SRILEKHA G, et al, International Journal of Research Sciences and Advanced Engineering [IJRSAE]™
Volume 2, Issue 17, PP: 130 - 137, JAN - MAR' 2017.

PRIVACY PRESERVING MULTI-KEYWORD POSITIONED SEARCH OVER ENCRYPTED CLOUD DATA

G SRILEKHA 1*, SIVAIAH 2*

1. M.Tech, Dept of CSE, CMR College of Engg & Tech.
2. Assoc. Prof, Dept of CSE, CMR College of Engg & Tech.

ABSTRACT: Empowering pivotal word seek straightforwardly over encoded information is an attractive method for powerful use of scrambled information outsourced to the cloud. Existing arrangements give multikeyword accurate pursuit that does not endure pivotal word spelling slip, or single watchword fluffy inquiry that endures grammatical errors to certain degree. The ebb and flow fluffy inquiry plans depend on building an extended list that covers conceivable pivotal word incorrect spelling, which prompt essentially bigger list record size and higher pursuit multifaceted nature. In this paper, we propose a novel multikeyword fluffy pursuit conspire by abusing the territory touchy hashing method. Our proposed plan accomplishes fluffy coordinating through algorithmic outline as opposed to extending the record document. It likewise takes out the need of a predefined word reference and adequately bolsters numerous pivotal word fluffy pursuit without expanding the record or hunt multifaceted nature. Broad investigation and analyses on certifiable information demonstrate that our proposed plan is secure, productive and exact. To the best of our insight, this is the first work that accomplishes multi-essential word fluffy hunt over encoded cloud information.

Keywords: searchable encryption, secure cloud outsourcing, multi-decisive word positioned pursuit, homomorphic encryption.

1. INTRODUCTION

Distributed computing is the since quite a while ago imagined vision of figuring as an utility, where cloud clients remotely store their information into the cloud in order to appreciate the on-interest brilliant applications and administrations from a mutual pool of configurable processing assets. It's awesome adaptability and monetary funds are spurring both people and endeavors to outsource their nearby complex information administration framework into the cloud. To ensure protection of information and restrict spontaneous gets to in the cloud and past it, touchy information, for occasion, messages, individual wellbeing records, photograph collections, expense archives, et cetera, maymust be scrambled by information proprietors some time recently

Outsourcing to the business open cloud; this, then again, obsoletes the customary information usage administration in view of plaintext essential word look. The inconsequential arrangement of downloading all the information and decoding generally is obviously unrealistic, because of the extensive measure of transfer speed cost in cloud scale frameworks. Pictures additionally contain valuable and imperative data, so proposed framework likewise gives picture labeling in MRSE plan [1]. Besides, beside disposing of the nearby stockpiling administration, putting away information into the cloud doesn't fill any need unless they can be effortlessly looked and utilized.[2]Hence, investigating security saving and successful hunt benefit over scrambled cloud information is of extraordinary significance. Considering possibly enormous number of on-interest information clients and vast measure of outsourced information reports in the cloud, this issue is especially difficult as it is to a great degree hard to meet likewise the necessities of execution, framework ease of use, and versatility. Archive positioning is accommodated quick pursuit, however the needs of all the information reports is kept same so that the cloud administration supplier and outsider stays unconscious of the vital records, in this manner, keeping up protection of information. Positioned inquiry can likewise exquisitely wipe out pointless system activity by sending back just the most applicable information, which is very attractive in the "pay-as-you-utilize" cloud paradigm.[3] For security assurance, such positioning operation, be that as it may, ought not release any pivotal word related data. Plus, to enhance query output exactness and to upgrade the client seeking knowledge, it is additionally vital for such positioning framework to bolster numerous watchword look, as single essential word seek frequently yields excessively coarse results. As a typical practice demonstrated by today's web internet searchers (ex.

Google look), information clients may have a tendency to give an arrangement of decisive words rather than stand out as the pointer of their inquiry enthusiasm to recover the most significant information. Alongside the security of information and proficient looking plans, genuine security is gotten just if the client's personality stays avoided the Cloud Service Provider (CSP) and also the outsider client on the cloud server.

2. BACKGROUND AND RELATED WORK

Associations, organizations store more profitable data is on cloud to shield their information from infection, hacking. [4]The advantages of the new registering model incorporate however are not constrained to: alleviation of the inconvenience for capacity organization, information access, and evasion of high consumption on equipment system, programming, and so forth. Positioned pursuit enhances framework ease of use by typical coordinating documents in a positioned request in regards to certain importance criteria (e.g., essential word frequency),As specifically outsourcing pertinence scores will dribbles a considerable measure of touchy data against the pivotal word security, We proposed uneven encryption with positioning consequence of questioned information which will give just expected information.

A. Existing framework

Existing searchable encryption plans permit a client to safely seek over scrambled information through essential words without first decoding it, [8]these systems bolster just customary Boolean decisive word look, without catching any importance of the documents in the query output. At the point when specifically connected in huge collective information outsourcing cloud environment, they experience taking after weakness.

Disadvantages of existing framework

1. Single-decisive word look without positioning

2. Boolean-decisive word look without positioning

3. Single-decisive word look with positioning

4. Try not to get significant information.

3. PROBLEM FORMULATION

A. Proposed system

For our system, we choose the principle of coordinate matching, to identify the similarity between search query and data documents.Specially,we use inner data correspondence, i.e., the number of query keywords appearing in a document, to evaluate the similarity of that document to the search query in coordinate matching principle.[12]Each document is linked with a binary vector as a sub index where each bit represents whether corresponding keyword is contained in the document.[1] The search query is also described as a binary vector where each bit means whether corresponding keyword appears in this search request, so the similarity could be exactly measured by inner product of query vector with data vector. However, directly outsourcing data vector or query vector will violate index privacy or search privacy. To meet the challenge of supporting such multi-keyword semantic without privacy breaches, we propose a basic SMS scheme using secure inner product computation, which is adapted from a secure k-nearest neighbour (kNN) technique, and then improve it step by step to achieve various privacy requirements in two levels of threat models.

1) Showing the problem of Secured Multi-keyword search over encrypted cloud data

2) Propose two schemes following the principle of coordinate matching and inner product similarity.

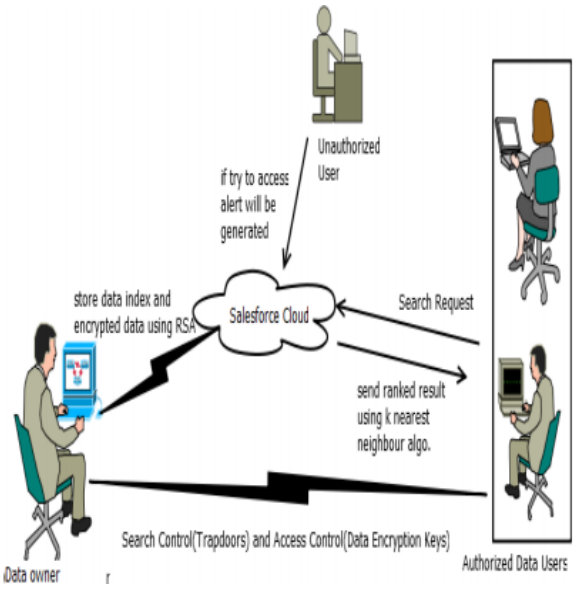


Fig1. Architecture of the search over encrypted cloud data

Considering three distinct substances, as delineated in Fig1. Information proprietor, information client, and

cloud server. Information proprietor has a gathering of information archives to be send to cloud server in the scrambled arrangement. To initiate the looking capacity over encoded information, information proprietor, before sending information, will first form a scrambled searchable indication (list), and after that outsource both the list and the scrambled report gathering to cloud server. To look the record, an approved client oblige a comparing trapdoor through pursuit systems, [13]Upon getting from information clients, cloud server is capable to look the file and return the relating arrangement of encoded records. natural harm too, since less power, aerating and cooling, Rackspace, et cetera, is needed for the same capacities. The expression "moving to cloud" likewise alludes to an association moving far from a customary CAPEX model (purchase the devoted equipment and devalue it over a stretch of time) to the OPEX model (utilize a mutual cloud framework and pay as you utilize it). Advocates guarantee that distributed computing permits organizations to stay away from forthright framework expenses, and concentrate on ventures that separate their organizations rather than foundation. Advocates likewise guarantee that distributed computing permits endeavors to get their applications up and running quicker, with enhanced sensibility and less upkeep, and empowers IT to all the more quickly alter assets to meet fluctuating and eccentric business request.

3.1 Multi-Keyword Ranked Search over Encrypted (MRSE)

Distributed computing is the since quite a while ago imagined vision of registering as an utility, where cloud clients can remotely store their information into the cloud in order to appreciate the on-interest brilliant applications and administrations from a common pool of configurable figuring assets. Its awesome adaptability and monetary investment funds are rousing both people and endeavors to outsource their nearby complex information administration framework into the cloud. To ensure information security and battle spontaneous gets to in the cloud and past, delicate information, for instance, messages, individual wellbeing records, photograph collections, expense archives, monetary exchanges, etc, may must be encoded by information proprietors before outsourcing to the business open cloud; this, be that as it may, obsoletes the conventional information usage administration in light of plaintext catchphrase look.

The minor arrangement of downloading all the information and unscrambling generally is obviously unrealistic, because of the immense measure of data transfer capacity cost in cloud scale frameworks. In addition, beside disposing of the nearby stockpiling administration, putting away information into the cloud fills no need unless they can be effortlessly sought and used. In this way, investigating protection safeguarding and viable pursuit benefit over encoded cloud information is of foremost significance. Considering the conceivably vast number of on-interest information clients and colossal measure of outsourced information reports in the cloud, this issue is especially difficult as it is to a great degree hard to meet additionally the necessities of execution, framework ease of use, and versatility. From one perspective, to meet the powerful information recovery require, the huge measure of records request the cloud server to perform result importance positioning, rather than returning undifferentiated results. Such positioned inquiry framework empowers information clients to locate the most pertinent data rapidly, as opposed to burdensomely dealing with each match in the substance gathering. Positioned inquiry can likewise carefully kill pointless system movement by sending back just the most applicable information, which is exceedingly attractive in the "pay-as-you-utilize" cloud ideal model. [14]For security insurance, such positioning operation, nonetheless, ought not release any decisive word related data. Then again, to enhance the query output exactness and additionally to improve the client seeking knowledge, it is likewise vital for such positioning framework to bolster different pivotal words look, as single decisive word look frequently yields dreadfully coarse results. As a typical practice demonstrated by today's web indexes (e.g., Google seek), information clients may have a tendency to give an arrangement of essential words rather than stand out as the marker of their hunt enthusiasm to recover the most applicable information. Furthermore, each essential word in the hunt solicitation has the capacity help tight down the query item encourage. "Direction coordinating", whatever number matches as could be allowed, is a proficient likeness measure among such multi-magic word semantics to refine the outcome importance, and has been generally utilized as a part of the plaintext data recovery (IR) group. [16]However, how to apply it in the scrambled cloud information seek framework remains an extremely difficult errand due to natural security and protection hindrances, including different strict prerequisites like the information security, the list protection, the decisive word security, and numerous

others. Encryption is a useful method that regards scrambled information as records and permits a client to safely seek through a solitary watchword and recover reports of hobby. Nonetheless, coordinate use of these ways to deal with the safe huge scale cloud information usage framework would not be fundamentally suitable, as they are created as crypto primitives and can't oblige such high administration level necessities like framework convenience, client looking knowledge, and simple data revelation. Albeit some late plans have been proposed to bolster Boolean watchword look as an endeavor to enhance the pursuit adaptability, they are still not sufficient to furnish clients with satisfactory result positioning functionality.[17] Our initial works have been mindful of this issue, and give answers for the safe positioned inquiry over scrambled information issue yet just for questions comprising of a solitary pivotal word. Step by step instructions to outline a productive encoded information seek component that backings multi-catchphrase semantics without protection ruptures still remains a testing open issue.

In the undertaking, surprisingly, characterize and tackle the issue of multi-magic word positioned inquiry over encoded cloud information (MRSE) while saving strict framework savvy security in the distributed computing standard. Among different multi-decisive word semantics, pick the productive comparability measure of "direction coordinating," i.e., however many matches as could reasonably be expected, to catch the importance of information records to the pursuit inquiry. In particular, internal item comparability the quantity of inquiry essential words showing up in a report, to quantitatively assess such similitude measure of that archive to the hunt question. Amid the record development, every report is connected with a double vector as a sub-list where every bit speaks to whether comparing essential word is contained in the archive. The hunt question is likewise portrayed as a double vector where every bit implies whether comparing essential word shows up in this pursuit demand, so the similitude could be precisely measured by the inward result of the inquiry vector with the information vector. Be that as it may, straightforwardly outsourcing the information vector or the inquiry vector will damage the record protection or the hunt security. To meet the test of supporting such multi pivotal word semantic without protection ruptures, we propose an essential thought for the MRSE utilizing secure inward item calculation, which is adjusted from a safe k-closest neighbor (kNN) procedure, and after that give two fundamentally enhanced MRSE conspires in a regulated way to accomplish different stringent protection prerequisites in two danger models with expanded assault capacities. Our commitments are outlined as takes after:

1. Interestingly, we investigate the issue of multi pivotal word positioned hunt over encoded cloud information, and set up an arrangement of strict protection necessities for such a safe cloud information use framework.

2. We propose two MRSE plans in light of the comparability measure of "direction coordinating" while meeting diverse protection necessities in two distinctive danger models.

3. We research some further improvements of our positioned inquiry system to bolster more pursuit semantics and element information operations

4. Careful examination researching security and productivity sureties of the proposed plans is given, and trials on this present reality information set further demonstrate the proposed plans without a doubt present low overhead on reckoning and correspondence.

Contrasted and the preparatory adaptation of this paper, this diary variant proposes two new instruments to bolster more hunt semantics. This variant likewise mulls over the backing of information/list motion in the component plan. Besides, we enhance the exploratory works by including the examination and assessment of two new plans. Notwithstanding these enhancements, we include more examination secure inward item and the protection part.

System Architecture:

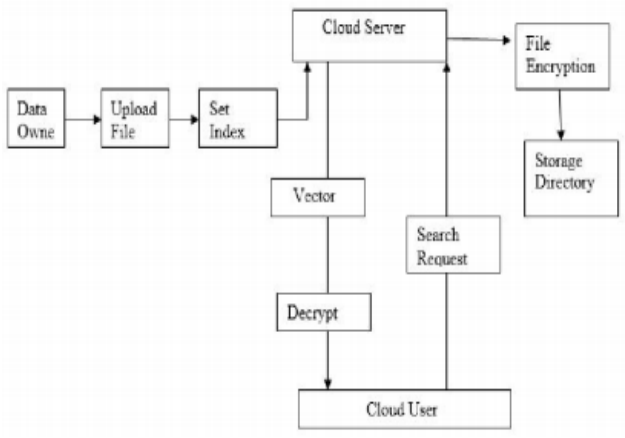


Fig.2 Architecture diagram of the MRSE Implementation.

4. MRSE FRAMEWORK

For simple presentation, operations on the information records are not demonstrated in the system since the information proprietor could without much of a stretch utilize the customary symmetric key cryptography to encode and after that outsource information. With spotlight on the file and question, the MRSE framework comprises of four calculations as takes after

1. Setup(t)

Taking a security parameter ℓ as info, the information proprietor yields a symmetric key as

2. BuildIndex(F, SK)

Taking into account the dataset F, the information proprietor assembles a searchable list I which is scrambled by the symmetric key SK and afterward outsourced to the cloud server. After the list development, the report accumulation can be autonomously encoded and outsourced.

3. Trapdoor(fW)

With t watchwords of enthusiasm for fW as info, this calculation produces a comparing trapdoor TfW.

4. Query (TfW, k, I)

At the point when the cloud server gets a question ask for as (TfW, k), it performs the positioned inquiry on the record I with the assistance of trapdoor TfW, lastly returns FfW, the positioned id rundown of top-k reports sorted by their likeness with fW.

A. Security and Privacy Requirements for MRSE Framework

The delegate security ensure in the related writing, for example, searchable encryption, is that the server ought to learn only list items. With this general protection depiction, we investigate and set up an arrangement of strict security prerequisites particularly for the MRSE system. Concerning the information security, the information proprietor can fall back on the conventional symmetric key cryptography to encode the information before outsourcing, and effectively keep the cloud server from prying into the outsourced information. Regarding the list protection, [9][10] if the cloud server reasons any relationship in the middle of watchwords and scrambled records from list, it may take in the significant subject of an archive, even the substance of a short report. In this way the searchable file ought to be built to keep the cloud server from performing such sort of affiliation assault. While information and list protection sureties are requested of course in the related writing, different pursuit security prerequisites included in the question technique are more intricate and hard to handle as takes after.

Keyword Privacy:

As clients ordinarily want to keep their hunt from being presented to others like the cloud server, the most imperative concern is to cover up what they are seeking, i.e., the watchwords demonstrated by the comparing trapdoor. In spite of the fact that the trapdoor can be created in a cryptographic manner to secure the inquiry decisive words, the cloud server could do some factual examination over the query item to make an evaluation As customers customarily need to keep their chase from being introduced to others like the cloud server, the most basic concern is to conceal what they are looking for, i.e., the watchwords exhibited by the contrasting trapdoor. Disregarding the way that the trapdoor can be made in a cryptographic way to secure the request unequivocal words, the cloud server could do some verifiable examination over the question thing to make an assessment

Trapdoor Unlinkability:

The trapdoor era [5] [6] capacity ought to be a randomized as opposed to being deterministic. Specifically, the cloud server ought not to have the capacity to derive the relationship of any given trapdoors, e.g., to figure out if the two trapdoors are shaped by the same hunt demand. Something else, the deterministic trapdoor era would give the cloud server favorable position to amass frequencies of diverse hunt solicitations with respect to distinctive keyword(s), which may further damage the previously stated catchphrase protection prerequisite. So the key assurance for trapdoor Unlinkability is to bring adequate no determinacy into the trapdoor era technique.

Access Pattern:

Inside of the positioned pursuit, the entrance example is the grouping of list items where each query item is a

situated of records with rank request. In particular, the item for the question pivotal word set fW is meant as FfW, comprising of the id rundown of all archives positioned by their significance to fW. At that point the entrance example is meant as (FfW1, FfW2 , . . .) which are the consequences of successive pursuits. In spite of the fact that a couple of searchable encryption meets expectations, e.g., [11] has been proposed to use private data recovery (PIR) strategy [28], to shroud the entrance design, our proposed plans are not intended to secure the entrance design for the effectiveness concerns. This is on account of any PIR based procedure must "touch" the entire dataset outsourced on the server which is wasteful in the huge scale cloud framework

In our more propelled configuration, rather than basically evacuating the amplified measurement in the inquiry vector as we plan to do at the first look, we safeguard this measurement broadening operation yet allocate another arbitrary number t to the expanded measurement in every question vector. Such a recently added irregularity is required to build the trouble for the cloud server to take in the relationship among the got trapdoors. Moreover, as specified in the essential word security necessity, [7] irregularity ought to likewise be painstakingly balanced in the output to muddle the report recurrence and decrease the chances for re-recognizable proof of catchphrases. Presenting some irregularity in the last comparability score is a successful way towards what we expect here. All the more particularly, dissimilar to the arbitrariness included in the inquiry vector, we embed a sham decisive word into every information vector and dole out an irregular worth to it. Every individual vector Di is reached out to (n+2)- measurement rather than (n + 1), where an arbitrary variable εi speaking to the sham pivotal word is put away in the broadened measurement.

The entire plan to accomplish positioned pursuit with various magic words over encoded information is as per the following.

1. Setup The information proprietor arbitrarily creates a (n + 2)- bit vector as S and two (n+2)×(n+2) invertible grids {M1,M2}. The mystery key SK is as a 3-tuple as {S, M1, M2}.

2. Construct Index(F, SK) The information proprietor creates a double information vector Di for each archive Fi, where every paired bit Di[j] speaks to whether the comparing decisive word Wj shows up in the record Fi. In this manner, each plaintext sub record $\vec{}$D i is produced by applying measurement amplifying and part methodology on Di. These systems are comparable with those in the protected kNN processing aside from that the (n + 1)- th passage in $\vec{}$D i is situated to an arbitrary number εi, and the (n + 2)- th section in $\vec{}$D i is situated to 1 amid the measurement developing. $\vec{}$D I is consequently equivalent to (Di, εi, 1). At long last, the sub file is constructed for each encoded archive Ci.

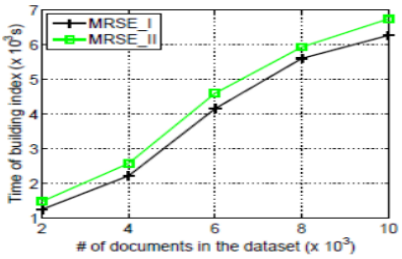
3. Trapdoor (fW) With t magic words of enthusiasm for fW as information, one double vector Q is created where every bit Q[j] shows whether Wj ∈ fW is genuine or false. Q is initially stretched out to n + 1- measurement which is situated to 1, and after that scaled by an arbitrary number r≠ 0, lastly reached out to a (n + 2)- measurement vector as $\vec{}$Q where the last measurement is situatdom number t. $\vec{}$Q is along these lines equivalent to (rQ, r, t). In the wake of applying the same part and encoding procedures as over, the trapdoor TfW is created as

4. Query (TfW, k, I) With the trapdoor TfW, the cloud server figures the similitude scores of every archive Fi as in comparison 1. WLOG, we expect r > 0. In the wake of sorting all scores, the cloud server gives back the top-k positioned id list FfW. $\vec{}$ Note that in the first case, the last score is just

B. Efficiency Analysis

1) Index Construction: To fabricate a searchable sub file Ii for every archive Fi in the dataset F, the first step is to delineate catchphrase set removed from the record Fi to an information vector Di, took after by scrambling each information vector. The time expense of mapping or scrambling depends straightforwardly on the dimensionality of information vector which is controlled by the span of the word reference, i.e., the quantity of recorded decisive words. Furthermore, the time expense of building the entire record is likewise identified with the quantity of sub list which is equivalent to the quantity of archives in the dataset. Fig. 2(a) demonstrates that, given the same word reference where |W| = 4000, the time expense of building the entire list is almost direct with the extent of dataset since the time expense of building every sub list is altered. Fig. 2(b) demonstrates that the quantity of magic words recorded in the lexicon decides the time expense of building a sub file. The real reckoning to produce a sub list in MRSE I includes the splitting

process and two multiplications of a (n + 2) × (n + 2) matrix and a (n + 2) 2)



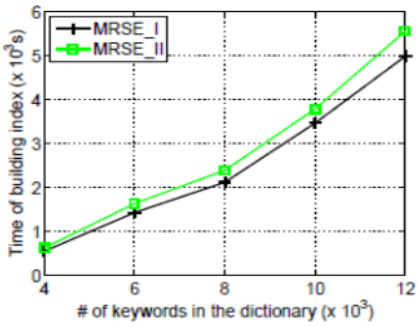


Fig. 3 a) Time cost of building Index for n=4000

b) Time cost of building Index for m=1000

Trapdoor Generation: Fig. 4(a) demonstrates that the time to create a trapdoor is significantly influenced by the quantity of decisive words in the lexicon. Like record development, each trapdoor era brings about two augmentations of a lattice and a split inquiry vector, where the dimensionality of network or question vector is diverse in two proposed plans and gets to be bigger with the expanding size of word reference. Fig. 3(b) exhibits the trapdoor era cost in the MRSE II plan speaks the truth 20 rates bigger than that in the MRSE I conspire. Like the sub record era, the distinction of expenses to produce trapdoors is majorly brought about by the diverse dimensionality of vector and frameworks in the two MRSE plans. All the more vitally, it demonstrates that the quantity of question decisive words has little impact on the overhead of trapdoor era, which is a critical point of preference over related chips away at multi-catchphrase searchable encryption.

Fig. 4(a) Time cost of generating trap door for t= 10

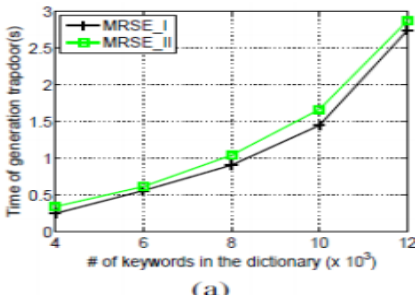
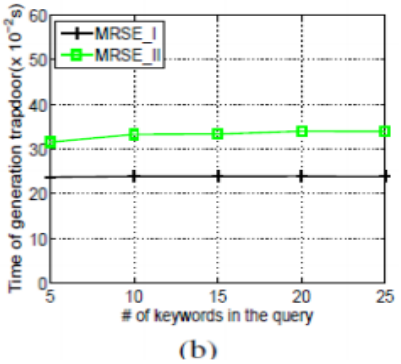


Fig. 4(a) Time cost of generating trap door for t= 10



4 (b) for different number of query keywords n= 4000

3) Query: Query execution in the cloud server consists of computing and ranking similarity scores for all documents in the dataset. Fig. 6 shows the query time is dominated by the number of documents in the dataset while the number of keywords in the query has very slight impact on it like the cost of trapdoor generation above

V. CONCLUSION

In this paper, we propose a light-weight pursuit approach that backings proficient multi-pivotal word positioned hunt in distributed computing framework. Our essential plan utilizes the polynomial capacity to conceal the encoded magic word and quest examples for productive multi-decisive word positioned inquiry. We then enhance the essential plan and propose a protection safeguarding plan which uses the safe internal item technique for securing the protection of the looked multi-magic words. Intensive examination on the security surety of our proposed plans is given, and broad investigations taking into account this present reality dataset are additionally led. The analysis results exhibit that our plan can empower the scrambled multi-watchword positioned hunt administration with high proficiency in distributed computing.

REFERENCES

[1] IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014 Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data Ning Cao, Member, IEEE, Cong Wang, Member, IEEE, Ming Li, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE.

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

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

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

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

[8] E. J. Goh, "Secure Indexes," Cryptology ePrint Archive, http://eprint.iacr.org/2003/216. 2003.

[9] Y. C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[10] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.

[11] 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.

[12] M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and Efficiently Searchable Encryption," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '07), 2007.

[13] 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.

[14] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[15] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W.E.S. III, "Public Key Encryption That Allows PIR Queries," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '07), 2007.

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

[17] 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.