STM JOURNALS

Journal of
Advances in Shell Programming

ISSN: 2395-6690
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoASP

https://journals.stmjournals.com/joasp

Review JoASP

Privacy-preserving Multi-keyword Search in Multi-owner Setting Using Blockchain

Chethan P.J.[1], Akash Kumar B.S.[2], Sanjay G.B.[3], Sudeep C.P.[4,*], Yogesh Kumar S.S.[5]

Abstract

Searchable encryption (SE) has become an essential cryptographic technique, allowing users to securely search through encrypted data. However, most existing SE schemes rely on a single intermediary, such as a cloud server, leading to potential single-point failures, privacy breaches, and untrustworthy results. Many blockchain-based SE schemes have been proposed to address these issues. However, they frequently encounter difficulties such as supporting a multi-keyword, multi-owner model, ensuring query privacy, and maintaining data storage availability. In this paper, we introduce a novel approach for privacy-preserving multi-keyword search in a multi-owner setting. Our scheme allows searching over encrypted data in a trustworthy, private, and efficient manner. We integrate the attribute Bloom filter into our scheme to construct indexes, enhancing query privacy and improving index generation performance. To ensure datastorage availability, our scheme utilizes the interplanetary file system (IPFS) for storing a large scale ofencrypted data. We offer a security proof and comparative analysis showing that our scheme is more secure and efficient than existing ones. Furthermore, experiments conducted on a real-world dataset validate the practical feasibility of our approach. By addressing the limitations of existing schemes, our approach offers a robust solution for privacy-preserving multi-keyword search in a multi-owner setting, making it suitable for various applications where data privacy and security are paramount.

Keyword: Searchable encryption, privacy-preserving multi-keyword search, blockchain-based scheme, encrypted data

INTRODUCTION

With the internet and cloud storage becoming increasingly prevalent, many organizations opt to store theirlarge-scale data with third-party providers to reduce their own storage and maintenance overheads. However, this practice can lead to issues like privacy breaches and unauthorized access since the data's ownership and control are separated. Encrypting the data before outsourcing helps mitigate these risks, but it introduces the challenge of conducting searches on encrypted data. Searchable encryption (SE) has emerged as a solution, allowing users to search for specific information while keeping the data secure. In a typical SE setup, data owners encrypt keywords and indexes before sending them to a cloud server along with the encrypted data. Users can then create search queries without revealing sensitive information. SE is now widely adopted across various sectors such as healthcare, smart gridmanagement, and the internet of things (IoT) to ensure data security during searches [1]. In recent years, blockchain technology has been integrated into searchable symmetric encryption

***Author for Correspondence**
Sudeep C.P.
E-mail: sudeepc.219@gmail.com

[1]Assistant Professor, Department of Computer Science and Engineering, PES Institute of Technology and Management, Shivamogga, Karnataka, India
[2-5]Student, Department of Computer Science and Engineering, PES Institute of Technology and Management, Shivamogga, Karnataka, India

Received Date: May 07, 2024
Accepted Date: June 10, 2024
Published Date: July 04, 2024

Citation: Chethan P.J., Akash Kumar B.S., Sanjay G.B., Sudeep C.P., Yogesh Kumar S.S. Privacy-preserving Multi-keyword Search in Multi-owner Setting Using Blockchain. Journal of Advances in Shell Programming. 2024; 11(2): 12–18p.

(SSE), enabling decentralized, transparent, and immutable execution of SSE operations. While existing SSE schemes leveraging blockchain ensure trustworthiness and fairness, they face several challenges. Firstly, most of these schemes only support either single-keyword single-owner or multi-keyword single-owner scenarios, lacking support for multi-keyword multi owner setups. Secondly, there is a risk of privacy leakage despite efforts to preserve privacy in SSE schemes, as demonstrated by potential side-channelattacks [2]. Thirdly, storing encrypted data locally or outsourcing it to a centralized server impacts data availability, with the risk of data loss in the event of system crashes, rendering it unrecoverable even with matching trapdoors. To address these challenges, this paper proposes the Privacy preserving multikeyword search in multi owner setting scheme in a multi-owner setting. Privacy preserving multi keyword search in multi owner setting aims to achieve trustworthy and private searches while enhancing data storage availability and system efficiency. Specifically, to support multi-keyword multi-owner scenarios in blockchain-based SSE while safeguarding against privacy leaks, the privacy-preserving multi-keyword search in multi owner setting scheme enhances the multi-keyword secure-search scheme for multiple data owners (MKSSMDO) approach by incorporating attribute Bloom filters [3]. Additionally, privacy-preserving multi-keyword search in a multi-owner setting utilizes the interplanetary file system (IPFS) for distributed encrypted data storage, further improving efficiency and system robustness.

LITERATURE SURVEY

The paper by Yin et al. [4] titled "Secure Conjunctive Multi-Keyword Ranked Search over Encrypted Cloud Data for Multiple Data Owners" introduces a system that addresses the challenges associated with conducting secure searches over encrypted cloud data in a multi-owner setting. The system employs encryption techniques to ensure the privacy and confidentiality of cloud-stored data, allowing users to perform searches using multiple keywords. Thepotential use of blockchain technology enhances decentralization, contributing to a tamper resistant and transparent record of search activities. Additionally, the system may utilize smart contracts for access control, enabling data owners to define and enforce rules governing search permissions. The advantages include privacy preservation, secure search operations, support for multikey word searches,ranked search results, multi-owner compatibility, decentralization, access control, auditability, scalability, user anonymity, and potential efficiency improvements. Overall, the paper makes valuable contributions to the field by addressing privacy concerns, improving search functionalities, and ensuring secure data access in collaborative, cloud-based environments. A disadvantage could be the computational overhead associated with the use of encryption techniques for securing cloud data. Encryption processes may introduce latency, impacting the speed of search operations, especially whendealing with large datasets. Additionally, the integration of blockchain, while providing decentralization and transparency, might introduce complexities related to scalability and performance, especially in environments with a high volume of transactions. Another consideration is the potential challenges associated with managing access control through smart contracts, as defining and maintaining intricate permission structures might lead to increased system complexity.

Chen et al.'s article [5] titled "Blockchain Based Searchable Encryption for Electronic Health Record Sharing" explores an innovative approach to securing electronic health records (EHRs) through the integration of blockchain technology and searchable encryption. In this system, the authors leverage the decentralized and transparent nature of blockchain to enhance the security and traceability of EHR sharing. The use of searchable encryption allows authorized entities to perform searches on encrypted EHRs without compromising the privacy of sensitive patient information. The blockchain ensures tamper-resistant and auditable records of access and modifications to health records, contributing to the integrity and trustworthiness of the shared data. The approach addresses critical concerns related to patient privacy and data security in the healthcare domain, offering a potential solution for secure and transparent EHR sharing. The paper likely delves into the technical details of the blockchain-based searchable encryption mechanism, its implementation, and the advantages it brings to the realm of

electronic health record management and sharing. One key benefitlies in the heightened security and privacy measures afforded by the integration of blockchain technology. The decentralized and tamper-resistant nature of blockchain enhances data integrity and ensures that EHRs are securely stored and shared. The use of searchable encryption adds an additionallayer of privacy, enabling authorized entities to conduct searches on encrypted records without compromising the sensitive information contained within. This not only protects patient confidentialitybut also facilitates efficient retrieval of relevant health information. Disadvantages that should be considered are as follows: One notable challenge is the computational overhead associated with the encryption and decentralized nature of blockchain. The complex cryptographic processes involved in searchable encryption may introduce latency, potentially impacting the speed of searches and retrieval of EHRs.Additionally, the consensus mechanisms inherent in many blockchain implementations may lead to scalability issues, particularly in healthcare systems with a high volume of transactions.

Problem Statement

In this project implementing the multi-keyword multi-owner setting in blockchain-based SSE aims to achieve more secure and efficient storage, which improves the data availability and practical feasibility [6].

Problem Description

The project focuses on enhancing information security in collaborative environments with distributed data ownership. By integrating blockchain technology and advanced cryptography, it enables secure multi-keyword searches, preserving data privacy. Emphasizing decentralization and transparency, the project utilizes smart contracts for automated governance. The goal is to establish a tamper resistant system that ensures privacy, trust, and accountability in multi-owner settings [7]. The “Privacy-preservingmulti-keyword search in multi-owner setting using blockchain” project tackles the intricacies of retrieving information in collaborative environments marked by distributed data ownership. By seamlessly integrating blockchain technology and advanced cryptographic techniques, the project aimsto establish a secure framework for executing multi-keyword searches. This innovative approach ensures the privacy and integrity of data, addressing the challenges posed by collaborative data settings [8].

Objectives

- Encrypting a file and storing in IPFS
- Storing a CID(Content IDentifier) and secure index on a blockchain
- Search on the blockchain
- Authorization and decrypting the key and search on IPFS

Existing System

The current system employs blockchain technology to facilitate privacy-preserving multi-keyword search within a multi-owner framework. Traditional SSE methodologies have been augmented with blockchain's decentralized, transparent, and immutable characteristics to ensure integrity and fairness. However, existing SSE schemes encounter several obstacles [9]. Firstly, they often cater only to single-keyword single-owner or multi-keyword single-owner scenarios, neglecting support for multi-keyword multi-owner setups. Secondly, despite efforts to uphold privacy in SSE protocols, the risk of privacy breaches persists due to potential side-channel attacks. Lastly, the storage of encrypted data either locally or on centralized servers impacts data availability, posing the risk of irretrievable data loss during system crashes. To address these challenges, the proposed blockchain-based privacy-preserving multi-keyword search (PMSB) scheme aims to refine existing methodologies [10]. By integrating attribute Bloom filters and leveraging the IPFS, PMSB seeks to enable secure and efficient multi-keyword search operations while enhancing data storage availability and system resilience in a multi-owner environment.

System Design

The authentication method can refer to the scheme proposed in. Specifically, data owner uses a symmetric encryption algorithm to encrypt owned files, sends them to the IPFS, and records the identifier of each file returned by the IPFS in step 1. As shown in step 2, data owner then utilizes a self-chosen temporary key to encrypt the pre-extracted keyword set into an index for each data file. The index along with the identifier of the corresponding file is sent to the blockchain. Because our PMSB supports multi-owner setting, different data owners are allowed to use independent and distinct keys to generate indexes [11]. A data user who wants to search encrypted data sends authentication request to corresponding data owners in step 3, and data owner who grants the permission shares public parameters with the authenticated data user u in step 4. In step 2, u uses the public parameters and two randomly selected keys to convert the query keyword set of interest into a trapdoor and sends it to the blockchain. It should be pointed out that in our PMSB, u can generate the trapdoor without knowing the keys that are owned by different data owners for index generation [12].

METHODOLOGY

According to the trapdoor, the operation of matching indexesis implemented by smart contract on the blockchain and the identifiers of matched files are sent back tou as shown in step 3. u then requests Data Owners for the access authorization of the corresponding encrypted files and obtains the decryption keys step and step. The identifiers of matched files are sentto the IPFS by u in step 1, and finally the encrypted files that can be decrypted by u are returned in step 4 as shown in Figure 1.

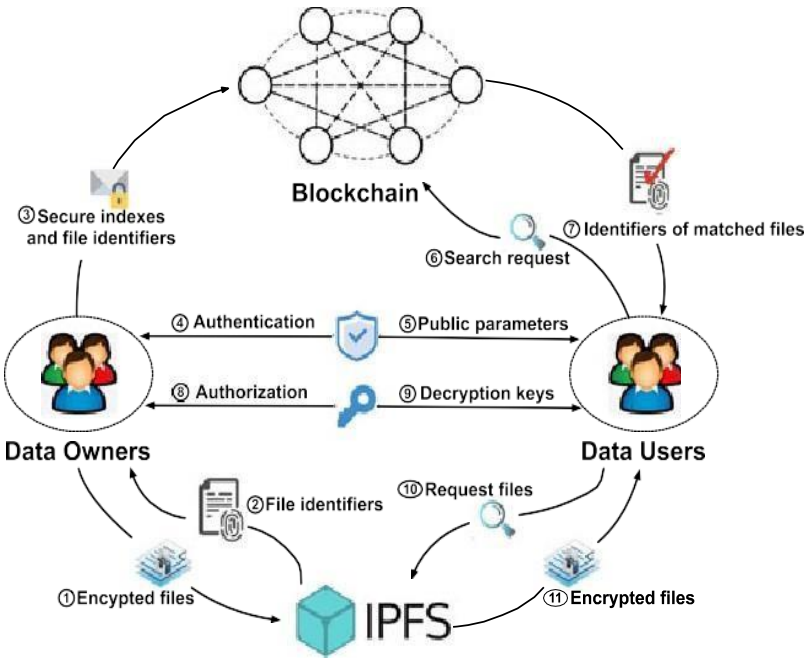

Figure 1. Blockchain methodology.

Inference Model

The inference model for a privacy-preserving multi-keyword search in a multi-owner setting using blockchain is crucial for ensuring secure and efficient user interactions as shown in Figure 2. Users to securely log in and access only the data and features relevant to their roles [13]. The search interface must enable users to enter multiple keywords for their queries, providing real-time feedback on search results and allowing for additional search criteria customization. Privacy settings should offer users granular control over data sharing and encryption, while blockchain integration should present transaction details and smart contract interactions clearly. Facilitating multi-owner benefits of privacy-preserving search in a blockchain-based environment [14].

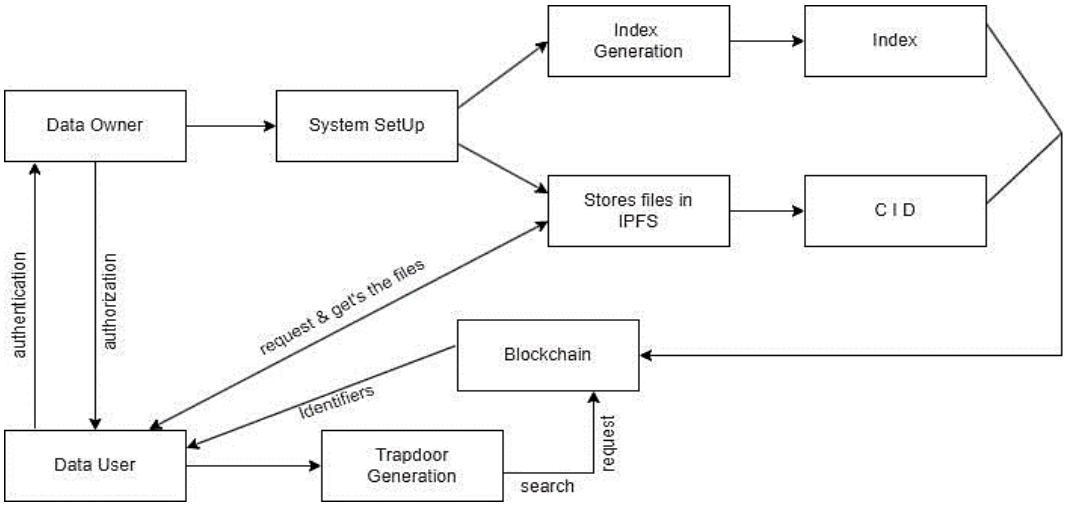

Figure 2. Inference model.

SYSTEM IMPLEMENTATION AND RESULTS

Five Phases of System Implementation

1. *System initialization:* In the system initialization phase of our project, given a large security parameter, data owner is strictlyauthenticated before entering the system can run system setup to generate global parameters.
2. *Secure index construction:* In our project, data owners run GenIndex to generate the secure index for a data file.
3. *Query trapdoor generation:* To protect query privacy with the search keyword set Q, we should generate the trapdoor T in a securemanner against side channel attack.
4. *Search on the blockchain:* Each node in the consortium blockchain runs the Search algorithm that can be implemented using smartcontract to match the trapdoor with the index.
5. *Search in the IPFS:* The data user u sends it to any network node in the IPFS. To obtain an encrypted data file, the node first needs to determine which nodes that store the blocks corresponding to the data file [15].

RESULTS

Evaluation of Operations on the Blockchain

In our PMSB, the Search algorithm implemented by using smart contract is run on the blockchain.To quantify the throughput and average latency of the Search algorithm as shown in Figure 3.

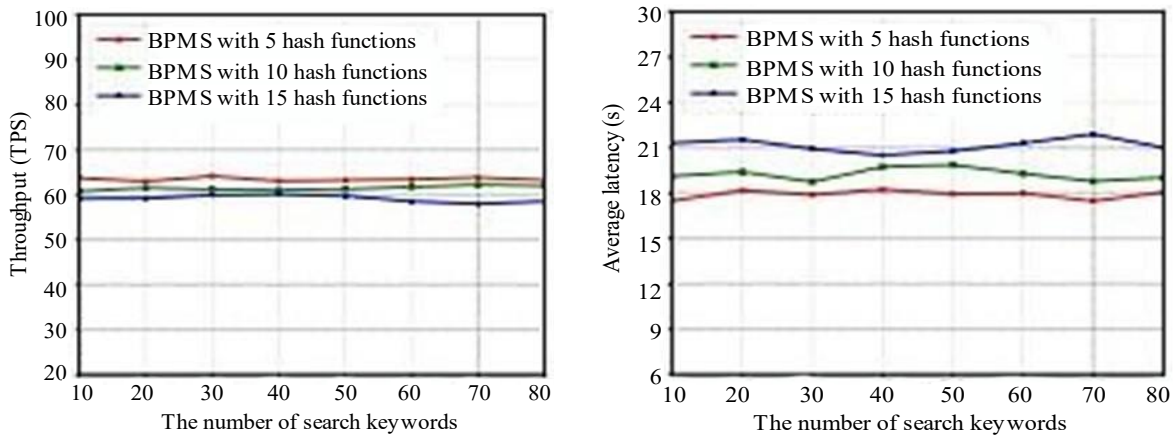

Figure 3. Performance of Search algorithm on the blockchain: (a) the transaction throughput for different number of search keywords, (b) the average latency with different number of search keywords.

CONCLUSION

In this paper, we propose PMSB, a blockchain-based scheme that ensures privacy-preserving multi-keyword searches and supports trustworthy searches in a multi-keyword, multi-owner environment. Our PMSB exploitsthe attribute Bloom filter to guarantee query privacy in an efficient manner. By introducing IPFS in our PMSB, we can achieve more secure and efficient storage, which improves the data availability andpractical feasibility. Our theoretical analysis and experimental evaluation show that our PMSB can expand functionality while improving privacy and efficiency.

Acknowledgments

We take this opportunity to express our deep sense of gratitude to our guide Mr. Chethan PJ, Professor, Department of CSE, PESITM, Shivamogga for his kind support, guidance, and encouragement throughout the course of this work.

We would like to express our sincere gratitude to Mr. Raghavendra K., Assistant Professor and Mr. Sunil Kumar H. R., Assistant Professor, Department of CSE, PESITM, Shivamogga for their keen interest and invaluable support throughout the course of this work.

We are highly grateful to Dr. Arjun U., Associate Professor. and Head, Department of CSE, PESITM, Shivamogga for his kind support and encouragement throughout the course of this work.

We are highly grateful to Dr. Yuvaraju B. N., Principal, PESITM, Shivamogga for providing us an opportunity to fulfill our most cherished desire of reaching the goal.

We would like to thank all the teaching and non-teaching staff of the Department of CSE, for their kind cooperation during the course of the work. The support provided by the college and departmental library is gratefully acknowledged.

REFERENCES

1. Hu S, Cai C, Wang Q, Wang C, Luo X, Ren K. Searching an encrypted cloud meets blockchain: a decentralized, reliable and fair realization. In: IEEE INFOCOM 2018 – IEEE Conference on Computer Communications, Honolulu, HI, USA, April 16–19, 2018. pp. 792–800.
2. Li H, Tian H, Zhang F, He J. Blockchain-based searchable symmetric encryption scheme. Computers Electric Eng. 2019; 73: 32–45.
3. Jiang S, Cao J, McCann JA, Yang Y, Liu Y, Wang X, Deng Y. Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In: 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, July 14–17, 2019. pp. 405–410.
4. Yin H, Qin Z, Zhang J, Ou L, Li F, Li K. Secure conjunctive multi-keyword ranked search over encrypted cloud data for multiple data owners. Future Generation Computer Syst. 2019; 100: 689–700.
5. Chen L, Lee WK, Chang CC, Choo KK, Zhang N. Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Syst. 2019; 95: 420–429.
6. Cai C, Weng J, Yuan X, Wang C. Enabling reliable keyword search in encrypted decentralized storage with fairness. IEEE Trans Depend Secure Comput. 2018; 18 (1): 131–144.
7. Wang C, Cao N, Li J, Ren K, Lou W. Secure ranked keyword search over encrypted cloud data. In: 2010 IEEE 30th International Conference on Distributed Computing Systems, Genoa, Italy, June 21–25, 2010. pp. 253–262.
8. Tahir S, Rajarajan M. Privacy-preserving searchable encryption framework for permissioned blockchain networks. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, Nova Scotia, Canada, July 30–August 3, 2018. pp. 1628–1633.

9. Ballard L, Kamara S, Monrose F. Achieving efficient conjunctive keyword searches over encrypted data. In: Qing S, Mao W, López J, Wang G, editors. Information and Communications Security: 7th International Conference, ICICS 2005, Beijing, China, December 10–13, 2005. Proceedings 7. Berlin, Germany: Springer; 2005. pp. 414–426.
10. Gao S, Chen X, Zhu J, Dong X, Ma J. TrustWorker: a trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing. IEEE Trans Serv Comput. 2021; 15 (6): 3577–3590.
11. Curtmola R, Garay J, Kamara S, Ostrovsky R. Searchable symmetric encryption: improved definitions and efficient constructions. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, October 30–November 3, 2006. pp. 79–88.
12. Golle P, Staddon J, Waters B. Secure conjunctive keyword search over encrypted data. In: Jakobsson M, Yung M, Zhou J, editors. Applied Cryptography and Network Security: Second International Conference, ACNS 2004, Yellow Mountain, China, June 8–11, 2004. Proceedings 2. Berlin, Germany: Springer; 2004. pp. 31–45.
13. Steichen M, Fiz B, Norvill R, Shbair W, State R. Blockchain-based, decentralized access control for IPFS. In: 2018 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom), and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, Nova Scotia, Canada, July 30–August 3, 2018. pp. 1499–1506.
14. Chen R, Mu Y, Yang G, Guo F, Huang X, Wang X, Wang Y. Server-aided public key encryption with keyword search. IEEE Trans Inform Forens Security. 2016; 11 (12): 2833–2842.
15. Gao S, Piao G, Zhu J, Ma X, Ma J. Trustaccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain. IEEE Trans Vehicular Technol. 2020; 69 (6): 5784–5798.

