International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com
doi : https://doi.org/10.32628/IJSRCSEIT

Efficient Public Integrity Auditing of Collaboratively Stored Data in Cloud Storage with User Privacy Preservation

Maheshwari Patil[1], **Dr. H K Krishnappa**[2]

[1]PG student, [2]Associate Professor

Department of Computer Science & Engineering, RV College of Engineering, Bengaluru-560059, India

ARTICLEINFO

Article History:

Accepted: 05 Sep 2023

Published: 20 Sep 2023

Publication Issue

Volume 9, Issue 5

September-October-2023

Page Number

140-144

ABSTRACT

People can efficiently check the accuracy of data kept in cloud storage using the Provable Information Possession (PDP) approach. This becomes more important when sensitive material is exchanged across numerous users via cloud storage, as maintaining the uploader's anonymity in the eyes of the auditor is crucial. During the auditing procedure, the auditor shouldn't be able to tell who uploaded the data. To address this challenge, numerous PDP schemes have been developed with a focus on preserving user identity privacy.

Nonetheless, numerous of these suggested approaches depend on Public Key Infrastructure (PKI) methods, which bring about the substantial challenge of managing certificates. Additionally, data auditors in most of these schemes are saddled with heavy computational costs, resulting in reduced efficiency. To overcome these shortcomings, we introduce an innovative identity-based PDP protocol designed to efficiently audit the integrity of data shared within a group while preserving the uploader's privacy. Leveraging the inherent structural advantages of identity-based cryptographic mechanisms, our PDP scheme mitigates the challenges associated with certificate management. Importantly, our approach diverges from prior works by establishing the relationship between the data and the data uploader during the proof generation phase rather than the integrity auditing phase. In summary, our identity-based PDP protocol offers an elegant solution to the problem of verifying data integrity in a group-shared context while safeguarding the privacy of the data uploader. By sidestepping the complexities of certificate management and optimizing the proof generation process, our scheme enhances the efficiency and security of data auditing in cloud storage scenarios.

Keywords : Provable Information Possession, Data Integrity

I. INTRODUCTION

In contemporary times, the exponential expansion of data has imposed a considerable load on both individuals and entities in terms of local data storage and administration. To alleviate this burden, an increasing population is turning to cloud storage services, opting to outsource their data to cloud servers as a means of cost reduction. Cloud storage not only offers cost savings but also provides convenient data sharing capabilities, enabling collaborative work among teams. However, it's important to note that cloud service providers (CSPs) are not always completely trustworthy. Data stored with CSPs can be vulnerable to corruption or deletion due to various factors such as hardware errors, network disruptions, software glitches, or human errors. To avoid the economic ramifications and protect their reputation, CSPs might not disclose the truth to data users when such incidents occur.
As a result, it becomes imperative for users to routinely validate the authenticity of their data stored on cloud servers. The Provable Data Possession (PDP) model presents an effective solution for users to remotely ascertain the integrity of their data residing in the cloud. PDP breaks down the outsourced data into smaller data blocks, associating each with a unique tag. As these tags contain the values of the respective data blocks, users can determine the integrity of each data block by verifying the validity of its associated tag. To date, several PDP schemes with public verification have been proposed.

Nonetheless, the majority of these PDP protocols primarily concentrate on verifying the integrity of data specific to individual users. In real-world situations, data sharing among multiple users is a prevalent practice, and this shared data is often accessible to any member within a collaborative workgroup. Consequently, the paramount challenge is to guarantee the integrity of shared data while safeguarding the anonymity of the data uploader in the presence of third-party auditors (TPAs). It is of utmost importance that TPAs remain unaware of the identity of the data uploader throughout the integrity auditing process. In pursuit of this objective, a concrete PDP protocol has been proposed, incorporating the concept of user privacy preservation for shared data. This protocol employs group signature techniques to protect user privacy from TPAs. Subsequently, several schemes with user privacy preservation have been put forward. Nevertheless, the majority of these PDP schemes rely on Public Key Infrastructure (PKI) techniques, which bring about certificate management challenges, including certificate generation, distribution, revocation, renewal, updating, and verification. To address these certificate management issues, some researchers have turned to identity-based cryptography and certificateless cryptography to design PDP schemes with user privacy preservation. However, these schemes have been found to lack computational efficiency for practical application. Hence, there is a pressing need to develop more efficient PDP schemes that preserve user privacy for cloud data auditing.In conclusion, the rapid expansion of data and the reliance on cloud storage have given rise to the need for robust integrity verification mechanisms. PDP models offer a solution, and efforts are ongoing to enhance these models, particularly in scenarios involving shared data and user privacy preservation, while addressing the challenges associated with certificate management and computational efficiency.

II. LITERATURE SURVEY

[1] The authors of the paper "SeDaSC: Secure data sharing in clouds" include M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya.

The paper titled "SeDaSC: Secure data sharing in clouds" introduces a novel approach to securely share data within cloud environments. The authors propose a secure data sharing scheme that ensures the confidentiality, integrity, and availability of data shared among multiple parties in a cloud setting.

This scheme is built upon the concept of secret sharing, which involves dividing the original data into multiple shares, each distributed among various parties. The scheme employs a hierarchical structure in which each party is assigned a role based on their level of trustworthiness. The more trustworthy the party, the more critical their role within the scheme.

[2] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and F. Liming, "Secure keyword search and data sharing mechanism for cloud computing," "In 'IEEE Transactions on Dependable and Secure Computing,' the article was made available in early access on January 3, 2020, with the digital object identifier (DOI) 10.1109/TDSC.2020.2963978."

The paper titled " A secure mechanism for keyword search and data sharing in cloud computing. " was published in the IEEE Transactions on Dependable and Secure Computing journal. It discusses a mechanism designed to enable secure keyword search and data sharing within cloud computing environments.

Cloud computing has gained popularity due to its cost-effectiveness, scalability, and flexibility. However, as data increasingly resides in the cloud, concerns regarding security and privacy have emerged. One significant concern involves the security of keyword searches in the cloud, as the cloud service provider may have access to plaintext data and search queries, potentially leading to privacy breaches.

[3] G. Chunpeng, Z. Liu, J. Xia, and F. Liming, ""Identity-Based Broadcast Proxy Re-encryption for Cloud Data Sharing with Revocability"," IEEE Trans. Dependable Secure Comput., early access, Feb. 14, 2019, doi: 10.1109/TDSC.2019.2899300.

The paper titled " "Revocable Identity-based Broadcast Proxy Re-encryption for Secure Data Sharing in Cloud Environments" " Presents an innovative approach for ensuring secure data sharing within cloud computing environments. This approach seamlessly integrates identity-based encryption, proxy re-encryption, and broadcast encryption techniques, empowering data owners to selectively grant access to user groups based on their identities.

The proposed scheme aims to overcome the limitations of existing data sharing schemes that rely on traditional encryption techniques, which typically necessitate sharing encryption keys with all authorized users, leading to inefficiencies and potential security risks, particularly in large-scale data sharing scenarios.

[4] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," In the proceedings of the conference "Hot Topics in Cloud Computing," held in San Diego, California, USA, in 2009,

The article titled "Towards Trustworthy Cloud Computing" was presented by N. Santos, K. P. Gummadi, and R. Rodrigues was presented at the Hot Topics in Cloud Computing Conference in San Diego, California, in 2009.

The paper explores the challenges and opportunities presented by cloud computing, which involves delivering computing resources (e.g., servers, storage, software) over the Internet. While cloud computing offers potential cost savings and increased efficiency for organizations, it also raises significant security and privacy concerns.

The authors argue that trust is a critical component of cloud computing, and cloud providers must adopt transparent and verifiable practices to establish trust with their customers. They propose a framework for building trusted cloud computing systems, encompassing mechanisms for measuring and enforcing security and privacy requirements, as well as providing transparency and accountability to customers. The paper also discusses specific techniques for achieving trust in cloud computing, including encryption, multi-factor authentication, and secure data deletion.

[5] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Inf. Sci., vol. 305, pp. 357–383, Jun. 2015.

The paper titled "Security in cloud computing: Opportunities and challenges," authored by M. Ali, S.

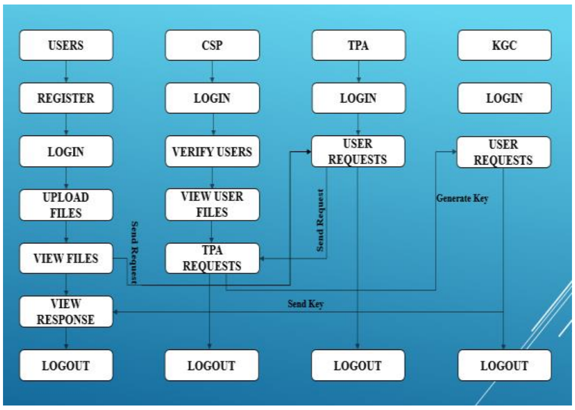
U. Khan, and A. V. Vasilakos, was published in the journal Information Sciences in June 2015. The paper delves into the security challenges and opportunities associated with cloud computing.

The paper provides an overview of cloud computing, including its various service models (SaaS, PaaS, IaaS) and its advantages such as cost-effectiveness, scalability, and flexibility. However, it also highlights the security challenges inherent in cloud computing, encompassing data privacy, data integrity, authentication, and access control. To mitigate these security risks, the authors discuss various security measures such as encryption, access control, and intrusion detection and prevention systems.

III.Methodology

3.3 Proposed System

We introduce a novel identity-based PDP protocol to efficiently audit the integrity of shared group data while protecting the uploader's anonymity. Our PDP system is able to get around the certificate management issue because of the identity-based crypto mechanism's intrinsic structural advantage. In contrast to earlier efforts, our technique maintains the relationship between the data and the data uploader at the generation of the evidence rather than during the integrity audition. As a result, neither the data uploader who extracted the challenged data nor the data auditor have any idea of the relationship. The computation required by the data auditor can be significantly decreased by establishing the association using cloud server during the evidence generation step.



Implementation:

ALGORITHM:

Derive Round Keys: The first step is to derive a set of round keys from the original cipher key. These round keys will be used in the subsequent rounds of encryption.

Initialize State Array: The state array is initialized with the plaintext data block, which is the 128-bit data that you want to encrypt. This data block is converted into a two-dimensional byte array of four rows and four columns.

Add Initial Round Key: The starting condition array receives the initial cycle key. The state arrays and the round key are bit-wise XO Red to accomplish this.

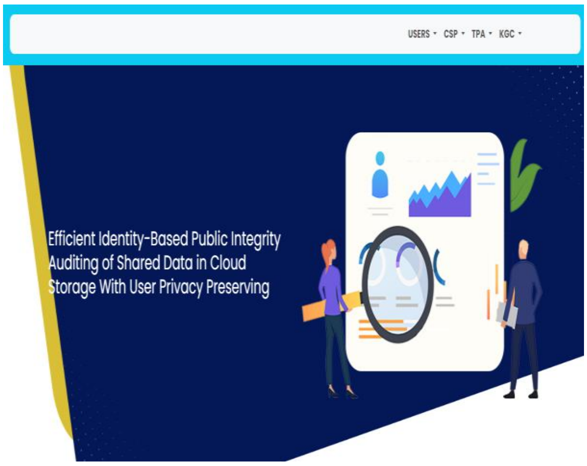
State Manipulation over Nine Rounds: AES frequently calls for state manipulation in nine cycles. The state of an array's bytes are substituted, permuted, and mixed during each round, and are made up of multiple operations. During these rounds, these procedures are carried out iteratively. Tenth and Concluding Round: The tenth and ultimate round of state manipulation distinguishes itself somewhat from the preceding nine rounds. It includes similar operations but without the final Mix Columns step.

Copy Final State Array: After the tenth round, the final state array represents the encrypted data, which is also known as the ciphertext. This state array is copied out as the output of the encryption process.

It's important to emphasize that AES functions with byte units, meaning the initial 128-bit data block is initially transformed into 16 bytes. The operations within AES are executed on the state array, structured as a two-dimensional byte array consisting of four rows and four columns. This array is manipulated in each round to achieve the encryption.

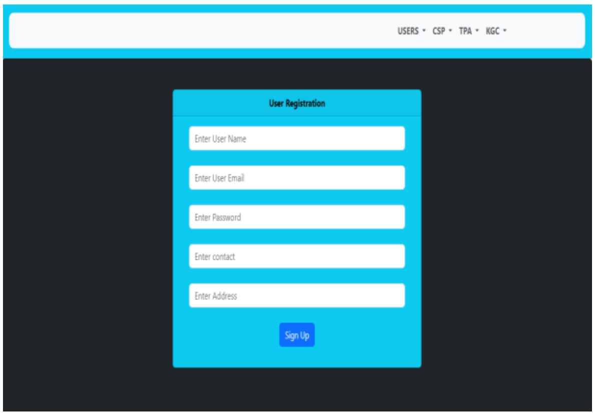
Implementation process:

Results: Home page: Efficient identity-based public integrity auditing with user privacy protection of shared data in cloud storage.



Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving

User Registration: user will register with the user name, email, password, contact, address



User Registration

Enter User Name

Enter User Email

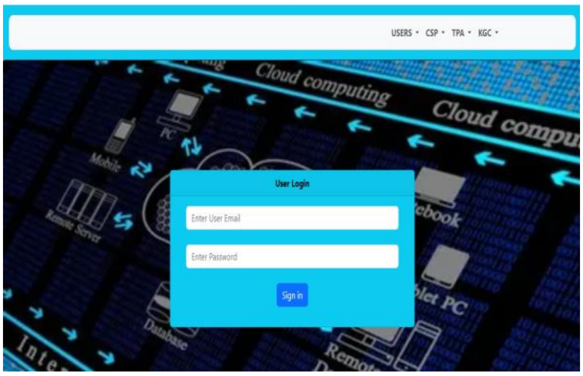
Enter Password

Enter contact

Enter Address

Sign Up

User Login:



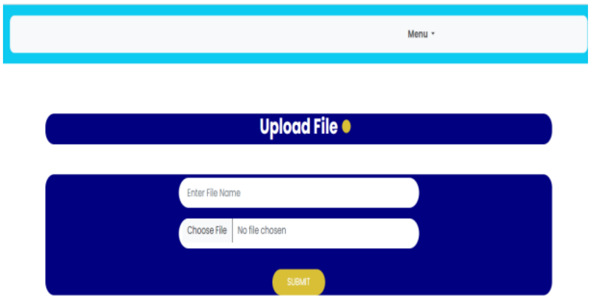
User Login

Enter User Email

Enter Password

Sign in

Upload file:



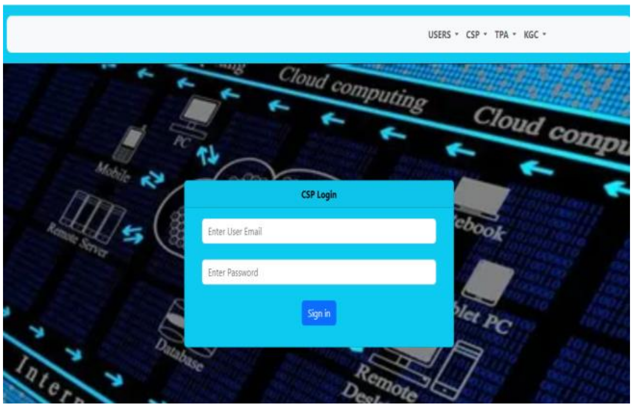
Upload File

Enter File Name

Choose File No file chosen

SUBMIT

Cloud server login:



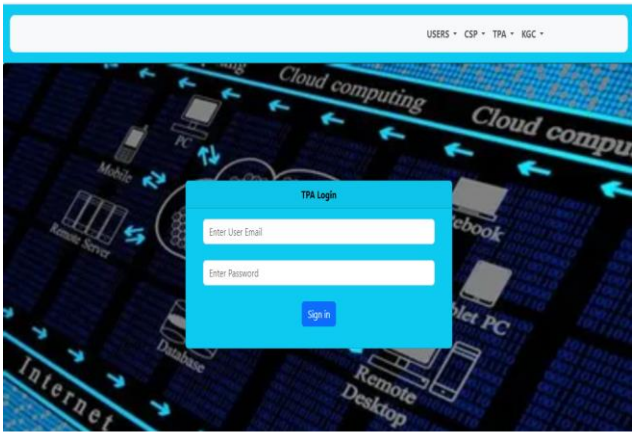
CSP Login

Enter User Email

Enter Password

Sign in

TPA login:



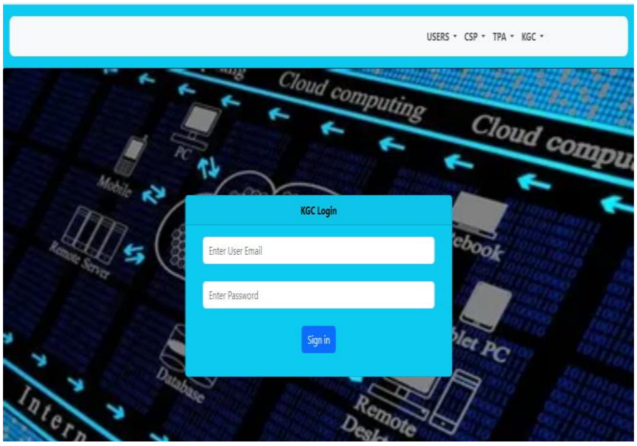
TPA Login

Enter User Email

Enter Password

Sign in

Kgc login:



IV.CONCLUSION

We present a publicly accessible identity-based Provable Data Possession (PDP) protocol meticulously crafted to protect the anonymity of numerous users from unwarranted scrutiny. This protocol empowers a Third-Party Auditor (TPA) to meticulously verify the integrity of data shared within a group, all while upholding the confidentiality of the uploader's identity, even in the event of any issues. Within our system, user privacy holds paramount importance. The TPA possesses the ability to thoroughly evaluate data integrity, yet it remains entirely unaware of the identity of the entity responsible for uploading any questionable content. This balance between data integrity verification and user privacy is a fundamental aspect of our protocol. We have established a comprehensive security model for our system, which has undergone rigorous testing to demonstrate its reliability, soundness, and its robust protection of user privacy. Our protocol represents an innovative approach to Provable Data Possession that effectively addresses the critical issue of user identity privacy.

V. REFERENCES

[1]. M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, “SeDaSC: Secure data sharing in clouds,” IEEE Syst. J., vol. 11, no. 2, pp. 395–404, Jun. 2017.

[2]. C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and F. Liming, “Secure keyword search and data sharing mechanism for cloud computing,” IEEE Trans. Dependable Secure Comput., early access, Jan. 3, 2020, doi: 10.1109/TDSC.2020.2963978.

[3]. G. Chunpeng, Z. Liu, J. Xia, and F. Liming, “revocable identitybased broadcast proxy re-encryption for data sharing in clouds,” IEEE Trans. Dependable Secure Comput., early access, Feb. 14, 2019, doi: 10.1109/TDSC.2019.2899300.

[4]. N. Santos, K. P. Gummadi, and R. Rodrigues, “towards trusted cloud computing,” in Proc. Conf. Hot Topics Cloud Comput., San Diego, CA, USA, 2009, pp. 14–19.

[5]. M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Inf. Sci., vol. 305, pp. 357–383, Jun. 2015.

[6]. L. Chen, J. Li, Y. Lu, and Y. Zhang, “Adaptively secure certificate-based broadcast encryption and its application to cloud storage service,” Inf. Sci., vol. 538, pp. 273–289, Oct. 2020.

[7]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Alexandria, VA, USA, 2007, pp. 598–609.

[8]. H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Melbourne, VIC, Australia, 2008, pp. 90–107.

[9]. A. Juels and B. S. Kaliski, “PORs: Proofs of retrievability for large files,” in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584–597.

[10]. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proc. 4th Int. Conf. Secur. Privacy Commun. Netowrks (SecureComm), 2008, pp. 1–10.

Cite this article as :

Maheshwari Patil, Dr. H K Krishnappa, "Efficient Public Integrity Auditing of Collaboratively Stored Data in Cloud Storage with User Privacy Preservation", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp. 140-144, September-October-2023.