International Journal of Science Engineering and Advance Technology

Achieving Privacy and Security In Multi Owner Cloud Using Novel Secure Search Protocol And AES

[1]V.B.T.Rajeswari, [2]R.Srinivas
[1,2]Dept. of CSE, Aditya Institute of Science & Technology, Surampalem, Kakinada, E.G.dt, AP, India.

Abstract - Cloud computing provide benefits of individual users and organizations which minimizes investment and resource usage cost. Data owners forwarding the data to cloud servers without local data management and data users retrieving the data from cloud. Privacy and security considerations earlier research done only single owner model along with secure search. To download all the encoded information and decrypt them locally. Be that as it may, this technique is clearly unrealistic on the grounds that it will bring about a colossal measure of correspondence overhead. Positioned multi-keyword search will cause substantial calculation and capacity costs.Existing schemes are incurring more communication overhead for secure search and these are supporting only single owner model. We present multi owner model with privacy preserving ranked multi-keyword search for re-encrypted cloud data by using AES 256 bit provides privacy of data, keywords and trapdoors. A novel dynamic secret key generation protocol is used to prevent attackers from secret key the fting and acting as valid user. Propose approaches minimizes computation and storage cost along with secure search.

Index Terms -Ranked keyword searches, multiple owners, privacy preserving, and dynamic secret key

1 INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet)[1]. The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Secure inquiry over encoded information has as of late pulled in light of a legitimate concern for some scientists. Cloud service suppliers (CSPs) would guarantee to guarantee proprietors' information security utilizing componentslike virtualization and firewalls. In any case, these mechanisms don't assure owners' advice aegis from the CSP itself, back the CSP has abounding ascendancy of billow equipment, programming, and proprietors' information. We adduce affairs to administer Privacy extenuative Ranked Multi-keyword Search in a Multi-proprietor archetypal (PRMSM). To empower billow servers toaccomplish defined following after alive the 18-carat advice of bothkeywords and trapdoors, we calmly advance a typical defended analysis convention. To rank theindexed lists and aegis the aegis of acceptationarray amid keywords and records, we adduce a typical Additive Order and Privacy Preserving function family.

2LITERATURE SURVEY

2.1 Searchable Encryption

Curtmola et[2] al. propose building records for each keyword, and use hash tables as a choice approach to manage searchable encryption. The main open key plan for catchphrase look over encoded information is displayed in and further improves the pursuit functionalities of searchable encryption by proposing plans for conjunctive keyword seek. The searchable encryption thinks for the most part about single catchphrase pursuit or Boolean keyword search. The keyword search over encrypted data using public key is presented in [3]. [4] And [5] further enrich the search functionalities of searchable encryption by proposing schemes for conjunctive keyword search.

Encryption helps cautious client information secrecy; it leaves the well-working yet basically effective secure pursuit capacities over encoded information a requesting issue. In this paper, we display a self-evident security saving multi-catchphrase content pursuit (MTS) plan with closeness based positioning to address this issue. To hold up multi-keyword search and query output positioning, we propose to fabricate the hunt list in light of term recurrence and the vector space model with cosine similitude figures to accomplish higher item rightness. To improve the pursuit productivity, we propose a tree-based record structure and

different versatile techniques for multi-dimensional (MD) algorithm so that the sensible hunt ability is vastly improved than that of linear search.

2.2 Secure Keyword Search in Cloud Computing

The Study on secure keyword inquiry are roused by the protection worries in cloud computing. Wang et al. The encrypted information over secure keyword search should be understand and characterize. In [6] The single keyword inquiry get the significant top-k documents by the proposed plan. Cao et al. [7], [8], and Sun et al. , [9] The multi-keyword inquiries are reached out by the protected keyword search. Their methodologies vectorize the rundown of catchphrases and apply grid augmentations to conceal the real keyword data from the cloud server. To discover top-k important date documents the server is still permitted. The element catchphrase word reference empowered by the proposed MKQE (Multi-Keyword positioned Query on Encrypted information) to evades the positioning request being twisted by a few high recurrence keywords [10] encoded cloud information going for resilience of both minor grammatical mistakes and organization irregularities for client's pursuit contribution by the proposed fluffy catchphrase. Further proposed security guaranteed similitude look components over outsourced cloud information. In geo-distributed cloud environment we proposed a protected, productive, and disseminated keywords search protocol. The information proprietor is considered by the past work of the framework show that infers in their answers. The information proprietor and information clients can without much of a stretch impart and trade mystery data. At the point when various information proprietors are included in the framework that causes the mystery data trading the extensive correspondence overhead. Secure attribute-based keyword search plans in the testing situation where numerous proprietors are included. Issues may emerge by applying the CPABE into the cloud framework for date client disavowal. i.e., need to upgrade the vast measure of information put away on it for an information client repudiation. Also, No backing to the protection saving positioned multi-keyword search. Framework model are totally contrast from the past studies with respect to the accentuation of various information proprietors. The parer anticipating that the arrangement plan should maximally unwind the necessities for information proprietors and clients, the distributed computing clients are extremely reasonable plan for the substantial number.

2.3 Order Preserving Encryption

The request protecting encryption is utilized to keep the cloud server from knowing the definite significance scores of catchphrases to an information file. The early work of Agrawal et al. proposed an Order Preserving symmetric Encryption (OPE) plan where the numerical request of plain messages is protected [11]. Boldyreva et al. further presented a particular request saving encryption in [12]. Yi et al [13] proposed a request protecting capacity to encode information in sensor systems. Pope et al. [14] as of late proposed a perfect secure request saving encryption plan. Kerschbaumet al. [15] The proposed plan is not just secure thought by it effective for request safeguarding encryption plan. Notwithstanding, those are not dependent by request safeguarding. As a correlative work to the past request safeguarding work, we propose another added substance request and security protecting capacities (AOPPF). The proprietors are effectively pick any capacities from the AOPPE family to encode their pertinence scores. The entirety of encoded significance scored and positions processes by the cloud server.

3 PROPOSED APPROACH

We deliberately develop a novel secure search protocol, which not just empowers the cloud serverto perform secure positioned keyword searchwithout knowing the genuine information of bothkeywords and trapdoors, additionally permitsinformation owners to re-encode information withwatchwords with self-picked keys and permitsvalidated information clients to question withoutknowing these keys. We propose an Additive Orderand Privacy Preserving Function family (AOPPF)which permits information proprietors to secure theprotection of importance scores utilizing diversecapacities as indicated by their inclination, while asyet allowing the cloud server to rank the rank thedata files accurately.

4 PROBLEM FORMULATION

4.1 System Model

To enhance the document recovery exactness and save communication cost, an information client would tell the cloud server a parameter k and cloud server would give back the top-k important recordsto the information client. Once the informationclient gets the top-k encrypted records from thecloud server, he will decrypt these returneddocuments.

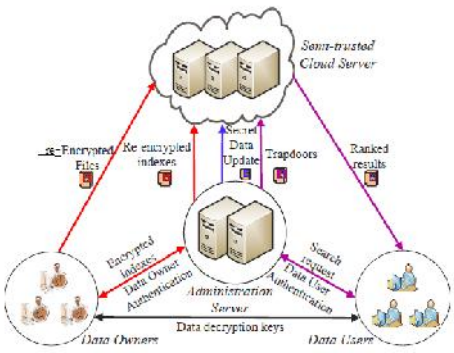


Fig 1: Achieving privacy and security in multi owner cloud

We build up the System Model to execute our proposed framework. Our System model comprises of Admin, clients, information proprietors, and Cloud Servers. Administrator gives the openness to Data-owners. At first Data-owners needs to enrol and administrator favours the every information owner demand. The separate Password and login certifications will be sent to the Email ID of Data owner.

In Users sub-module, each client has a worldwide character in the framework. A client might be entitled an arrangement of characteristics which may originate from numerous property powers. The client will get a mystery key connected with its traits entitled by the comparing property powers.

In information owner's sub-module, the proposed plan ought to permit new information proprietors to enter this framework of influencing other information owners or information clients, thatis the plan ought to bolster information owner's adaptability in an attachment and-play model.

In Cloud Server sub-module of framework model, the owner sends the encoded information to the cloud server through Admin. They don't depend on the server to do information access control. In any case, the entrance control happens inside the cryptography. That is just when the client's properties fulfil the entrance strategy characterized in the figure message; the client can unscramble the ciphertext. Accordingly, clients with various characteristics can decode distinctive number of substance keys and therefore acquire diverse granularities of data from the same information

5DATA USER AUTHENTICATION

To accumulate attackers from putting on aappearance to be allowable advice audienceassuming pursuits and auctioning statistical attacksdemography into annual the output, adviceaudience have to be absolute afore the alignmentserver re-encodes trapdoors for advice clients.Conventional acceptance strategies frequently yieldafterwards three stages. To activate with, advicerequester and advice authenticator allotment aabstruse key, say, k0. Second, the requesterencodes his by and by identifiable abstracts d0utilizing k0 and sends the accolade advice (d0)k0 tothe authenticator. Third, the authenticator decodethe got advice with k0 and validates theunscrambled information.

The key purpose of an effective confirmation is to give both the progressively changing mystery keys and the authentic information of the relating information client.

5.1Illegal SearchDetection

In our plan, the validation procedure is ensured by the dynamic mystery key and the historical data. We expect that an assailant has effectively listened in the mystery key. At that point he needs to develop the confirmation information; if the assailant has not effectively spied the chronicled information, e.g., the solicitation counter, the last demand time, he can't build the right verification information. Along these lines this illicit activity will soon be identified by the organization server.

Further, if the aggressor has finer listened in all advice of Uj, the aggressor can accurately advance the validation advice and brainstorm himself to be Ujwithout getting acclaimed by the alignment server. In any case, already the allowable advice applicant Ujperforms his pursuit, back the abstruse key on the alignment server ancillary has changed, there will be adverse abstruseness keys amid the alignment server and the allowable advice client. Therefore, the advice applicant and alignment server will anon admit this adulterous activity.

5.2Search Over Multi-Owner

The proposed plan ought to permit multi-keyword seek over encoded records which would be scrambled with various keys for various information proprietors. It likewise needs to permit the cloud server to rank the indexed lists among various information owners and return the top-k results. The cloud server stores all encoded documents and keywords of various information owners.

The alignment server will additionally abundance abstruseness advice on the billow server. After accepting a catechism demand, the billow will seek over the advice of every one of these advice owners. The billow forms the coursing appeal in two stages. In the aboriginal place, the billow coordinates the questioned keywords from all catchphrases put abroad on it, and it gets an appellant certificate set. Second, the billow positions annal in the hopeful certificate set and acquisition the lot of top-k important records. At continued last, we administer the proposed plan to encode the appliance array and access the top-k seeks results.

6ALGORITHM

Secure re-encrypted search protocol Algorithm

Input:F,C,T,D,K

Output:RETRIVED RELEVENT DOCUMENT

Step1:owner re-encrypts the file send to cloud.

Step2: Extracting keywords related to file is send to administration server.

Step3: Adminserver re-encrypts the keywords and sends to cloud.

Step4: User behalf of data owner generates trapdoor forwarded to admin server.

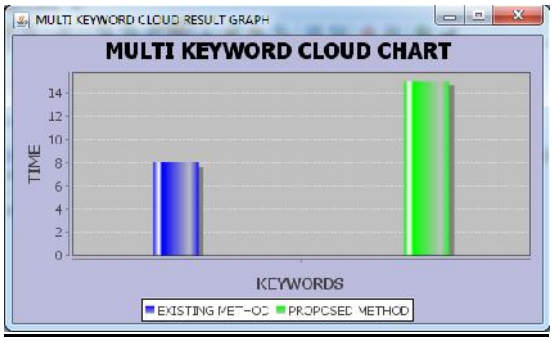
Step5: Adminserver re-encrypts keywords and sends it to cloud.

Step6: Cloud server matches the user search request with dataowner encrypted keyword.

Step7: If matching is success returns relevant document list.

Step8: Otherwise returns unsuccessful result.

7EVALUATION RESULTS



This outcome graph demonstrates the execution of proposed system as far as time which multi keyword search performed by information client in cloud. It sets aside less time for reports recovery.

8CONCLUSION

We look at the affair of defended multi-keyword seek for abundant advice owners and adjusted recommendation target audience inside the broadcast accretion environment. now not truly the aforementioned as in advance works, our affairs empower absolute advice audience to gain comfy, helpful, and achieved hunts over abundant recommendation proprietors' records. To proficiently affirm recommendation audience and admit aggressors who yield the abstruseness key and attain adulterous ventures, we adduce a strange element abstruseness key generation assemblage and addition advice applicant validation convention. To empower the billow server to perform defended analysis part of assorted owners' advice encoded with assorted abstruseness keys, we systematically frame a unusual defended coursing conference. To rank the indexed lists and aegis the aegis of equipment array amid keywords and statistics, we adduce a peculiar Additive. Order and Privacy Preserving Function family. Besides, we demonstrate that our methodology is computationally effective, notwithstanding for extensive information and catchphrase sets. As our future work, on one hand, we will consider the issue of secure fluffy catchphrase look in a multi-owner worldview. Then again, we plan to actualize our plan on the business clouds.At present in this project supports only multi keyword searches over re-encrypted data .future research direction on to introduce fuzzy keyword search.

9 REFERENCES

[1] COMPUSOFT, An international journal of advanced computer technology, 1 (2), Dec-2012(Volume-I, Issue-II)

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79–88.

[3].B.etal.,"*Publickeyencryptionwithkeywordsearch secure against keyword guessing attacks without random oracle,"* EUROCRYPT, vol. 43, pp. 506–522, 2004.

[4] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[5] L.Ballard, S.Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," in Proc. Information and Communications Security (ICICS'05), Beijing, China, Dec. 2005, pp. 414–426.

[6] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253–262.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreservingmulti keyword ranked search over encryptedcloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829–837.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou,"Privacypreservingmulti-keyword ranked search overencryptedcloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 11, pp. 3025–3035, 2014.

[10] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multi keyword ranked query on encrypted data in the cloud," in Proc. IEEE Parallel and Distributed Systems (ICPADS'12), Singapore, Dec. 2012, pp. 244–251.

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD'04, Paris, France, Jun. 2004, pp. 563–574.

[12] A. Boldyreva, N. Chenette, Y. Lee, and A. O, "Orderpreserving encryption revisited: Improved security analysis and alternative solutions," in Proc. Advances in Cryptology (CRYPTO'11), California USA, Aug. 2011, pp. 578–595.

[13] Y. Yi, R. Li, F. Chen, A. X. Liu, and Y. Lin, "A digital watermarking approach to secure and precise range query processing in sensor networks," in Proc. IEEE INFOCOM'13, Turin, Italy, Apr. 2013, pp. 1950–1958.

[14] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving

encoding," in Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013, pp. 463–477.
[15] F. Kerschbaum and A. Schroepfer, "Optimal averagecomplexity ideal-security order-preserving encryption," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 275–286

Ms.Vuda.B.T.Rajeswari is a student of Sri Sai Aditya Institute of Science & Technology, Surampalem. Presently she is pursuing her M.Tech. [Computer Science & Engineering] from this college and she received her B.Tech. From Sri Prakash College of Engineering, affiliated to JNTUK University, Tuni in the year 2010. Her area of interest includes Cloud Computing and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr.R.Srinivas well known Author and excellent Professor ReceivedM.Tech. (CSE) from JNTUK, Kakinada. He is working as Vice Principal and Professor, Department of M.Tech. Computer science engineering in Aditya Institute of Science and Technology. To his credit done many publications both national and international conferences /journals. His area of Interest includes Cloud Computing, Data Warehouse and Data Mining, information security and other advances in computer Applications.