Migration Letters

Volume: 21, No: S5 (2024), pp. 1628-1635

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Multi Authority Based Data Sharing And Time Server Data Searching In Cloud Computing

[1]Dr.M. Dhurgadevi, [2]Guruprasath S L, [3]Hari Balan T, [4]Harish B

Abstract

Searchable encryption shows promise as a technique for cloud-based information retrieval services, aiding in the organization of connections between files and keywords. Several people are choosing the cloud which stores data of them. This "cloud computing" trend lets you save all your files on remote servers accessible from anywhere with an internet server. With cloud services, users can seamlessly utilize on-demand applications without concerns about local infrastructure limitations. Collaborative connections among different users are common, making data sharing crucial for achieving productive benefits. In this research, we present a data sharing model based on shared authority to tackle the privacy issues associated with cloud storage. The project's goal is to create shared access authority by giving security and privacy equal priority through the use of an anonymous access request matching mechanism. To obtain access to the data, approval must be granted by both the cloud servers and the data owner. Symmetric key cryptography must be used in cloud computing environments to provide data security and privacy. As cloud users increasingly entrust cloud services with the storage, processing, and transportation of sensitive data, it becomes imperative to offer robust cryptographic algorithms. The data is transmitted to the shared access authority for distribution to the designated users in this project. There have been enhancements to the time server access mechanism within the secure cloud data search. To view the file list or initiate a search for a specific file, users are required to obtain permission from the central server. The user has 30 seconds after the main server accepts their request to either choose a file from the list or search for the file they want and request access to it. If there is no response from the user within this 30-second timeframe, the main server will automatically redirect the user to the homepage. If the user needs to see the file list again, he or she must connect to the main server.

Keyword: *Privacy, Data sharing, shared authority, Cloud Computing, Time sever.*

I INTRODUCTION

Cloud data out[1]sourcing services facilitate the smooth transmission of data from the user to the cloud server by giving users access to either an infinite or constrained pool of resources. The remote nature of data storage, retrieval, and sharing raises security concerns even while the costs of local data administration are significantly reduced. Access to cloud data must now be secured, and one key strategy is to use encryption, then outsourcing in conjunction with quick recovery support [2]. Keyword index data structures are frequently employed to improve the efficiency of data retrieval. By building connections between files and keywords, these structures let users find and filter relevant content with ease. In the

[1]Associate Professor, Department of Computer Science & Engineering, Sri Krishna college of Technology, Coimbatore, Tamil Nadu, India.
[2,3,4]Department of Computer Science & Engineering, Sri Krishna college of Technology, Coimbatore, Tamil Nadu, India.

case of encrypted cloud storage services, where data privacy is a top priority, this strategy is essential. Data owners encrypt their papers and the keywords linked to them before uploading them to the cloud in order to safeguard critical information. Effective keyword searches over the encrypted data are thus made possible by specialized data encryption techniques that are implemented within the cloud environment, guaranteeing anonymity while still permitting rapid retrieval. [2].

This paper presents a new way to share data securely in the cloud called "Multi-server." It lets readers access documents stored in someone else's cloud storage (the "data writer") without the cloud itself being able to figure out what keywords the reader is searching for. This is achieved using a special type of encryption called "boolean searchable symmetric encryption," where the reader's search query actually acts as the key for the data writer. Additionally, the data is split and stored across two separate cloud servers, preventing any single server from knowing the complete picture and acting maliciously. This "multi-server" approach also allows for checks to be performed on the reader's search patterns, ensuring they are valid and not just random guesses trying to crack the encryption.

Modern mail servers, file servers, IMAP servers [3], and other data storage servers typically require total trust because they have access to data and are counted on to protect it from unwanted exposure. In many applications, this reliance on trust leads to unfavorable security and privacy issues. The construction of secure mail servers and encrypted file systems has been demonstrated in earlier studies; nevertheless, these innovations frequently result in functionality being sacrificed in order to maintain security. Finding workable solutions for a wide range of computation problems over encrypted data is a major difficulty because of the intricacy of moving computation to data storage when the data is encrypted.

Song et al. introduced searchable encryption, which provides a cryptographic base for search operations on encrypted data files. It can appear in both pk and symmetric forms. The first, known as symmetric searchable encryption [6], performs admirably when it comes to search operations, but it struggles with data sharing because of the complex distribution of secret keys. The complexity emerges when clients need to share the required secret key for decryption while distributing an encrypted data file to others. On the contrary, public key searchable encryption [6], employed in data exchange, surpasses symmetric searchable encryption in terms of versatility. Using public key searchable encryption, a server can validate if an encrypted data file matches the associated query using a search token, all without obtaining any information about the specific query.

II BACKGROUND STUDY

The cloud has become a game changer, slashing the costs of computing resources like hardware and software. But keeping things secure has its own hurdles. That's why encrypting data before it sails off to the cloud has become standard practice. Now, the twist: searching and sharing encrypted data isn't nearly as smooth as working with the raw stuff. This throws a curveball at cloud service providers, because users still expect lightning-fast searches and accurate results, all while their data stays under lock and key. To address these challenges, we propose an approach centered around Our proposed solution, Ciphertext-Policy Attribute with Keyword Search and Data Sharing (CPAB-KSDS), is designed to enhance the security of encrypted cloud data. Unlike existing alternatives that focus on a single aspect, our system not only enables attribute-based keyword search but also supports attribute-based data sharing. Moreover, our platform allows for the modification of keywords during the sharing phase without requiring interaction with the Public Key Generator (PKG). This paper aims to introduce CPAB-KSDS, delineating its security model and offering a comprehensive explanation of the specific technique employed. Additionally, we will showcase its resilience against chosen ciphertext and chosen keyword attacks within the random oracle model. Finally,

performance and property comparisons will highlight the practicality and efficiency of the proposed construction[1].

Ming Zeng and his colleagues [6] highlight the significant role cloud storage plays in remote data management services, emerging as a primary industry. However, this development brings about security challenges, and encryption stands out as the most effective means to mitigate data disclosure risks. PKSE is particularly promising in this regard, allowing clients to efficiently search through encrypted data files. In the PKSE process, when a client initiates a query for data files, it creates a search token. This token is then employed by the cloud server to carry out the inquiry on encrypted data files. Notably, when PKSE encounters the cloud, it becomes susceptible to a major attack. Formally, the cloud server possesses the ability to extract information from a newly added encrypted data file, containing the previously requested keyword, using the received search tokens and privacy information. To tackle this concern, we introduce a forward-secure public key searchable encryption system, ensuring that the cloud server remains oblivious to any specifics about a recently added encrypted data file that includes the previously queried keyword. We outline the framework for constructing forward-secure F-(SEABE) and provide insights into the design methodology. Ultimately, the effectiveness of our approach is confirmed through experimental results.

Attribute-Based Encryption (ABE) emerges as a promising cryptographic method that significantly expands the scope of access control mechanisms [10]. The increasing complexity of ABE regulations poses computational challenges in key issuance and decryption processes. While existing Outsourced ABE systems can delegate specific computationally intensive tasks to a third party, ensuring the verifiability of outcomes remains an unexplored issue. To address this challenge, we introduce an innovative secure Outsourced ABE system that enables both the secure outsourcing of key issuance and decryption processes. Our novel approach assigns the responsibilities related to access policy and attribute management during key issuance or decryption processes to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively. This results in a well-defined set of straightforward tasks for attribute authorities and eligible users to perform locally. Additionally, we present an externally managed ABE framework that facilitates the efficient verification of the outsourced computation results, representing a groundbreaking advancement. Comprehensive evaluations of both security and performance confirm that the proposed systems are both resilient and practical [10].

III PROBLEM DEFINITION

Current systems addressing data sharing scenarios, particularly those not involving multiauthority data sharing, have failed to sufficiently acknowledge the inherent threat posed by keyword guessing. Moreover, the integration of these schemes with existing security measures against keyword guessing attacks appears uncomplicated, as modules like IBE or ABE might lead to increased data sharing costs. The growing dependence on cloud services enables individuals to freely upload and distribute more files than usual. However, persistent concerns related to security and privacy continue to present challenges. Additionally, shared files remain in the cloud indefinitely, escalating the risk of data exploitation by both members of the cloud group and service providers.

IV PROPOSED MODEL

In this research, we address the privacy concern mentioned earlier by proposing a shared authority model for cloud data storage. This model facilitates authentication and permission processes without compromising user confidentiality. We identify a new privacy challenge in cloud storage and specifically focus on addressing a nuanced privacy issue that arises when a user requests data sharing from the cloud server. In such a scenario, the requested access should not reveal the user's private information, even if access authority is granted.

We introduce an authentication system designed to enhance the privacy of user access requests, ensuring that anonymous access requests can still achieve shared access authority. The security and privacy of data in cloud computing environments heavily rely on symmetric key cryptography. Given the increasing reliance of cloud users on services for storing, processing, and transporting sensitive data, the provision of robust cryptographic algorithms becomes crucial.

Our project incorporates a system for anonymous access requests, fostering shared access authority while giving priority to security and privacy. Access to the data is contingent upon approval from both the cloud servers and the data owner, emphasizing a dual-layered authorization process. In this project, data is sent to the shared access authority for distribution to relevant users, enhancing the time server access technique in secure cloud data search.

To view the file list or search for a specific file, users must obtain permission from the main server. Upon accepting the user's request, the main server grants a 30second window for the user to select a file or perform a search and request access. If there is no response within 30 seconds, the primary server redirects the user to the homepage. Users need to reconnect to the main server to access the file list again.

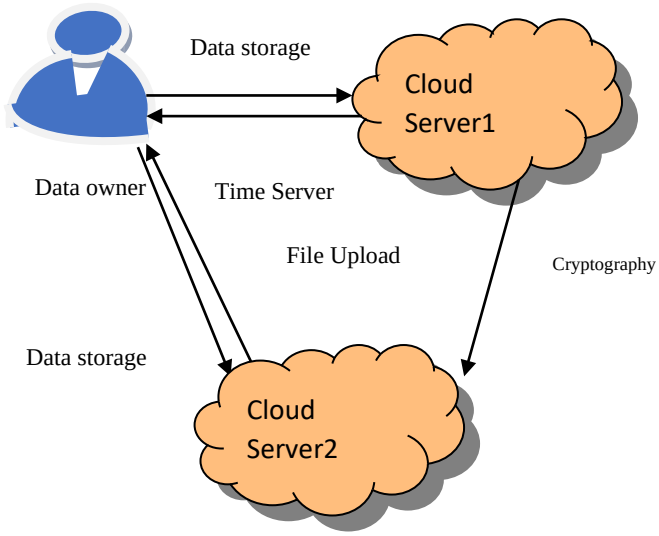

Fig.1.The system model

V RESULTS AND DISCUSSION

The architecture of the system is designed to be both scalable and adaptable to evolving requirements. It can easily accommodate fluctuations in data volume or the number of authorities without compromising performance or security. Introducing a time server to data searching introduces a temporal dimension, enabling users to access information based on specific time intervals.

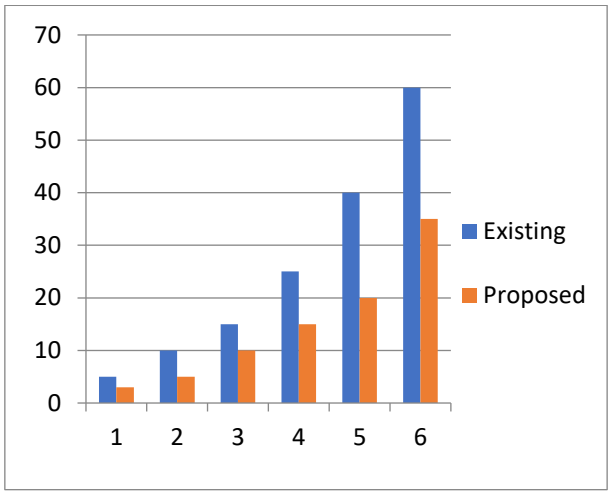

Fig.2. Communication cost in proof stage

Our analysis focuses on comparing the computational costs of our approach with three alternative methods in key stages, namely tag creation in the setup stage, proof generation in the proof stage, and proof verification in the proof stage. Our research is conducted within the framework of a multi-authority data exchange system. The evaluation initially addresses the communication burden during the proof phase. The proposed multi-authority based data sharing checks and dynamic data storage are implemented using Java for rigorous testing. We present a secure cloud storage system featuring a robust cloud security mechanism.

Furthermore, our findings are extended by enabling the multi-server to efficiently and concurrently perform audits for multiple clients.

KeyGen(M, K, S) → skS: The Public Key Generator (PKG) executes the KeyGenalgorithm with the inputs M, K, and an attribute set S, generating a private key skS as the result.

Enc(m, (M, ρ), KW) → CT: The entity that owns the record initiates the Enc algorithm, providing a message m, an access policy (M, ρ), and a keyword KW as inputs, leading to the creation of an original ciphertext CT.

Dec(skS, CT) → m: The Delegation algorithm is utilized to decrypt the initial ciphertext. The inputs include a ciphertext CT under the access policy (M, ρ) and a private key skS. The output is the plaintext m if the attribute set S matches (M, ρ); otherwise, a different result is obtained.

Algorithm	**Ref(1) Existing**	**Proposed Scheme**
KeyGen	12.954ms	9.572ms
Enc	6.525ms	4.472ms
Dec	8.219ms	7.674ms

Table I. Implementation Time

We conducted a thorough analysis, considering the following criteria: functionality, efficiency in theoretical Analysis, and implementation time.

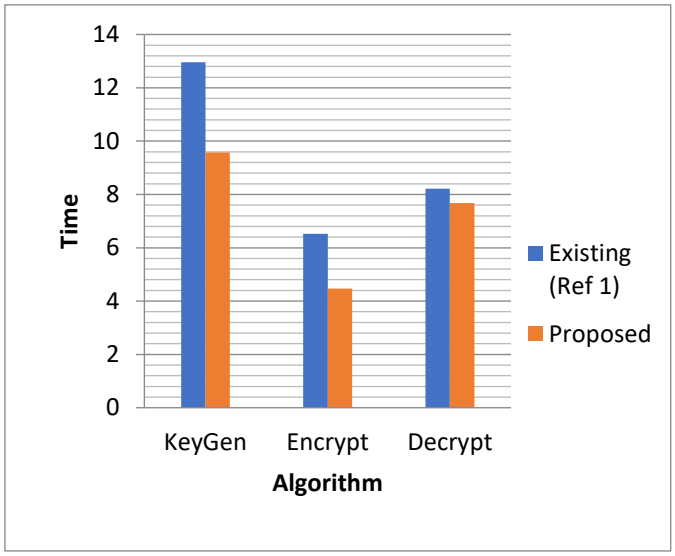

Fig.2.Implementation Time.

Our approach is evaluated against a recently introduced search encryption scheme through keyword search techniques. Additionally, we assess the implementation time of our scheme in comparison to previous ones, as they all utilize public keys and facilitate access policies based on user identification.

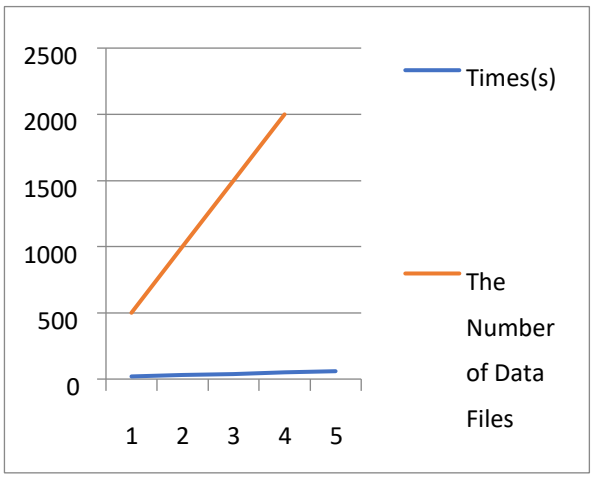

Fig.3.The Number of data files

Fig.3 illustrates that our scheme outperforms in search performance, a critical evaluation metric in a search system, by displaying the quantity of data files within a specified time limit.

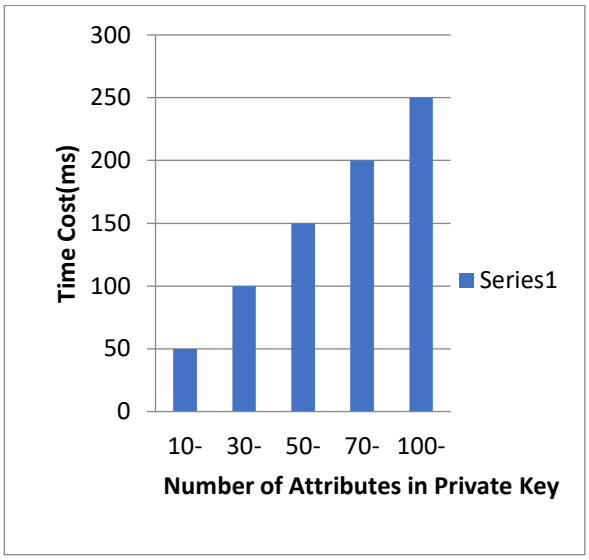

Fig.4. Implementation Cost

In Fig. 4, the time required for key blinding is at the millisecond level. However, it is important to note that key blinding can be implemented in an amortized model. More precisely, users can execute the key blinding process just once and subsequently benefit from efficient local decryption.

5.1 Security Analysis

Examining the security of a cloud computing system reliant on a multiauthority model for data sharing and time server data searching is crucial for ensuring resilience against potential threats. This model improves access control by allowing multiple authorities to supervise access rights for specific files, thereby reducing the likelihood of unauthorized access. To secure data both in transit and at rest, robust encryption algorithms are employed, guaranteeing the confidentiality of sensitive information. The multi-authority approach empowers each authority to independently oversee encryption keys, reducing the risk associated with a single point of compromise. The focus is on giving priority to the security of key management processes, encompassing secure procedures for key generation, storage, and distribution. The security analysis highlights that the system for data sharing

and time server data searching, based on multi-authority, integrates several robust security measures.

VI CONCLUSION

This research paper introduces a novel multi-authority-based system for data sharing and time server data searching in cloud computing, showcasing notable advancements in security, efficiency, and accessibility. The innovative approach effectively tackles challenges related to data sharing and searching in multiauthority settings, providing a robust solution for applications in the cloud. Through the implementation of a multiauthority framework, the system ensures secure data sharing, with distinct authorities managing specific aspects, creating a controlled and accountable environment for handling sensitive information. The decentralized nature of the system promotes efficient and seamless data sharing among multiple authorities, eliminating the necessity for a central authority to oversee all transactions. This decentralized model streamlines processes, reduces latency, and enhances overall system performance. The incorporation of a time server introduces a temporal dimension to data searching, enabling users to retrieve information based on specific time intervals. This feature is particularly valuable in

situations where time-sensitive data is crucial, offering users the capability to access historical records and track changes over time. The proposed multiauthority-based data sharing and time server data searching system represent a noteworthy advancement in cloud computing, providing a secure, efficient, and flexible solution for organizations and users managing data in a multi-authority environment. The positive outcomes observed in this implementation pave the way for further innovation and refinement in cloud-based data management systems.

REFERENCE

[1] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and L. Fang, "Secure keyword search and data sharing mechanism for cloud computing," IEEE Trans. Dependable Secure Comput., vol. 18, no. 6, pp. 2787–2800, Dec. 2020.
[2] Kai Zhang , Xiwen Wang , Jianting Ning , Member, IEEE, and Xinyi Huang "Dual-Server Boolean Data Retrieval for Highly-Scalable Secure File Sharing Services" IEEE Transactions on Information Forensics And Security, VOL. 18, 2023.
[3] D. Xiaoding Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy. (S&P), May 2000, pp. 44–55.
[4] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. Theory cryptography Conf. Berlin, Germany: Springer, 2007, pp. 535–554.
[5] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Outsourced symmetric private information retrieval," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2013, pp. 875–888.
[6] M. Zeng, H. Qian, J. Chen, and K. Zhang, "Forward secure public key encryption with keyword search for outsourced cloud storage," IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 426–438, Jan. 2019.
[7] K. Zhang, M.Wen, R. Lu, and K. Chen, "Multi-client sub-linear Boolean keyword searching for encrypted cloud storage with owner-enforced authorization," IEEE Trans. Dependable Secure Comput., vol. 18, no. 6, pp. 2875–2887, Nov. 2021.
[8] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Outsourced symmetric private information retrieval," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2013, pp. 875–888.
[9] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health 994 record using multi-authority attribute-based encryption with revocation," 995 International Journal of Information Security, vol. 14, no. 6, pp. 487– 996 497, 2015.
[10] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing 1026 attribute-based encryption with checkability," IEEE Transactions on 1027 Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2013.
[11] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re- 1044 encryption with delegating capabilities," in Proceedings of the 4th In- 1045 ternational Symposium on Information, Computer, and Communications 1046 Security, pp. 276–286, ACM, 2009.
[12] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. 1067 Phuong, and Q. Xie, "A dfa-based functional proxy re-encryption 1068 scheme for secure public cloud data sharing," IEEE Transactions on 1069 Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.
[13] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, "Cp-abse: 1092 A ciphertext-policy attribute-based searchable encryption scheme," IEEE 1093 Access, vol. 7, pp. 5682–5694, 2019.
[13] Dawn Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In Proceedings of the 2000 IEEE symposium on Security and Privacy (S&P 2000), 2000.
[14] Brent Waters, Dirk Balfanz, Glenn Durfee, and Dianna Smetters. Building an encrypted and searchabe audit log. In Proceedings of NDSS '04, 2004.
[15] M. Bellare, A. Boldyreva, and A. O'Neill. Deterministic and efficiently searchable encryption. In A. Menezes, editor, CRYPTO 2007, volume 4622 of LNCS, pages 535–552. Springer, Aug. 2007.