ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced Synonym Queries Supported Encrypted Cloud Multi-keyword Ranked Search System

K.Meghana
P.G. Scholar,
Dept. of CSE,
Modugula Kalavathamma Institute of Technology for Women, Rajampet,
Kadapa District.

T.Mallika Devi
Assistant Professor,
Dept. of CSE,
Modugula Kalavathamma Institute of Technology for Women, Rajampet,
Kadapa District.

Abstract:

As an enhancement we enhance the existing system and in this paper we propose an effective approach to solve the problem of multi-keyword ranked search over encrypted cloud data supporting synonym queries. The main contribution of this paper is summarized in two aspects: multi-keyword ranked search to achieve more accurate search results and synonym-based search to support synonym queries. Meanwhile, existing search approaches over encrypted cloud data support only exact or fuzzy keyword search, but not semantics-based multi-keyword ranked search. Therefore, how to enable an effective searchable system with support of ranked search remains a very challenging problem.

INTRODUCTION

Circulated processing is a field of software engineering that studies dispersed frameworks. A disseminated framework is a product framework in which segments situated on arranged PCs convey and facilitate their activities by passing messages. The parts cooperate with one another keeping in mind the end goal to accomplish a typical objective. There are numerous options for the message passing system, including RPC-like connectors and message lines. Three huge qua lities of conveyed frameworks are: simulta neousness of segments, absence of a worldwide clock, and free disappointment of segments. An imperative objective and test of conveyed frameworks is area straightforwardness. Cases of conveyed frameworks shift from SOA-based frameworks to hugely multiplayer web amuse ments to distributed applications. A PC program that keeps running in an appropriated framework is known as a disseminated program, and conveyed writing computer programs is the procedure of composing such projects. Conveyed figuring likewise alludes to the utilization of appropriated frameworks to tackle computational issues. In appropriated figuring, an issue is isolated into numerous errands, each of which is settled by one or more PCs, which speak with one another by message passing. The word circulated in wording, for example, "conveyed framework", "dispersed programming", and "disseminated calculation" initially alluded to PC systems where singular PCs were physically appropriated inside of some land region. The terms are these days utilized as a part of a much more extensive sense, notwithstanding alluding to self-ruling procedures that keep running on the same physical PC and collaborate with one another by message passing. While there is no single meaning of a conveyed framework, the accompanying characterizing properties are normally utilized:

Considering potentially huge number of on-demand data users and large amount of outsourced data documents in the cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements of performance, system usability, and scalability. Document ranking is provided for fast search, but the priorities of all the data documents is kept same so

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

that the cloud service provider and third party remains unaware of the important documents, thus, maintaining privacy of data. Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the "pay-as-you-use" cloud paradigm. For privacy protection, such ranking operation, however, should not leak any keyword related information. Besides, to improve search result accuracy as well as to enhance the user searching experience, it is also necessary for such ranking system to support multiple keyword search, as single keyword search often yields far too coarse results. As a common practice indicated by today's web search engines (ex. Google search), data users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. Along with the privacy of data and efficient searching schemes, real privacy is obtained only if the user's identity remains hidden from the Cloud Service Provider (CSP) as well as the third party user on the cloud server.

II. RELATED WORK

Organizations, companies store more and more valuable information is on cloud to protect their data from virus, hacking. The benefits of the new computing model include but are not limited to: relief of the trouble for storage administration, data access, and avoidance of high expenditure on hardware mechanism, software, etc. Ranked search improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency),As directly outsourcing relevance scores will drips a lot of sensitive information against the keyword privacy, We proposed asymmetric encryption with ranking result of queried data which will give only expected data.

A. Secured Multi-keyword Ranked Search over Encrypted Cloud Data

In cloud computing data possessor are goaded to farm out their complex data management systems from local sites to the commercial public cloud for greater flexibility and economic savings. To ensure safety of stored data, it is must to encrypt the data before storing. It is necessary to invoke search with the encrypted data also. The specialty of cloud data storage should allow copious keywords in a solitary query and result the data documents in the relevance order. In, main aim is to find the solution of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise privacy in the cloud computing paradigm. A variety of multi- keyword semantics are available, an efficient similarity measure of "coordinate matching" (as many matches as possible), to capture the data documents' relevancy to the search query is used. Specifically "inner product similarity", i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query is used in MRSE algorithm. The main limitation of this paper was, the user's identity (ID) is not kept hidden. Due to this, whoever puts the data on Cloud Service Provider was known. This may be risky in some situations where confidentiality of data needs to be maintained. Hence, this drawback is overcome in the proposed system.

B. Privacy Preserving Keyword Searches on Remote Encrypted Data

Consider the problem: a user U wants to store his files in an encrypted form on a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing specific keywords, keeping the keywords themselves secret and not to endanger the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In, solutions for this problem under well-defined security requirements are offered. The schemes are efficient as no public-key cryptosystem is involved. Indeed, the approach is independent of the encryption method chosen for the remote files.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

They are incremental too. In that, user U can submit new files which are secure against previous queries but still searchable against future queries. From this, the main theme taken is of storing data remotely on other server and retrieving that data from anywhere via mobile, laptop etc.

III. PROBLEM FORMULATION

A. Proposed System

In this paper, for the first time, we define and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system wise privacy in the cloud computing paradigm. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. Specifically, we use "inner product similarity", i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query. During the index construction, each document is associated with a binary vector as a sub-index where each bit represents whether corresponding keyword is contained in the document. The search query is also described as a binary vector where each bit means whether corresponding keyword appears in this search request, so the similarity could be exactly measured by the inner product of the query vector with the data vector. However, directly outsourcing the data vector or the query vector will violate the index privacy or the search privacy. To meet the challenge of supporting such multi keyword semantic without privacy breaches, we propose a basic idea for the MRSE using secure inner product computation, which is adapted from a secure k-nearest neighbor (kNN) technique, and then give two significantly improved MRSE schemes in a step-by-step manner to achieve various stringent privacy requirements as shown in Fig.1.

Advantages of Proposed System:

- Search result should be ranked by the cloud server according to some ranking criteria.
- To reduce the communication cost.

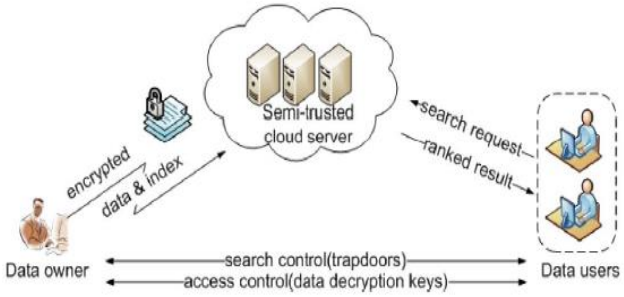

Fig.1. System Architecture.

The following modules are implemented in this technique

- Cloud Setup
- Cryptography cloud Storage
- Vector Model

Cloud Setup: In this module we have setup data owner and cloud server. So the data owner is going push the data into the cloud sever. When users outsource their private data onto the cloud, the cloud service providers are able to control and monitor the data and the communication between users and the cloud will be secured.

Cryptography Cloud Storage: In this module while the data is uploaded into the storage and retrieve services. Since data may contain sensitive information, the cloud servers cannot be fully entrusted in protecting data. For this reason, outsourced files must be encrypted. Any kind of information leakage that would affect data privacy are regarded as unacceptable.

Vector Model: In this model we used a series of searchable symmetric encryption schemes have been enable search on cipher text. In the former, files are ranked only by the number of retrieved keywords, which impairs search accuracy.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

IV. RESULTS

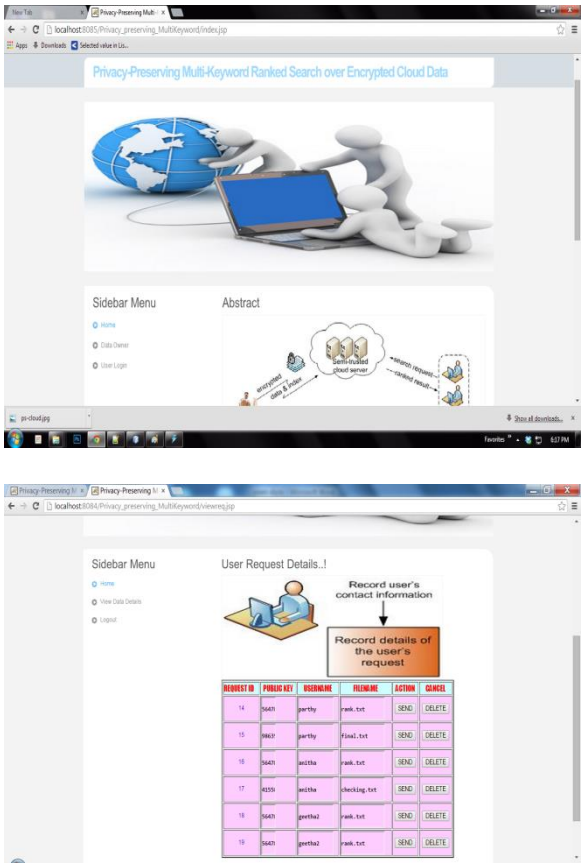

Fig 3 User Request Details Page

V. CONCLUSION

In this paper, interestingly we characterize and take care of the issue of multi-decisive word positioned seek over encoded cloud information, and set up an assortment of security necessities. Among different multi-essential word semantics, we pick the proficient comparability measure of "direction coordinating," i.e., however many mat ches as could be expected under the circum stances, to successfully catch the pertinence of outsourced archives to the inquiry catchphrases, and utilization "inward item similitude" to quantitatively assess such closeness measure. For meeting the test of supporting multi-decisive word semantic without protection ruptures, we propose an essential thought of MRSE utilizing secure inward item calculation. At that point, we give two enhanced MRSE plans to accomplish different stringent protection prerequisites in two distinctive danger models.We additionally explore some further improvements of our positioned look system, including supporting more hunt sema ntics, i.e.,TF_IDF, and element information operations. Careful examination exploring security and productivity assurances of proposed plans is given, and tests on this present reality information set demonstrate our proposed plans present low overhead on both calculation and correspondence. In our future work, we will investigate checking the rank's honesty request in the query output expecting the cloud server is untrusted.

VI. REFERENCES

[1] Ning Cao, Member, IEEE, Cong Wang, Member, IEEE, Ming Li, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Enhanced Synonym Queries Supported Encrypted Cloud Multi-Keyword Ranked Search System", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, January 2014.

[2] 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.

[3] 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.

[4] 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.

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

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

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.
[9] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216. 2003.
[10] 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.