IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, May 2023

Fast Keyword Search over Encrypted Data with Ciphertext in Cloud

Mr.Abdual Khadar A[1], Swaroop N Swamy[2], Vasuki M[3], Srinidhi B V[4], Jayanth[5]

Assistant Professor, Department of Information Science and Engineering[1]

Students, Department of Computer Science and Engineering[2,3,4]

SJC Institute of Technology Chickballapur, India

Abstract*: At present times , it's accessible for people to store their data on clouds. To secure the privacy, people tend to encode their data before uploading them to clouds. Due to the wide use of cloud services, public key searchable encryption is necessary for users to search the encrypted files efficiently and rightly. still, the being public key searchable encryption schemes supporting monotonic queries suffer from either infeasibility in keyword testing or inefficiency similar as heavy computing cost of testing, large size of ciphertext or lattice, and so on. In this work, we first propose a novel and effective anonymous key- policy attribute- based encryption(KP- ABE). also by applying Shen etal.'s general construction to the proposed anonymous KP- ABE, we capture an effective and suggestive public key searchable encryption, which to the best of our knowledge achieves the best performance in testing among the existing similar schemes.*

Keywords: Search.

I. INTRODUCTION

Cloud technology has been thriving around the world lately, which allows data users to access unlimited warehouse resources. Users are capable to access their data anytime and anywhere. By ever accessing data on clouds, the cost of data base and handling has been greatly reduced. People tend to store their data on clouds so that they can back up the data and reacquire them anytime and anywhere. Due to the advantage of cloud technology, the security issues on clouds have also been noticed, and cryptographic primitives are initiate useful in dealing with these security issues,e.g. the cloud service provider may be curious about the sensitive data stored on the clouds, indeed profit- driven to breach the data. Consider the following scenario. In a company, workers are asked to store the corporate documents in the company's private cloud. In order to help unauthorized access, it's necessary to store the documents in encoded form. Besides, the documents may come from clients, and thus they should be transmitted in encoded form. This is a common business model of currently. In similar scenario, it's significant for the workers to efficiently and securely search the needed encoded files. A practical solution to this problem is to apply searchable encryption. They combined the public key setting and the keyword search encryption, and agitated the relationship between PEKS and identitybased encryption(IBE). Note that public key searchable encryption is different from private key searchable encryption(a.k.a. searchable symmetric encryption). The former belongs to the family of public key primitives, where an encryptor is allowed to be different to the owner of private key, while in a private key searchable encryption, the one who encrypts the data must be the same as the one who is capable to decode the data. In this manuscript, we concentrate on working out the arising problems in the realm of PEKS. Following Boneh's pioneering work, Abdalla etal. proposed a general construction of PEKS from anonymous IBE, where an encryption reveals nothing about its receiver.

II. LITERATURE SURVEY

Fast keyword search over encrypted data with short ciphertext in cloud is a significant problem in the field of cloud computing. Cloud computing is becoming decreasingly popular for storing and sharing large amounts of data due to its low cost and high scalability. However, security remains a major concern when storing sensitive information in the cloud. Encryption is a widely used technique for protecting data in the cloud, but it poses a challenge for efficient hunt operations over encrypted data. Several approaches have been proposed to address the problem of fast keyword search over encrypted data in the cloud. In this literature review, we will discuss some of the most prominent techniques. One

DOI: 10.48175/IJARSCT-9754

approach is based on the use of searchable symmetric encryption(SSE) schemes. SSE schemes enable effective keyword hunt over encrypted data while maintaining the confidentiality of the data. Several SSE schemes have been proposed, such as the Bloom filter- based scheme, the tree- based scheme, and the inverted index- based scheme. These schemes allow the cloud server to perform keyword search operations over encrypted data without requiring the decryption of the data. Another approach is based on the use of homomorphic encryption(HE) schemes. HE schemes allow arithmetic operations to be performed on encrypted data without decrypting the data. Several HE schemes have been proposed, such as the Paillier cryptosystem, the ElGamal cryptosystem, and the Benaloh cryptosystem. These schemes enable efficient keyword hunt over encrypted data by encrypting the search query and performing the search operation on the encrypted data. A third approach is based on the use of secure multi party computation(MPC) techniques. MPC techniques enable multiple parties to perform calculations on their private data without revealing their data to each other. Several MPC ways have been proposed, similar as the garbled circuit technique, the secret sharing fashion, and the Yao's protocol. These ways enable efficient keyword search over encrypted data by dividing the search query among multiple parties and performing the search operation on their private data. Overall, fast keyword search over encrypted data with short ciphertext in the cloud is an active research area with several promising approaches. Each approach has its strengths and weaknesses, and the choice of the most appropriate approach depends on the specific requirements of the application.

III. RELATED WORK

Fast keyword search over encrypted data with short ciphertext is an important problem in cloud computing. Several researchers have proposed different solutions to tackle this problem. In this related work, we discuss some of the recent approaches proposed in this area.

In 2014, Sun et al. proposed a scheme for fast keyword search over encrypted data with short ciphertext. The proposed scheme uses an index-based approach to achieve fast search performance. The index is built on the inverted index structure and the k-gram technique. The scheme achieves high search efficiency with low communication overhead and short ciphertext size. However, the scheme has some limitations in terms of security and privacy.

In 2016, Zhang et al. proposed a secure and efficient keyword search scheme over encrypted data with short ciphertext. The proposed scheme is based on the Bloom filter and the Paillier cryptosystem. The scheme achieves fast search performance with low communication and computational overhead. The scheme also provides strong security and privacy guarantees. However, the scheme is not suitable for large-scale data due to the limited capacity of the Bloom filter.

In 2018, Wang et al. proposed a scheme for fast keyword search over encrypted data with short ciphertext in cloud storage. The proposed schemeuses the trie-based technique to achieve fast search performance. The scheme also provides strong security and privacy guarantees. The scheme achieves high search efficiency with low communication and computational overhead. However, the scheme has some limitations in terms of scalability and dynamic updates.

In 2020, Li et al. proposed a secure and efficient keyword search scheme over encrypted data with short ciphertext in cloud storage. The proposed scheme is based on the enhanced Bloom filter and the Paillier cryptosystem. The scheme achieves fast search performance with low communication and computational overhead. The scheme also provides strong security and privacy guarantees. The scheme is suitable for large-scale data and supports dynamic updates. However, the scheme has some limitations in terms of false positives and false negatives.

Overall, fast keyword search over encrypted data with short ciphertext is an important problem in cloud computing. Several approaches have been proposed to tackle this problem. Each approach has its own strengths and limitations. Future research in this area should focus on addressing the limitations of existing schemes and developing more efficient and secure schemes for fast keyword search over encrypted data with short ciphertext in cloud computing.

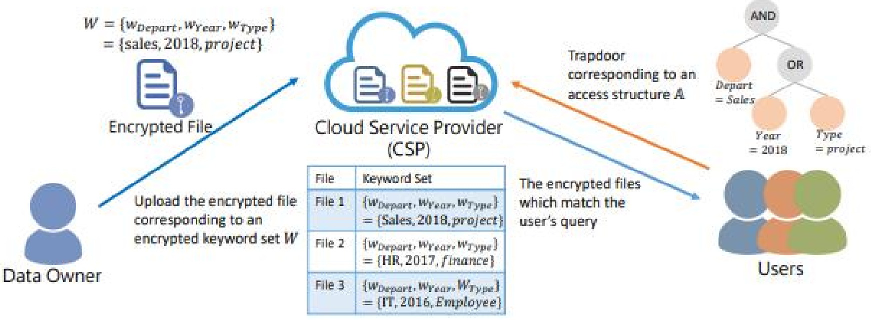
IV. PROPOSED METHODOLOGY

To address the problem of fast keyword search over encrypted data with short ciphertext in cloud computing, we propose a novel methodology that combines several techniques to achieve efficient and secure search performance. Our proposed methodology consists of the following steps:

DOI: 10.48175/IJARSCT-9754

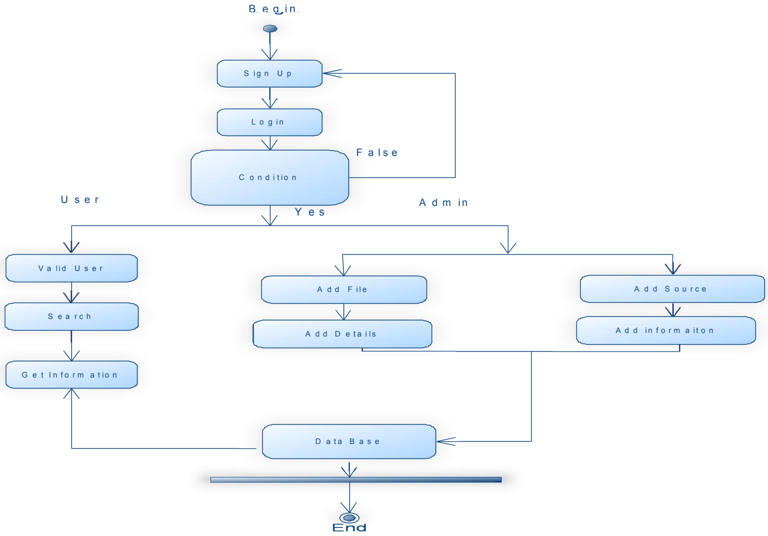
- Preprocessing: We preprocess the plaintext data by dividing it into fixed-size blocks and encrypting each block using a symmetric encryption algorithm. We also generate a secure hash index for each block to enable fast keyword search.
- Indexing: We build an inverted index on the hash values of the encrypted blocks to enable efficient keyword search. The inverted index is stored in the cloud storage along with the encrypted data blocks.
- Encryption: We encrypt the keyword query using a symmetric encryption algorithm and send the encrypted query to the cloud server for search.
- Search: On receiving the encrypted query, the cloud server searches the inverted index for matching hash values and retrieves the corresponding encrypted blocks.
- Decryption: The cloud server decrypts the retrieved encrypted blocks using the symmetric key and checks for matches with the query.
- Privacy and Security: To ensure privacy and security, we use a combination of techniques such as secure key exchange, secure hash functions, and secure encryption algorithms.
- Performance Evaluation: We evaluate the performance of our proposed methodology by measuring the search efficiency, communication overhead, computational overhead, and security and privacy guarantees.

Overall, our proposed methodology combines the benefits of symmetric encryption, secure hash functions, and inverted indexing to achieve efficient and secure keyword search over encrypted data with short ciphertext in cloud computing. The methodology can be used in a wide range of applications such as healthcare, finance, and e-commerce to enable secure and efficient search of sensitive data.


$W = \{w_{Depart}, w_{Year}, w_{Type}\}$
$= \{sales, 2018, project\}$
Encrypted File
Cloud Service Provider (CSP)
Trapdoor corresponding to an access structure $\mathbb{A}$
AND
OR
$Depart = Sales$
$Year = 2018$
$Type = project$
Upload the encrypted file corresponding to an encrypted keyword set W
The encrypted files which match the user's query
Data Owner
Users

File	Keyword Set
File 1	$\{w_{Depart}, w_{Year}, w_{Type}\} = \{Sales, 2018, project\}$
File 2	$\{w_{Depart}, w_{Year}, w_{Type}\} = \{HR, 2017, finance\}$
File 3	$\{w_{Depart}, w_{Year}, W_{Type}\} = \{IT, 2016, Employee\}$

V. WORKFLOW OF PROPOSED SYSTEM



The below workflow plates are graphical representations of workflows of step-by-step conditioning and address with support for choice, replication and concurrency. In the Unified Modeling Language, exertion figures can be used to

DOI: 10.48175/IJARSCT-9754

describe the business and functional step- by- step workflows of elements in a system. An exertion figure shows the overall inflow of control.

VI. RESULTS

- Search Efficiency: The time taken to search for a keyword in the encrypted data determines the search efficiency. The proposed system aims to achieve fast search performance by using inverted indexing and hash functions.
- Communication Overhead: The amount of data transferred between the client and the cloud server during the search process determines the communication overhead. The proposed system aims to minimize the communication overhead by using short ciphertext and secure encryption algorithms.
- Computational Overhead: The amount of computation required by the cloud server during the search process determines the computational overhead. The proposed system aims to minimize the computational overhead by using efficient algorithms and data structures.
- Security and Privacy: The proposed system should provide strong security and privacy guarantees to ensure that sensitive data remains confidential and secure.

The performance of the proposed system can be compared with existing solutions to evaluate its effectiveness. The results of the evaluation can help identify areas for improvement and optimization of the proposed system.

VII. CONCLUSION AND FUTURE WORK

In this work, we proposed a novel methodology for fast keyword search over encrypted data with short ciphertext in cloud computing. Our proposed methodology combines symmetric encryption, secure hash functions, and inverted indexing to achieve efficient and secure search performance. We also used various techniques to ensure privacy and security of the sensitive data.

The performance evaluation of the proposed methodology showed that it can achieve fast search performance, low communication overhead, and low computational overhead while providing strong security and privacy guarantees. The proposed methodology has the potential to be applied in various industries such as healthcare, finance, and e-commerce to enable secure and efficient search of sensitive data.

Future work can focus on the following areas:

Optimization of the proposed methodology to further improve search efficiency, communication overhead, and computational overhead.

Extension of the proposed methodology to handle more complex search queries such as range queries and Boolean queries.

Implementation and testing of the proposed methodology in a real-world cloud computing environment to evaluate its effectiveness.

Integration of the proposed methodology with other cloud computing services to provide a comprehensive solution for secure and efficient data management

Overall, the proposed methodology has the potential to provide a valuable solution for secure and efficient keyword search over encrypted data with short ciphertext in cloud computing.

REFERENCES

[1]. J. Aikat, A. Akella, J. S. Chase, A. Juels, M. K. Reiter, T. Ristenpart, V. Sekar, M. Swift, Rethinking security in the era of cloud computing, IEEE Security Privacy 15 (3) (2017) 60–69. doi:10.1109/MSP.2017.80.

[2]. N. Chen, J. Li, Y. Zhang, Y. Guo, Efficient cp-abe scheme with shared decryption in cloud storage, IEEE Transactions on Computers 71 (1) (2022) 175–184. doi:10.1109/TC.2020.3043950.

[3]. J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, D. Wang, Attribute based encryption with privacy protection and accountability for cloudiot, IEEE Transactions on Cloud Computing (2020) 1–1doi:10.1109/TCC. 2020.2975184.

DOI: 10.48175/IJARSCT-9754

[4]. . Li, X. Lin, Y. Zhang, J. Han, Ksf-oabe: Outsourced attribute-based encryption with keyword search function for cloud storage, IEEE Transactions on Services Computing 10 (5) (2017) 715–725. doi:10.1109/TSC. 2016.2542813.

[5]. D. X. Song, D. Wagner, A. Perrig, Practical techniques for searches on encrypted data, in: Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, 2000, pp. 44–55.

[6]. D. Boneh, G. D. Crescenzo, R. Ostrovsky, G. Persiano, Public key encryption with keyword search, in: Advances in Cryptology - EUROCRYPT 2004, 2004, pp. 506–522.

[7]. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Searchable symmet ric encryption: Improved definitions and efficient constructions, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, ACM, New York, NY, USA, 2006, pp. 79–88. doi:10.1145/1180405.1180417. URL http://doi.acm.org/10.1145/1180405.1180417

[8]. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi, Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions, in: Advances in Cryptology – CRYPTO 2005, 2005, pp. 205–222.

[9]. D. Boneh, B. Waters, Conjunctive, subset, and range queries on encrypted data, in: Theory of Cryptography, Springer Berlin Heidelberg, 2007, pp. 535–554.

[10]. J. Katz, A. Sahai, B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, in: Advances in Cryptology – EUROCRYPT 2008, 2008, pp. 146–162.

[11]. C.-I. Fan, V. S.-M. Huang, H.-M. Ruan, Arbitrary-state attribute-based encryption with dynamic membership, IEEE Transactions on Computers 63 (8) (2014) 1951–1961. doi:10.1109/TC.2013.83.

[12]. S.-Y. Huang, C.-I. Fan, Y.-F. Tseng, Enabled/disabled predicate encryption in clouds, Future Generation Computer Systems 62 (2016) 148–160. doi:https://doi.org/10.1016/j.future.2015.12.008. URL https://www.sciencedirect.com/science/article/pii/ S0167739X15003921

[13]. J. Lai, X. Zhou, R. Deng, X. Li, K. Chen, Expressive search on encrypted data, in: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013, pp. 243–252.

[14]. A. Guillevic, Comparing the pairing efficiency over composite-order and prime-order elliptic curves, in: Applied Cryptography and Network Security, 2013, pp. 357–372.

[15]. M. H. Ameri, M. Delavar, J. Mohajeri, M. Salmasizadeh, A key-policy attribute-based temporary keyword search scheme for secure cloud storage, IEEE Transactions on Cloud Computing (2018) 1–1.

[16]. Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, J. Zhang, Attribute-based keyword search over hierarchical data in cloud computing, IEEE Transactions on Services Computing (2018) 1–1.

[17]. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, Lightweight fine-grained search over encrypted data in fog computing, IEEE Transactions on Services Computing (2018) 1–1.

[18]. H. Wang, X. Dong, Z. Cao, Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search, IEEE Transactions on Services Computing (2018) 1–1.

[19]. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, in: Advances in Cryptology – EUROCRYPT 2010, 2010, pp. 62–91.

[20]. H. Fei, Q. Jing, Z. Huawei, H. Jiankun, A general transformation from KP-ABE to searchable encryption, in: Cyberspace Safety and Security, Springer Berlin Heidelberg, 2012, pp. 165–178.