IJARES/June 2015/Volume-3/Issue-6/1906-1910 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

OUTSOURCING OF DATA IN CLOUD SYSTEM FOR FLEXIBILITY MANAGEMENT

P.Yeshwanth Kumar[1], G.V.Koti Reddy[2]

[1]**M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India**

[2]**Assistant Professor, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India**

ABSTRACT:

Complexity of preserving privacy in multi-keyword ranked search on encrypted data within cloud computing was solved for the first time, while protecting strict system wise privacy in cloud computing concept. In our work we work out complicatedness of preserving privacy in multi-keyword ranked search on encrypted data within cloud computing. We put forward to utilize inner product similarity to achieve multi-keyword ranked search, to quantitatively assess well-organized similarity measure coordinate matching. Due to inherent security as well as privacy obstacles application of coordinate matching in encrypted system of cloud data remains an extremely challenging mission. To improve the result relevance coordinate matching is a well-organized similarity measure between multi-keyword semantics, and has been extensively used in plaintext information retrieval. We suggest two multi-keyword ranked search schemes on basis of similarity measure of coordinate matching while gathering different privacy needs in two different threat representations such as Privacy-Preserving Scheme in recognized Cipher text representation and the other is privacy-preserving system in recognized Background representation.

Keywords: Multi-keyword, Cipher text, Privacy, Coordinate matching, Information retrieval, Cloud computing.

1. INTRODUCTION:

Cloud computing provides improved flexibility and economic savings for outsourcing their confined complex data management. Exploration of effective search service on encrypted data is of main importance [1]. For fulfilling retrieval need of essential information, the huge amount of documents require cloud server to carry out result relevance ranking, rather than returning undifferentiated results. These ranked search system facilitates data users to discover most appropriate information rapidly, to a certain extent than burdensomely sorting through each match in collecting content. For protecting privacy, it however, should not escape any keyword connected information. To get better search result accurateness and to enhancing user searching practice, it is essential for ranking system to maintain several keywords search, whereas single keyword search yields extreme coarse results. In literature, searchable encryption is a cooperative method that treats encrypted data as documents and permits a user to steadily search throughout a single keyword and recover documents of interest. Correlated works on searchable encryption spotlight above single keyword search, and not often sort search results [2]. In our work we solve the difficulty of preserving privacy in multi-keyword ranked search on encrypted data within cloud computing.

2. OVERVIEW OF PROPOSED SYSTEM MODEL:

Scheming of an efficient encrypted data search method supporting multi-keyword semantics devoid of privacy violations still remains a demanding problem. For the first time, the difficulty of preserving privacy in multi-keyword ranked search on encrypted data within cloud computing was solved while protecting strict system wise privacy in cloud computing concept. Between varieties of multi-keyword semantics, we prefer well-organized similarity measure of coordinate matching, to confine importance of data documents to search query. A cloud data hosting service was considered in fig1 including different entities, such as data owner, user, as well as cloud server. The data owner includes data documents that are to be outsourced towards cloud server in encrypted form. To facilitate searching capability over encrypted form for effectual data utilization, data owner, earlier than outsourcing, will build an encrypted searchable index room data documents, and

subsequently outsource index and encrypted document collection on the way to cloud server. To explore document collection for specified keywords, an approved user obtains analogous Trap door all the way through search control methods. Upon receiving Trap door from a data user, cloud server is accountable to look for index and return equivalent set of encrypted documents. To recover document retrieval accurateness, search result has to be ranked by cloud server consistent with a number of ranking criteria [3][4]. To decrease communication cost, the data user might send an optional number all along with the trapdoor so that cloud server sends reverse top-k documents that are appropriate towards search query. Mechanism of access control is utilized to supervise decryption capabilities specified to users and data collection is updated in terms of inserting novel documents, updating traditional documents, and erasing existing documents.

3. EXPOSURE TOWARDS RESOURCEFUL MULTI-KEYWORD RANKED SEARCH:

To attain multi-keyword ranked search, we put forward to utilize inner product similarity to quantitatively assess well-organized similarity measure coordinate matching. Coordinate matching is a well-organized similarity measure between multi-keyword semantics to improve the result relevance, and has been extensively used in plaintext information retrieval. Application of coordinate matching in encrypted system of cloud data remains an extremely challenging mission due to inherent security as well as privacy obstacles. Usage of inner product similarity specifically number of query keywords coming out in a document, to evaluate similarity measure of document to search query. During index construction, each document is linked by means of a binary vector as a sub index where every bit represents whether corresponding keyword is enclosed in document. The search query is moreover described as a binary vector where every bit means whether equivalent keyword emerges in this search request, hence similarity might be precisely measured by inner product of query vector by means of data vector [5]. Directly outsourcing data vector will go against index privacy. We put forward two multi-keyword ranked search schemes on basis of similarity measure of coordinate matching while gathering different privacy needs in two different threat representations such as Privacy-

Preserving Scheme in recognized Cipher text representation and the other is privacy-preserving system in recognized Background representation. In privacy-preserving scheme in recognized cipher text representation rather than removing absolute dimension in query vector since we plan to do at initial glance, we save this dimension extending procedure however allocate a novel random number towards the complete dimension in every query vector and such a recently added randomness is likely to augment the complexity for cloud server to become skilled at relationship between arriving trapdoors. As revealed in keyword privacy necessity, randomness has to be carefully calibrated in search result to conceal document frequency and weaken chances for re-identification of keywords. Introduction of some randomness in concluding similarity score is an effectual way toward what we imagine. Unlike randomness concerned in query vector, we introduce dummy keyword into every data vector and allocate a random value to it. In preserving of privacy in recognized background representation when cloud server has information of some background information on outsourced data set, correlation association of two specified trapdoors, assured keyword privacy are assured by this scheme since cloud server can utilize scale analysis to assume keyword particular information [6].

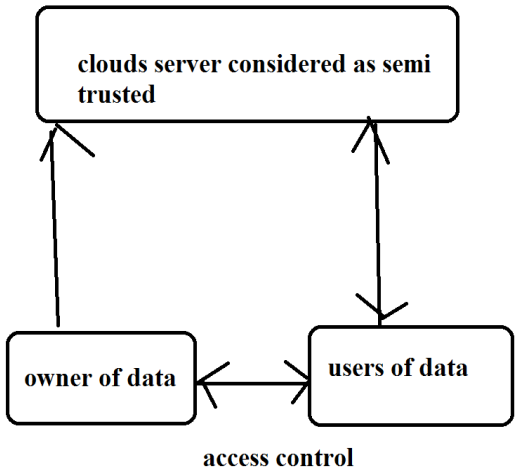

Fig1: overview of search above encrypted cloud data.

4. CONCLUSION:

The huge amount of documents require cloud server to carry out result relevance ranking, rather than returning undifferentiated results for fulfilling retrieval need of essential information. Designing of a competent encrypted data search method supporting multi-keyword semantics devoid of privacy violations still remains a demanding problem. In our work we resolve intricacy of preserving privacy in multi-keyword ranked search on encrypted data within cloud computing. We choose well-organized similarity measure of coordinate matching, between varieties of

multi-keyword semantics, to confine importance of data documents to search query. We put forward to utilize inner product similarity to quantitatively assess well-organized similarity measure coordinate matching to achieve multi-keyword ranked search. Between multi-keyword semantics coordinate matching is a well-organized similarity measure to improve the result relevance, and has been extensively used in plaintext information retrieval. As a result of inherent security as well as privacy obstacles application of coordinate matching in encrypted system of cloud data remains an extremely challenging mission. We propose two multi-keyword ranked search schemes on basis of similarity measure of coordinate matching while gathering different privacy needs in two different threat representations such as Privacy-Preserving Scheme in recognized Cipher text representation and the other is privacy-preserving system in recognized Background representation. Practice of inner product similarity specifically number of query keywords coming out in a document, to evaluate similarity measure of document to search query.

REFERENCES

[1] J. Katz, A. Sahai, and B. Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products," Proc. 27th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2008.

[2] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption," Proc. 29th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '10), 2010.

[3] E. Shen, E. Shi, and B. Waters, "Predicate Privacy in Encryption Systems," Proc. Sixth Theory of Cryptography Conf. Theory of Cryptography (TCC), 2009.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, 2010.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, 2010.

[6] S. Zerr, E. Demidova, D. Olmedilla, W. Nejdl, M. Winslett, and S. Mitra, "Zerber: r-Confidential Indexing for Distributed Documents," Proc. 11th Int'l Conf. Extending Database Technology (EDBT '08), pp. 287-298, 2008.