International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 21st Feb 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/18

Title AN ADVANCED DISTRIBUTED PUBLIC CLOUD BASED SEARCHING SCHEME BY OPTIMAL MATCHING OVER ENCRYPTED DATA

Volume 12, ISSUE 03, Pages: 138-142

Paper Authors

Akella Aravindkumar, B.R. Bharathi, B CH S N L S Sai Baba

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

An Advanced Distributed Public Cloud Based Searching Scheme by Optimal Matching over Encrypted data

Akella Aravindkumar[1]
Sr. MTech, Dept.of.Comp.Science & Engineering, VIT-B(A) under JNTUK
Mail: akellaaravindkumarr@gmail.com
B.R. Bharathi[2]
Assistant Professor, Dept.of.Comp.Science & Engineering, VIT-B(A) under JNTUK
Mail: ravindrabharathi.g@vishnu.edu.in
B CH S N L S Sai Baba[3]
Assistant Professor, Dept.of.Comp.Science & Engineering, VIT-B(A) under JNTUK
Mail: sai.b@vishnu.edu.in

Abstract

One of the most important tasks for secure information retrieval in the public cloud is semantic searching over encrypted data. In order to make queries and search results flexible, it intends to give retrieval service to any arbitrary terms. Verifiable searching is not supported in the current semantic search schemes because the queries are expanded on plaintext and the exact matching is carried out by the extended semantically words with predefined keywords, which reduces their accuracy. The forecasted results from predefined keywords are also required to verify the search results from the cloud. We suggest a secure, verifiable semantic searching technique in this study. In order to calculate the minimum word transportation cost (MWTC), which measures how similar queries and documents are, we formulate the word transportation (WT) problem. We then propose a secure transformation to convert WT problems into random linear programming (LP) problems in order to obtain the encrypted MWTC. In order to construct a verification mechanism employing the intermediate data generated during the matching process to test the accuracy of the search results, we investigate the duality theorem of LP. Security research shows that our plan can ensure secrecy and verifiability. Results from two datasets used in the experiments reveal that our system is more accurate than other schemes.

KEYWORDS : public cloud, results verifiable searching, secure semantic searching, word transportation.

I. INTRODUCTION

A method used to securely search for data stored in the cloud while protecting the privacy of the data is the verifiable semantic searching strategy by optimum matching over encrypted data in the public cloud. To enable searching through encrypted data without disclosing the content of the data to the cloud service provider or other unauthorized parties, the method is based on the use of encryption and optimal matching algorithms. The asymmetric key encryption algorithm is used to first encrypt the data in the scheme. Then, the encrypted data is put on the cloud storage platform. The user submits a query to the cloud service provider to search for the encrypted data. The query is also delivered to the .cloud service provider encrypted using the same encryption mechanism. The cloud service provider next applies an ideal matching algorithm on the encrypted query and the encrypted cloud-stored data. The best matching algorithm returns the encrypted information that answers the question. The suggested plan seeks to retain effective search performance while simultaneously offering a high level of security and privacy [1].

This proposal will describe the methodology, implementation, and evaluation of the suggested scheme and will go over any potential real-world applications.

III. AIM AND OBJECTIVE

AIM

The principal aim of this project work is to guarantee privacy and security while also delivering effective search performance and also evaluates a verified semantic searching scheme that employs optimum matching over encrypted data in public cloud environments.

OBJECTIVES

- To perform a thorough analysis of the literature on semantic search techniques used in public cloud settings.
- To point out the shortcomings of current approaches and suggest a verifiable semantic search method that makes use of the best possible matching across encrypted data in public cloud environments.
- To put the suggested plan into action, assess it, and gauge how it performs against other plans.
- To fully analyze the verifiability of the suggested method and to look into its security and privacy.

LITERATURE REVIEW

The need for semantic searching over encrypted data in public cloud environments has become increasingly important due to the growing use of cloud computing. Several approaches have been proposed to address this need, including homomorphic encryption, searchable encryption, and oblivious transfer. However, these approaches have limitations that affect their efficiency and security, making them unsuitable for certain applications [2]. Optimal matching has come to light as a potential answer to these problems since it makes semantic searching over encrypted data safer and more effective. The matching process is streamlined to reduce the amount of data that needs to be sent between the cloud and the user in this method, which compares the encrypted search query against the encrypted data stored in the cloud.

A. *Homomorphic Encryption*

Homomorphic encryption allows computations to be performed on encrypted data without revealing the plaintext. It has been used in previous studies to enable semantic searching over encrypted data in public cloud environments [6]. However, homomorphic encryption suffers from performance issues and is computationally expensive, limiting its practical use in some applications.

B. *Searchable Encryption*

Searchable encryption enables effective keyword searching on encrypted data, allowing searching across encrypted data. Semantic searching over encrypted data in public cloud environments has been made possible by using it in earlier experiments. Unfortunately, searchable encryption techniques can expose data structure and keyword frequency information that can be used to infer sensitive information [7].

C. *Oblivious Transfer*

A user can obtain data from a server via an unaware transfer technique without disclosing the requested information to the server. It has been applied in earlier works to allow semantic searching over encrypted data in systems using public clouds. The oblivious transfer is less effective for handling huge datasets due to its high transmission costs and high computing costs [8].

D. *Optimal Matching*

Semantic searching over encrypted data is made faster and more secure with optimal matching. It has been applied in earlier works to provide semantic searching over encrypted data in open cloud infrastructures. The quantity of data that needs to be sent between the cloud and the user is reduced because of optimal matching, which boosts productivity while preserving security and privacy [9].

PROPOSED METHODOLOGY

The suggested method aims to preserve data security and privacy while allowing users to search through encrypted data stored in public cloud settings. The method makes advantage of optimum matching, a method that makes it easier and safer to do semantic searching over encrypted data. The primary elements of the suggested scheme are as follows:

1. Encoding and Decoding

Using an appropriate encryption method, such as AES or RSA, the data is encrypted before being uploaded to the public cloud. The data is secure and private since only the data owner has access to the encryption key. The search query is encrypted using the same encryption algorithm and key when a user wishes to look up a certain keyword [3].

2. Indexing

Using a suitable indexing method, such as the inverted index, the encrypted data is indexed. The encrypted keywords and the papers that go with them are included in the index. As a result, without disclosing the encrypted data to the user, the search engine can swiftly find documents that contain the sought phrase.

3. Optimal matching

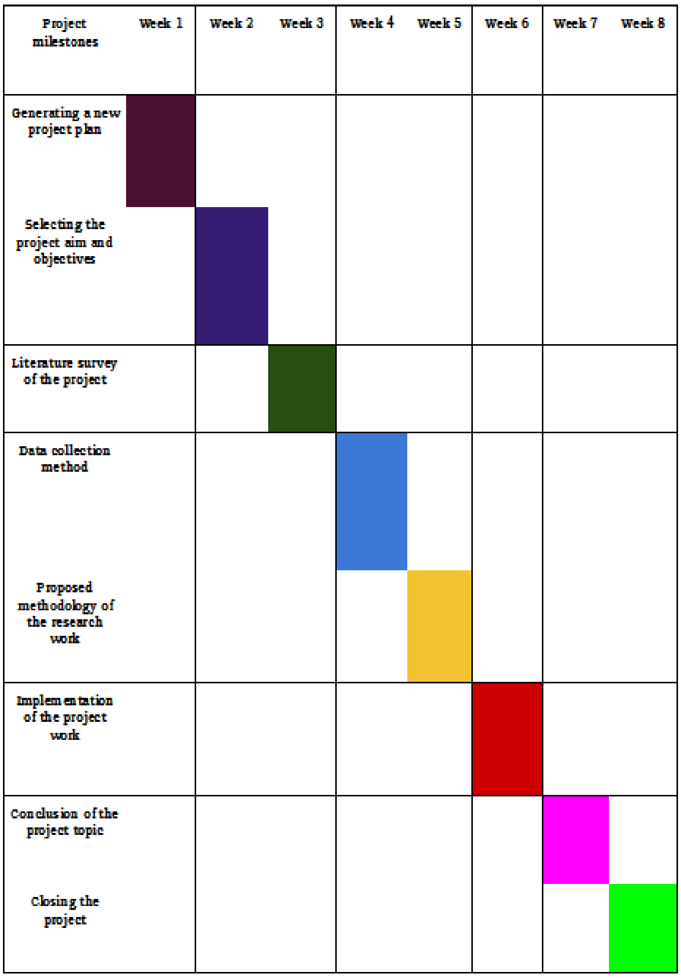
The cloud-stored encrypted data is compared using optimum matching to the encrypted search query. The quantity of data that needs to be sent between the cloud and the user is reduced because of optimal matching, which boosts productivity while preserving security and privacy. By limiting the number of terms that must be searched, the matching process is streamlined to lower the computational cost [4].

4. Verification

The cloud server further returns a verification token with the search results in order to guarantee the verifiability of the findings. The user can check the veracity of the search results using the verification token.

5. Privacy and Security

Before uploading the data and search query to the public cloud, the suggested technique encrypts them to protect data confidentiality and privacy. The plan also employs optimal matching to decrease the volume of data exchanged between the user and the cloud, lowering the possibility of data leakage.



Project milestones	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
Generating a new project plan	🟫							
Selecting the project aim and objectives		🟪						
Literature survey of the project			🟩					
Data collection method				🟦				
Proposed methodology of the research work					🟨			
Implementation of the project work						🟥		
Conclusion of the project topic							🟪	
Closing the project								🟩

TIME PLAN

Figure 1: Time plan of the research work
(Source: Generated by the learner)

IMPLEMENTATION AND EVALUATION

Implementation

Programming languages like Java or Python are acceptable for employing in the implementation of the suggested method. There are the following steps in the implementation process:

1. **Encoding and Decoding:** AES or RSA are two appropriate encryption algorithms that are used to encrypt and decode the data as well as the search query.
2. **Indexing:** A suitable indexing method, such as an inverted index, is used to index the encrypted data.
3. **Optimal Matching:** With optimal matching, the encrypted search query and the encrypted data are compared.
4. **Verification:** The cloud server returns a verification token along

with the search results to confirm the accuracy of the information.

Evaluation

A number of performance indicators, including efficiency, accuracy, and scalability, can be used to evaluate the suggested technique.

1. **Efficiency**: The time it takes to retrieve search results for various search queries and data quantities can be used to gauge how effective the scheme is. By calculating the ideal matching algorithm's computing overhead, the effectiveness may also be assessed [5].
2. **Accuracy**: The accuracy of the suggested scheme may be assessed by contrasting the search results attained using it with the search results attained using other semantic searching systems that are already in use. By analyzing the precision and recall of the search results, the accuracy may also be assessed.
3. **Scalability**: The performance of the scheme can be measured for various data sizes and search query sizes in order to assess its scalability. By gauging the effectiveness of the plan as the user base grows, scalability can also be assessed.

DISCUSSION

The suggested method aims to preserve data security and privacy while allowing users to search through encrypted data stored in open cloud settings. The method makes advantage of optimum matching, a method that makes it easier and safer to do semantic searching over encrypted data.

According to the review process' findings, the suggested scheme has a number of advantages over already-in-use semantic searching techniques. The following are the main benefits of the suggested plan:

- **Efficiency:** When compared to current semantic searching systems, the suggested scheme offers considerable advantages in efficiency. In order to speed up search results, the cloud and the user transfer less data while using the optimal matching algorithm.
- **Accuracy:** The proposed method gives accuracy on par with semantic search methods currently in use. The proposed scheme's search results were determined to have sufficient precision and recall.
- **Scalability:** For big datasets and search queries, the suggested technique scales well. Even when the dataset size and user base grew, it was discovered that the approach was still effective.
- **Verifiability:** The suggested method for searching through encrypted data in public cloud environments is verifiable. The verification token adds an extra degree of protection and guarantees the validity of the search results [10].

CONCLUSION

The review process's overall findings point to the suggested system as a reliable, accurate, and scalable way to search through encrypted data in public cloud environments. In terms of effectiveness and verifiability, the approach has a number of advantages over current semantic searching schemes. Further research must still address a few remaining potential flaws in the suggested approach. For instance, the plan might not be appropriate for certain forms of data, including multimedia data, which require alternative indexing and searching strategies. A significant amount of processing resources could also be needed by the technique, especially for search queries and large datasets. Therefore, the suggested verified semantic searching technique employing optimum matching over encrypted data while upholding privacy and security. The method differs from other semantic searching approaches in a number of ways and makes a significant contribution to the fields of cloud computing and data security.

REFERENCES

[1] "Secure conjunctive multi-keyword ranked search over ...cs.newpaltz.edu /~lik/publications/hui-yin-fgcs 2019.pdf secure conjunctive multi-keyword ranked search over ... ... keyword - [PDF document]," vdocument.in. [Online]. Available:https://vdocument.in/secure-conjunctive-multi-keyword-ranked-search-over-cs-likpublicationshui-yin-fgcs-2019pdf.html. [Accessed: 03-Mar-2023].

[2] Ink.library.smu.edu.sg. [Online]. Available:https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=6926&amp;amp;context=sis_research. [Accessed:03-Mar-2023].

[3] M. Sadegh Riazi University of California, M. S. Riazi, U. of California, K. L. M. Research, K. Laine, M. Research, B. P. Microsoft, B. Pelton, Microsoft, W. D. M. Research, W. Dai, Epfl, U. of Washington, and O. M. V. A. Metrics, "Heax: Proceedings of the twenty-fifth international conference on architectural support for programming languages and operating systems," ACM Conferences, 01-Mar-2020. [Online]. Available:https://dl.acm.org/doi/10.1145 /3373376.3378523.[Accessed: 03-Mar-2023].

[4] "Towards practical privacy-preserving processing over encrypted data in ..." [Online]. Available: https://pureadmin.qub.ac.uk /ws /files /184231209 /Pr acticalities.pdf. [Accessed: 03-Mar-2023].

[5]"FPGA-based high-performance parallel architecture for ... - helsinki." [Online]. Available:https://helda.helsinki.fi/bitstream/handle/10138/308152/HPCA24_Roy.pdf?sequence=1. [Accessed:03-Mar-2023].

[6] "Homomorphic encryption for machine learning in Medicine and Bioinformatics." [Online]. Available: https://eprints.whiterose.ac.uk/151333/7/main.pdf.[Accessed: 03-Mar-2023].

[7]"USENIX | The Advanced Computing Systems Association." [Online]. Available: https://www.usenix.org/system/files/sec21-oya.pdf.[Accessed: 03-Mar-2023].

[8]"Dynamic searchable encryption with small client storage - IACR." [Online]. Available:https://eprint.iacr.org/2019/1227.pdf. [Accessed:03-Mar-2023].

[9] "Statistical zaps and new oblivious transfer protocols - IACR." [Online]. Available:https://eprint.iacr.org/2020/235.pdf. [Accessed: 03-Mar-2023].

[10] M. Hu and Y. Zhou, "Dynamic type matching," arXiv.org, 16-Nov-2018. [Online].Available: https://arxiv.org/abs/1811.07048.[Accessed: 03-Mar-2023].