www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 334-336

e-ISSN : 2583-1062

Impact Factor : 5.725

CIPHERTEXT INDEX RETRIEVAL SCHEME

Sureshkumar T[1], Hariharan N[2], Jayakumar K K[3], Jotheeswaran H[4], Kowsik G[5]

[1]Assistant Professor, Nandha College of Technology, Perundurai 638 052, Tamilnadu, India

[2,3,4,5]UG Students - Final Year, Department of Information Technology, Nandha College of Technology, Perundurai 638 052, Tamilnadu, India

ABSTRACT

The project, which was developed using JAVA as the front-end and MySQL server 2005 as the back-end, was dubbed "A Scheme for Effective Ciphertext Index Retrieval Based on Edge Computing Framework." Due to cloud computing's increased flexibility and cost savings, data owners are motivated to outsource their complex data management systems from local sites to commercial public clouds. However, sensitive data must be encrypted prior to outsourcing in order to protect privacy. This renders the previous method of data utilization, which relied on plaintext keyword searches, obsolete. Consequently, it is essential to enable an encrypted cloud data search service. Given the large number of cloud data users and documents, it is essential for the search service to support multi-keyword queries and provide result similarity ranking in order to effectively meet the requirement for data retrieval. It is difficult to distinguish between search results because related research on searchable encryption focuses primarily on Boolean keyword search or a single-keyword search. We define and solve the difficult problem of privacy-preserving multi-keyword ranked search (MRSE) over encrypted cloud data for the first time. In addition, we establish stringent privacy requirements for a secure system that uses cloud data.

Keywords: Searchable Encryption, Multi-Keyword Ranked Search over Encrypted Cloud Data, Triple-DES Algorithm, Trapdoor Function.

1. INTRODUCTION

Algorithms for data mining produce knowledge, and the results rarely infringe on privacy because they typically reveal knowledge at a higher level than individual data instances. Privacy advocates have a valid concern because combining data to support data mining makes misuse easier. The problem is with the method of data mining, not with data mining itself. The Solutions to the Problem with Privacy and Data Mining (PPDM) era of data mining research looks for potential privacy breaches in data mining algorithms. The primary objective of PPDM is the creation of efficient algorithms for extracting relevant information from a large amount of data and preventing the leakage or deduction of sensitive data and information. The third method for solving PPDM problems is the cryptographic method.

2. LITERATURE REVIEW

3 3, March 2023 March

2.1 Keyword Searches on Remote Encrypted Data with Privacy

Protecting the secrecy of the keywords as a whole without endangering the remote storage's security user U wishes to save his data safely on a distant file server S. Afterwards, user U wishes to rapidly retrieve some of the encrypted files containing specific keywords. Yet, user U does not want to jeopardise the remote storage's security. For example, a user may wish to keep encrypted copies of prior email messages on a Yahoo or another major vendor-managed server in order to recover certain messages while on the road with a mobile device. [2] Solves this issue by outlining the security requirements in detail.

2.2 Cryptographic Cloud Storage

Despite the apparent benefits, using public cloud architecture poses major security and privacy issues. In reality, it appears that the biggest barrier to the adoption of cloud storage—and cloud computing in general—is worries about data security and confidentiality. [3] Presents a summary of the benefits of a cryptographic storage service, such as lowering legal liability for consumers and cloud providers and ensuring regulatory compliance. In addition, a few cloud services that may be developed on top of a cryptographic storage service, such as safe data sharing and e-discovery, are briefly described.

2.3 Effective and Secure Multi-Keyword Search on Cloud Data

On the one hand, users who do not necessarily have prior knowledge of the encrypted cloud data must post-process each file that is recovered in order to discover the files that most closely match their interests. In contrast, with the present pay-as-you-go cloud model, accessing all files containing the query term invariably results in unnecessary network traffic. The challenge of efficient and safe ranked keyword search over encrypted cloud data has been described and solved in this study [4]. By returning the matched files in a ranked ontology keyword mapping and

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 334-336

e-ISSN : 2583-1062

Impact Factor : 5.725

search, we increase system usability and move one step closer to the practical implementation of privacy-preserving data hosting services in Cloud Computing.

2.4 Easy Fuzzy Keyword Search Over Encrypted Data in Cloud Computing

The fundamental goal of this research is to do privacy-preserving fuzzy keyword searches on encrypted cloud data [7]. This basic idea has been used, but our suggested system uses a new multi-keyword raked search (BKCM) technique. [8] Recommends a stable and secure cloud storage solution with near-optimal overall performance.

2.5 Securing, Scalability, and Fine-Grained Data Access Control in Cloud Computing

Access control cannot provide fine-grainedness, scalability, and data secrecy all at the same time. The work [9] addresses this difficult open issue by defining and enforcing access policies based on data attributes and allowing the data owner to delegate the majority of computation tasks associated with fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. [10] Proposes a privacy-preserving public auditing mechanism for cloud computing data storage security. It uses a homomorphic linear authenticator and random masking to guarantee that the TPA does not learn anything about the content of the cloud server's data throughout the efficient auditing procedure.

3. EXISTING SYSTEM

For fast data retrieval, the search engine must allow multi-keyword searches and give similarity ranking owing to the enormous number of cloud data users and documents. Instead of discriminating between search results, searchable encryption focuses on single keyword or Boolean keyword searches.

4. PROPOSED SYSTEM

4.1. System Flow Diagram

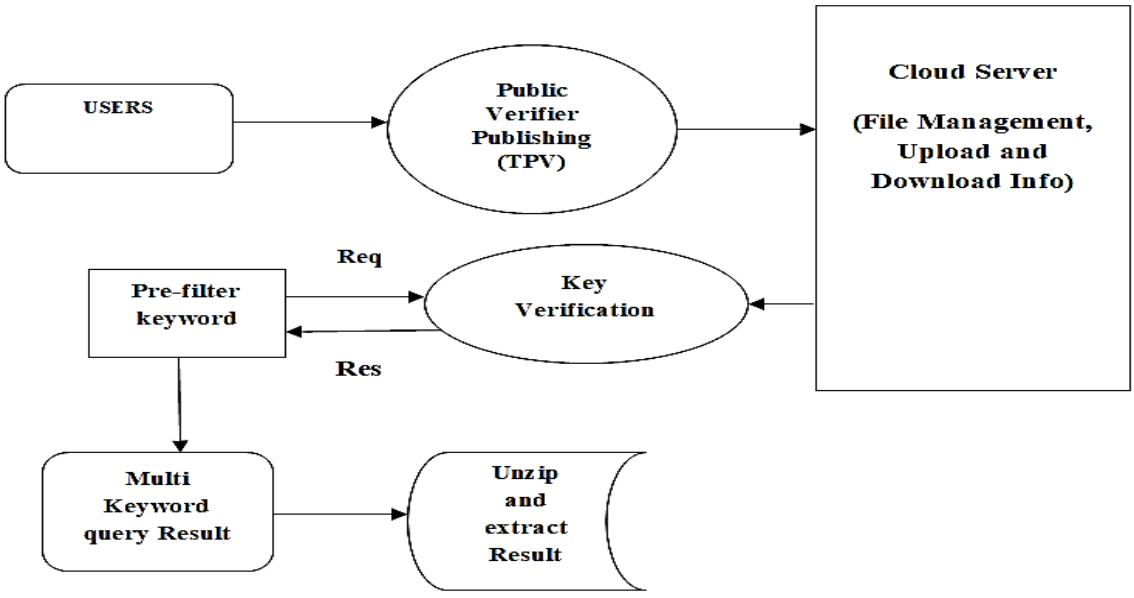

Figure 1. System Flow

In order to make a safe cloud data usage system a reality, we describe and solve the tough issue of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE) and propose a set of strict privacy criteria. The effective principle of "coordinate matching" is chosen from among a number of multi-keyword semantics. We create a set of privacy regulations for a safe cloud data usage system and propose Secured Multi-keyword Search (SMS) over encrypted cloud data (ECD). To determine the closeness of the search query and data, we use the extremely efficient rule of coordinate matching from a set of multi-keyword semantics. Using inner data correspondence, we quantitatively formalize this principle for measuring similarity for further matching.

4.2. Encrypt Module

This module helps the server use the TRIPLE DES algorithm to encrypt the document, turn it into a Zip file with an activation code, and then send the activation code to the user so they can download it.

4.3 Client Module

This module assists the client in searching the file using numerous key phrases and obtaining an accurate list of results depending on the user's query. Prior to entering the activation code, the user will pick the appropriate file, register their user details, and get an email from the "customerservice404" address. The user can then extract the Zip file.

4.4 Multi-Keyword Module

This module assists the client in searching the file using numerous key phrases and obtaining an accurate list of results depending on the user's query. Prior to entering the activation code, the user will pick the appropriate file, register their user details, and get an email from the "customerservice404" address. The user can then extract the Zip file.

4.5 Admin Module

This module allows the server to securely upload files and see information. The log key is used by administrators to keep track of login times. Change the log key before the administrator logs out. After signing in and updating the password, the administrator may check the user downloading and file request count data on a flowchart. When the file has been converted to Zip format, the administrator can upload it.

4.6 File Upload Module

This module allows the server to safely upload files and see data. Administrators use the log key to keep track of login times. Before the administrator logs out, update the log key. After signing in and updating the password, the administrator may see the user downloading and file request count data on a flowchart. After converting the file to Zip format, the administrator can upload it.

5. RESULTS

The usage of encryption to secure sensitive data has grown dramatically in recent years. Nevertheless, because encryption is so widely used, it is difficult to swiftly access encrypted data when needed. Ciphertext indexing, which includes indexing ciphertexts based on their properties to speed up retrieval, is one option. Conventional ciphertext indexing approaches, on the other hand, usually need substantial processing power, resulting in exorbitant prices and lengthy retrieval times. To solve these challenges, an edge computing framework-based solution for effective ciphertext index retrieval has been developed. To perform ciphertext indexing and retrieval tasks, this strategy makes use of the computing capacity of edge devices such as mobile phones and Internet of Things (IoT) devices.

6. CONCLUSION

This work defines and solves multi-keyword ranked search over encrypted cloud data, as well as a variety of privacy constraints. To formalize this rule for quantitative comparability estimate, "internal item closeness" is utilized. We select the proficiency standard of "coordinate coordinating," which implies that there should be as many matches as possible across the different multi-catch meanings. We first propose a foundational MRSE approach that uses secure inner product computing to fulfill privacy criteria in two tiers of threat models. This enables us to tackle the problem of offering multi-keyword semantics while protecting user privacy. The strategy is then extensively enhanced to suit privacy needs. As a result, our suggested techniques feature little computation and communication overhead.

7. REFERENCES

[1] Singhal A, “Modern information retrieval: A brief overview,” IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2019.

[2] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. of EUROCRYPT, 2019.

[3] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. of S&P, 2020.

[4] E.-J. Goh, “Secure indexes,” Cryptology ePrint Archive, 2003, http:// eprint.iacr.org/2019/216.

[5] Witten I. H, A. Moffat, and T. C. Bell, “Managing gigabytes: Compressing and indexing documents and images,” Morgan Kaufmann Publishing, San Francisco, May 2019.

[6] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Comput. Commun.Rev.,vol. 39, no. 1, pp. 50–55, 2019.

[7] M. Bellare, A. Boldyreva, and A. ONeill, “Deterministic and efficiently searchable encryption,” in Proc. of CRYPTO, 2019.

[8] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proc. of ACM CCS, 2019

[9] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in RLCPS, January 2020 LNCS. Springer, Heidelberg.

[10] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Proc. of ACNS, 2019.