International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

A Secure Dynamic Multi-Keyword Ranked Search in Encrypted Cloud Environment

Gauri Bodkhe, Prof. Gurudev B. Sawarkar

Department of Computer Science and Engineering, G. H. Raisoni institute of Technology and Engineering, Nagpur, Maharashtra, India

ABSTRACT

The approach of disseminated figuring, data proprietors are awakened to outsource their psyche boggling data organization systems from neighborhood goals to business open cloud for exceptional versatility and financial hold reserves. In any case, for guaranteeing data assurance, unstable data must be encoded before outsourcing, which obsoletes ordinary data use in perspective of plain text keyword look. In this way, engaging an encoded cloud data look for organization is of focal importance. Considering the broad number of data customers and reports in cloud, it is basic for the chase organization to allow multi-keyword question and give result similarity situating to meet the convincing data recuperation require. Related tackles searchable encryption focus on single keyword request or Boolean keyword look for, and on occasion isolate the question things. In this paper, curiously, we describe and handle the testing issue of assurance sparing multi-keyword situated investigate encoded cloud data (MRSE), and set up a game plan of strict insurance necessities for such a sheltered cloud data utilize system to wind up unmistakably a reality. Among various multi-keyword semantics, we pick the capable run of "organize planning", i.e., whatever number matches as could sensibly be normal, to get the similarity between interest request and data chronicles, and further use "inner thing likeness" to quantitatively formalize such rule for closeness estimation. We initially propose a central MRSE plot using secure inward thing figuring, and after that through and through upgrade it to meet differing insurance necessities in two levels of hazard models. Concentrated examination investigating security and adequacy confirmations of proposed arrangements is given, and examinations on this present reality dataset also show proposed plots without a doubt introduce low overhead on computation and correspondence.

Keywords : Cloud Computing, Encryption, Inner Product Similarity, Single Keyword Search, Multi-Keyword Search, Ranking.

I. INTRODUCTION

Online interpersonal organizations (OSNs) are most prominent and it is the motivation behind why a large number of clients gets to Internet. By this interpersonal organizations clients are share their data between the companions effectively. On-request figuring is a sort of Internet-based registering that gives the information, assets and additionally data to PCs and different gadgets. Data is put away and in addition prepared by outsider server farms and the distributed computing and also stockpiling arrangements given to associations and clients with various abilities. Base of distributed computing is a huge idea of united framework and shared administrations and it is based over dispersion of assets to acquire consistency and economies of scale, same to an administration on a system.

Inside information systems, singular administration providers store private individual data of particular information proprietors. All the data sharing is expert in the perception of solid get to control rules. These information systems have the accompanying essential capacities:

- Contributors together not believe each other in different area
- Have obligation of offering protection to proprietors
- It is critical to share data between suppliers from an application point of view.

In information Networks, information proprietors are allowed to store their documents on number of appropriated servers. It gives administrations to its clients to store and also get to their data in and from number of server frame anyplace and furthermore by any gadget. Giving successful inquiry over circulated documents and moreover give the security to proprietors records it is an exceptionally troublesome assignment. In existing framework a procedure used to take care of this issue called protection safeguarding ordering. The essential goal of PPI is to bolster a worldwide pursuit office which is controlled by an outsider substance. The design of PPI is appropriate for the suppliers, for example, whole get to control over individual records and secures their protection.

PPI [1] is a catalog benefit accessible inside an open cloud. Open cloud has control over various private servers. The data put away over number of private servers by disseminated way. This framework grants diverse clients for discovering documents over conveyed information. For looking proper documents client give a question along related keywords to the PPI [1] [3] server. From that point forward, this open server return gives a rundown of private servers inside the system.

At that point client gets to the private server shown in applicant list and after that client asking for confirmation before looking locally there. In this framework, data put away in plain content way on private server, along these lines client can scan straightforwardly for required records. Yet, security of information is basic; along these lines, in the proposed frameworks, information is put away in scrambled way over private servers. In this manner client needs to verify and after validation, client approaches encoded records from private server. In the wake of acquiring scrambled documents, unscrambling of records are finished by using the KDC. In cryptography, a key conveyance focus (KDC) is a part of a cryptosystem anticipated that would decrease the risks natural in exchanging keys. KDCs consistently work in structures inside which customers may have agreed to use certain administrations at a few times and not at others. KDC give a key to approved clients for decode the documents. When original documents are amassed, then framework executes TF-IDF positioning over records, to acquire best results in positioning arrangement.

II. PROBLEM STATEMENT

Quite number of on-demand data customers and tremendous measure of data documents in the cloud, this inconvenience is trying. It is major for the chase office to permit multi keyword look question and make open result connection situating to see the practical data recuperation essential. To develop the question yield exactness and notwithstanding improve the customer looking foundation, it is furthermore major for such situating structure to support numerous keywords chase, as single keyword request as often as possible yields exceptional coarse results. The searchable encryption method support to give encoded data urges a customer to steadfastly investigate single keyword and recuperate files of concern.

III. LITERATURE SURVEY

Qin Liu et al. proposed Secure and assurance sparing keyword look for in [1]. It gives keyword insurance, data assurance and semantic secure by open key encryption. The guideline issue of this chase is that the correspondence and computational cost of encryption and unscrambling is more.

Ming Li et al. proposed Authorized Private keyword Search (APKS) in [2]. It gives keyword security, Index and Query Privacy, Fine-grained Search Authorization and Revocation, Multi-dimensional Keyword Search, Scalability and Efficiency. This interest procedure manufactures the chase efficiency using quality chain of significance however before long every one of the attributes are not different levelled.

Cong Wang et al in [3] proposed Secure and Efficient Ranked Keyword Search which lights up get ready overhead, data and keyword insurance, minimum correspondence and figuring overhead. It is not useful for various keyword missions, Also there is a modest piece of overhead in record building.

Kui Ren et al. [4] proposed Secured cushioned keyword look for with symmetric searchable encryption (SSE). It doesn't reinforce soft interest with open key based searchable encryption, furthermore it can't play out numerous keywords semantic chase. The redesigns for feathery searchable document are not capably performed.

Ming Li et al. [5] proposed Privacy ensured searchable distributed storage technique. It is executed using SSE, Scalar-Product-Preserving Encryption and Order-Preserving Symmetric Encryption. It reinforces the security and utilitarian essentials. This arrangement does not reinforce open key based searchable encryption.

Wei Zhou et al. [6] proposed K-gram based feathery keyword Ranked Search. In this proprietor make k-gram soft keyword petition for records D and tuple <I, D> is exchanged to request server (SS) which is implanted to grow channel for size controlling. The mixed record D is exchanged to limit server. In any case, the issue is that, the measure of the k-gram develop cushioned keyword set depends in light of the jacquard coefficient regard.

J. Baek et al. in [7] proposed Secure Channel Free Public Key Encryption with Keyword Search (SCF-PEKS) system. In these methodology bundle servers makes its own particular open and private key join however this procedure encounters outside attacker by KGA.

H. S. Rhee et al. [8] proposed Trapdoor in recognisability Public-Key Encryption with Keyword Search (IND-PEKS). In this outsourcing is done as SCF-PEKS. It encounters outside assailant using KGA and separating the repeat of occasion of keyword trapdoor.

Peng Xu et al. [9] proposed Public-Key Encryption PEFKS with Fuzzy Keyword Search, in this customer makes feathery keyword trapdoor Tw and right keyword trapdoor Kw for W. Customer requests Tw to CS. By then CS checks Tw with soft keyword document and sends superset of organizing figure messages by Fuzz Test estimation that is executed by CS. The customer strategy Exact Test counts for checking figure works with Kw and recoup the encoded records. The route toward making cushioned keyword document and right keyword rundown is troublesome for immense size database.

Ning et al. [10] proposed Privacy Preserving Multi Keyword Ranked Search (MRSE). It is useful for known figure content model and establishment exhibit over mixed data. It gives low computation and correspondence overhead. The office planning is decided for multi-keyword looks for. The drawback is that MRSE have minimal standard deviation which decreases the keyword security.

IV. PROPOSED SOLUTION

We propose a powerful framework where any approved client can do a pursuit on scrambled information with multiple keywords, without uncovering the keywords he looks for, nor the information of the records that match by the question. Approved clients can make seek forms by distinct keywords on the cloud to recover the pertinent reports. Our proposition framework encourages that a gathering of clients can inquiry the database gave that they have purported trapdoors for the hunt terms that approve the clients to incorporate them in their inquiries. Our proposed framework can play out multiple keyword hunts in a solitary question and positions the outcomes so the client can recover just the most important matches in a requested way. Also, we build up an arrangement of strict protection prerequisites. Among various multi keyword semantics, we select the viable rule of "organize coordinating".

V. SYSTEM OVERVIEW

The framework engineering is worried by making a straightforward auxiliary structure for a framework. It characterizes the general edge of the venture which quickly depicts the working of the structure and the motivation behind the venture stage is to arrange an answer of the issue distinguished by the need document. The underneath Figure 1 demonstrates the framework of the structure. We consider three sections in our framework engineering: Data Owner, Data client and Cloud Server.

- Data Owner is in charge of the making of the database.
- Data Users are the devotees in a gathering who can utilize the documents of the database.
- Cloud Server bargains information offices to confirmed clients. It is fundamental that server be torpid to substance of the database it keeps.

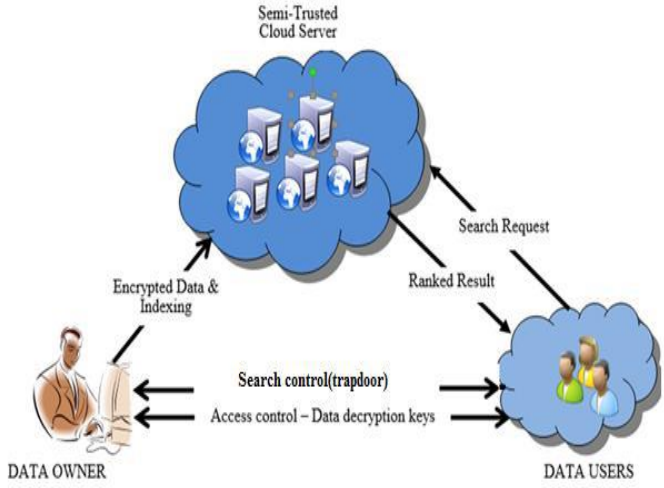

Figure 1: Search over Encrypted Cloud

Information proprietor has measure of information records that he wishes to outsource on cloud server in blended edge. Before outsourcing, information proprietor will at first collect a protected searchable record from a game-plan of shifting keywords removed from the report amassing and store both the once-over and the encoded document on the cloud server. We attempt the guaranteeing between the information proprietor and clients are finished. To scan the record gathering for a given keyword, ensured client makes and shows a demand in a mystery packaging a trapdoor of the keyword to the cloud server. In the wake of getting the pursuit ask for, the server is in control to search for the record and give back the arranging strategy of reports to the client. We think the guaranteed arranged keyword look dangerous as takes after: the question yield must be returned obliging clear arranged importance standards, to make record recovery accuracy for clients. Regardless, cloud server must review dim or irrelevant about the essential rules themselves as they uncover basic touchy information against keyword protection. To rot trade speed, the client may send conceivable respect k adjacent the trapdoor and cloud server just sends back the top-k most fitting documents to the client's concerned keyword. Plot Goals: To permit arranged yield for expert utilization of outsourced cloud information under the effectively indicated appear, our framework setup ought to quickly complete security and execution validations as takes after.

Multi-keyword Ranked Search: To configuration search for game plans which permit multi-keyword question and give result closeness arranging to productive information recovery, rather than returning undifferentiated outcomes.

Protection Preserving: To shield the cloud server from taking in extra information from the dataset and the record, and to meet security.

Feasibility: Above objectives on support and security ought to be master with low correspondence and estimation overhead. Engineer Matching: "Create arranging" [2] is a broadly engaging resemblance measure which utilizes the measure of question keywords showing up in the response to survey the criticalness of that narrative to the demand. Precisely when clients perceive the correct subset of the dataset to be recuperated, Boolean ask for complete well with the correct pursue require conveyed by the client. It is more versatile for clients to see an outline of keywords displaying their anxiety and recover the most basic reports with a rank request.

VI. METHODOLOGY

A. Stemming

In phonetic morphology and data recovery, stemming is the way toward decreasing bent (or once in a while determined) words to their pledge stem, base or root shape—for the most part a composed word frame. The stem require not be indistinguishable to the morphological foundation of the word; it is generally adequate that related words guide to a similar stem, regardless of the possibility that this stem is not in itself a substantial root. Calculations for stemming have been considered in software engineering since the 1960s. Many web indexes treat words with an indistinguishable originate from equivalent words as a sort of question extension, a procedure called conflation. Stemming projects are regularly alluded to as stemming calculations or stemmers.

A stemmer for English, for example, should identify the string "cats" (and possibly "catlike", "catty" etc.) as based on the root "cat", and "stems", "stemmer", "stemming", "stemmed" as based on "stem". A stemming algorithm reduces the words "fishing", "fished", and "fisher" to the root word, "fish". On the other hand, "argue", "argued", "argues", "arguing", and "argus" reduce to the stem "argu" (illustrating the case where the stem is not itself a word or root) but

"argument" and "arguments" reduce to the stem "argument".

B. Suffix-stripping algorithms:

Suffix-stripping algorithms don't depend on a query table that comprises of curved structures and root frame relations. Rather, a commonly littler rundown of "tenets" is put away which gives a way to the calculation, given an information word shape, to discover its root frame. A few cases of the principles include:

- if the word ends in 'ed', remove the 'ed'
- if the word ends in 'ing', remove the 'ing'
- if the word ends in 'ly', remove the 'ly'

Addition stripping approaches appreciate the advantage of being considerably easier to keep up than savage constrain calculations, accepting the maintainer is adequately educated in the difficulties of etymology and morphology and encoding postfix stripping rules. Addition stripping calculations are here and there viewed as unrefined given the poor execution when managing remarkable relations (like "ran" and 'run'). The arrangements delivered by postfix stripping calculations are restricted to those lexical classes which have surely understood additions with couple of special cases. This, notwithstanding, is an issue, as not all parts of discourse have such an all-around planned arrangement of standards. Lemmatization endeavors to enhance this test.

C. Stop-Words

In registering, stop words will be words which are sifted through before or subsequent to handling of normal dialect information (text).Though stop words more often than not allude to the most widely recognized words in a dialect, there is no single all inclusive rundown of stop words utilized by all common dialect preparing apparatuses, and in fact not all devices even utilize such a rundown. A few apparatuses particularly abstain from evacuating these stop words to bolster state seek.

Any gathering of words can be picked as the stop words for a given reason. For some web crawlers, these are the absolute most normal, short capacity words, for example, the, is, at, which, and on. For this situation, stop words can bring about issues when scanning for expressions that incorporate them, especially in names, for example, "The Who", "The", or "Take That". Other web crawlers expel the absolute most normal words—including lexical words, for example, "need"— from an inquiry with a specific end goal to enhance execution.

Hans Peter Luhn, one of the pioneers in data recovery, is credited with begetting the saying and utilizing the idea. The expression "stop word", which is not in Luhn's 1959 introduction, and the related terms "stop rundown" and "stoplist" show up in the writing in the blink of an eye a short time later.

A forerunner idea was utilized as a part of making a few concordances. For instance, the principal Hebrew concordance, Meir local, contained a one-page rundown of unindexed words, with no substantive relational words and conjunctions which are like present day stop words.

D. TF-IDF

TF-IDF remains for term recurrence opposite archive recurrence, and the TF-IDF weight is a weight regularly utilized as a part of data recovery and content mining. This weight is a factual measure used to assess how critical a word is to a record in an accumulation or corpus. The significance builds relatively to the quantity of times a word shows up in the archive yet is balanced by the recurrence of the word in the corpus. Varieties of the TF-IDF weighting plan are regularly utilized via web search tools as a focal apparatus in scoring and positioning an archive's importance given a client inquiry.

One of the least difficult positioning capacities is figured by summing the TF-IDF for each question term; numerous more complex positioning capacities are variations of this straightforward model.

TF-IDF can be effectively utilized for stop-words separating in different subject fields including content outline and characterization.

Commonly, the tf-idf weight is formed by two terms: the principal processes the standardized Term Frequency (TF), otherwise known as. The quantity of times a word shows up in a report, isolated by the aggregate number of words in that archive; the second term is the Inverse Document Frequency (IDF), processed as the logarithm of the quantity of the records in the corpus partitioned by the quantity of records where the particular term shows up.

TF: Term Frequency, which measures how much of the time a term, happens in a report. Since each record is distinctive long, it is conceivable that a term would seem significantly more circumstances in long reports than shorter ones. Along these lines, the term recurrence is regularly separated by the report length (otherwise known as. the aggregate number of terms in the record) as a method for standardization:

TF (t) = (Number of times term t appears in a document) / (Total number of terms in the document).

IDF: Inverse Document Frequency, which measures how important a term is. While computing TF, all terms are considered equally important. However it is known that certain terms, such as "is", "of", and "that", may appear a lot of times but have little importance. Thus we need to weigh down the frequent terms while scale up the rare ones, by computing the following:

IDF (t) = log_e (Total number of documents / Number of documents with term t in it).

E. Build Index Tree

Input: the document collection F = ff1, f2, ..., fn g with the identifiers FID = {FID—FID = 1, 2... n }.

Output: the index tree T

1. for each document fFID in F do
2. Construct a leaf node u for fFID,
3. Insert u to CurrentNodeSet;
4. end for
5. while the number of nodes in CurrentNodeSet is larger than 1 do
6. if the number of nodes in CurrentNodeSet is even, i.e. 2h then
7. for each pair of nodes u0 and u00 in CurrentNodeSet do
8. Generate a parent node u for u0 and u00 ,
9. Insert u to TempNodeSet;
10. end for
11. else
12. for each pair of nodes u0 and u00 of the former (2h 2) nodes in CurrentNodeSet do
13. Generate a parent node u for u0 and u00 ;
14. Insert u to TempNodeSet;
15. end for
16. Create a parent node u1 for the (2h - 1)-th and 2h-th node, and then create a parent node u for u1 and the (2h + 1)-th node;
17. Insert u to TempNodeSet;
18. end if
19. Replace CurrentNodeSet with TempNodeSet and then clear TempNodeSet;
20. end while
21. return the only node left in CurrentNodeSet, namely, the root of index tree T ;

F. BDMRS

SK⟵ Setup () initially, the data owner generates the secret key set SK, including 1) A randomly generated m-bit vector S where m is equal to the cardinality of dictionary, and 2) two (m X m) invertible matrices M1 and M2. Namely, SK = {S, M1, M2}.

I⟵ GenIndex (F, SK) First, the unencrypted index tree T is built on F by using

T⟵ BuildIndexTree (F) Secondly, the data owner generates two random vectors (D'u, D"u) for index vector Du in each node u, according to the secret vector S. Specifically, if S[i] = 0, D'u[i] and D"u[i] will be set equal to Du[i]; if S[i] = 1, D'u[i] and Du"u[i] will be set as two random values whose $\{M_1^T D'_u, M_2^T D''_u\}$ sum equals to Du[i]. Finally, the encrypted index tree I is built where the node u stores two encrypted index vectors Iu=

TD⟵GenTrapdoor (Wq, SK) with keyword set Wq, the unencrypted query vector

Q with length of m is generated. If wi "Wq, Q[i] stores the normalized IDF value of wi; else Q[i] is set to 0. Similarly, the query vector Q is split into two random vectors Q' and Q". The difference is that if S[i] = 0, Q? [i] and Q" [i] are set to two random values whose sum equals to Q[i]; else Q' [i] and Q" [i] are set as the same as Q[i]. $\{M_1^{-1} D'_u, M_2^{-1} D''_u\}$ Finally, the algorithm returns the trapdoor TD =

Relevance Score⟵ SRScore (Iu, TD) With the trapdoor TD, the cloud server computes the relevance score of node u in the index tree I to the query.

G. EDMRS Scheme

The enhanced EDMRS scheme is almost the same as BDMRS scheme except that:

SK⟵ Setup (): In this algorithm, we set the secret vector S as a m-bit vector, and set M1 and M2 are (m +

m') (m + m') invertible matrices, where m' is the number of phantom terms.

I⟵ GenIndex (F; SK): Before encrypting the index vector Du, we extend the vector Du to be a (m+m') - dimensional vector. Each extended element Du [m+ j], j = 1... m', is set as a random number"j .

TD ⟵GenTrapdoor (Wq, SK) The query vector Q is extended to be a (m + m')- dimensional vector. Among the extended elements, a number of m" elements are randomly chosen to set as 1, and the rest are set as 0.

Relevance Score⟵ SRScore(Iu, TD) After the execution of relevance evaluation by cloud server, the final relevance score for index vector Iu equals to Du ˆA $\Sigma\varepsilon v$, where v ε {j|Q[m + j] = 1}

VII. IMPLEMENTATION

A. Data User Module

Data customers are customers on this system, will's personality prepared to download archives from the cloud that are exchanged by the data proprietors. Since the archives set away on the cloud server could be in tremendous numbers, there is an interest office provided for the customer. The customer should have the ability to do a multi-keyword look on the cloud server. Once, the result appears for the specific interest, these customers should have the ability to send a request to the individual data proprietors of the archive through the system (similarly called trap-passage request) for downloading these records. The data customers will similarly be given a request support screen, where it will tell if the data proprietor has recognized or rejects the request. If the request has been avowed, the customers should have the ability to download the decoded record.

B. Information Owner Module

In this module, the information proprietors ought to be able to trade the records. The reports are encoded before the records are traded to the cloud. The information proprietors are given another choice to enter the keywords for the record that are traded to the server. These keywords are utilized for the asking for reason which helps the intrigue return values rapidly. These records when once accessible on the cloud, the information clients ought to be gifted enthusiasm utilizing the keywords. The information proprietors will in addition be furnished with a demand endorsing screen so they can support or reject the demand that is gotten by the information clients.

C. Document Upload and Encryption Module

In this module, the information proprietors ought to be able to trade the documents. The records are blended before the reports are traded to the cloud. The information proprietors are given a differentiating choice to enter the keywords for the record that are traded to the server. These keywords are utilized for the asking for reason which helps the pursuit return values rapidly. These records when once open on the cloud, the information clients ought to be able to pursue utilizing keywords. The information proprietors will in like way be equipped with a demand endorsing screen so they can support or reject the solicitations that are gotten by the information clients. The record before trade should be encoded with a key so that the information clients can't simply download it without this key. This key will be asked for by the information clients through the trap-gateway. The encryption of these records utilizes RSA figuring so that unapproved clients won't be able to download these documents.

D. Document Download and Decryption Module

Information clients are clients on this structure, will's character arranged to download records from the cloud that are traded by the information proprietors. Since the records set away on the cloud server could be in tremendous numbers, there is an intrigue office accommodated the client. The client ought to be able to do a multi-keyword search for on the cloud server. Once, the outcome shows up for the particular intrigue, the clients ought to be able to send a demand to the individual information proprietors of the report through the framework (additionally called trap-entryway ask for) for downloading these records. The information clients will in like way be given a demand bolster screen, where it will tell if the information proprietor has perceived or rejects the demand. On the off chance that the demand has been grasped, the clients ought to be able to download the unscrambled document. The record before download should be unscrambled with a key. This key will be asked for by the information clients through the trap-passage ask. Once the key is

given amidst the download, the information clients will be able to download the record and utilize them.

E. Rank-Search Module

This module allows the data customers to look for the reports with multi-keyword rank looking. This model uses the once in a while used rank chasing figuring down present the yield for multi-keywords. "Encourage Matching" rule will be grasped for the multi-keyword chasing. This module in like manner manages making a document for speedier chase.

VIII. EXPERIMENTAL RESULT

Fig. 2 shows look time relationship outline; in thunder graph X-center point exhibits the count by which records are looked for while Y-turn demonstrate time required for looking for question related in ms

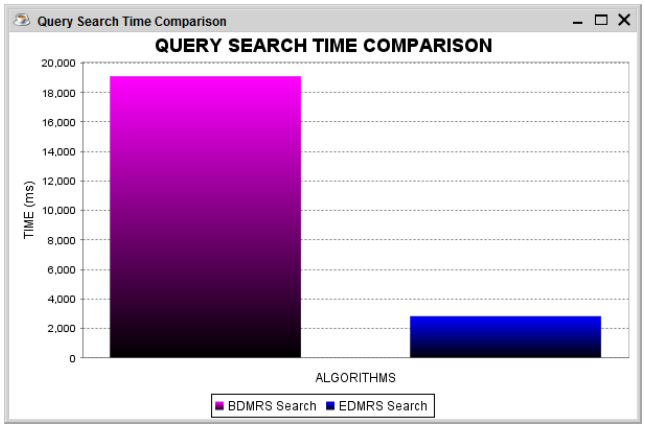

Figure 2: Query Search Time Comparison

Fig. 3 shows time outline; in above diagram X-rotate shows number of records in social occasion while Y-center point exhibit time required for delivering document tree in ms, with augmentation in number of files the time required to make list tree is furthermore increase.

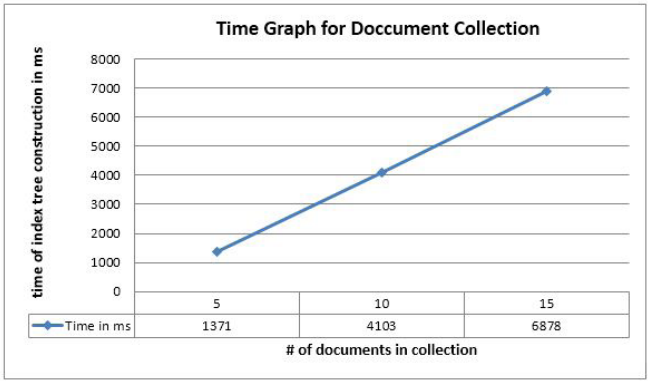

Figure 3: Time Graph for Document Collection

Fig. 4 shows time outline; in above diagram X-center point shows number of keywords in word reference while Y-turn exhibit time required for delivering record tree in ms, with augmentation in number of keywords the time required to make list tree is moreover increase.

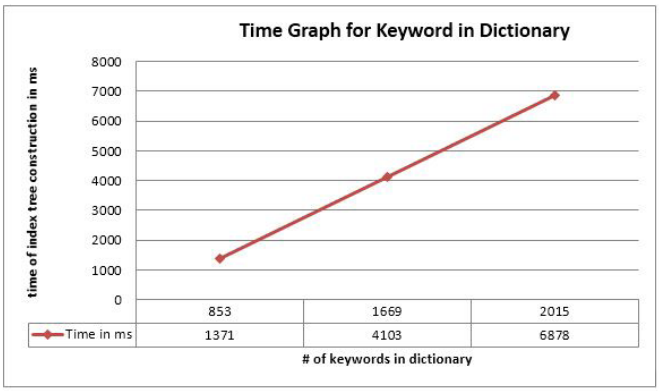

Figure 4: Time Graph for Keyword in Dictionary

IX. CONCLUSION

In this work, firstly we portray and resolve the troublesome of multi-keyword positioned look over scrambled cloud information, and make an assortment of protection necessities. Between various multi-keyword semantics, we select the compelling likeness measure of "facilitate coordinating", i.e., as different matches as likely, to adequately catch the importance of outsourced archives to the question correspondence .In our future work, we will seek supporting other multi keyword semantics over encoded information and checking the honesty of the rank request in the item keywords. For tradition the test of steady multi-keyword semantic without security breaks, we propose an essential thought of MRSE. At that point we give two better MRSE diagrams to acknowledge numerous stringent security necessities in two divergent risk models. Nitty gritty examination contemplating security and effectiveness assurances of proposed plans is given, and trials on this present reality information set demonstrate our future frameworks present low overhead on both calculation and correspondence.

X. REFERENCES

[1]. Qin Liuy, Guojun Wangyz, and Jie Wuz,"Secure and privacy preserving keyword searching for cloud storage services", ELSEVIER Journal of Network and computer Applications, March 2011

[2]. Ming Li et al.," Authorized Private Keyword Search over Encrypted Data in Cloud Computing,IEEE proc. International conference on distributed computing systems, June 2011,pages 383-392

[3]. Cong Wang et al.,"Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE Transactions on parallel and distributed systems, vol. 23, no. 8, August 2012

[4]. Kui Ren et al., "Towards Secure and Effective Data utilization in Public Cloud", IEEE Transactions on Network, volume 26, Issue 6, November / December 2012

[5]. Ming Li et al.,"Toward Privacy-Assured and Searchable Cloud Data Storage Services", IEEE Transactions on Network, volume 27, Issue 4, July/August 2013

[6]. Wei Zhou et al., "K-Gram Based Fuzzy Keyword Search over Encrypted Cloud Computing "Journal of Software Engineering and Applications, Scientific Research , Issue 6, Volume 29-32,January2013

[7]. J. Baek et al., "Public key encryption with keyword search revisited", in ICCSA 2008, vol. 5072 of Lecture Notes in Computer Science, pp. 1249 - 1259, Perugia, Italy, 2008. Springer Berlin/Heidelberg.

[8]. H. S. Rhee et al., "Trapdoor security in a searchable public-key encryption scheme with a designated tester," The Journal of Systems and Software, vol. 83, no. 5, pp. 763-771, 2010.

[9]. Peng Xu et al., Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack",IEEE Transactions on computers, vol. 62, no. 11, November 2013

[10]. Ning Cao et al.," Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, jan 2014

[11]. D. X. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. S & P, BERKELEY, CA, 2000, pp. 44.

[12]. C. Wang, N. Cao, K. Ren, and W. J. Lou, Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data, IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467-1479, Aug. 2012.

[13]. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. ASIACCS, Hangzhou, China, 2013, pp. 71-82.

[14]. R. X. Li, Z. Y. Xu, W. S. Kang, K. C. Yow, and C. Z. Xu, Efficient multi-keyword ranked query over encrypted data in cloud computing, Futur. Gener. Comp. Syst., vol. 30, pp. 179-190, Jan. 2014.

[15]. Gurdeep Kaur, Poonam Nandal, "Ranking Algorithm of Web Documents using Ontology", IOSR Journal of Computer Engineering (IOSR-JCE) eISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VIII (May-Jun. 2014), PP 52-55