International Conference on Modern Trends in Engineering Science and Technology
© 2019 IJSRSET | Volume 5 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Survey on Efficient Searching in Encrypted Cloud Data

Abhishek Nimonkar[1], Mukul Wagh[1], Payal Kale[1], Pranali Bajirao[1], Yash Nathani[1], Prof. A.V. Dehankar[2]
[1]BE Student, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India
[2]Assistant Professor, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

Cloud computing is an on-request for computing. It is Internet-based computing. Around there shared resources, data and information are given on demand to PCs and distinctive devices. It also gives the organizations over the web. In conveyed computing, pro associations have the ability to give storing at the server according to customers requirements. They allow customers to store and recoup the data in cloud server on demand from wherever and on a device. This control of data at cloud server offers climb to such an assortment of security issues since data is gotten to over web. For security, reason data is stored in encoded sorted out. In this, the client has no prompt control over data once it is exchanged on a cloud server. In this paper, we look at the idea behind single watchword chase over encoded data and besides multi catchphrase situating. Cloud data proprietors require their records in a mixed edge with the true objective of security sparing. Thusly it is essential to make productive and strong ciphertext look for frameworks. One test is that the association between records will be usually shrouded amid the time spent encryption, which will provoke basic request exactness execution degradation.

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

I. INTRODUCTION

As we adventure into the huge data time frame, terabyte of data is made in general each day. In the late 1960's the likelihood of "Utility computing" that was wrote by MIT PC researcher and Turing gift champ John McCarthy was in a perfect world known as appropriated computing over a framework. Ventures were searching for some sort of critical course of action, since utility computing ended up getting the chance to be something of a noteworthy business for associations, for instance, IBM. Undoubtedly, Martin Greenberger pointed out the possibility that "bleeding edge arithmetical machines without limits" were right now being used institutionally for coherent figuring and research just as for business limits, for instance, accounting and stock. Advance, he predicted his bit of work in which PCs would be far-reaching essentially like the genuine power associations running wires wherever in due time. Tries and customers who have a great deal of data usually redistribute their important data to cloud office with an explicit true objective to reduce data organization cost and storeroom spending. Consequently, data volume in circulated stockpiling workplaces is experiencing an enthusiastic augmentation. In spite of the way that cloud server providers (CSPs) ensure that their cloud organization

is equipped with strong wellbeing endeavors, security and assurance are genuine blocks keeping the more broad affirmation of circulated computing organization [1]. An ordinary way to deal with decline information spillage is data encryption. Nevertheless, this will make server-side data use, for instance, looking on encoded data, transform into an extraordinarily troublesome task. In the present years, examiners have proposed various ciphertext look for plans by joining the cryptography techniques. These procedures have been shown with provable security, yet their methodologies require tremendous tasks and have high time multifaceted nature. Subsequently, past procedures are not proper for the tremendous data circumstance where data volume is colossal and applications require online data taking care of. Likewise, the association between chronicles is canvassed in the above methodologies. The association between reports addresses the properties of the documents and therefore keeping up the relationship is basic to totally express a record. For example, the relationship can be used to express its grouping. In case a record is independent of some different reports beside those chronicles that are related to diversions, at that point it is straightforward for us to express this file has a place with the grouping of the amusements. On account of the outwardly debilitated encryption, this indispensable property has been canvassed in the standard techniques. Subsequently, proposing a technique which can keep up and utilize this relationship to speed the interest organize is charming. On the other hand, in light of programming/hardware dissatisfaction, and limit corruption, data list things returning to the customers may contain hurt data or have been bent by the vindictive director or gatecrasher. As such, an irrefutable instrument should be given to customers to check the precision and climax of the rundown things. On account of a dynamic change in the field of undertakings over past decade, there has been augmentation looked for after of redistributing of data over a broad assortment of framework. With an explicit true objective to control this huge proportion of data in fiscally sagacious way adventure has balanced a dominating advancement considered appropriated computing that oust the heaviness of data organization. In this data-driven condition attempt will in general store their data onto cloud that includes gainful asset of customer data like messages, singular prosperity data, etc. Appropriated computing is winding up being most basic perspective in the enhancement of information development which offer versatile get to, inescapable, on demand get to and capital utilization saving.

II. LITERATURE REVIEW

Qin Liu et al. proposed Secure and insurance sparing catchphrase look for in [1]. It gives watchword assurance, data insurance and semantic secure by open key encryption. The standard issue of this interest is that the correspondence and computational expense of encryption and translating is more.

Ming Li et al. proposed Authorized Private catchphrase Search (APKS) in [2]. It gives watchword security, Index and Query Privacy, Fine-grained Search Authorization and Revocation, Multi-dimensional Keyword Search, Scalability and Efficiency. This chase method fabricates the request viability using attribute chain of significance yet eventually all of the qualities are not dynamic.

Cong Wang et al in [3] proposed Secure and Efficient Ranked Keyword Search which comprehends getting ready overhead, data and catchphrase assurance, minimum correspondence and count overhead. It isn't significant for various catchphrase looks for, Also there is a tiny bit of overhead in record building.

Kui Ren et al. [4] proposed Secured fleecy catchphrase look for with symmetric searchable encryption (SSE). It doesn't reinforce soft interest with open key based searchable encryption; in like manner it can't play out different watchwords semantic chase. The updates for

cushy searchable rundown are not adequately performed.

Ming Li et al. [5] proposed Privacy ensured searchable appropriated stockpiling method. It is executed using SSE, Scalar-Product-Preserving Encryption and Order-Preserving Symmetric Encryption. It reinforces the security and valuable necessities. This arrangement does not support open key based searchable encryption.

Wei Zhou et al. [6] proposed K-gram based fleecy watchword Ranked Search. In this proprietor make k-gram feathery watchword list for records D and tuple <I, D> is exchanged to request server (SS) which is installed to grow channel for size controlling. The encoded record D is exchanged to limit server. Notwithstanding, the issue is that, the proportion of the k-gram build cushioned catchphrase set depends as for the jacquard coefficient regard.

J. Baek et al. in [7] proposed Secure Channel Free Public Key Encryption with Keyword Search (SCF-PEKS) methodology. In these system cluster servers makes its own open and private key match yet this method encounters outside assailant by KGA.

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

Peng Xu et al. [9] proposed Public-Key Encryption PEFKS with Fuzzy Keyword Search, in this customer makes feathery catchphrase trapdoor Tw and right watchword trapdoor Kw for W. Customer requests Tw to CS. By then CS checks Tw with cushy watchword list and sends superset of planning figure messages by Fuzz Test estimation that is executed by CS. The customer method Exact Test count for affirming ciphertexts with Kw and recoup the mixed records. The path toward making soft watchword list and right catchphrase list is troublesome for gigantic size database.

Ning et al. [10] proposed Privacy Preserving Multi Keyword Ranked Search (MRSE). It is important for realized figure content model and establishment show over encoded data. It gives low count and correspondence overhead. The encourage organizing is picked for multi-catchphrase look for. The drawback is that MRSE have minimal standard deviation which diminishes the watchword security.

III. RELATED WORK

A. Secure and privacy preserving keyword search

Qin Liu [16] proposed in this paper the request that gives catchphrase insurance, data assurance and semantic secure by open key encryption. CSP is incorporated into partial decipherment by decreasing the correspondence and computational raised in unraveling process for end customers. The customer's available the watchword trapdoor encoded by users‟ private key to CS (Cloud Server) securely and recoup the mixed reports.

B. Secure and Efficient Ranked Keyword Search

Cong Wang [17] proposed look which enlightens taking care of overhead, data and watchword assurance, slightest correspondence and estimation raised. The data proprietor amass document close by the catchphrase repeat based significance scores for records. Customer requests “w” to cloud server with optional "k‟ as Tw using the private key. The cloud server looks for the record with scores and sends encoded archive in light of situated progression.

C. Single Keyword Search Over Encrypted data on cloud

Practical searchable encryption plot consent to a customer to determinedly search for over mixed data through catchphrases without first applying deciphering on it, the proposed strategies reinforce

simply normal Boolean watchword look, without getting any real nature of the documents in the thing. Right when clearly associated in enormous joint data redistributing cloud condition, they encounter next inadequacy.

D. Privacy-preserving Multi-keyword Text Search

Wenhai Sun [19] proposed this request gives similarity based thing situating, catchphrase security, Index and Query protection and Query Unlink limit. The encoded archive is worked by vector space demonstrate supporting hardened and specific record look. The searchable record is collected using Multidimensional B tree. Proprietor makes mixed request vector $\bar{Q}$ for record watchword set. The customer gets the individual mixed inquiry vector of W from proprietor which is given to CS. Directly CS looks list by Merkle– Damgård advancement estimation and ponders cosine proportion of archive and request vector and returns best k encoded records to the customer.

E. Secure Multi-keyword Top-k Retrieval Search

Jiadi [20] proposed this interest using Two round searchable encryption (TRSE). In the first round, customers present different catchphrase "REQ" 'W‟ as a mixed request for satisfying data, watchword security and make trapdoor (REQ, PK) as Tw and send to the cloud server. By then cloud server finds out the score from the encoded document for records and returns the mixed score result vector to the customer. In the second round, customer unravels N with riddle key and figures the archive situating and after that request records with Top k scores. The situating of the archive is done on the client side and scoring is done on the server side.

F. Privacy Preserving Multi-Keyword Ranked Search (MRSE)

Ning [21] proposed this output for realized figure content model and establishment show over mixed data giving the low count and correspondence overhead. At that point organize planning is chosen for multi-watchword looks for. They used internal thing resemblance to quantitatively evaluate equivalence for situating records. The drawback is that MRSE has minimal standard deviation σ which incapacitates catchphrase security.

G. Attribute-based Keyword Search

Wenhai Sun [22] proposed Attribute-based Keyword Search that gives conjunctive watchword look for; catchphrase semantic security and Trapdoor unlink limit. The proprietors make list with all watchwords and get the chance to list with the course of action a characteristic which demonstrates the customer's list endorsed for looking for. Directly proprietors scramble the report, list with getting too rundown using ciphertext approach property based encryption technique. To have a customer investment organization, they used go-between re-encryption and lazy re-encryption procedures to share the outstanding burden to CS. The customer requests the Tw to CS using its private key. By and by CS recoups Tw and chases the encoded records and return documents just if the client's characteristics in Tw satisfies get to approaches in records which makes coarse-grained dataset look for endorsement.

H. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data

This proposed method has portrayed and handled the issue of convincing anyway shielded and sound position watchword look for over Encrypted cloud data [23]. Situated look immensely overhauls structure convenience by giving back the organizing documents in a situated mastermind as for certain fundamental criteria (for example watchword repeat) along these lines making one phase closer towards reasonable usage of secure data encouraging organizations in Cloud Computing. These papers have portrayed and handled the testing issue of security sparing and productive multi watchword situated look for over mixed cloud data accumulating (MRSE), and set up a game plan of strict security necessities for such a guaranteed cloud data use the system to twist

up unmistakably a reality. The proposed situating procedure ends up being productive to retreat to an extraordinary degree essential files contrasting with submitting a look for terms. The proposed situating system is used as a piece of our future structure with an explicit true objective to enhance the security of information on Cloud Service Provider.

I. A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data

This proposed system [24] suggest an ensured tree-based chase plan over the encoded appropriated stockpiling, which reinforces multi watchword situated look for close by a component task on report gathering open at the server. The vector space model and term repeat (TF) × inverse file repeat (IDF) demonstrate are commonly used as a piece of the advancement of document and period of request to give multi watchword situated look for yield. To get high-interest capability comes to fruition, maker builds up a tree-based record structure and proposed a Greedy Depth-first Search figuring in perspective of this rundown tree. In light of this unprecedented structure of tree-based record, the proposed look plan can adaptably achieve sub straight request time and can effectively deal with the deletion and expansion of chronicles. The kNN figuring is associated with scramble the record and request vectors and till then certification exact congruity score check between encoded rundown and question vectors.

IV. CONCLUSIONS

This paper concentrates diverse procedures of looking in the encoded cloud data stockpiling. We have methodically presents the security and data use issues in the appropriated stockpiling related to all open looking for methodology. Thus recognized the essential issues that are to be satisfied for secured data utilize are catchphrase assurance, Data security, Index security, Query Privacy, Fine-grained Search, Scalability, Efficiency, Result situating, Index mystery, Query grouping, Query Unlinkability, semantic security and Trapdoor Unlinkability. By far most of the looking systems for the most part focus on security and some on data utilize. The obstacles of all the looking for strategies are also discussed. By the above survey, security can be given by Public-Key Encryption and capable data use by soft catchphrase look. We assume that this review will make the pros to shape their issue in the scope of data use in conveyed stockpiling.

V. 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] 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

[16] 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

[17] 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

[18] International Journal of Computer Applications (0975 –887) Volume 126 – No.14, September 2015

[19] Wenhai Sun et al., "Privacy-Preserving Multikeyword Text Search in the Cloud Supporting Similarity-based Ranking", the 8th ACM Symposium on Information, Computer and Communications Security, Hangzhou, China, May 2013.

[20] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue,Member, IEEE Computer Society, and Minglu Li,"Toward Secure Multikeyword Top k Retrieval over Encrypted Cloud Data", IEEE Journal of Theoretical and Applied Information Technology 10th August 2014.

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

[22] Wenhai Sun et al., "Protecting Your Right: Attributebased Keyword Search with Finegrained Ownerenforced Search Authorization in the Cloud", IEEE INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014

[23] Secure Ranked Keyword Search over Encrypted Cloud Data, IEEE PAPER, 2010.

[24] Zhihua Xia, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL: PP NO: 99 YEAR 2015

Cite this article as :

Abhishek Nimonkar, Mukul Wagh, Payal Kale, Pranali Bajirao, Yash Nathani, Prof. A.V. Dehankar, "A Survey on Efficient Searching in Encrypted Cloud Data", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), ISSN : 2456-3307, Volume 5 Issue 5, pp. 22-27, February 2019. Journal URL : http://ijsrset.com/IJSRSET195505