International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January2017

A Review on Secure And Dynamic Multi Keyword Ranked Search Scheme Over Encrypted Cloud Data

[1]D. Subhadra & [2]Mrs.K.Harika

[1]M.Tech(CSE) from JAGRUTI INSTITUTE OF ENGINEERING AND TECHNOLOGY
[2] Assistant Professor, Department of Computer Science and Engineering, JAGRUTI INSTITUTE OF ENGINEERING AND TECHNOLOGY, Telangana State, India.

ABSTRACT
Present days growing popularity of cloud computing, the data owners are outsource their data to cloud servers for prominent convenience and reduced cost in facts control. However, sensitive information need to be encrypted before outsourcing for privacy requirements, which obsoletes statistics usage like key-word-primarily based record retrieval. In this paper we resolve the trouble of multi-keyword ranked search over encrypted cloud data (MRSE) which simultaneously supports dynamic update operations like deletion and insertion of files sensible information inside the cloud computing concept. As an end result, allowing an encrypted cloud. In view of the huge variety of information customers and files within the cloud, it's far vital to allow several key phrases inside the seek call for and go back files inside the order in their applicable to these key phrases. comparable mechanism on searchable encryption makes centre on unmarried key-word seek or Boolean keyword search, and infrequently type the quest effects. within the middle of numerous multi-key-word semantics, determining the properly-prepared similarity measure of "coordinate matching," it way that as many fits as feasible, to seize the suitable data documents to the hunt query. in particular, we recall "internal product similarity" and additionally we construct tree-based totally index shape, every file is hooked up with a binary vector as a sub index where each bit symbolize whether matching keyword is contained within the file. The Ranked result presents pinnacle ok retrieval results. Additionally we advise an alert machine which will generate alerts whilst un-legal user attempts to get right of entry to the information from cloud, the alert will generate inside the shape of mail and message. And the ElGamal Cryptosystem allow customers to occupy inside the rating whilst the recognition of computing work is completed on the server facet via method handiest on cipher textual content which leads information leakage and statistics safety is confident.

Keywords— Dynamic multi keyword ranked search, inner product similarity, ElGamal Cryptosystem, top k retrieval

1 .INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. . Cloud Computing means a remote server that access through the internet which helps in business applications and functionality along with the usage of computer software. Cloud computing saves money that users spend on annual or monthly subscription. Due to advantage of cloud services, more and more sensitive information are being centralized into the cloud servers, such as emails, personal health records, private videos and photos, company finance data, government documents, etc. To shield data privacy, exclusive records has to be encrypted before outsourcing, with a purpose to provide end-to-end facts confidentiality assurance in the cloud. statistics encryption makes effective records usage a completely tough mission given that there can be a huge quantity of outsourced information documents. except, in Cloud Computing, data owners can also percentage their outsourced records with a huge wide variety of customers, who would possibly want to simplest retrieve certain unique information documents they may be interested in throughout a given consultation. one of the most popular approaches to achieve this is through keyword-based search. This keyword seek approach allows customers to selectively retrieve files of interest and has been widely carried out in plaintext search eventualities. sadly, records encryption, which restricts user's capability to perform keyword seek and in addition demands the protection of key-word privateness, makes the conventional plaintext search strategies fail for encrypted cloud data. Ranked search substantially improves device usability via regular matching files in a ranked order concerning to positive relevance criteria (e.g., key-word frequency).

2. BACKGROUND AND RELATED WORK:

Now a day's cloud computing has become essential for many utilities, where cloud customers can slightly store their data into the cloud so as to benefit from on-demand high-quality request and services from a shared pool of configurable computing resources. Its huge suppleness and financial savings are attracting both persons and enterprise to outsource their local complex data management system into the cloud. To safe guard data privacy and struggle unwanted accesses in the cloud and away from, sensitive data, for example, emails, personal health records, photo albums, videos, land documents, financial transactions, and so on, may have to be encrypted by data holder before outsourcing to the business public cloud; on the other hand, obsoletes the

traditional data use service based on plaintext keyword search. The insignificant solution of downloading all the information and decrypting nearby is clearly impossible, due to the enormous amount of bandwidth cost in cloud scale systems. Furthermore, apart from eradicating the local storage management, storing data into the cloud provisions no purpose except they can be simply searched and operated. Thus, discovering privacy preserving and effective search service over encrypted cloud data is one of the ultimate implication. In view of the potentially large number of on-demand data users and vast amount of outsourced data documents in the cloud, this difficulty is mostly demanding as it is really difficult to gather the requirements of performance, system usability, and scalability.

On the one hand, to congregate the efficient data retrieval requirement, the huge amount of documents orders the cloud server to achieve result relevance ranking, as an alternative of returning undifferentiated results. Such ranked search system allows data users to discover the most appropriate information quickly, rather than burdensomely sorting during every match in the content group. Ranked search can also gracefully remove redundant network traffic by transferring the most relevant data, which is highly attractive in the "pay-as-you-use" cloud concept. For privacy protection, such ranking operation on the other hand, should not reveal any keyword to related information. To get better the search result exactness as well as to improve the user searching experience, it is also essential for such ranking system to support multiple keywords search, as single keyword search often give up far too common results. As a regular practice specifies by today's web search engines i,e Google search, data users may lean to offer a set of keywords as an alternative of only one as the indicator of their search interest to retrieve the most relevant data. And each keyword in the search demand is able to help narrow down the search result further. "Coordinate matching", as many matches as possible, is an efficient resemblance measure among such multi-keyword semantics to refine the result significance, and has been widely used in the plaintext information retrieval (IR) community. Though, the nature of applying encrypted cloud data search system remains a very demanding task in providing security and maintaining privacy, like the data privacy, the index privacy, the keyword privacy, and many others. Encryption is a helpful method that treats encrypted data as documents and allows a user to securely search through a single keyword and get back documents of interest. On the other hand, direct application of these approaches to the secure large scale cloud data utilization system would not be necessarily suitable, as they are developed as crypto primitives and cannot put up such high service-level needs like system usability, user searching experience, and easy information discovery. Even though some modern plans have been proposed to carry Boolean keyword search as an effort to improve the search flexibility, they are still not sufficient to provide users with satisfactory result ranking functionality. The solution for this problem is to secure ranked search over encrypted data but only for queries consisting of a single keyword. The challenging issue here is how to propose an efficient encrypted data search method that supports multi-keyword semantics without privacy violation. In this paper, we describe and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving exact system wise privacy in the cloud computing concept. Along with various multi-keyword semantics, select the efficient resemblance measure of "coordinate matching," it means that as various matches as possible, to confine the significance of data documents to the search query. Particularly, inner product similarity the numbers of query keywords show in a document, to quantitatively calculate such similarity assess of that document to the search query. For the period of the index construction, each document is associated with a binary vector as a sub-index where each bit signifies whether matching keyword is contained in the document. The search query is also illustrates as a binary vector where each bit means whether corresponding keyword appears in this search request, so the resemblance could be exactly calculated by the inner product of the query vector with the data vector. On the other hand, directly outsourcing the data vector or the query vector will go against the index privacy or the search privacy. To face the challenge of cooperating such multi keyword semantic without privacy breaches, we propose a basic idea for the MRSE using secure inner product computation, which is modified from a secure k-nearest neighbour (kNN) method, and then give two considerably improved MRSE method in a step-by-step way to accomplish different severe privacy needs in two risk models with enlarged attack competence.

3. SYSTEM STUDY

3.1 Presented System:

Existing searchable encryption schemes allow a user to securely search over encrypted data through keywords without first decrypting it, these techniques support only conventional Boolean keyword search, without capturing any relevance of the files in the search result. When directly applied in large collaborative data outsourcing cloud environment, they go through following disadvantage.

Drawbacks of existing system

1. Single-keyword search without ranking
2. Boolean- keyword search without ranking
3. Single-keyword search with ranking
4. Do not get relevant data.

3.2 Proposed system

As our proposed system we choose the principle of coordinate matching, to identify the similarity between search query and data documents. Specially, we use inner data correspondence, i.e., the number of query keywords appearing in a document, to evaluate the similarity of that document to the search query in coordinate matching

principle. Each document is linked with a binary vector as a sub-index where each bit represents whether corresponding keyword is contained in the document.[1] the hunt question is also described as a binary vector wherein every bit approach whether or not corresponding keyword appears on this seek request, so the similarity may be precisely measured by internal manufactured from question vector with information vector. however, directly outsourcing statistics vector or query vector will violate index privateness or seek privacy. to satisfy the undertaking of assisting such multi-key-word semantic with out privacy breaches, we suggest a simple SMS scheme the usage of relaxed inner product computation, which is tailored from a comfortable okay-nearest neighbour (kNN) approach, after which enhance it grade by grade to achieve numerous privacy requirements in ranges of chance fashions.

1) Showing the problem of Secured Multi-keyword search over encrypted cloud data

2) Propose two schemes following the principle of coordinate matching and inner product similarity.

And we proposed alert system which will generate alerts when un-authorized user tries to access the data from cloud, the alert will generate in the form of mail and message. and the DES encryption allow users to occupy in the ranking while the popularity of computing work is done on the server side by process only on cipher text which leads data leakage and data security is assured.

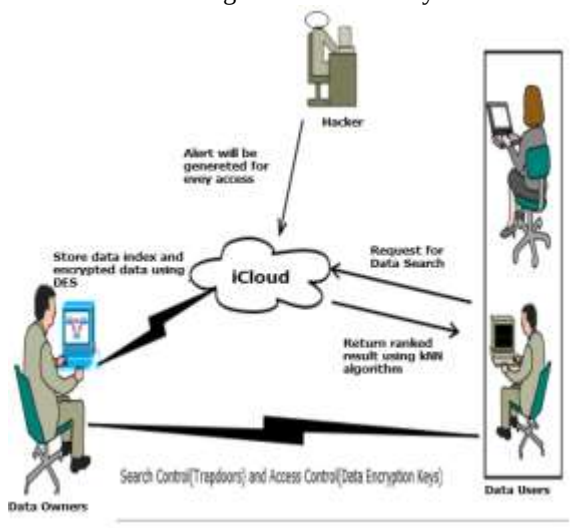
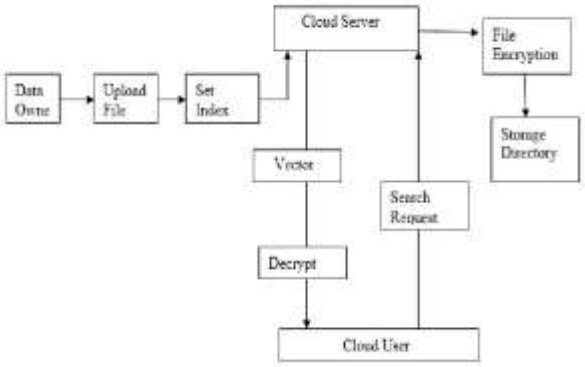


Fig1. System Architecture for search over encrypted cloud data

Considering three different entities, as illustrated in Fig1. Data owner, data user, and cloud server. Data owner has a collection of data documents to be send to cloud server in the encrypted format. To activate the searching capability over encrypted data, data owner, before sending data, will first build an encrypted searchable manifestation (index), and then outsource both the index and the encrypted document collection to cloud server. To search the document, an authorized user require a corresponding trapdoor through search mechanisms, Upon receiving from data users, cloud server is responsible to search the index and return the corresponding set of encrypted documents. To improve document retrieval accuracy, search result should be ranked by cloud server according to some ranking criteria. Cloud server only sends back top-k documents that are most relevant to the search query. In Fig1.There is one another entity is shown i.e. Unauthorized User(Hacker). If that Unauthorized user tries to access any data from clod then alert will be generated in the form of mail and message. The alert is given to the authorized person who is owner of that data.

4. SYSTEM IMPLEMENTATION.



.

Fig.2 Architecture diagram of the MRSE Implementation.

In this technique the following are the different things which we have to implement

i) Cloud Setup

ii) Cryptography cloud Storage

iii)Vector Model

Cloud Setup

Firstly, we have to setup data owner and cloud server. So the data owner will then push the data into the cloud servers. When users outsource their confidential data onto the cloud, the cloud service providers are capable to control and check the data and the communication between users and the cloud will be secured.

Cryptography cloud Storage

Secondly, while the data is uploaded into the iCloud and retrieve services. Since data may have confidential information, the cloud servers cannot be fully hand over in protecting data. For this cause, outsourced files must be encrypted. Any kind of information leakage that would change data privacy is regarded as Unacceptable.

Vector Model

We used a series of searchable symmetric encryption systems that have been allowing search on cipher text. In the earlier, files are ranked only by the number of get back keywords, which damage search correctness.

5. DESIGN GOALS AND SYSTEM FEATURES

1. Encryption Module This module is used to help the server to encrypt the document using DES Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download.

2. Multi-keyword Module This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list.

3. File upload Module This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart. The admin can upload the file after the conversion of the Zip file format.

5.1 System Features

To activate ranked search for effective utilization of outsourced cloud data, our system design should simultaneously achieve security and performance guarantees as follows.

1. Secured Multi-keyword Ranked Search: To design search schemes which allow multi-keyword query and provide result similarity ranking for valuable data retrieval, instead of returning undifferentiated results.

2. Privacy: To prevent cloud server from learning additional information from dataset and index, and to meet privacy requirements.

3. Effectiveness with high performance: Above goals on functionality and privacy should be achieved with low communication and computation overhead.

6. CONCLUSION

Thus we proposed the problem of multiple-keyword ranked search over encrypted cloud data, and construct a variety of security requirements. From various multikeyword concepts, we choose the efficient principle of coordinate matching. We first propose secure inner data computation. Also we achieve effective ranking result using k-nearest neighbour technique.

References

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, Apr, 2011.

[2] 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, 2009.

[3] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan. 2010.

[5] A. Singhal, "Modern Information Retrieval: A Brief Overview," IEEE Data Eng. Bull., vol. 24, no. 4, pp. 35-43, Mar. 2001.

[6] I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.

[7] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.

[8] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216. 2003.

[9] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[10] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.

[11] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2004.

[12] M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and Efficiently Searchable Encryption," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '07), 2007.

[13] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable Encryption Revisited: Consistency Properties, sRelation to Anonymous Ibe, and Extensions," J. Cryptology, vol. 21, no. 3, pp. 350-391, 2008.