A REVIEW ON EFFECTIVE MULTI KEY DATA SEARCH OVER CIPHER TEXT IN CLOUD DATA ENVIRONMENT

[1]A. Savarimouthou Flory,[2] Dr. R. Vidya

[1]Research Scholar, [2]Assistant Professor, PG & Research Department of Computer Science,

St.Joseph's College of Arts and Science (Autonomous), Cuddalore ,Tamil Nadu ,India.

ABSTRACT

Cloud computing could be a one sort of computer model for storing and obtaining access to the records and application over the community .Now an afternoon's most of the knowledge proprietors are inspired to add their terribly own file into the cloud servers because of its low value in control and additional convenience. The touchy data and data ought to be encoded before uploading to the cloud for privateness wants that retrieve facts the usage of key-word based totally record retrieval. This work mentioned an effective multi-key data search over cipher text in cloud storage. Here, Vector space Model and TF-IDF Model are used to mixed within the index creation and query generation. A Greedy Depth first Search has in addition been used index shape and it supply an efficient multi-key data search within the cipher text cloud surroundings. A KNN algorithm is employed encrypt the index query vector. Thus calculate the appropriate rating between encoded index and query vector.

Keyword: Vector Space Model, TF-IDF Model, Greedy Depth First Search, KNN Algorithm.

1. INTRODUCTION

Cloud computing has become a reality and organizations are uploading their information to cloud for having completely different services. Once information is outsourced, it should be subjected to thievery or any attack. Therefore the data owners' information's are speculated to write in code data before Outsourcing it. This approach will defend knowledge from attacks. However, the search operations become troublesome because the knowledge is write in code and stored. Therefore it's essential to own mechanism for having multi keyword graded search. The effective information retrieval wants the big quantity of document demand the cloud server to perform result relevance ranking rather than returning dedifferentiated results. such graded search system change information users to seek out the foremost relevant information quickly, instead of burdensomely sorting through each match within the content assortment to protect privacy of data and be in opposition to unwelcome accesses within the cloud and additional than it, vulnerable knowledge, for illustration, e-mails, personal health records, picture albums, documents, and so on, might need to be encrypted by data owners before Outsourcing to the cloud; however, obsoletes the traditional knowledge employment service supported plain text keyword investigate. The irrelevant way out of downloading all the information and decrypting domestically is clearly unreasonable, because of the massive amount of information bandwidth price in cloud scale systems. Moreover, apart from eliminating the native storage management, storing knowledge into the cloud. Hence, explore effective search service over encrypted cloud data is of vast consequence. Graded search also can stylishly get eliminate unneeded network traffic by sending back solely the bulk relevant knowledge. For privacy protection, such ranking operation, however, shouldn't leak any keyword related information. On the opposite hand, to enhance the search result accuracy furthermore on enhance the user searching expertise, it's conjointly necessary for such ranking system to support multiple keywords searches.

2. RELATED WORKS

Ning Cao, Cong Wang, Ming Li, KuiRen, Wenjing Lou [1] The innovation in cloud computing has Encouraged data owners to outsource their data managing system from native sites to profitable public cloud for excessive flexibility and profitable savings. But people like full advantage of cloud computing, if they are ready to report terribly real secrecy and security issues that go along with loading sensitive personal information. permitting an encrypted cloud data search facility is of nice significance. In view of the massive variety of Information users, documents within the cloud, it's necessary for the search facility to agree multi keywords query and organize for result comparison ranking to fulfill the particular want of information recovery search and not frequently distinguish the search results. related mechanisms on searchable encryption on single keyword search or Boolean keyword search, and often sort the search outcomes.

Zhihua Xia, XinhuiWang, Xingming Sun, Qian Wang [2] In this work, they present a secure multi-keyword ranked search scheme over encrypted cloud data that at the same time supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF×IDF model are combined within the index construction and query generation. They construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. The kNN algorithm is used to encode the index and query vectors, and meanwhile ensure accurate relevance score calculation between encoded index and query vectors. Due to the utilization of our special tree-based index structure, the proposed scheme is able to do sub-linear search time and influence the deletion and insertion of documents flexibly.

Zhangjie Fu, KuiRen, JiangangShu, Xingming Sun [3] This work, for the primary time, they study and solve the problem of personalized multi-keyword ranked search over encrypted data(PRSE) whereas conserving privacy in cloud computing. With the assistance of semantic ontology Word Net, they have a tendency to build a user interest model for individual user by analyzing the user's search history, and adopt a grading mechanism to specific user interest well, to deal with the constraints of the model of "one size fit all" and keyword precise search, they propose two PRSE schemes for various search intentions in depth experiments on real-world dataset validate our analysis and show that our proposed solution is incredibly efficient and effective.

Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, WeixinXie [4] Cipher text-policy attribute-based encryption (CPABE) has been a most popular encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared information files typically have the characteristic of multilevel hierarchy, notably within the area of health care and also the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. This work, for an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into single access structure, and then, the hierarchical files are encrypted with the integrated access Structure. The cipher text elements related with attributes can be shared by the files. Therefore, each cipher text storage and time value of encryption is saved. Moreover, the proposed scheme is proved to be secure under the quality assumption. Experimental simulation shows that the proposed scheme is efficient in terms of encryption and decryption. With the amount of the files increasing, the benefits of our scheme become more and more conspicuous.

Z. Fu, X. Sun, Z. Xia, L. Zhou and J. Shu [5] In this work planned an efficient methodology that solves the problem of synonym-based multi-keyword ranked search on cloud data, which is encrypted. They need worked on two facts: synonym-based search as well as similarity ranked search. The outcomes of finding may be accomplished when approved cloud clients input the equivalent words of the redefined keywords, not same or fuzzy matching keywords.

Table 1: Survey Table

SL.NO	PAPER / PUBLICATION	AUTHOR	METHODS
1	"Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Information Forensics and Security, January 2014.	Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen	Propose two MRSE schemes supported the similarity measure of "coordinate matching" to supply as several matches as attainable to effectively capture the relevance of outsourced documents to the query keywords while meeting totally different privacy needs. "Inner product similarity" is used to quantitatively evaluate similarity measure.
2	"A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, February 2016	Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang	Scheme supports dynamic update operations like deletion of documents and insertion of documents. Tree-based index structure and "Greedy Depth Fist Search" algorithms used to provide efficient multi-keyword graded Search.
3	"Enabling Fine-Grained Multi-Keyword Search Supporting Classified Sub- Dictionaries over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, May / June 2016	Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou	Relevance scores and preference factors of keywords use to allow precise keyword search and customized user expertise. Support sophisticated logic search by using the mixed "AND", "OR" and "NO" operations of keywords. Classified sub-dictionaries technique is employed to attain higher potency on index building, trapdoor generating and query.

4	An Efficient File Hierarchy Attribute Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information orensics and Security, June 2016	Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen	Uses Cipher text-policy attribute-based encryption (CP-ABE) encoded technology to slove the difficult drawback of secure data Sharing in cloud computing. Efficient file hierarchy attribute-based encrypted scheme is proposed in cloud computing
5	"Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing," 2013 IEEE 32nd (IPCCC), San Diego, CA, 2013, pp. 1-8.	Z. Fu, X. Sun, Z. Xia, L. Zhou and J. Shu	They have worked on two facts: synonym-based search furthermore as similarity ranked Search. The outcomes of finding may be accomplished when approved cloud clients input the equivalent words. of the predefined keywords, not same or fuzzy matching keywords

3. SYSTEM ARCHITECTURE

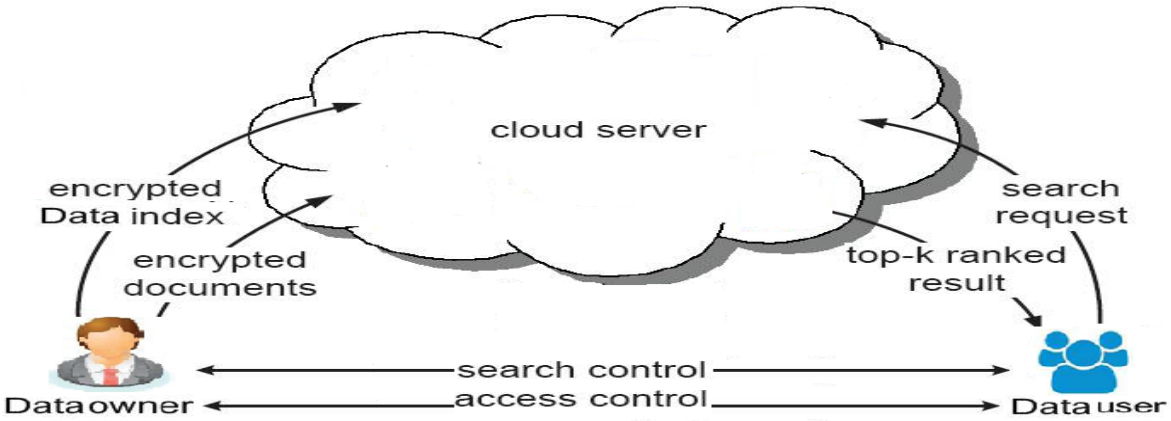

Figure 1: System Architecture

4. METHODOLOGY

MODULES

- **Data User Module :** This module contains the user registration login details.
- **Data Owner Module :** This module helps the data owner to register them details and additionally include login details also.
- **File Upload Module:** This module helps the owner to upload his file with encoded using some algorithm. This ensures the files to be shielded from unauthorized users.
- **Encryption**
  - Rank Search Module: Rank Search Module module ensures the user to search the files that are searched frequently using rank search.
  - File Download Module: File Download Module module allows the user to download the file using his secret key to decrypt the downloaded data.
- **Decryption**
  - View Uploaded and Downloaded File: These module permit the owner to view the uploaded files as well as downloaded files.

5. CONCLUSION

Data protection and privacy is one the most important contests in cloud computing. These searching strategies are helpful for the searching of specific information over encrypted records in cloud. This survey summarized some recent searching and ranking techniques. These searching techniques area unit helpful for the searching of explicit information over encoded information in cloud and ranking strategies area unit used for build the ranking of search results.

6. REFERENCES

[1] Ning Cao, Cong Wang, Ming Li, KuiRen, Wenjing Lou, "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, January 2014.

[2] Zhihua Xia, XinhuiWang, Xingming Sun, Qian Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems, Vol. 27, No. 2, February 2016.

[3] Zhangjie Fu, KuiRen, JiangangShu, Xingming Sun, Fengxiao Huang, "Enabling Personalized Search Over Encrypted Outsourced Data With Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, Vol. 27, No. 9, September 2016.

[4] Shulan Wang, Junwei Zhou, Joseph K. Liu, Jianping Yu, Jianyong Chen, WeixinXie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 11, No. 6, June 2016.

[5] Z. Fu, X. Sun, Z. Xia, L. Zhou and J. Shu, "Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing," 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC), San Diego, CA, 2013, pp. 1-8.

[6] N. S. Khan, C. R. Krishna and A. Khurana, "Secure ranked fuzzy multi-keyword search over outsourced encrypted cloud data," Computer and Communication Technology (ICCCT), 2014 International Conference on, Allahabad, 2014, pp. 241-249.

[7]. C. Wang, N. Cao, J. Li, K. Ren, and W. J. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," in Proc. of IEEE 30th International Conference on Distributed Computing Systems 2010, pp. 253-262.

[8] M. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," In Proc.of NDSS'12, 2012.

[9]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. j. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. of IEEE INFOCOM'10 Mini-Conference, San Diego, CA, USA, March 2010.

[10]. C. Liu, L. H. Zhu, L. Li, and Y. Tan, "Fuzzy Keyword Search on Encrypted Cloud Storage Data with Small Index," in Proc. of IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), 2011, pp. 269-273.

[11] C. Wang, K. Ren, S. C. Yu, and K. M. R. Urs, "Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data," in Proc. of IEEE INFOCOM 2012, 2012, pp. 451-459.

[12] N. Cao, C. Wang, M. Li, K. Ren. W. J. Lou, "Privacy- Preserving Multi-keyword Ranked Search over Encrypted Cloud Data," in Proc. of IEEE INFOCOM 2011, 2011, pp. 829-837.