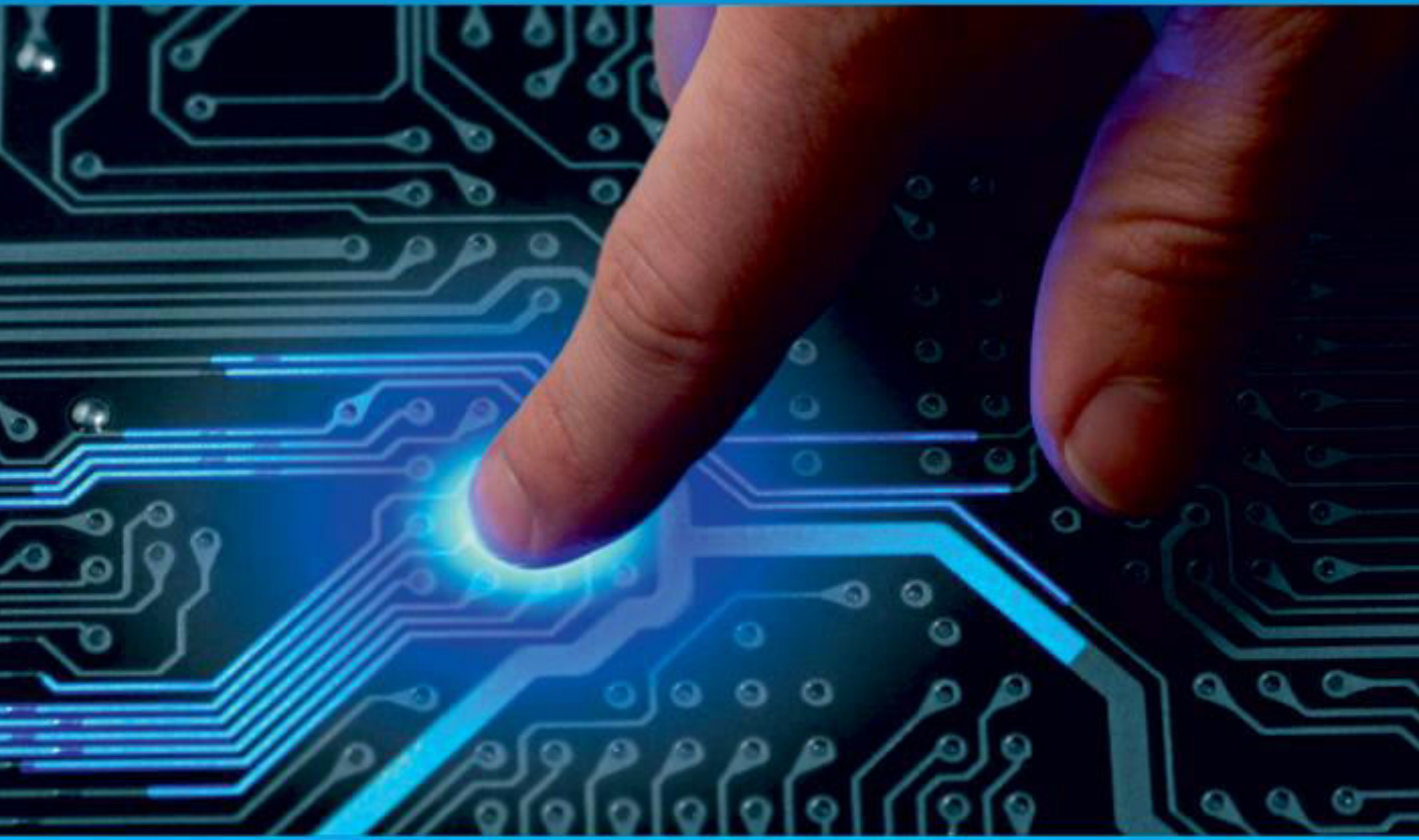
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

Lightweight Cloud Storage Auditing with Deduplication and Privacy

Dr. V. Subrahmanyam, Sanjay Kumar Katta, Anish Sai Bikkumalla, Sanjay Kumar Reddy Rapolu

Associate Professor, Department of CSE, Anurag University, Hyderabad, Telangana, India

Department of CSE, Anurag University, Hyderabad, Telangana, India

ABSTRACT: Cloud storage auditing with deduplication is a method for ensuring data integrity in cloud storage while minimizing storage space by only retaining one copy of duplicated files. However, current schemes are susceptible to brute-force dictionary attacks, compromising user privacy. This paper introduces a novel approach to thwart such attacks in cloud storage auditing with deduplication, prioritizing strong privacy protection. Our scheme ensures that user file privacy remains intact even if files are predictable or originate from a limited space. Key features include a unique method for generating file indexes for duplicate checks and an innovative strategy for file encryption key generation. Moreover, users experience minimal computational burden, as they only need to conduct lightweight operations for data authentication, integrity verification, and file retrieval from the cloud. Rigorous security proofs and performance assessments underscore the effectiveness and efficiency of our proposed scheme.

KEYWORDS: Agency Server (AS), Data encryption, Lightweight computations, Security analysis, Privacy protection, Inter-user deduplication, Encryption keys, File indices.

I. INTRODUCTION

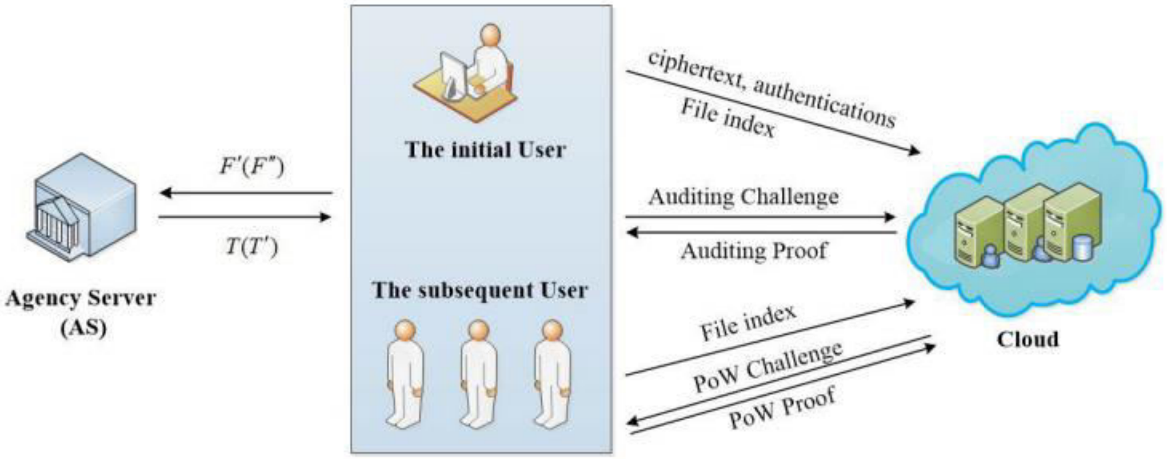
The widespread adoption of cloud computing has led to a surge in the use of cloud storage solutions by both individuals and businesses. This is mainly due to their advantages, including easy access, cost-effectiveness, and flexible services. However, this shift also brings about concerns regarding the security and confidentiality of data stored in the cloud. There's always a risk of data being corrupted or lost due to various factors like errors in operations or failures in hardware. Additionally, a considerable amount of data in the cloud consists of duplicated copies, prompting the need for techniques like data deduplication to make storage more efficient. In response to these challenges, our proposed system focuses on improving the process of auditing cloud storage while also ensuring strong protection of users' privacy. Traditional methods, like convergent encryption (CE), lack sufficient security measures, leaving them vulnerable to attacks like brute-force dictionary attacks. To address this vulnerability, we introduce a fresh approach for generating file indices and implement an innovative method for encrypting files. By using an Agency Server (AS) to generate file indices and employing file labels for encryption key derivation, our system effectively shields user privacy from potential threats posed by the cloud and other parties. Furthermore, our system facilitates efficient deduplication of data and authenticators among users who have identical files, thereby enhancing storage efficiency within the cloud environment. Additionally, to ease the computational burden on users, our system minimizes the amount of computation required for various tasks such as generating data authenticators, verifying the integrity of cloud data, and retrieving files. Through thorough security analysis and practical implementations, our proposed scheme demonstrates its effectiveness in achieving accuracy, reliability, and robust privacy protection, thereby ensuring the safety and integrity of user data stored in the cloud.

II. RELATED WORK

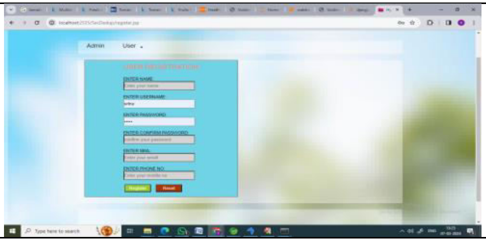
Users often encrypt their data before storing it in the cloud to maintain the confidentiality of their sensitive information from both the cloud provider and other potential threats. Convergent encryption (CE) emerged as a solution to enable deduplication of encrypted data. CE encrypts data using a key derived deterministically from the data itself, typically through techniques like hashing. This means that identical files will produce identical ciphertexts, facilitating deduplication. However, CE has its vulnerabilities, especially when dealing with predictable files or those from a limited space, making it susceptible to brute-force dictionary attacks. To address this issue, Li et al. proposed a scheme integrating a key server to assist users in generating convergent keys securely. This scheme prevents the cloud from deducing the convergent key directly from the file content by embedding a secret "seed" within the convergent key. Despite this enhancement, the scheme remains vulnerable to brute-force attacks since the key server can potentially guess or derive the file's content from its hash value, undermining its effectiveness in preventing such attacks. Moreover, in most deduplication schemes, users are required to generate a file index and provide it to the cloud for duplicate checking. Typically, the hash value of the file serves as the file index. However, this approach poses a risk to data privacy, as malicious parties could potentially infer the file's content through brute-force dictionary attacks on the hash value. Therefore, ensuring deduplication while maintaining strong privacy protection in cloud storage auditing is a crucial challenge that previous schemes have struggled to address adequately due to their vulnerability to brute-force attacks.

III. PROPOSED SYSTEM

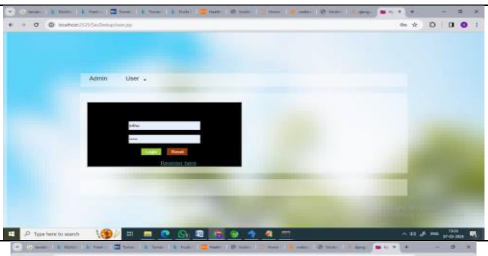
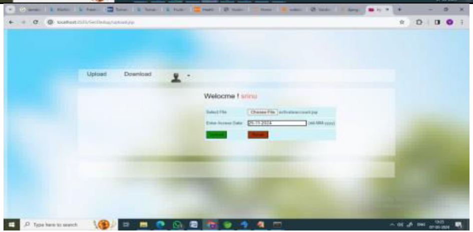
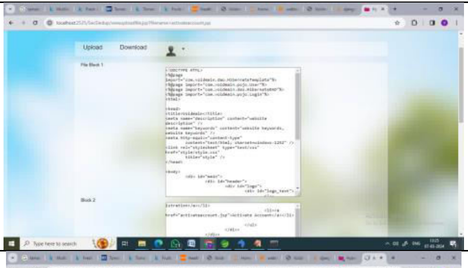
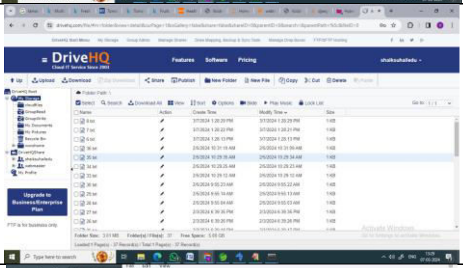
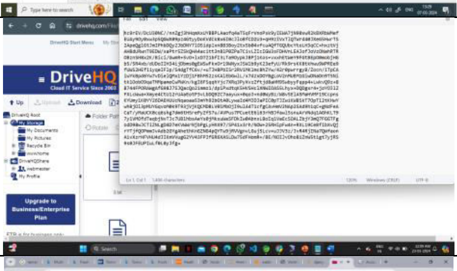
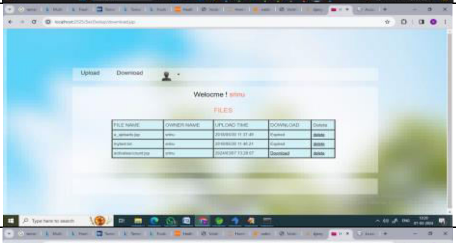
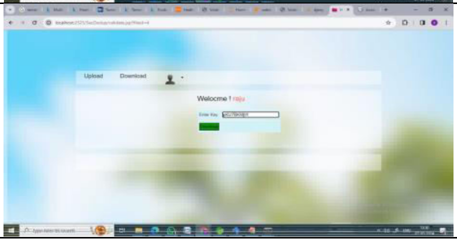
This paper delves into the challenge of thwarting brute-force dictionary attacks and achieving robust deduplication with stringent privacy protection in cloud storage auditing. A specific scheme is proposed to address this concern comprehensively. To ensure robust deduplication while safeguarding privacy, innovative methods are devised for both file index generation and encryption key derivation. Notably, the file index is crafted with assistance from an Agency Server (AS), deviating from the conventional reliance solely on file hash values. Encryption keys are generated using a combination of the file itself and a confidential file label, known only to the user. This approach shields the privacy of user files from potential breaches by both the cloud and the AS. To optimize storage efficiency, users with identical files can produce identical ciphertexts and authenticators, facilitating effective data and authenticator deduplication. Moreover, to alleviate computational strain on users, lightweight computations suffice for tasks such as authenticator generation, cloud data integrity verification, and file retrieval from the cloud. Through a comprehensive security analysis, the proposed scheme is demonstrated to fulfill correctness, soundness, and robust privacy protection criteria. Furthermore, concrete implementations underscore the efficiency of the proposed approach.



IV. EXPERIMENTAL RESULTS

Image	Description
	The user registration page, here the user who is new must provide the details and register themselves. The user can login directly if they are already registered.

ENTER NAME
ENTER USERNAME
ENTER PASSWORD
ENTER CONFIRM PASSWORD
ENTER MAIL
ENTER PHONE NO

	The login page, student and admin can login with their credentials Student's credentials will be created by admin and shared with students.
	This is the page that opens once the user logins. Here, the user needs to upload the file that he wants to and enter the access date and then click on the upload button. Access date here is the date up to which the file can be accessed.
	After the user uploads the file, the file which is uploaded by the user is divided into different blocks based on the file size or the file length.
	This is the cloud storage. All the files uploaded by the user are stored here after they are divided into blocks. If the content of any two blocks is same it won't be stored again.
	The files stored in the cloud are in the encrypted form. Even if someone tries to open any block of the file, the encrypted form of the file is opened.
	This shows the files of the current user. The user can access the files uploaded. The user can delete the file uploaded by him. And download the file uploaded by him until the file has reached the access date. He can not download the file once it is expired.
	This is the key validation of the other user. The user enters the key given by the other user and validates it for the file download of the other user.

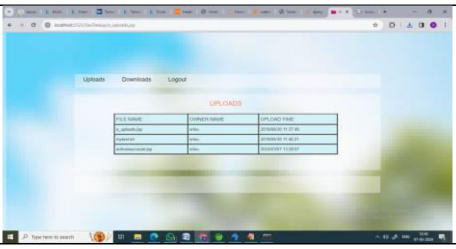
 Uploads Downloads Logout UPLOADS FILE NAME | OWNER NAME | UPLOAD TIME a_uploads.jsp | [illegible] | [illegible] mytest.txt | [illegible] | [illegible] [illegible] | [illegible] | [illegible]	This is the admin portal where all the details of the file are available. The admin portal shows the file details like name of the file, who uploaded it, when was it uploaded and also the access date of the file.

Table: Output and the description

V. Conclusion and Future Work

In summary, the proposed scheme for auditing cloud storage with deduplication presents a robust solution to the challenges of maintaining data integrity and privacy in cloud environments. By introducing innovative techniques for creating file indices and encryption keys, utilizing an Agency Server for index management, and streamlining computations to reduce user workload, this system effectively addresses existing limitations. Rigorous security assessments and practical implementations validate its ability to protect user privacy, enhance storage efficiency, and uphold strong security standards. Therefore, this approach holds promise for improving cloud storage auditing while ensuring robust privacy safeguards for user data.

Looking ahead, future efforts could concentrate on enhancing the scalability and compatibility of the proposed system to handle larger data volumes and diverse cloud setups. Additionally, exploring the integration of cutting-edge technologies like blockchain and homomorphic encryption could further elevate security and privacy standards. Moreover, conducting real-world deployments and trials in collaboration with cloud providers and businesses would offer valuable insights into the practicality and effectiveness of the proposed solution. Overall, ongoing refinement and development of this scheme have the potential to significantly advance cloud storage auditing and privacy protection in the ever-evolving realm of cloud computing.

References

[1] The Gnu Multiple Precision Arithmetic Library (GMP). Accessed: Oct. 2019. [Online]. Available: http://gmplib.org/

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song,‘‘Provabledatapossessionatuntrustedstores,’’inProc.14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.

[3] M.Bellare, S.Keelveedhi, and T.Ristenpart,‘‘Message-locked encryption and secure deduplication,’’ in Proc. Annu. Int. Conf. Theory Appl. Crypto- graph. Techn. Berlin Germany: Springer, 2013, pp. 296–312.

[4] H.Cui, R. H. Deng,Y. Li,andG. Wu,‘‘Attribute-based storage supporting secure deduplication of encrypted data in cloud,’’ IEEE Trans. Big Data, vol. 5, no. 3, pp. 330–342, Sep. 2019.

[5] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, ‘‘Lightweight privacy- preserving identity-based verifiable IoT-based health storage system,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8393–8405, Oct. 2019.

[6] J. Gantz and D. Reinsel. (2012). The Digital Universe Decade– Are You Ready (2010). [Online]. Available: http://www.emc.com/collateral/analyst-reports/idcdigital-universe-are-you-ready.pdf

[7] X. Ge, J. Yu, H. Zhang, C. Hu, Z. Li, Z. Qin, and R. Hao, ‘‘Towards achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification,’’IEEE Trans. Dependable Secure Com- put., to be published.

[8] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, and J. Ma, ‘‘Data integrity auditing without private key storage for secure cloud storage,’’ IEEE Trans. Cloud C.

[9] S. Keelveedhi, M. Bellare, and T. Ristenpart, ‘‘Dupless: Server-aided encryption for deduplicated storage,’’ in Proc. 22nd Secur. Symp., Washington, DC, USA, 2013, pp. 179–194.

[10] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. M. Hassan, and A. Alelaiwi, ‘‘Secure distributed deduplication systems with improved reliability,’’ IEEE Trans. Comput., vol. 64, no. 12, pp. 3569–3579, Dec. 2015.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details