isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 3 ,Apr,2024 ,ISSN_NO: 2321-3337

EFFICIENT REGULAR LANGUAGE SEARCH FOR SECURE CLOUD STORAGE

Keerthanaa M[1], Padma priya S[2], Shobana U[3], Thivakaran M[4*]
[123] UG Scholar-Dept.CSE, Grt Institute of Engineering and Technology Tiruttani, India
[4*]Assistant professor-Dept.CSE, Grt Institute of Engineering and Technology Tiruttani, India.
keerthimk56@gmail.com, Padmapriyapadma55@gmail.com, shobe762@gmail.com
***Corresponding author: thivakaran.m@grt.edu.in**

Abstract

This paper concerns the fundamental problem of processing conjunctive queries that contain both keyword and range conditions on public clouds in a privacy preserving manner. No prior Searchable Symmetric Encryption (SSE) based privacy preserving conjunctive query processing scheme satisfies the three requirements of adaptive security, efficient query processing, and scalable index size. In this paper, we propose the first privacy preserving conjunctive query processing scheme that satisfies all the above three requirements. To achieve adaptive security, we propose an Indistinguishable Bloom Filter (IBF) data structure for indexing. To achieve efficient query processing and structural indistinguishability, we propose a highly balanced binary tree data structure called Indistinguishable Binary Tree (IBtree). To achieve scalable and compact index size, we propose an IBtree space compression algorithm to remove redundant information in IBFs. To optimize search efficiency, we propose a traversal minimization algorithm. To make our scheme dynamic, we propose update algorithms. We prove that our scheme is adaptive secure under the IND-CKA secure model. The key contribution of this paper is on achieving conjunctive query processing with both strong privacy guarantee and practical efficiency in terms of both speed and space. We implemented our scheme in C++, evaluated and compared its performance with the prior KRB scheme for keyword queries and the prior scheme for range queries on two real-world data sets. Experimental results show that our scheme is both fast and scalable. For example, Processing a query only takes a few milliseconds for millions of records.

***Keywords**: Cloud computing, secured policy, indistinguishable bloom filter, EGRQ(Efficient and Geometric Range Query scheme).*

1. Introduction

Cloud storage system is a service model in which data are maintained, managed and backup remotely on the cloud side, and meanwhile data keeps available to the users over a network. Mobile Cloud Storage (MCS) denotes a family of increasingly popular on-line services, and even acts as the primary file storage for the mobile devices. MCS enables the mobile device users to store and retrieve files or data on the cloud through wireless communication, which improves the data availability and facilitates the file sharing process without draining the local mobile device resources. The data privacy issue is paramount in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud, and data users retrieve the interested data by encrypted search scheme. In MCS, the modern mobile devices are confronted with many of the same security threats as PCs, and various traditional data encryption methods are imported in MCS. However, mobile cloud storage system incurs new challenges over the traditional encrypted search schemes, in consideration of the limited computing and battery capacities of mobile device, as well as data sharing and accessing approaches through wireless communication.

Therefore, a suitable and efficient encrypted search scheme is necessary for MCS.

2. Related Work

This paper proposes a privacy-preserving searchable encryption (PPSE) scheme leveraging public and private block chains. It stores encrypted indices in a private block chain and outsources encrypted documents to a public one. This approach reduces storage overhead, enhances transaction efficiency, and ensures data security. A smart contract introduces a secondary verification access control mechanism, safeguarding data privacy and access control correctness. Security analysis and experiments demonstrate the scheme's enhanced security and query efficiency compared to existing approaches [1].

Cloud storage is vital for remote data management, but it faces security concerns, which encryption helps address. Public key encryption with keyword search (PKSE) is promising, allowing clients to search encrypted data efficiently. However, PKSE has a vulnerability when used with cloud servers: they can learn about newly added files with searched keywords, compromising privacy. To counter this, we propose a forward secure PKS scheme, preventing servers from learning about new files. We base this on attribute-based searchable encryption. Our experiments confirm the efficiency of our scheme [2].

Cloud computing relies on remote access to resources, posing security challenges for secure communication. Key agreement protocols address these challenges but face issues like connection delay and certificate management. To address these, we propose a certificate less 0-rtt anonymous aka protocol, improving efficiency and eliminating the need for certificates. Our protocol ensures security and user privacy while resisting bad randomness [3].

Cloud storage has seen significant growth, prompting the need to encrypt sensitive data for security and privacy. Searchable public key encryption (SPKE) allows retrieval of data cipher texts by keyword without decryption, but many Existing schemes are vulnerable to keyword guessing attacks. Public key Authenticated encryption with keyword search (peaks) was introduced to address this, but current schemes are only secure against designated-targets attacks. We refine the adversary model for peaks to combat adaptively chosen targets, formalize security definitions, and propose a lightweight peaks scheme without time-consuming bilinear pairing operations. Our scheme outperforms existing ones in computation and communication, making it suitable for resource-constrained mobile devices [4].

3. Objective

Both enterprises and end users have been increasingly outsourcing their data and computing services to public clouds for lower cost, higher reliability, better performance, and faster deployment. However, privacy has become the key concern as data owner may not fully trust public clouds. First, clouds may have corrupt employees. For example, in 2010, a Google engineer broke into the Gmail and Google Voice accounts of several children. Second, clouds may be hacked and customers may not be informed. Third, cloud facilities may be operated in some foreign countries where privacy regulations are difficult to enforce. The index I should leak no information about the data items in D. Note that a data item di could be a record in a rational database table or a text document in a document set.

4. Proposed System

We propose an Efficient and Geometric Range Query scheme (EGRQ) supporting searching and access control over encrypted spatial data. In EGRQ, we employ secure Knn(K-nearest neighbour) computation, polynomial fitting technique and order-preserving encryption to protect the security and privacy during the range query. In order to improve the efficiency, we also utilize R-tree to reduce the searching space and matching times in our scheme. We have adopted a novel strategy of spatial data access control to realize the permission assignment in our proposed geometric range query scheme in a more efficient way. We modified our scheme to support dynamic updating process.

5. Architecture Diagram

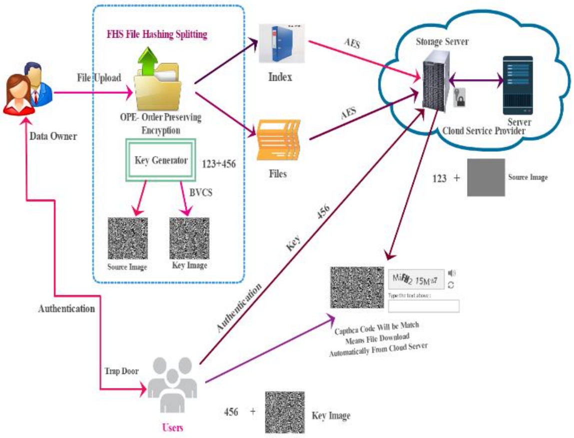


Fig 5.1 Architecture Diagram

6. Algorithm

6.1. Order Preserving Encryption Algorithm

Order-preserving encryption (OPE) is a deterministic symmetric encryption scheme that produces cipher texts that preserve the numerical ordering of plaintexts. It is a type of encryption scheme that maintains the order of data elements after encryption. This means that if two plaintext values are ordered in a certain way, their corresponding cipher text values will also be ordered in the same way. However, it's important to note that ope has certain limitations and trade-offs, such as security concerns and the inability to support certain operations like range queries.

6.2. File Hashing Splitting Algorithm

The file hashing splitting algorithm involves two main steps: hashing the file and then splitting it based on the hash values. First, a cryptographic hash function like sha-256 is applied to the file in blocks, generating a unique hash value for each block. These block hash values are concatenated to create an overall hash value for the entire file. Next, predetermined hash ranges are used to split the file into smaller parts. As each block's hash value is computed, it is assigned to the corresponding hash range, and the block is appended to the appropriate split file. This process continues until the entire file is processed and split into multiple smaller files based on the hash ranges. The algorithm's effectiveness depends on the chosen hash function, granularity of splitting, handling of hash collisions, and the sequential read of the file.

6.3. BVCS algorithm (binocular visual cryptography techniques system)

Binocular visual cryptography (bvc) schemes encrypt an image into two shares (share a and share b) using a random noise image (key). Each share individually reveals no information about the original image. To decrypt, the shares are viewed separately with binocular glasses or a device; share a' seen by the left eye and share b' by the right. Only the combined view reveals the original image, requiring both shares for decryption. The randomness and secrecy of the key image are crucial for security. Bvc combines cryptography and visual perception, providing a form of two-factor authentication. Robustness against attacks like visual analysis is an ongoing research area in bvc schemes

7. Implementation

7.1. Secure File Uploading

In this module, to mitigate the security leakages it is implemented with security enhancement in consideration of the modified encrypted search procedure in order to mitigate statistics information leak and keywords-files association leak. The file is uploaded with secured images and password which is generated using File homomorphic Encryption algorithm. The main goal of these modules is to prevent the unauthorized user gaining the access of this file.

7.2. Splitting Encrypted File

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer system or transmitted via the internet or other computer system. Modern encryption algorithm plays a vital role in the security assurance of IT system and communication as they can provide not only confidentiality but also the integrity and non-de-duplication. Encryption is the most effective way to achieve data security. The Cloud provider uploaded the User files that will be encrypted into two parts like encrypted Index and encrypted files by using AES (Advanced Encryption Standard) Algorithm before sending them to the cloud. The encrypted file have to been stored in storage node with their respective file Id.

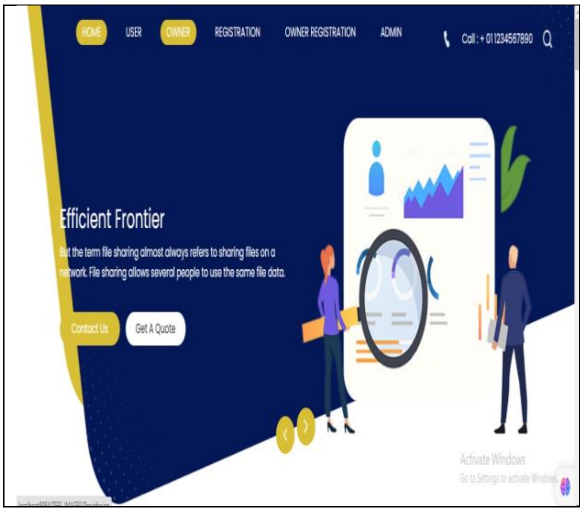
7.3. Image Split-up Using BVCS

Image splitting is a technique most often used to slice a larger image into smaller parts to make it load faster. Cloud provider upload the user file with secured image, that image should be splitting into two images like source and key image by using BVCS (Binocular Visual Cryptography schemes algorithm. Then, the key image and the password will be send to the particular user and the necessary file can then be downloaded. The password is generated which is then splitted into source image and key image and they are stored to the user and cloud server.

7.4. Verification

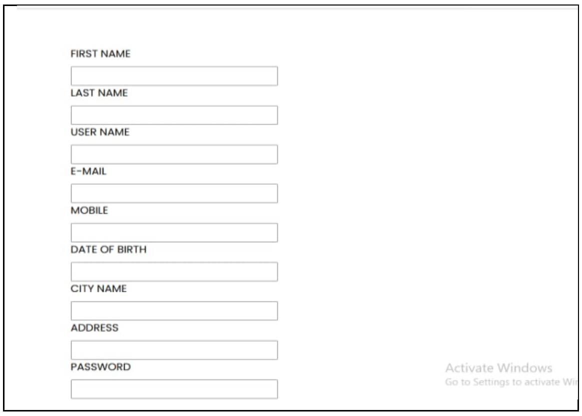
Verification is the act of reviewing, inspecting or testing a technical standards. Now the user has to send the key image to the cloud for accessing the files. The cloud matches the key image with the source image it already has. When both matches, it will send the file in the form of a captcha. Then it can be downloaded easily. It is the act of reviewing, inspecting or testing in order to establish and document that a product, service or system meets regulatory or technical standards.

8. Experimental Results



But the term file sharing almost always refers to sharing files on a network. File sharing allows several people to use the same file data.

Fig 8.1 Homepage



FIRST NAME

LAST NAME

USER NAME

E-MAIL

MOBILE

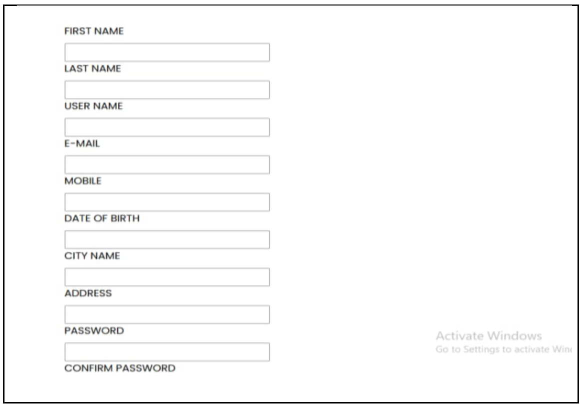
DATE OF BIRTH

CITY NAME

ADDRESS

PASSWORD

Fig 8.2 User Register



FIRST NAME

LAST NAME

USER NAME

E-MAIL

MOBILE

DATE OF BIRTH

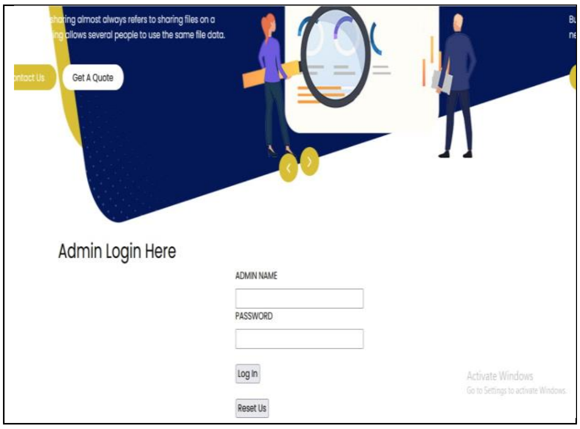
CITY NAME

ADDRESS

PASSWORD

CONFIRM PASSWORD

Fig 8.3 Owner Register



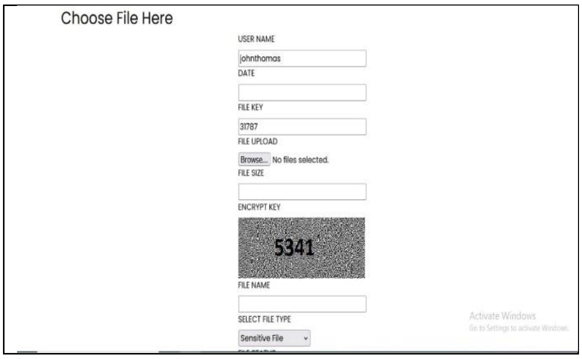
sharing almost always refers to sharing files on a ing allows several people to use the same file data.

Admin Login Here

ADMIN NAME

PASSWORD

Fig.8.4 Admin Login Page



Choose File Here

USER NAME: johnthomas

DATE:

FILE KEY: 31787

FILE UPLOAD: Browse... No files selected.

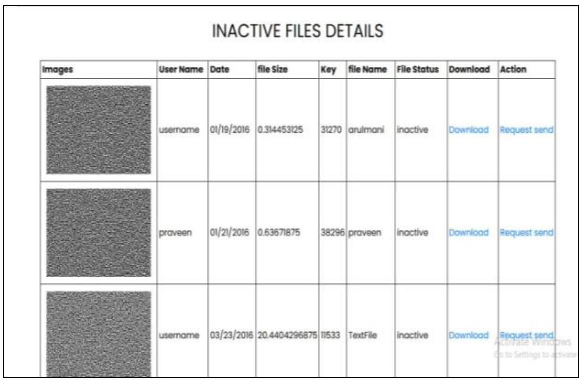
FILE SIZE:

ENCRYPT KEY: 5341

FILE NAME:

SELECT FILE TYPE: Sensitive File

Fig.8.5 File Upload



INACTIVE FILES DETAILS

Images	User Name	Date	file Size	Key	file Name	File Status	Download	Action
	username	01/19/2016	0.314453125	31270	arulmani	inactive	Download	Request send
	praveen	01/21/2016	0.63671875	38296	praveen	inactive	Download	Request send
	username	03/23/2016	20.4404296875	11533	TextFile	inactive	Download	Request send

Fig.8.5 File Request

9. Conclusion & Future Work

We make four key contributions. First, we propose the first privacy preserving conjunctive query processing scheme that achieves all three requirements of adaptive security, efficient query processing, and scalable index size. Our scheme embraces several novel ideas such as IBFs and IBtrees. Second, we propose the first probabilistic trapdoor computation algorithm to generate different trapdoors for the same query. Third, we propose IBtree space compression algorithm and IBtree traversal minimization algorithm to achieve space efficiency and query time efficiency. Fourth, we evaluated our scheme on two real-world data sets. Experimental results show that our scheme is fast in terms of query processing time and scalable in terms of index size and Future enhancement, Our future upgrade will be by transferring numerous records into the cloud server in order to keep away from pointless hacking the cloud and furthermore to give security less cost in order to enable the clients to store their information in a productive way.

Reference

[1] Ruizhong Du, Caixia Ma, and Mingyue Li, Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Block chains, SINGHUA SCIENCE AND TECHNOLOGY ISSNl l1 0 0 7- 0 21 4 0 2/ 1 8 p p1 3 – 26 DOI: 10.26599/TST.2021.9010070 Volume 28, Number 1, February 2023.

[2] Ming Zeng, Haifeng Qian, Jie Chen, and Kai Zhang, Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage, IEEE Transactions on Cloud Computing (Volume: 10, Issue: 1, 01 Jan.-March 2022).

[3] Xinyu Meng, Lei Zhang, Burong Kang, Fast Secure and Anonymous Key Agreement Against and the title is as to be Bad Randomness for Cloud Computing,IEEE TRA NSACTIONS ON CLOUD COMPUTING, VOL. 14, NO. 8, JUNE 2022.

[4] Yang Lu and Jiguo Li, Lightweight Public Key Authenticated Encryption with Keyword Search against Adaptively-Chosen-Targets Adversaries for the application Mobile Devices, IEEE Transactions on Mobile Compu ting (Volume: 21, Issue: 12, 01 December 2022).

[5] Chengliang Tian, Jia Yu, Hanlin Zhang, Haiyang Xue, Cong Wang, Kui Ren, Novel Secure Outsourcing of Modular Inversion for Arbitrary and to Variable Modulus, IEEE TRANSACTIONSON SERVICES COMPUTING, VOL.,NO. 2022.

[6] J. Li, H. Yan, and Y. Zhang, “Identity-based privacy preserving remote data integrity checking for cloud storage,” IEEE Systems Journal, vol. 15, no. 1, pp. 577-585, Mar. 2022.

[7] X. Ge et al., “Towards achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification,” IEEE Trans. Dependable Secure Computer. vol. 18, no. 1, pp. 490–504, Jan./Feb. 2021.

[8] Guoxiu Liu, Geng Yang, Member, and to Shuangjie Bai, Huaqun Wang, and Yang Xiang, Senior Member, FASE: A Fast and Accurate Privacy-Preserving Multi-keyword Top-k Retrieval Scheme over Encrypted Cloud Data, IEEE Transactions on the Services Computing (Volume: 15, Issue: 4, 01 July-Aug. 2022)

[9] Payal Chaudhari and Manik Lal Das, title Privacy Preserving Searchable Encryption with Fine-grained Access Control, IEEE TRANSACTIONS ON to the CLOUD COMPUTING, VOL. 14, NO. 8, JULY 2022

[10] Cheng Guo, Xue Chen, Yingmo Jie, Zhangjie Fu Member, IEEE, Mingchu Li, and Bin Feng, Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption, IEEE transactions on cloud computing, vol. 14, no. 8, may 2020.

[11] S. Kamara, C. Papamanthou, and T. Roeder, Dynamic searchable symmetric encryption, in Proc. 2012 ACM Conf. on Computer and Communications Security, Raleigh, NC, USA, 2012, pp. 965–976.

[12] E. Stefanov, C. Papamanthou, and E. Shi, Practical dynamicsearchable encryption with small leakage, in Proc. of Network and Distributed System Security Symposium, San Diego, CA, USA, pp. 72–75, 2014.

[13] R. Bost, Po'o&: Forward secure searchable encryption, in Proc. 2016 ACM SIGSAC Conf. on Computer and Communications Security, Vienna, Austria, 2016, pp. 1143– 1154.

[14] R. Bost, B. Minaud, and O. Ohrimenko, Forward and backward private searchable encryption from constrained cryptographic primitives, in Proc. 2017 ACM SIGSAC Conf. on Computer and Communications Security, Dallas, TX, USA, 2017, pp. 1465–1482.

[15] J. G. Chamani, D. Papadopoulos, C. Papamanthou, and R. Jalili, New constructions for forward and backward private symmetric searchable encryption, in Proc. 2018 ACM SIGSAC Conf. on Computer and Communications Security, Toronto, Canada, 2018, pp. 1038–1055.