority
2. Data Publisher
3. Sanitizer
4. Receiver
5. Cloud Server

Modules Description

- ***Authority Module***
  The governance system oversees and manages the entire framework. In SACS, the authority is considered a trusted entity responsible for maintaining the master encryption key. It assigns unique private keys to each registered user, ensuring that these credentials are securely managed and not shared with unauthorized individuals.
- **Data Publisher Module**
  The data publisher is responsible for generating and encrypting raw data before storing it in the cloud. Encryption is performed using a designated encryption key, and an access control policy is defined to regulate data usage. Data publishers may operate with integrity or act maliciously. While both encrypt data, a malicious publisher might intentionally distribute encryption keys to unauthorized users, leading to security breaches and unauthorized access.
- **Cloud Server Module**
  The cloud server functions as a storage platform for encrypted data. Users with the required decryption keys can retrieve encrypted data from the server. The cloud server receives encrypted files from the sanitization process, ensuring that stored information remains secure.
- **Sanitizer Module**
  The sanitizer plays a crucial role in securing data by transforming potentially compromised encrypted records into a protected format. After receiving encrypted data from the publisher, the sanitizer processes it and ensures that only authorized users can access it. The sanitizer strictly follows security protocols and does not alter the original meaning of the data.
- **Receiver Module**

A receiver is an entity that requires access to encrypted data stored on the cloud server. Before gaining access, the receiver must register in the system and obtain a private key from the authority. Only authorized receivers who meet the specified access conditions can decrypt and retrieve raw data from the publisher. To maintain security, recipients do not share their private keys with unauthorized parties.

- **Cloud Server Security Considerations**
  The cloud server provides a platform for encrypted data storage and retrieval. Any registered user with the appropriate decryption key can access stored information. However, in some cases, a cloud server might engage in malicious activities, such as data deletion or manipulation. The security of SACS is designed to mitigate these risks by ensuring that encryption mechanisms remain robust, regardless of the server's integrity.

VI. RESULTS

Fig 2: Figure of Home Page

Fig 3: Figure of Authority Log in Page

Fig 4: Figure of Data Publisher Registration Page

Fig 5: Figure of Data Publisher Log-in Page

Fig 6: Figure of Authority Home Page

Fig 7: Figure of Data Publishers Approval Page

Fig 8: Figure of Active Data Publishers Page

Fig 9: Figure of Uploading files Page

Fig 10: Figure of Uploaded File List Page

Fig 11: Figure of Downloaded File List

VII. CONCLUSION

Our research focused on enhancing cloud storage security by addressing the risks posed by malicious data publishers. In real-world scenarios, unauthorized users may gain access to encrypted data due to vulnerabilities in existing access control mechanisms. To counteract this, we developed a secure system architecture that effectively mitigates such threats.

The proposed system includes a structured security framework designed to prevent unauthorized decryption attempts. By implementing this approach, we ensure the integrity and confidentiality of stored data. Additionally, our performance analysis validates the effectiveness of the system in maintaining secure access control.

This study serves as a foundation for further advancements in cloud security. Future research can build upon our findings to refine encryption methodologies and strengthen data protection in evolving cloud environments.

REFERENCE

[1] S. Berger et al., "Security intelligence for cloud management infrastructures," IBM J. Res. Develop., vol. 60, no. 4, pp. 11:1–11:13, 2016.

[2] Secure access control for cloud storage. Accessed: Feb. 13, 2021. [Online]. Available: https://www.research.ibm.com/haifa/projects/storage/cloudstorage/secure_access.shtml.

[3] M. T. Beck et al., "Practical strongly invisible and strongly accountable sanitizable signatures," in Proc. Australas. Conf. Inf. Secur. Privacy, 2017, pp. 437–452.

[4] J. Camenisch, D. Derler, S. Krenn, H. C. P€ohls, K. Samelin, and D. Slamanig, "Chameleon-hashes with ephemeral trapdoors – and applications to invisible sanitizable signatures," in Proc. Int. Workshop Public Key Cryptogr., 2017, pp. 152–182.

[5] N. Fleischhacker, J. Krupp, G. Malavolta, J. Schneider, D. Schr€oder, and M. Simkin, "Efficient unlinkable sanitizable signatures from signatures with re-randomizable keys," in Proc. Int. Workshop Public Key Cryptogr., 2016, pp. 301–330.

[6] I. Damgard, H. Haagh, and C. Orlandi, "Access control encryption: Enforcing information flow with cryptography," in Proc. Theory Cryptogr. Conf., 2016, pp. 547–576.

[7] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," IEEE Comput., vol. 48, no. 2, pp. 85–88, Feb. 2015.

[8] P. Patil and M. Sangeetha, ‘‘Blockchain-based decentralized KYC verification framework for banks,’’ Proc. Comput. Sci., vol. 215, pp. 529–536, Jan. 2022, doi: 10.1016/j.procs.2022.12.055.

[9] V. Mani, M. M. Ghonge, N. K. Chaitanya, O. Pal, M. Sharma, S. Mohan, and A. Ahmadian, ‘‘A new blockchain and fog computing model for blood pressure medical sensor data storage,’’ Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108202, doi: 10.1016/j.compeleceng.2022.108202.

[10] X. Qin, Y. Huang, Z. Yang, and X. Li, ‘‘A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing,’’ J. Syst. Archit., vol. 112, Jan. 2021, Art. no. 101854, doi: 10.1016/j.sysarc.2020.101854.

[11] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, ‘‘Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks,’’ Comput. Ind., vol. 144, Jan. 2023, Art. no. 103801, doi: 10.1016/j.compind.2022.103801.

[12] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, ‘‘High-frequency trading on decentralized on-chain exchanges,’’ in Proc. IEEE Symp. Secure. Privacy (SP), May 2021, pp. 428–445, doi: 10.1109/sp40001.2021.00027.

[13] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, ‘‘LedgerDB: A centralized ledger database for universal audit and verification,’’ Proc. VLDB Endowment, vol. 13, no. 12, pp. 3138–3151, Aug. 2020, doi: 10.14778/3415478.3415540.

[14] C. Yue, T. T. A. Dinh, Z. Xie, M. Zhang, G. Chen, B. C. Ooi, and X. Xiao, ‘‘GlassDB: An efficient verifiable ledger database system through transparency,’’ Proc. VLDB Endowment, vol. 16, no. 6, pp. 1359–1371, Feb. 2023, doi: 10.14778/3583140.3583152.

[15] P. Liu, Q. He, and W. Y. Liu, ‘‘CP-ABE scheme supporting attribute revocation and outsourcing decryption,’’ Netinfo Secur., vol. 20, no. 3, pp. 90–97, 2020, doi: 10.3969/j.issn.1671-1122.2020.03.012.