IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁂ Impact Factor 7.105 ⁂ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96121

A SECURE AND DYNAMIC MULTI-KEYWORD RANKED SEARCH SCHEME

Aravind Ganesh S[1], Seema Nagaraj[2]

Student, Department of MCA, Bangalore Institute of Technology, Bangalore, India[1]

Asst.Prof, Department of MCA, Bangalore Institute of Technology, Bangalore, India [2]

Abstract: Many data owners outsource their data management to cloud servers for simplicity and lower expenses. Encrypting critical data before outsourcing ensures its privacy. Law requires this. Thus, many data-use tactics, such as keyword-based document retrieval, are antiquated. Our method decrypts cloud-stored data without putting users at risk. This method allows simultaneous adjustments. The system allows document deletion and addition. Vector space models and TF-IDF models help indexing and query creation. Using "Greedy Depth First Search," you may search for terms in our tree-based database. Users may search for multiple keywords in the order they appear in results. Secure kNN encrypts both index and query vectors. Encrypting the index and query vectors allows for accurate relevance scoring. This method encrypts index and query vectors. Phantom words conceal search results and protect the index vector against statistical attacks. This safeguards the index. Our tree-based index structure speeds up searches using the suggested strategy. Quickly removing and inserting files are other benefits. The index's tree-like structure enables this. The proposed approach will be tested thoroughly.

Keywords: Multi Keyword Search, Encrypted, Cloud, Data, Cloud Servers.

I. INTRODUCTION

Using computer resources (hardware and software) provided as a service across a network (in this case, the Internet) (known as "Cloud Computing" (typically the Internet). A cloud-shaped symbol was used to depict a system diagram's complex architecture, which led to its moniker. The name "cloud" was coined as a result of this behaviour. The user's data, software, and processing power are stored and managed by third parties in a system known as cloud computing. The term "cloud computing" refers to the practise of making computer hardware and software resources available through the internet through the use of a third-party managed service. Use these resources to do calculations. In many cases, these services provide access to high-end computer networks, including server hardware and advanced software. The military and scientific research institutions are the primary purchasers of high-performance computing power.. Cloud computing can do trillions of operations per second thanks to supercomputing, also known as high-performance computing. Early adopters of cloud computing, such as Amazon Web Services (AWS) and Microsoft Azure, A few examples of how this technology may be put to use include delivering customised information, storing data, powering massively immersive computer games, and constructing financial portfolios.

Data processing tasks are distributed among a large number of servers using a variety of low-cost consumer PC-based servers. A network of dedicated connections connects all of these servers. An enormous number of businesses share this IT infrastructure, which is made up of several interconnected pools of linked systems. Virtualization technologies are often used to improve cloud computing performance.

II. LITERATURE SURVEY

reethi R et all[1] demonstrated that this attempt solves MRSE to protect cloud privacy. Cloud storage is flexible, simple, and huge. Encrypt sensitive data before using plaintext keyword search in the cloud. Decrypting data is crucial. Using keywords, cloud users can find related documents. This searchable encryption method rarely arranges results for single-keyword or Boolean searches.

Zhihua Xia et all[2] addressed that Cloud computing's convenience and cost-savings have led to more data outsourcing. Encrypting data before outsourcing eliminates keyword-based document retrieval. We describe a safe multi-keyword ranked search engine that allows document deletion and insertion. Vector space and TFIDF models power indexing and querying. "Greedy Depth-first Search" ranks keywords efficiently.

Cheng Guo et all[3] addressed that Cloud computing saves money and provides flexibility when managing personal data. Sensitive data must be encrypted before being outsourced to cloud servers, making raw keyword search impossible. We offer multi-keyword ranked cloud data search. Our keyword ranking method uses vector space, TF IDF, and cosine similarity. Traditional solutions are costly. BloomFilter is used to generate a sub-linear search index tree.

Gadee Manasa et al[4] proposed that as cloud computing grows, more data owners outsource their data for convenience and cost savings. Encrypting sensitive data before outsourcing removes keyword-based document retrieval. We describe a safe multi-keyword ranked search system that enables dynamic document deletion and insertion. Indexing and querying use vector space and TF-IDF models.

C Mareswari et al[5] addressed that High-level encryption should be employed to safeguard data during transfer, however this may cause complications for cloud users. Researchers are developing new data encryption techniques. Encrypting data before outsourcing protects it. All data is inaccessible. Ranked search minimises network traffic and speeds up data retrieval. Rankings must support multi-keyword searches.

Sowmya Murali et al[6] demonstrated that Cloud computing stores and accesses data and programs online. With more data, many document owners outsource to the cloud for convenience. Before cloud outsourcing, sensitive data should be encrypted for privacy. Vector space model represents documents. Vector space indexing employs TF*IDF. Two safe search techniques are used: BDMRS in the cipher text model and EDMRS in the background model.

Gangam Divya et al[7] addressed that more data owners are outsourcing their data because of cloud computing's development. Encrypting sensitive data eliminates keyword-based document retrieval. Ghost phrases obscure statistical search results. Our tree-based index structure offers sub-linear search performance and document deletion/insertion. Extensive tests validate the plan.

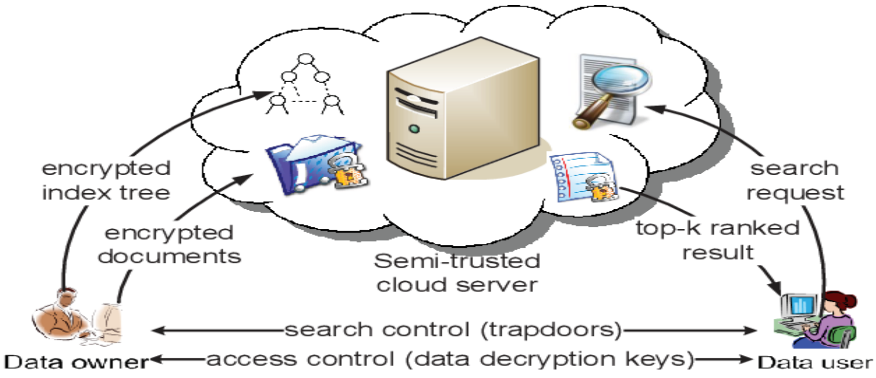
K Divya Vani et al[8] proposed that more data owners are outsourcing their data to cloud servers for convenience and cost savings in data management. To outsource sensitive data, it must be encrypted for privacy, which eliminates keyword-based document retrieval. Secure tree-based search offers multi-keyword ranked search and dynamic document operation. Index development and query generation mix vector space and TF-IDF models.

Arati Deshmukh et al[9] addressed that this project aims to ensure MRSE privacy. Complex data management systems may be outsourced to the cloud for flexibility and cost savings. We measure a document's search query match using "interior product similarity." Each document's binary vector sub-index determines if a phrase matches. Each bit of the search query's binary vector indicates occurrence. Multiplying query by data determines match.

M Gomathi et al[10]demonstrated that data owners are outsourcing to cloud servers for convenience and lower costs. Encrypt sensitive data before outsourcing tasks like keyword-based document retrieval. Encrypted cloud data controls multi-keyword searches and dynamic document removal and import. Focus on symmetric encryption data security. First, emphasise privacy's relevance and robustness.

III. METHODOLOGY

This module will help the owner register details and logins. This module enables the owner upload RSA-encrypted files. This prevents illegal access to files. Data owner wishes to outsource encrypted documents F =f1; f2; :::; fn to the cloud server for effective use. The data owner develops a safe searchable tree index I from management structure F, then encrypts F. The data owner then outsources the encrypted collection C and secure index I to the cloud server and securely distributes trapdoor generation and document decryption keys to approved data users. The data owner must update his cloud-stored documents. The data owner updates locally and webserver[1]. It includes login information. This module helps clients search files using different keywords and receive accurate results depending on user queries. The user will pick the appropriate file, register, and get an activation code through email before entering it. After downloading Zip, users can extract it. Data users can access owner's papers. An authorised person can create a trapdoor TD with t query keywords to get k encrypted documents from a cloud server. With the shared secret key, the data user can decrypt the documents[2]. It helps the server encrypt documents using RSA Algorithm and convert them to Zip files with activation codes for download. Cloud server holds the owner's encrypted document collection C and tree index I. The cloud server searches the index tree I for the trapdoor TD and returns the top k encrypted documents. The server must update index I and document collection C after receiving update information from the data owner. "Honest-but-curious" cloud servers are used in several studies on safe cloud data search[3]. This guarantees that rank search finds commonly searched files. This module lets the user download a file and decrypt it using his secret key. This module displays uploaded and downloaded files to the Owner. The suggested approach provides multi-keyword queries, reliable result ranking, and dynamic document collection updates. The strategy prevents the cloud server from learning about the document collection, index tree, and query[4].



IV. MODULES

- DATA OWNER MODULE
- DATA USER MODULE
- CLOUD SERVER AND ENCRYPTION MODULE
- RANK SEARCH MODULE

Data Owner Module:

This module offers guidance to the owner in the process of registering such information and, where applicable, also gives login data. This module simplifies the process of the owner submitting the encrypted version of his content by using the RSA encryption method. This ensures that the data will be protected from being accessed by people who are not authorised to do so. The owner of the data would want to move his collection of documents, which is represented by the notation F = f1; f2……fn, to a cloud server in an encrypted format while preserving the ability to conduct searches on them. The papers will be able to be utilised more effectively as a result of this. In our system, the owner of the data first creates an encrypted document collection C for the document collection F, and then continues to build a secure searchable tree index I from the documents in the document collection F. This process is repeated until all of the documents in the document collection F have been indexed. After that, the owner of the data will outsource the encrypted collection C and the secure index I to a cloud server. Following that, the owner of the data will securely distribute the key information for document decryption and trapdoor generation to the authorised users of the data. A further point to consider is that the owner of the data is the one who is accountable for the maintenance and upkeep of any of his documents that are stored on the cloud server. When an update is carried out, the owner of the data prepares the update information locally, and then sends it to the server when it has been uploaded.

Data User Module:

This module is responsible for storing the necessary login information for the user registration process. This module's objective is to first aid the client in their search for the file by making use of the concept of many key words, and then to supply the customer with an accurate result list based on the user's query. This will be accomplished by using the idea of several key phrases. The user must first choose the appropriate file, then register their user details, and then check their email for their activation code before they will be allowed to enter their activation code. After that, the user may choose to either extract the contents of the archive or download the compressed archive to their computer. Users of the data are those who have been given authorization to access the files that are the property of the owner of the data. An authorised user has the ability to construct a trapdoor TD in accordance with the search control methods by using t query keywords; once this is accomplished, the user has the potential to get k encrypted documents from a cloud server. After then, the person who uses the data will be able to decode the documents by using the shared secret key.

Cloud Server and Encryption Module:

By using the RSA Algorithm, this module is utilised to provide assistance to the server throughout the process of encrypting the document. After the document has been encrypted, it is then transformed into a Zip file that contains an activation code, and the user is then given the opportunity to download the activation code. On behalf of the data owner, the cloud server is responsible for keeping the encrypted document collection C as well as the encrypted searchable tree index I.

Rank Search Module:
After the cloud server has been given the trapdoor TD by the data user, it will conduct a search over the index tree I, and at some point, it will provide the data user a collection of the top-k rated encrypted documents that are relevant to the search. Additionally, as soon as the server receives the update information from the data's owner, the server is obligated to update both the index I and the document collection C according to the information that was received. This is the case regardless of whether or not the owner of the data requested the update information. The cloud server that is employed in the strategy that has been offered is referred to as "honest-but-curious," which is language that is used by a significant number of works on secure cloud data search.

V. CONCLUSION

Our research provides a dynamic, secure search engine that permits dynamic document deletion and insertion and correct multi-keyword ranking. "Greedy Depth-first Search" is more efficient than linear search on a keyword-balanced binary tree index. Parallel search reduces search time. Safe kNN protects the scheme from two attack models. Experiments show our strategy's efficacy. Symmetric SE schemes have several problems. This model's owner creates and maintains cloud server data. The unencrypted index tree and related data are needed to compute IDF values. Active data owners may not like cloud computing. Building a dynamic searchable encryption system that can only be updated by a cloud server may be a desirable but tough future undertaking. As with other searchable encryption techniques, ours focuses on cloud servers. Multi-user systems have security challenges. In symmetric SE, all users create trapdoors using the same secure key. This circumstance makes user removal tough. To revoke a user's access, rebuild the index and provide new secure keys to all authorised users. Second, symmetric SE assumes all data consumers are trustworthy. Untruthful users generate security difficulties, making it unfeasible. Dishonest data users may analyse documents and provide encrypted copies to unauthorised parties. A dishonest user may give away secret keys. We'll update SE to address these issues.

REFERENCES

[1]Preethi R,”A Multi Keyword Ranked Search Scheme over Audit free Cloud Storage”,International Journal of Advance Research in Science and Engineering,Volume 07,Issue 2,ISSN:2319-8354.
[2]Zhihua Xia,” A Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”.
[3]Cheng Guo,” A Dynamic Multi Keyword Ranked Search Scheme over Encrypted Cloud Data “.
[4]Gadee Manasa,” A Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”,International Journal & Magazine of Engineering,Technology,Management and Research,ISSN:2348-4845.
[5]C Mareswari,” A Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”,Internation Research Journal of Advanced Engineering & Sciences,ISSN:2455-9024.
[6]Sowmya Murali,” A Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”,International Research Journal of Engineering and Technology,Volume 4,Issue 11,ISSN:2395-0056.
[7]Gangam Divya,” A Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”,JETIR ,Volume 3,Issue 10,ISSN:2349-5162.
[8]K Divya Vani,”Multi Keyword Ranked Search Model over Encrypted Cloud Data”,International Conference on Recent Innovations in Science,Technology and Environment,ISBN:978-81-931039-1-3..
[9]Arati Deshmukh,” A Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”,International Journal of Advance Research,Ideas and Innovations in Technology,Volume 3,Issue 1,ISSN:2454-132X.
[10]M Gomathi,” Enchanced Dynamic Multi Keyword Ranked Search Scheme over Encrypted Cloud Data”,International Journal of Computer Science and Engineering Communications,Volume 4,Issue 2,ISSN:1337-1342.