International Journal For Technological Research In Engineering
Volume 4, Issue 5, January-2017 *ISSN (Online): 2347 - 4718*

A NOVEL SCHEME FOR ENCRYPTED CLOUD STORAGE FOR MULTI- KEYWORD SEARCH AND DYNAMIC OPERATIONS

K. Rajitha[1], Sayeeda Khanum Patham[2]
[1]M. Tech Student, [2]Assistant Professor
Department of CSE, Aurora's Scientific Technological & Research Academy, Village Pallecheruvu, Mandal Bandlaguda, District Ranga Reddy, Telangana, India

ABSTRACT: Cloud storage becomes additional and a lot of well-liked in recent years as a result of its advantages like quantifiability, accessibility, low cost service over ancient storage solutions. Organizations are impelled to migrate of their information from native web site to central industrial public cloud server. By outsourcing information on cloud users gets relief from storage maintenance. Though there are several advantages to migrate information on cloud storage it brings several security issues. Thus the information owners hesitate to migrate of the sensitive data. During this case the control of information goes towards cloud service supplier. This security drawback induces knowledge owners to write information at consumer facet and outsource the info. By encrypting information improves the information security however the info potency is reduced as a result of looking on encrypted data is tough. The search techniques that are used on plain text cannot be used over encrypted information. The prevailing solutions supports only identical keyword search, linguistics search isn't supported. Within the paper we have a tendency to projected semantic multi-keyword graded search system. To enhance search efficiency this method includes linguistics search by exploitation Word Net library. Vector area model and TF-IDF model is used for index construction and query generation.

I. INTRODUCTION

Cloud computing could be an informal phrase used to express a spread of dissimilar sorts of computing ideas that occupy large number of computers that are connected through a time period communication network i.e. Internet. In science, cloud computing is that the capability to run a program on several joined computers at an equivalent time. The celebrity of the term may be recognized to its use in advertising to sell hosted services within the sense of application service provisioning that run client server software package on a distant location. Cloud computing depends on sharing of resources to realize consistency and economic system alike to a utility (like the electricity grid) over a network. The cloud conjointly centers on maximize the effectiveness of the shared resources. Cloud resources are typically not only shared by multiple users however as well as dynamically re-allocated as per demand. This can perform for distribution resources to users in dissimilar time zones. as an example, a cloud computing service that serves yank users throughout yank business timings with a particular application (e.g. email) whereas an equivalent resources are getting reallocated and serve Indian users during Indian business timings with another application (e.g. net server).

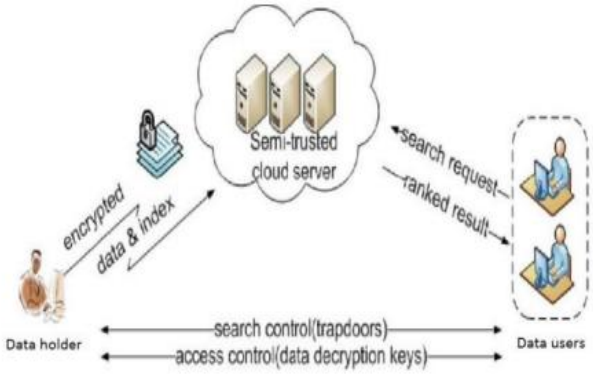


Fig. Design of the search over encrypted cloud data.

This mechanism should take full advantage of the use of computing powers therefore decreasing environmental harm also, since less power, air conditioning then on, is critical for the same functions. The expression "moving to cloud" conjointly explains to a company moving away from a conventional CAPEX model i.e. buy the devoted hardware and reduce in worth it over a period of your time to the OPEX model i.e. use a shared cloud infrastructure and pay as you employ it. Proponents maintain that cloud computing Permit Corporation to avoid direct infrastructure costs, and specialize in comes that distinguishes their businesses as another of infrastructure. Proponents conjointly maintains that cloud computing permit schemes to urge their applications ought to run faster, with higher manageableness and fewer maintenance, and modify IT to a lot of quickly adjust resources to fulfill random and changeable business demand.

II. RELATED WORK

Searchable coding has been an import analysis space and many researchers and organizations have investigated search techniques to look on chipper text information. Searchable encryption permits storing information in encrypted format and you can apply keyword search over chipper text information. These search techniques builds searchable index tree specified its contents are hidden from server but it still permits performing document looking out. These solutions dissent from one another largely in terms of whether they enable single keyword, multi-keyword, similarity search, graded search. By exploitation multi-keyword ranked search user will question with multiple keywords and retrieve correct search result. However of these search schemes does

not enable word primarily based queries. Searching Techniques are

a) Boolean Keyword Search over Encrypted information

Ning Caoy et al. targeted on mathematician Keyword Searchable Encryption. This system has 2 drawbacks. In this scheme user ought to processes each and every came file to find the specified one, as a result of user conscious of a pre knowledge of the encrypted cloud information. Second the search sends back all files that are only depend upon presence or absent of query keywords. This will increase inessential network traffic and consumes information measure.

b) Ranked Keyword Search

Cong Wang et al discuss the main disadvantages of traditional searchable coding schemes and provide the higher technique of keyword search. During this technique the search results are well stratified. This system provides user most relevant document within the connection order with query. And user gets relief from sorting through each match within the content assortment. This system avoids inessential traffic. However they're only helpful single keyword search

c) Multi-keyword stratified Search

Cao et al is that the initial to outline and solve privacy protective problem of multi-keyword stratified search and establish a variety of privacy necessities. In this theme the lexicon words are extracted from documents. And therefore the queries and documents are expressed as vectors. The weather within the vector is the normalized TF values. The documents within the result are graded by matching the vector co ordinates. The importance (weight age) of different keyword isn't taken in account.

d) Secure multi-keyword search

Sun et al describes secure multi-keyword search that support similarity search. During this theme the searchable index tree is built by exploitation vector area model. The cosine similarity with TF*IDF is employed to seek out the relevant score between document and query vectors query vectors and results are came in ordering. This rule search time is best than linear search however the exactitude isn't sensible.

e) Secure kNN algorithm

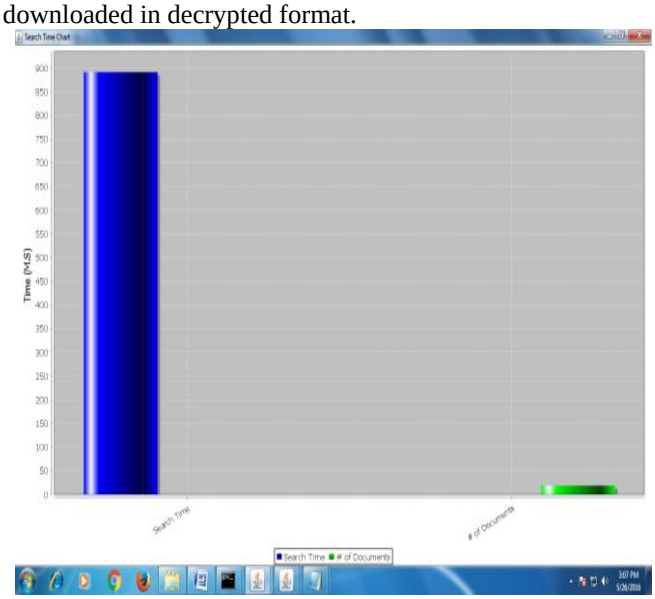
W. K. Wang focuses on query process over encrypted cloud info. During this theme the space between the documents and query are computed to seek out the closest neighbor to the query. In secure KNN technique initial information owner code every attribute of info is encrypted. And the encrypted info is kept on cloud. The approved user WHO need access k highest documents to his query, encrypt the query keywords and therefore the coded tokens are send to cloud server for looking out. The info additionally as query is encrypted thus the query and info confidentiality is preserved.

III. FRAME WORK

This paper proposes a secure tree-based search theme over the encrypted cloud information that supports multi-keyword ranked search and dynamic operation on the document collection. Specifically, the vector area model and therefore the widely-used "term frequency (TF) × inverse document frequency (IDF)" model are combined within the index construction and query generation to produce multi-keyword ranked search. So as to get high search potency, we construct a tree-based index structure and propose a "Greedy Depth-first Search" rule supported this index tree. The secure kNN rule is employed to write in code the index and query vectors, and meantime guarantee correct relevancy score calculation between encrypted index and query vectors. To resist totally different attacks in several threat models, we have a tendency to construct two secure search schemes: the essential dynamic multi-keyword ranked search (BDMRS) theme within the noted cipher text model, and therefore the increased dynamic multi-keyword stratified search (EDMRS) theme within the noted background model. Attributable to the special structure of our tree-based index, the proposed search theme will flexibly come through sub-linear search time and traumatize the deletion and insertion of documents. We have a tendency to style a searchable secret writing theme that supports both the correct multi-keyword stratified search and flexible dynamic operation on document assortment. Attributable to the special structure of our tree-based index, the search quality of the projected theme is fundamentally kept to power. And in apply, the proposed theme can do higher search potency by executing our "Greedy Depth-first Search" rule. Moreover, parallel search are often flexibly performed to further cut back the time price of search method.

IV. EXPERIMENTAL RESULTS

First start cloud server screen. Cloud owner register to register a data owner. Click on cloud user register to register a data user: After successfully registering a data user: Click on cloud owner login to login as a data owner. Click on upload file to upload the data on to cloud. After successfully uploading the data the data will be stored on cloud, in owner folder in the encrypted format and the trap door file will be created (indexing) in index.txt file. User searching for keywords: To download, select any result then click on download button then the corresponding file will be downloaded in decrypted format.



V. CONCLUSION

In this paper, we propose secure search scheme supporting multi-keyword ranked search over encrypted cloud data. We make contributions mainly in two aspects are similarity ranked search for more accurate search result and tree-based searchable index for more efficient searching.

REFRENCES

[1]. K. Ren, C. Wang, Q. Wang *et al.*, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[2]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*. Springer, 2010, pp. 136–149.

[3]. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[4]. O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," *Journal of the ACM (JACM)*, vol. 43, no. 3, pp. 431–473, 1996.

[5]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in CryptologyEurocrypt 2004*. Springer, 2004, pp. 506–522.

[6]. D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith III, "Public key encryption that allows pir queries," in *Advances in Cryptology-CRYPTO 2007*. Springer, 2007, pp. 50–67.

[7]. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*. IEEE, 2000, pp. 44–55.

[8]. E.-J. Goh *et al.*, "Secure indexes." *IACR Cryptology ePrint Archive*, vol. 2003, p. 216, 2003.

[9]. Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proceedings of the Third international conference on Applied Cryptography and Network Security*. Springer-Verlag, 2005, pp. 442–455.

[10]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 79–88.

