International Journal of Science Engineering and Advance Technology

An Efficient Data User Authentication Protocol to Enable Data User Revocation

1P.Vinod Kumar, 2S.N. Ansari
1,2Dept. of CSE, VSM College of Engineering., Ramachandhrapuram, E.G.dt, AP, India

Abstract— Cloud computing offer favorable circumstances to individual customers and affiliations which minimizes endeavor and resource use cost. Information owners sending the data to cloud servers without adjacent data organization and data customers recovering the data from cloud. Insurance and security considerations earlier investigation done simply single owner model nearby secure request. Existing arrangements are cause more correspondence overhead for secure interest and these are backings simply single owner model. We give multi owner model security ensuring situated multi-keyword look over re-encrypted cloud data by using AES 256 bit gives security of data, keywords and trapdoors novel component secret key period tradition is used to keep aggressors from secret key the fting and going about as authentic customer. Proposed approaches minimizes figuring and limit cost close by secure request.

KEYWORDS: Ranked keyword search, multiple owners, privacy preserving, dynamic secret key

Introduction:

Secure request over encoded data has starting late pulled in light of an honest to legitimate concern toward a few researchers. Cloud service suppliers (CSPs) would ensure to ensure owners' data security using parts like virtualization and firewalls. Regardless, these components don't shield owners' data security from the CSP itself, since the CSP has full control of cloud equipment, programming, and owners' data. We propose plans to oversee Privacy Preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To enable cloud servers to perform secure interest without knowing the honest to goodness data of both watchwords and trapdoors, we effectively build up a novel secure request convention. To rank the filed records and shield the security of hugeness scores between keywords and records, we propose a novel Additive Order and Privacy Preserving Function family.

Literature survey:

[1] This exhibits an anonymous benefit control plan AnonyControl to address not just the information protection issue in a cloud storage, additionally the client character security issues in existing access control plans. By utilizing various powers as a part of cloud computing framework, our proposed plan accomplishes unknown cloud information get to and fine-grained benefit control. Our security evidence and execution investigation demonstrates that AnonyControl is both secure and productive for cloud computing environment.

[2] We assemble a private trie-traverse searching index, and show it accurately accomplishes the characterized similarity search usefulness with steady inquiry time complexity. We formally demonstrate the privacy-preserving surety of the proposed instrument under thorough security treatment. To exhibit the simplification of our component and further advance the application range, we additionally demonstrate our new development actually bolsters fluffy hunt, a formerly concentrated on thought pointing just to endure grammatical mistakes and representation irregularities in the client searching info. The broad examinations on Amazon cloud stage with genuine information set further show the legitimacy and common sense of the proposed mechanism.

Problem definition

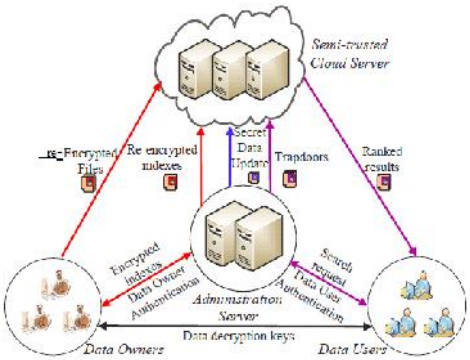
To download all the encoded data and unscramble them locally. In any case, this method is unmistakably improbable because it will realize a colossal measure of correspondence overhead. Positioned multikeyword search will bring about significant figuring and limit costs[3].

V. Proposed Approach

We intentionally develop up a novel secure search protocol, which not simply engages the cloud server to perform secure situated keyword look without knowing the certified data of both keywords and trapdoors, also allows data owners to re-encode data with keywords with self-picked keys and allows accepted data

customers to address without knowing these keys. We propose an Additive Order and Privacy Preserving Function family (AOPPF) which grants data owners to secure the insurance of significance scores using differing limits as demonstrated by their slant, while up 'til now permitting the cloud server to rank the rank the information documents accurately[4,5,6].

VI. System Architecture:



VII. Proposed Methodology:

System Model

We develop the System Model to execute our proposed structure. Our System model contains Admin, customers, data owners, and Cloud Servers. Administrator gives the openness to Data-owners. At first Data-owners needs to enlist and director supports the each data owner request. The different Password and login certifications will be sent to the Email ID of Data owner[7].

In Users sub-module, every client has an overall character in the system. A client may be entitled an arrangement of attributes which may start from various property powers. The customer will get a secret key associated with its attributes entitled by the looking at property powers.

In data owner's sub-module, the proposed arrangement should allow new data owners to enter this system without impacting other data owners or data customers, i.e., the arrangement should reinforce data owner's adaptability in a connection and-play model[8,9].

In Cloud Server sub-module of framework model, the owner sends the encoded data to the cloud server through Admin. They don't rely on upon the server to do data access control. Regardless, the passage control happens inside the cryptography. That is exactly when the customer's properties satisfy the passage technique portrayed in the figure message; the customer can unscramble the ciphertext. As needs be, customers with different attributes can interpret particular number of substance keys and along these lines secure assorted granularities of information from the same data

Data User Authentication

To keep attackers from putting on a show to be legal data clients performing interests and dispatching factual assaults considering the yield, data customers must be confirmed before the association server re-encodes trapdoors for data customers. Conventional affirmation methodologies much of the time take after three phases. In the first place, data requester and data authenticator share a secret key, say, k0. Second, the requester encodes his before long identifiable information d0 using k0 and sends 1the mixed data (d0)k0 to the authenticator. Third, the authenticator unravels the got data with k0 and approves the unscrambled data. The key purpose behind a successful affirmation is to give both the logically changing puzzle keys and the credible data of the relating data customer [10,11].

Illegal Search Detection

The acceptance strategy is guaranteed by the dynamic puzzle key and the historical information. We expect that an attacker has effectively listened in the riddle key. By then he needs to develop up the affirmation data; if the aggressor has not effectively saw the chronicled data, e.g., the requesting counter, the last request time, he can't manufacture the right confirmation data. Thusly this unlawful action will soon be distinguished by the association server.

In our Further, if the attacker has adequately listened in all data of Uj, the aggressor can precisely develop up the acceptance data and envision himself to be Uj without being recognized by the association server. Regardless, once the legal data client Uj performs his interest, since the secret key on the association server side has changed, there will struggle riddle keys between the association server and the legal data client. In this way, the data customer and association server will soon remember this illicit activity[12].

Search Over Multi-Owner:

Our proposed plan should allow multi-keyword look for over encoded records which would be mixed with different keys for different data owners. It moreover needs to allow the cloud server to rank the recorded records among different data owners and return the top-k comes about. The cloud server stores all encoded reports and keywords of different data owners.

The association server will moreover store a riddle data on the cloud server. Subsequent to tolerating an inquiry request, the cloud will look for over the data of each one of these data owners. The cloud frames the chase request in two phases. In any case, the cloud organizes the addressed keywords from all catchphrases set away on it, and it gets a candidate archive set. Second, the cloud positions records in the cheerful report set and finds the most top-k important records. Finally, we apply the proposed plan to encode the relevance scores and gain the top-k list items[13].

VIII. Algorithm:

Secure re-encrypted search protocol Algorithm:[14]

Input: F,C,T,D,K

Output: RETRIVED RELEVENT DOCUMENTS

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

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

Step3: admin server re-encrypt the keywords and send to cloud.

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

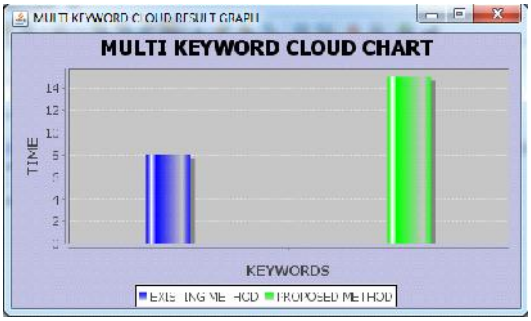
Step5: admin server re-encrypt keywords and send it to cloud.

Step6: cloud server matches the user search request with data owner encrypted keyword.

Step7: if matching is success returns relevent document list.

Step8: otherwise returns unsuccess result.

IX.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[15].

Conclusion & Future Work:

We suggest a novel dynamic secret key generation protocol and another data client acceptance tradition. To engage the cloud server to perform secure request among different owners' data encoded with different puzzle keys, we efficiently manufacture a novel secure chase tradition. To rank the filed records and defend the assurance of congruity scores between keywords and records, we propose a novel Additive Order and Privacy Preserving Function family. Moreover, we exhibit that our approach is computationally effective, despite for broad data and catchphrase sets. As our future work, on one hand, we will consider the issue of secure cushioned catchphrase look in a multi-owner perspective. Of course, we plan to complete our arrangement on the business clouds. This work supports only multi keyword search over re-encrypted data .future research direction on to introduce fuzzy keyword search [15]

References:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” *Communication of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreserving public auditing for secure cloud storage,” *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[3] D.Song, D.Wagner, and A.Perrig, “Practical techniques for searches on encrypted data,” in *Proc. IEEE International Symposium on Security and Privacy (S&P’00)*, Nagoya, Japan, Jan. 2000, pp. 44–55.

[4] E. Goh. (2003) Secure indexes. [Online]. Available: http://eprint.iacr.org/

[5] 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.

[6] D. B. et al., “Public key encryption with keyword search secure against keyword guessing attacks without

random oracle," *EUROCRYPT*, vol. 43, pp. 506–522, 2004.

[7] 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.

[8] 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.

[9] 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.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," in *Proc. IEEE INFOCOM'11*, Shanghai, China, Apr. 2011, pp. 829–837.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 222–233, 2014.

[12] 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.

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

[14] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. IEEE INFOCOM'10*, San Diego, CA, Mar. 2010, pp. 1–5.

[15] M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in *Proc. IEEE 31th International Conference on Distributed Computing Systems (ICDCS'11)*, Minneapolis, MN, Jun. 2011, pp. 383–392.

Mr.P.Vinod Kumar is a student of VSM College of Engineering & Technology, Ramachandhrapuram.Presently he is pursuing his M.Tech [CSE] from this college and he received his B.Tech from Swarnandhra college of engineering and Technology , affiliated to JNT University, Kakinada in the year 2013 .He is the Diploma holder in computer science from C.R.R Polytechnic in the year 2010, Eluru. His area of interest includes Computer Networks and Network security, all current trends and techniques in Computer Science.

Mr., S.N Ansari he is an excellent teacher.He Received M.C.A(Andhra university), M.Tech (Nagarjuna University and (PhD) Rayalaseema Universitry. He is working as Associate Professor and HOD Department of Computer Science and engineering,VSM College of Engineering. He has 20 years of teaching experience. His area of Interest includes Artificial intelligence, data warehousing data mining and other advances in computer Applications.