ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (195-198), Month: April - June 2015, Available at: www.researchpublish.com

Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

[1]Pradeep Kumar Vishwakarma, [2]Mritunjay Kumar Chubey, [3]Kerana Henrix D

[1, 2] Dept. of C.S.E., Bharath University, Chennai, Tamil Nadu, INDIA.
[3] Associate Professor, Dept. of C.S.E., Bharath University, Chennai – 600073. INDIA.

Abstract: **With the advent of cloud computing, data authorisers are motivated to outsource their management systems of complex data from local sites to commercial public cloud for higher reliability and economic savings. To secure data privacy, sensitive data has to be encrypted or encoded before outsourcing, which is less in used traditional data utilization based on without coded text keyword search. Thus, to enable encrypted cloud data search service is of predominant importance. Considering the high number of data users and documents in cloud, it is essential for the search service to allow multi-keyword query and provide output similarity ranking to meet the effective data receiving is needed. In search for the encryption focusing on single keyword search or Boolean keyword search initially and then rarely differentiate the search results. In this paper, we define and solve the most intriguing problem of security-preserving multi-keyword ranked search over encrypted cloud data and establish a set of complicated privacy requirements to secure data utilization system to become a reality. Among multiple multi-keyword semantics, we choose the best principle according to "coordinate matching", i.e., to capture the analogy between search query and data files, and after this use "inner product analogy" to quantitatively formalize such principle for analogical measurement. We first introduce a basic MRSE scheme using a secure inner product computational formation, and then specifically improve it to meet various privacy requirements in two levels determining the threat models. Thorough analysis of investigating privacy and efficiency guarantees of introduced schemes is given, and experiments performed on the real-world data collections further show introduced schemes indeed mainly to introduce low overhead on computation and communication purpose.**

Keywords: **Privacy Multi-Keyword Ranked, Encrypted Cloud Data.**

I. INTRODUCTION

Cloud Computing is the one of the hot topic buzzing around us and seen as best computing as a utility, where cloud customers can remotely and securely store and process their data into the cloud with great maintenance so as to enjoy the on demand high quality reliable applications and services from a shared pool of ongoing configurable computing resources [1]. Its great flexibility and robust economic savings are motivating all the sector including individuals and enterprises to outsource their local complex data management system on the larger scale into the cloud, especially when the produced data by them that need to be stored for process and utilization is rapidly increasing. Due to today's threat to privacy has increased the concern to protect data privacy and combat unsolicited accesses in cloud and beyond which is a great threat to sensitive data like emails personal health records, tax related documents, transaction, photo albums, etc. may have to be encrypted by data owners before outsourcing to commercial public cloud [2]; but this however is obsoletes type of the traditional data utilization service based on plain text keyword search. The problem exists with the solution of downloading all the data and decrypting locally is very much difficult as it requires huge amount of bandwidth cost in cloud systems. Moreover, apart from eliminating the local storage management, holding data into the cloud serves no purpose unless they can be easily searched and utilized. Thus, to explore privacy-preserving and effective search service over encrypted cloud data it is required on a great importance. Considering the potentially large number of on demand high data users and huge amount of traffic which is being outsourced in cloud, this problem is particularly challenging as it is very much difficult to meet also the requirements of performance, system scalability and usability.

On the one hand, to meet the effective data requirement need, large amount of documents demand cloud server to perform result on relevance ranking, instead of returning the whole undifferentiated result. Such types of ranked search system enables data users to find the most relevant information quickly, rather than sorting on burdensomely through every match in the content collection [3]. On the ground of ranked search it can also elegantly eliminate unnecessary network traffic by sending back only the most required relevant data, which is highly desirable in the "pay-as-you-use" cloud paradigm. For the concern of privacy protection, it should be taken utmost care of not leaking any keyword related information during ranking operation. Apart from this, to improve search result accuracy as well as to enhance user searching experience, it is also very important for such ranking system to support multiple keywords search, because single keyword search often yields far too coarse and unwanted result.

In this paper, we define and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving the strict system-wise privacy in cloud computing paradigm. However Among various multi-keyword semantics, we have chosen the efficient principle of "coordinate matching", i.e., as many matches as possible, to hold and capture the similarity between search query and data documents. Specifically, we have used "inner product similarity" [4] define the no of query keywords which is appearing in a document to evaluate quantitatively the similarity of that document to the search query in coordinate matching principle. Also each documents associated with a binary vector on the basis of a sub-index where each bit represents whether corresponding keyword is contained in the document during index construction. However, directly outsourcing data vector or query vector will directly violates index privacy or search privacy. In order to meet the challenge of supporting such multi keyword semantic without privacy breaches, we have proposed a basic MRSE scheme which uses secure inner product computation adapted from a secure k-nearest neighbour (kNN) technique [4], and then to improve it step by step to achieve required various privacy in two levels of threat models. Our contributions can summarized as follows,

II. RELATED WORK

Single Keyword Searchable secret writing a single keyword searchable secret of the writing schemes [5]–[13], [22] usually build AN encrypted searchable index fixed its content is hidden to the server unless it's given applicable trapdoors generated via secret key(s) [2]. it's initial studied by Song et al. [5] at intervals the excruciate key setting, and enhancements and advanced security definitions unit given in Goh [6], Yangtze et al. [7] and Molecular et al. [8]. Our early work [22] solves secure stratified keyword search that utilizes keyword frequency to rank results instead of returning not differentiate results. However it only supports single keyword search. at intervals the general public key setting, Boonah et al. [9] gift the first searchable secret writing with construction where are anyone with the public key can be write to the information hold on on server but only approved users with private key can search. Public key solutions of the computation all having a high price however. Moreover, the ranked order in search result and privacy guarantees in the more then stronger threat model.

III. EXISTING SYSTEM

Such inefficiency disadvantage also limits their practical performance when deployed in the cloud. Our early work has been aware of this problem, and provides solutions to the multi-keyword ranked search over encrypted data problem. On a different front, the research on top-k retrieval in database community is also loosely connected to our problem. That is problem particularly challenging as it is extremely difficult to meet also the requirements of performance system usability and scalability.

Encrypted data problem but only for queries consisting of a single keyword. We present the first solution to the problem of private information retrieval (PIR) which can handle multiple users while being close to optimal Proposed System More importantly it shows that the number of the query keywords has been little influence on the overhead of trapdoor generation which is a significant advantage over related works on multi-keyword searchable with respect to both communication and computation.

The operation of deleting to existing documents introduces less then computation and communication cost since it is only requires updating the document frequency of all the keywords contained by these documents.

IV. PROPOSED SYSTEM

More significantly, it shows that the quantity of question keywords has very little influence on the overhead of trapdoor generation, that could be a important advantage over connected works on multi-keyword searchable secret writing.

The trapdoor generation perform ought to be a randomised one rather than being settled the settled trapdoor generation would provide the cloud server advantage to accumulate frequencies totally different|of various} search for the requests concerning different keyword(s), which can any violate the aforesaid keyword privacy demand.

The basic protection for the trapdoor unlinked ability test is to introduce ample no determinacy into the trapdoor generation procedure.

We then integrate a recent crypto primitive order-preserving biradial secret writing (OPSE) and properly modify it to develop a one-to-many order-preserving mapping technique for our purpose to shield those sensitive we have a tendency to the too strict information , whereas providing economical hierarchal search functionalities.

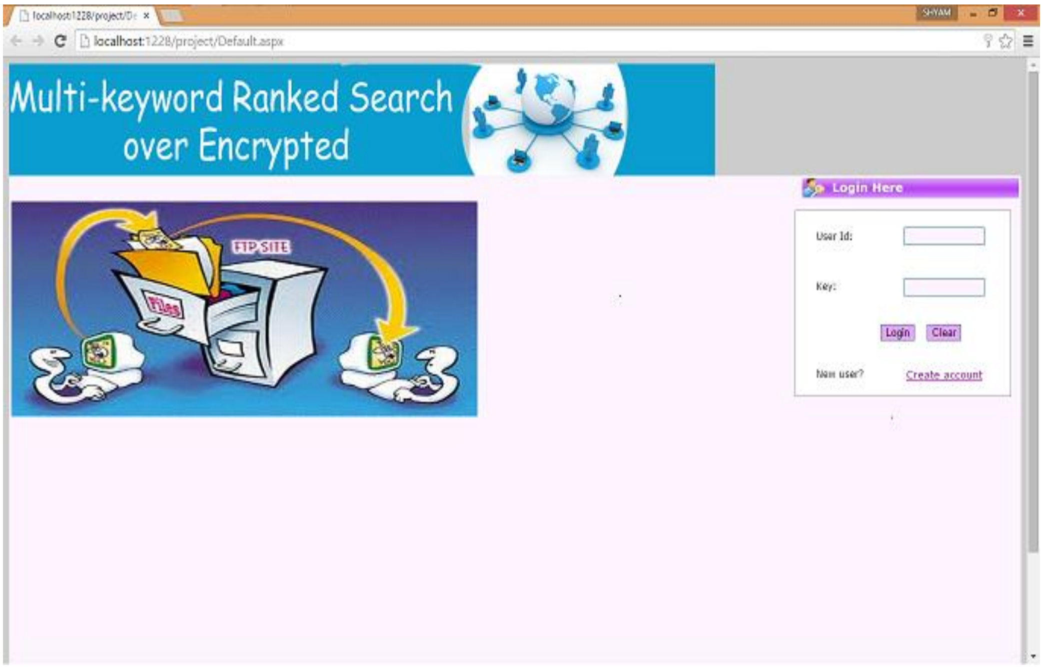
Privacy As for the information privacy, ancient biradial key secret writing techniques might be properly utilised here and isn\'t among the scope of this paper and therefore the projected to utilize personal info retrieval (PIR) technique

V. CONCLUSION

In this paper, for the primary time we tend to ar outline each ar the solve the matter of multi-keyword hierarchical search over encrypted for the cloud information and established a distribution on the privacy needs. a lots of the varied multi-keyword in linguist atlas, we elected auditor the economical principle of “coordinate matching”, i.e., as several matches achievable to capture similarity between question keywords and outsourced documents, and use “inner product similarity” to quantitatively formalize such a principle for similarity being action For meeting the challenge of the supporting multi-keyword linguistics while not privacy breaches, we tend to 1st propose a basic MRSE theme exploitation secure for the product computation and consider improve it to realize privacy needs in 2 levels of threat models. Thorough analysis work privacy and potency guarantees of projected schemes is provided, and experiments on the practical world data collection define our projected schemes introduce low overhead

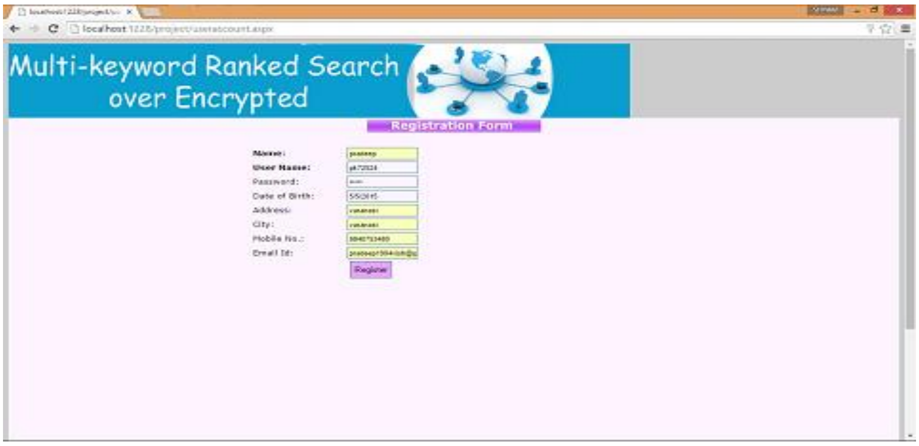
VI. MODULE

A. Server module:


localhost:1228/project/De
SHYAM
localhost:1228/project/Default.aspx
Multi-keyword Ranked Search
over Encrypted
FTP SITE
Files
Login Here
User Id:
Key:
Login
Clear
New user?
Create account

If we have account then put the user id and key then login other-wise we don’t have account then create an account And login the page then put the master key and download the file and it will be gives encryption and decryption ranked

B. Client module:


localhost:1228/project/useraccount.aspx

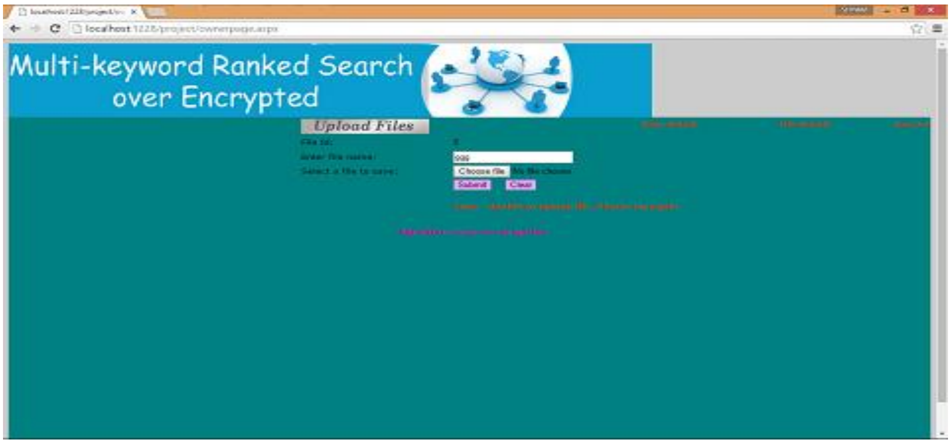
Multi-keyword Ranked Search over Encrypted

Registration Form

Name: pradeep
User Name: pk72024
Password:
Date of Birth: 5/5/2015
Address: varanasi
City: varanasi
Mobile No.:
Email Id:

If we don’t have account then create an account with the help of name, user name password
Date of birth, mobile number and email id then click on register page then it will be gives an master user id and password

C. Router:


localhost:1228/project/ownerpage.aspx

Multi-keyword Ranked Search over Encrypted

Upload Files

File Id:
Enter file name:
Select a file to save: Choose file No file chosen

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

[5] 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.

[6] 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, Relation to Anonymous Ibe, and Extensions,” J. Cryptology, vol. 21, no. 3, pp. 350- 391, 2008.

[7] P. Golle, J. Staddon, and B. Waters, “Secure Conjunctive Keyword Search over Encrypted Data,” Proc. Applied Cryptography and Network Security, pp. 31-45, 2004.

[8] L. Ballard, S. Kamara, and F. Monrose, “Achieving Efficient Conjunctive Keyword Searches over Encrypted Data,” Proc. Seventh Int’l Conf. Information and Comm. Security (ICICS ’05), 2005.