International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 12th Dec 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-13

Title: **THE DYNAMIC DELETION AND INSERTION OF DOCUMENTS WITH MULTI RANK KEYWORD SEARCH SCHEME**

Volume 07, Issue 13, Pages: 366–376.

Paper Authors

MD. MEENAAZ HAJIRAK KULSUM, G.KIRANMAI, K. BRAHMAIAH CHOWDARY

PB Siddhartha College of arts and science, vijayawada

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

THE DYNAMIC DELETION AND INSERTION OF DOCUMENTS WITH MULTI RANK KEYWORD SEARCH SCHEME

[1]MD. MEENAAZ HAJIRAK KULSUM, [2]G.KIRANMAI, [3]K. BRAHMAIAH CHOWDARY

[1]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, vijayawada

[2]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, vijayawada

[3]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, Vijayawada

mmeenaaz@gmail.com

Abstract: Cloud computing is gift development as another procedure show in assortment of business zones. significant amounts of escalated scale workplaces are commencing to move the educational on to the cloud condition. With the face of capability as a company fluctuated adventures are moving their essential knowledge to the cloud, since it prices less, adequately issue and should be gotten to from anywhere at no matter purpose. dilated explicit multi-watchword situating interest contrive with best key by recommends that of confused cloud knowledge that at the indistinguishable time supports dynamic revive errands as deleting and embeddings records. prehensile significance starting look computation is suited capability multi watchwords on place and record structure. Cryptography is one in everything concerning setting up trust models. Open security can be a cryptological system to convey up security. In assortment of investigators are cacophonic endlessly at creating security and profitable open coding sorts. we tend to tend to require new unimaginable cryptological frameworks energetic concerning knowledge structures like CRSA and B-Tree to support the part of security. we tend to tend to propose new multi-watchword look question over encoded cloud learning in worn out best k scored records. The vector house model and TFIDF indicate are wont to produce document and request age. This paper bases on multi trademark get eager concerning situating over a confused cloud data. The chase uses the piece of closeness and interior factor alikeness coming up with . we tend to tend to propose to assist the smallest amount complicated k Multi-full-content explore for security and execution examination exhibit that the organized model guarantees a high welfare and customary sense and dynamic revive exercises, for instance, eradicating and in addition reports. The check results show that the overhead in calculation and correspondence is low.

Index Terms: Advanced Symmetric Encryption Certified Authority, Cloud data, -Multi keyword Retrieval, Cloud data, Data security, Ranked Search, Similarity Matching.

1. INTRODUCTION

Distributed computing may be a term acclimated with portraying a meet of IT focal points that are given to a vendee over a framework on a chartered introduce and with the capability to resize or down their organization conditions. Fogs are way reaching pools of with success usable and open virtualized resources. These blessings are with competence reconfigured to adapt to a variable load (scale), permitting good resource utilize. it is a buy each use seem within that the Infrastructure supplier byways for revamped Service Level Agreements (SLAs)[1] offers guarantees often abusing a pool of benefits. Affiliations and different people can profit by the mass procedure and capability centers, outfitted by Brobdingnagian associations with relentless and robust cloud constructions. Security contemplations are that the basic troubles in distributed computing. The instrumentation and programming security instruments like firewalls and afterward on are utilized by the cloud provider. These game plans are not such as protect info within the cloud from unapproved patrons in light-weight of the low dimension of straightforwardness [2]. Since the cloud vendee and on these lines the cloud provider is within the actual sure in-house, the re-appropriated information probably may be given to the vulnerabilities [2] [3]. on these lines, said putting off from the productive info within the cloud, the data ought to be encoded [5]. info cryptography ensures the data protection and characteristic. to protect {the info | the knowledge | the information} security we've to mastermind relate on the market count that bargains with addled data [6]. to make sure info insurance, mystery, and knowledge security, sensitive information like individual prosperity records, messages, appraise chronicles, image accumulations, cash associated trades, and so on, should be discontinuous by info proprietors before redistributing to the last world cloud [7]. all things thought of, the standard plaintext maxim look information utilize profit is obsolete. Downloading all the data and unscrambling at the information vendee perspective is that the inconsequentially unreasonable cluster to a wide life of exchange speed esteem is needed in cloud-scale structures. the are simply exploring for when and utilized a lot of typically than no purpose behind putt away info within the cloud. on these lines, work convincing and secure request over difficult cloud learning is of sometimes very important. this is often relate particularly hard issue; it ruins the execution of structure accommodation and size. it's particularly debilitative to meet the wants of system simple utilize, execution and suppleness by harrowing regarding the massive assortment of on-task for info patrons and a heavy assortment of decentralized learning records within the cloud. to meet triple-crown learning recovery, the monstrous live of files asks for the cloud server to perform applicability score during this manner, rather reestablishing all result records. Such a situating structure urges learning patrons to find the principal material info apace, rather than hard tending to every match within the data aggregation [8]. Be that since it may, this could finish in an infinite esteem regarding info, convenience. for example, this model for watchword essentially based mostly info recovery, that's oftentimes utilized on the plaintext learning, cannot be associated significantly to the encoded information. exchange all info within the cloud and to unscramble regionally is clearly surreal. to want care of the upper than a difficulty, examiners have some all around confirmatory courses of action with fully homomorphic cryptography or externally disabled RAMs [9] created. These ways in which are not wise thanks to their high methodology value for every the cloud Sever and patrons. organized value more highly to reach adaptable interest sub-straight request time and pander to the dropping and thought of reports.

RELATED WORK

Many trying to find routes over encoded cloud data have organized. S.Deshpande [11] organized a framework needing over befuddled cloud knowledge exploitation wool watchwords. They used Edit partition to measure catchword closeness and created a pair of frameworks on building wool watchword sets to realize practiced capability and depiction overheads. Cong wang et al. [12] Has organized a method placed trademark live through encoded cloud data exploitation watchword redundancy and demand protective cryptography. It supports simply single catchphrases specifically. is that the watchword reduplication selecting report archive score. Rank given to every record keen about the importance score of that report. high placed records have sent to consumers rather all reports. to upgrade look utility N. Cao et al. [13] Have organized a thought supporting conjunctive catchphrases get. it's security – defensive multi-catchphrase placed get technique exploitation spread cryptography. M. Chou et al. [14] organized a solution for fleece multi-watchword live through encoded cloud data exploitation security cognizant Bed Tree. They used a co-occasion chance on account of take under consideration acknowledge vital multi-catchphrases for conveyance of title knowledge, records and material wool trademark sets created exploitation alter isolated. They structured record tree for all knowledge, reports, where each leaf center purpose having the hash estimation of a trademark, a pair of data vectors that addresses n-gram of that watchword and grow channels for every alter separate value. Chi Chen, has organized a numerous leveled gathering methodology to a substantial live of request reinforce linguistics and consequently the passion for fast passphrase - Search meet amid a stimulating knowledge condition [15] . The organized dynamic approach teams the files bolstered slightest pertinence limit , and later fragments the subsequent dynamic bunch is return to , the limitation on the chief extraordinary size of the bunch [15]. within the chase stage can deliver the goods associate degree at once machine whimsy stood out from Associate in Nursing exponential addition within the vary of record-assembling this framework. to check the legitimacy of the inquiry things, a structure referred to as slightest hash sub tree is organized amid this paper. The organized procedure has vantage over the quality system within the Rank Privacy as essential documents.

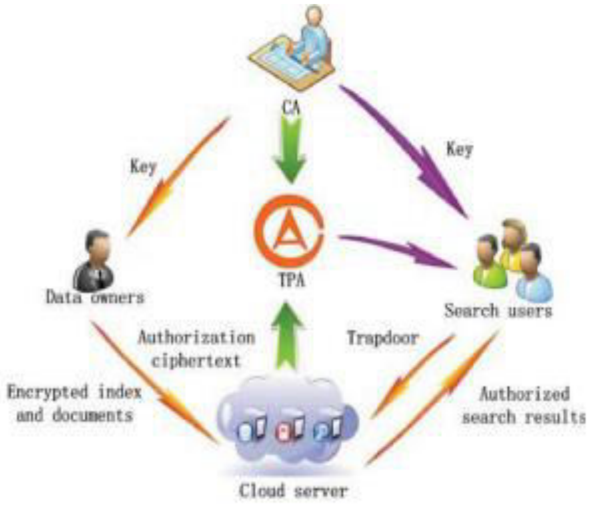

Fig No 1. Hash Sub Tree Designed

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

2. SYSTEM MODEL

We thought of a distributed computer system indicate having three clear components. Those are learning Owner, Cloud Service supplier and knowledge. the requirement of each half is in keeping with the accompanying: data Owner (DO): DO embrace an occasion data records DC= with the sensitive learning to be redistributed to the cloud server. to administer data assurance, the reports are encoded before re-appropriating. DO makes a word reference eager regarding catchphrases isolated from the all m files energetic regarding Term Frequency Inverted Document Frequency (TFIDF) [16] that are printed in stage four. The wordbook consolidates identical expressions of each watchword from the synonym discoverer [17]. The lexicon has and watchwords, and for each maxim might have t proportionate words, with the target that the wordbook gauge is n × t. DO makes a stock vector for every document energetic regarding the catchphrases liberated from the report. The vary of the record vector is loved the number of catchphrases within the workbook that relates degree. every estimating within the summary vector stores mix of the arrival of apothegm and correlation identical words within the workbook is shown as term come (TF) in our structure. Record vectors of all files are difficult before dispersive to the cloud. DO assemble request vector excited regarding watchwords entered by data shopper. to administer client security, request vector encoded, as Trapdoor and send to data shopper. {the data the training the information} man of undertakings send a request to neglect to manage to the supported data emptor.

A. data customers:

Data consumers are the consumers UN agency visiting difficult data from the cloud. The cloud server look catchphrases or proportionate words acknowledged with files, that have an interest to learning shopper and sends to the info man of undertakings. {the learning {the data|the info|the data} the information} emptor gets trapdoor and appears to urge the chance to manage of knowledge man of problems and sends trapdoor and acquire to direct to the cloud server to recoup needed information from the cloud.

B. Cloud Service provider (CSP):

Cloud server gets wooly data and encoded list vectors from data man of undertakings and stores into data proprietor's distributed storage. Cloud server having the flexibility to need the knowledge enkindle from buyer and check the chase get the prospect to direct the client. it's going to recoup the reports from distributed storage trusting on the favorable circumstances to need to Associate in Nursing assortment of records. To grow the training healing exactness from the cloud server, the most effective scored reports return to data buyer from the cloud server. The model for multi-catchphrase synonym request over encoded cloud data.

C. Danger display:

The cloud server is measurable as "bona fide but curious" [18] in our organized system. The cloud server seeks once the organized system explicit and besides watches learning in its distributed storage {and data {and data|and knowledge|and information} and knowledge} that are gotten from data shopper through the treating to be told extra information. we have a tendency to expect of one as hazard seem for our structure with varied strike limits that are in keeping with the accompanying: commonplace figure content show: amid this model, the cloud server is aware of regarding primarily difficult data and encoded list vectors, that are re-appropriated from data man of undertakings.

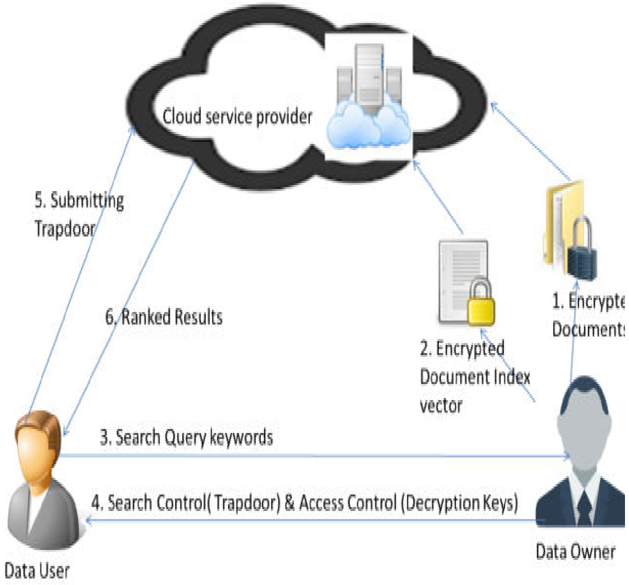

Fig No 2 System Model

3. PROPOSED SYSTEM

The main symmetrical accessible encryption (SSE) plot and the hunt of the plan is direct in the span of the information gathering. Proposed formal security definitions for SSE and built up a framework dependent on Bloom channel. It is recommended that two frameworks (SSE - 1 and 2) that the ideal pursuit time is come to. Your SSE 1 conspire is secure against assaults Chosen-Keyword (CKA1) and SSE - 2 is secure against versatile picked catchphrase assaults (CKA2). These early works are single catchphrase Boolean hunt conspires that are exceptionally basic as far as usefulness. After a lot of plants have been proposed under various risk models to seek different pursuit capacities, for example, single watchword look, likeness look more catchphrase Boolean inquiry space and multi catchphrase seek on place, and so forth. Multi - catchphrase Boolean pursuit permits accomplish the client to enter different question watchwords to ask for proper records. Among these works, joining catchphrase look frameworks give just the records that contain the majority of the question watchwords. Disjunctive Keyword Schemes restore all archives that contain catchphrases proposed [19] .Predicate seek plots a subset of the inquiry, both interfacing troublesome to help look. Every one of these plans More Keyword recover query items dependent on the nearness of catchphrases, which can give not satisfactory outcome positioning usefulness [20]. Proposed guide can accomplish sublinear look time adaptable and manage the erasing and embeddings records. The safe kNN calculation used to scramble the list and question vectors, meanwhile precise importance score estimation between encoded file and inquiry vectors [21] .Ensure to withstand different assaults in various danger models, manufacture two secure hunt frameworks: the dynamic best k multi-catchphrase look conspire chose in the realized ciphertext demonstrate, and enhanced powerful best k multi-watchword space seek method in the realized foundation show. For our framework, we pick the B-tree as ordering information structure to distinguish the match between inquiry question and data records. Exceptionally, we utilize inward records correspondence, i.e., the quantity of question catchphrases showing up in report, to finding the likeness of that archive to the hunt inquiry. Each record is changed to a fair B-tree as indicated by the catchphrases and scrambled utilizing CRSA. At whatever point client needs to look, He makes a trapdoor for the catchphrases. Our point is to manufacture and examine the execution of different watchwords positioned look design utilizing Commutative RSA calculation and B-tree information structure for accessible list tree.

Commutative Encryption (CRSA):

The RSA cryptosystem is outstanding amongst alternative open key cryptography approaches. nonetheless, its general power gets restricted due to a way encoding and larger a part of existing RSA demonstrate expertise the unwell effects of reordering problems. after, with the top goal to create this framework minimum convoluted and simpler, a strategy known as independent RSA has been projected. during this arrange, the request within which encoding has been done wouldn't influence the coding on the off probability that it's exhausted an analogous request. encoding is that the settled strategy for creating a correspondence non-public. With the various cryptological methodologies, our framework pursues the independent RSA calculation. The numerical arrange for enjoying out this encoding is depicted by a pseudo calculation.

2. BMS Tree Index Construction:

In the method file tree development, we tend to produce hub for every archive within the record gathering. These hubs are set about as leaf hubs within the tree. the within hubs are formed obsessed with these leaf hubs. The record tree development method is pictured within the calculation one. A case of BMS list tree for our arrange that is developed on plaintext. the data structure of the hub is characterized as (ID, F, juvenile [], DID), wherever I may be a one in every of a sort id created utilizing GenID() work, F is file vector, child[] is tips that could offspring of the hub and DID may be a record ID. within the calculation, we tend to utilized 2 factors Current Node assortment and worker Node assortment to store accumulation of hubs. Current Node assortment stores the arrangement of without delay handling hubs that haven't any guardians and worker Node assortment stores set of recently formed hubs. Fu[i] faithfully stores the best TF estimation of among its youngsters. The conceivable biggest importance score of its youngsters is assessed utilizing this procedure.

Algorithm 1 Build BMS Index Tree(DC)

```
For each data document Ddid in DC do Construct leaf node l for Ddid l.ID=GenID(), l.child[i]=null for i=1,…, b; l.DID=DID, and F[i]=TFDdid,ki for i=1,…, n;

 Insert l to CurrentNodeCollection;

 End for While the number of nodes in CurrentNodeCollection is more than 1 do

 For each five of nodes u1, u2, u3, u4, and u5 in

 CurrentNodeCollection do

 Generate a parent node u for u1, u2, u3, u4, and u5with u.ID=GenID(), u.child[i] = uifor
```

```
i = 1to 5; u.DID = 0, and D[i] = max{ui.F[j] for i=1 to 5} for each j=1 to n;
 Insert u to TempNodeCollection;
 End for
The remaining nodes (less than 5 nodes) in CurrentNodeCollection generate a parent node u like above;
Insert u to TempNodeCollection;
 Replace CurrentNodeCollection with TempNodeCollection and then free the TempNodeCollection;
 End while
 Return only one node, left in the CurrentNodeCollection called the root node;
```

1. Search Process using DFST:

The hunt procedure of MSRQE conspire is that the algorithmic capability upon the BMS tree name as Depth initial Search Technique calculation. we have a tendency to create Associate in Nursing outcome reports as RankedList, whose part is indicated as (Score, DID). Here, the score is that the significance score among Fdid and question vector letter, that is computed utilizing formula(1). The RankedList stores high k scored archives to the inquiry. The elements of RankedList are in the slippery request as indicated by score work amid the inquiry procedure. The DFST calculation is introduced in calculation two. Kth score may be the littlest relevancy score in RankedList.

Algorithm 2 DFST(Index Tree Node u)

```
If the node u is not a leaf node then
 If Score(Fu, Q) >kth score then
 Sort the children of u in descending order according to scores of children
 For i=1 to the number of children of u do
GDFS(u.child[i]);
End for
 Else
 Return;
 End if
 Else
 If Score(Fu, Q) >kth score then
 Delete the element with a smallest relevance score from
RankedList;
 Insert a new element (Score (Fu, Q), u.ID) and sort all elements of RankedList in descending order;
 End if
 Return;
 End if.
```

Planning accessible coding conspires, the structures got with sub-straight pursuit time, specifically, dynamic hunt is basic, passing parallel and might beyond any doubt handle updates. specifically, for n records on m watchwords and with p centers (processors) showed accessible and it underpins advanced inquiries and multi-customer settings utilizing SSE as a recorder. to ensure that our data structures and connected business exercises that is bolster for dynamic databases and it bolster computer memory unit - Scale databases in these a lot of extravagant/complex encoded look settings. The dynamic development keeps up the perfect record live and simply basic size knowledge.

3. MRSE FRAMEWORK

For a simple introduction, tasks on {the data|the knowledge|the data} reports don't seem to DFT within the system since the data businessman may while not a lot of a stretch utilize the traditional bilaterally symmetric key cryptography to scramble and at the moment spread information. With spotlight on the file and inquiry, the MRSE framework contains of 4 calculations as pursues

1. Setup(ℓ) Taking a security parameter ℓ as information, the data businessman yields a bilaterally symmetric key as SK.

2. BuildIndex(F, SK) supported the dataset F, the data businessman constructs Associate in Nursing accessible record I that is the bilaterally symmetric key SK and later re-appropriated to the cloud server. when the record development, the archive gathering are often autonomously disorganized and decentralized .

3. Trapdoor(FW) With t watchwords of enthusiasm for FW as data, this calculation produces a comparison trapdoor TfW.

4. Query(TfW, k, I) once the cloud server gets a matter to elicit as (TfW, k), it plays out the positioned pursuit on the record I with the help of trapdoor TfW, in conclusion, returns FfW, the positioned id summation of best k reports organized by their closeness with fW. The agent protection guarantee within the connected writing, for instance, accessible coding, is that the server should get the suspend of solely things. With this general security portrayal, we have a tendency to investigate and build up an appointment of strict protection stipulations significantly for the MRSE structure. With relevance the data protection, the data businessman will rely upon the traditional bilaterally symmetric key cryptography to code the data before redistributing, and effectively keep the cloud server from prying into the re-appropriated data.

2. RESULTS AND DISCUSSION

The planned set up, info shoppers will accomplish distinctive wants on pursuit accuracy of protection by the quality deviation of modification which will be treated as a pay parameter. The examination of frameworks with Associate in Nursing in progress work that accomplishes high inquiry effectiveness. BDMRS plot calls the list things by correct count of archive vector and question vector. on these lines, top-k look exactness of BDMRS plot is one hundred pc. Be that because it could, based mostly and similitude Multi-watchword sq. hunt style, the elemental set up in experiencing loss of accuracy thanks to the aggregation of sub-vectors with the list development . The take a look at is rehashed multiple times, and therefore the traditional accuracy of ninety one the concerns. Amid the inquiry, once the relevancy of the hub is a lot of outstanding than the bottom importance in results Rlist, appearance at the cloud server, the offspring of the hub; else it returns. Such a major range of hubs not ought to amid a real hunt. we have a tendency to indicate the number of leaf hubs that contain a minimum of one watchwords within the question. it's by and huge a lot of noteworthy than the number of records needed k, nevertheless so much not precisely the cardinality of the archive accumulation n. As a good parallel tree, the tallness of the file n is log are preserved, and therefore the many-sided nature of the computation is positioned relevancy O (m).

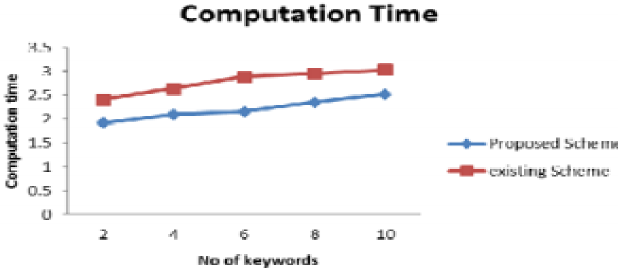

Figure 3: Time Comparison

The chart the examination of the inquiry calculation time in seconds of our planned framework against the RSA based mostly framework. for 2 catchphrases look for, the time taken by the RSA based mostly set up is roughly two.5 seconds, tho' our planned framework takes around zero.5 seconds less. because the number of watchwords dilated for inquiry, the calculation time for a hunt in addition increments directly within the 2 plans. Be that because it could, CRSA based mostly set up is found to perform higher. during this manner, it's obvious that coding calculation CRSA with B Tree as record tree performs superior to something RSA and B tree Combination

4. CONCLUSION

We expect to offer plausible answers for multi-catchphrase word positioned question problems over disorganized cloud info whereas safeguarding strict framework smart security in cloud computing worldview. the primary multi-watchword look for, the second word based mostly hunt, third comparison positioned look and therefore the latter is skillful info recovery with BMS tree and DFST seeking calculation. Our precedent delineation additional shows skillful and precise best k records recovery of planned conspire with sub-direct time complexity. Multi-rank phrase look for conspiring is planned, that not simply backings real multi-watchword look on house, nevertheless additionally the dynamic cancellation and inclusion of records. we have a tendency to fabricate a novel phrase adjusted twofold tree because of the record. what is a lot of, the hunting procedure can be performed in parallel to decrease the time, cost? the safety of the framework is ensured against 2 danger models through secure best k recovery calculation. The alpha outcomes demonstrate the adequacy of our planned setup. Careful examination researching security and product certifications of planned plans is given, and analyses on this gift reality dataset demonstrate our planned set up presents low overhead on each calculation and correspondence.

5. FUTURE WORK

The future work would specialize in utilizing Elliptic Curve Cryptography (ECC) coding strategy for higher execution. Further, we have a tendency to arrange to examine the conduct of our planned system(s) for the multi-user setting. The dynamic task, as an example, refreshing and erasure have to expect with protection and security methods.

6. REFERENCES

[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] Cloud Security Alliance, ‘Security Guidance for Critical Areas of Focus in Cloud Computing,’ http://www.cloudsecurityalliance.org, 2009.

[3] R. Brinkman, ‘Searching in encrypted data,’ in University of Twente, PhD thesis, 2007.

[4] S. Kamara and K. Lauter, ‘Cryptographic cloud storage,’ in RLCPS, January 2010, LNCS. Springer, Heidelberg.

[5] A. Singhal, ‘Modern information retrieval: A brief overview,’ IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2001.

[6] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, ‘Secure knn computation on encrypted databases,’ in Proc. of SIGMOD, 2009.

[7] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, Jan. 2010.

[8] Zhihua Xia, Xinhui Wang, Xingming Sun, and Qian Wang, “A Secure and Dynamic Multi-keyword RankedSearch Scheme over Encrypted Cloud Data,” IEEE Transactions on Parallel and Cloud Systems, 2015

[9] KawserWazedNafi, TonnyShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem, “A Newer User Authentication, File encryption and Cloud Server Based Cloud Computing security architecture “Lecturer, Stamford University, Bangladesh, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[10] Chinua Xia, Xinhui Wang,” A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data”, DOI 10.1109/TPDS. 2401003, IEEE Transactions on Parallel and Cloud Systems, 2015.

[11] S. Deshpande, "Fuzzy keyword search over encrypted data in cloud computing",World Journal of Science and Technology, vol. 2, no. 10, (2013).

[12] D.X.Song,D. Wagner and A.Perrig,"Practical techniques for searches on encrypted data, In Security and Privacy", 2000. S&P 2000,IEEE, (2000).

[13] N. Cao,C. Wang, M. Li, K. Ren, and W. Lou,"Privacy-preserving multi-keyword ranked search over encrypted cloud data", INFOCOM, 2011 Proceedings IEEE, (2011).

[14] C. Wang, KuiRen, Shucheng Yu, Urs, K.M.R "Achieving usable and privacy-assured similarity search over outsourced cloud data", INFOCOM, 2012 Proceedings IEEE, (2012)

[15] Chi Chen, Xiaojie Zhu, “An Efficient Privacy-Preserving Ranked Keyword Search Method”, Member, IEEE, IEEE DOI 10.1109/TPDS.2425407, IEEE Transactions on Parallel and Cloud Systems, 2015.

[16] Yi Yang, Hongwei Li, Wenchao Liu, Haomiao Yao, Mi Wen,” Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost”, School of Computer Science and Engineering,

University of Electronic Science and Technology of China, Globecom - Communication and Information System Security Symposium, 2014.

[17] Chi Chen, Xiaojie Zhu, “An Efficient Privacy-Preserving Ranked Keyword Search Method”, Member, IEEE, IEEE DOI 10.1109/TPDS.2425407, IEEE Transactions on Parallel and Cloud Systems, 2015.

[18] Hongwei Li, Dongxiao Liu, Kun Jia, and XiaodongLinss“Achieving Authorized and Ranked MultikeywordSearch over Encrypted Cloud Data” School of Computer Science and Engineering, University of Electronic Science and Technology of China. IEEE ICC - Communication and Information Systems Security Symposium,2015

[19] Zhangjie Fu, KuiRen, JiangangShu, Xingming Sun “Enabling Personalized Search over Encrypted OutsourcedData with Efficiency Improvement”, DOI 10.1109/TPDS.2506573, IEEE Transactions on Parallel and Cloud System, 2015

[20] Wenhai Sun, Bing Wang, Ming Cao,”Privacy-preserving Multi-keyword Text Search in the Cloud SupportingSimilarity-based Ranking “asia ccs’13, May 8– 10, Hangzhou, China. Copyright 2013 acm 978-1-4503- 1767-2/13/05, 2013.

[21] KawserWazedNafi, TonnyShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem, “A Newer UserAuthentication, File encryption and Cloud Server Based Cloud Computing security architecture “Lecturer,Stamford University, Bangladesh, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012 [12] Chinua Xia, Xinhui Wang,” A Secure.