International Journal of Science Engineering and Advance Technology

An Additive Order And Privacy Preserving Function Family (AOPPF)

1V.Gowtham, 2B.Srinivas
1,2Dept. of CSE, Srinivasa Institute of Engineering and Technology, Cheyyeru.E.G,AP,India

Abstract— The plentiful benefits of cloud computing, for privacy concerns, individuals and enterprise users are disinclined to outsource their susceptible data, including emails, personal health records and government confidential files, to the cloud. This is as once sensitive data are outsourced to a inaccessible cloud, the analogous data owners lose direct control of these data. We identify a multi-owner model for privacy preserving keyword search over encrypted cloud data. We recommend an capable data user , which not only prevents attackers from eavesdropping secret keys and imaginary to be illegal data users performing searches, but also facilitate data user certification and revocation.

KEYWORDS: Cloud computing, ranked keyword search, multiple owners, privacy preserving, dynamic secret key

INTRODUCTION:

Most cloud servers in carry out do not just serve one owner; in its place, they hold multiple owners to share the reimbursement brought by cloud computing. We offer schemes to transaction with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To facilitate cloud servers to achieve secure search without knowing the actual data of both keywords and trapdoors, we thoroughly construct a novel secure search protocol. To status the search results and defend the privacy of relevance scores between keywords and files, we advise a novel Additive Order and Privacy Preserving Function family. To thwart the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we put forward a novel dynamic secret key generation protocol and a new data user authentication protocol. As a new model of computing, cloud computing supply abundant benefits counting easy access, decreased costs, quick deployment and flexible resource management, etc.

LITERATURE SURVEY:

[1]The primary request saving plan that accomplishes perfect security. Our principle procedure is variable ciphertexts, implying that after some time, the ciphertexts for a small number of plaintext qualities change, and we demonstrate that impermanent ciphertexts are required for perfect security. Our resulting protocol is intuitive, with a little small of associations.

[2]We propose a safe cloud storage framework supporting privacy-preserving public auditing. We facilitate extend our outcome to empower the TPA to perform reviews for different clients all the while and productively. Broad security and execution analysis demonstrate the proposed plans are provably secure and exceedingly productive. Our preparatory test led on Amazon EC2 example advance shows the quick execution of the outline.

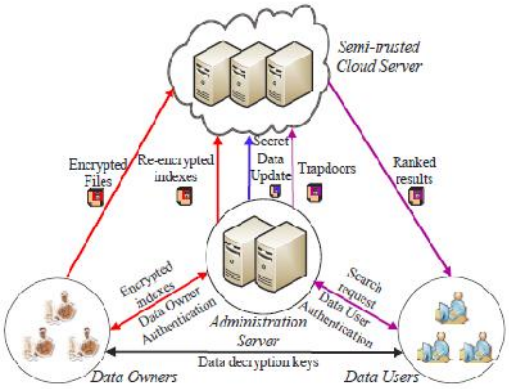
PROBLEM DEFINITION:

Cloud service providers (CSPs) would pledge to make sure owners' data security using method like virtualization and firewalls. However, these mechanisms do not protect owners' data privacy from the CSP itself, since the CSP possesses filled control of cloud hardware, software, and owners' data. Data encryption makes the customary data utilization service based on plaintext keyword search a very demanding difficulty.

PROPOSED APPROACH:

We recommend PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model. To facilitate cloud servers to perform protected search without knowing the actual value of both keywords and trapdoors, we thoroughly construct a narrative secure search protocol. As a result, different data owners use different keys to encrypt their files and keywords. Authenticated data users can concern a query without knowing secret keys of these dissimilar data owners.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

RANKED MULTI-KEYWORD SEARCH OVER MULTIOWNER:

The planned scheme be supposed to permit multi-keyword search over encrypted files which would be encrypted with different keys for different data owners. It also needs to let the cloud server to rank the search results amongst different data owners and return the top-*k* results.

DATA OWNER SCALABILITY:

The projected scheme should allow new data owners to enter this system lacking affecting other data owners or data users, i.e., the scheme should prop up data owners scalability in a plug-and-play model.

DATA USER REVOCATION:

The anticipated scheme should make sure that only authenticated data user scan execute correct searches. In addition, once a data user is withdraw, he can no longer perform correct searches over the encrypted cloud data.

ALGORITHM:

Secure re-encrypted search protocol Algorithm:

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.

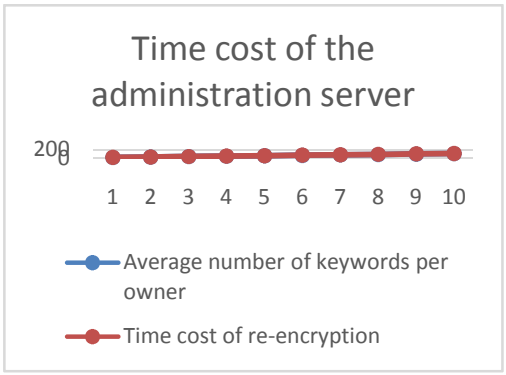
STEP5:admin server re-encrypt keywords and send it to cloud.

STEP6:cloud server matches the user search request with data owner encrypted keyword.

STEP7: if matching is success returns relevant document list.

STEP8:otherwise returns unsuccess result.

RESULTS:



Shows the re-encryption time cost of the administration server in PRMSM. As we can see, for the same average number of keywords per owner, the more data owners are involved, the more time is spent on re-encryption.

CONCLUSION:

Our proposal facilitate authenticated data users to accomplish secure, convenient, and efficient searches over multiple data owners' data. To capably authenticate data users and detect attackers who embezzle the secret key and carry out illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To allow the cloud server to perform secure search in the midst of multiple owners' data encrypted with different secret keys, we methodically put up a novel secure search protocol. To rank the search results and protect the privacy of significance scores between keywords

and files, we recommend a novel Additive Order and Privacy Preserving .

FUTURE WORK:

We will consider the issue of secure fuzzy keyword search in a multi-proprietor worldview. Then again, we plan to actualize our plan on the commercial clouds.

REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz,A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, andM. Zaharia, "A view of cloud computing," *Communication ofthe ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreservingpublic 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 forsearches on encrypted data," in *Proc. IEEE International Symposiumon 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, "Searchablesymmetric encryption: improved definitions and efficientconstructions," in *Proc. ACM CCS'06*, VA, USA, Oct. 2006, pp. 79–88.
[6] D. B. et al., "Public key encryption with keyword search secureagainst keyword guessing attacks without random oracle,"*EUROCRYPT*, vol. 43, pp. 506–522, 2004.
[7] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keywordsearch over encrypted data," in *Proc. Applied Cryptographyand Network Security (ACNS'04)*, Yellow Mountain, China,Jun. 2004, pp. 31–45.
[8] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficientconjunctive keyword searches over encrypted data," in *ProcInformation 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 rankedkeyword search over encrypted cloud data," in *Proc. IEEEDistributed Computing Systems (ICDCS'10)*, Genoa, Italy, Jun.2010, pp. 253–262.
[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreservingmulti-keyword ranked search over encrypted clouddata," in *Proc. IEEE INFOCOM'11*, Shanghai, China, Apr. 2011,pp. 829–837.
[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreservingmulti-keyword ranked search over encrypted clouddata," *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 inthe cloud supporting similarity-based ranking," *Parallel andDistributed 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 multikeywordranked 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, "Fuzzykeyword 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 solutionfor fuzzy multi-keyword search over encrypted data," in *Proc.IEEE 31th International Conference on Distributed ComputingSystems (ICDCS'11)*, Minneapolis, MN, Jun. 2011, pp. 383–392.

Mr.V.Gowtham is a student of Srinivasa Institute of Engineering and Technology, Cheyyeru. Presently he is pursuing his M.Tech [Computer Science] from this college and he received his B.Tech from B.V.C Institute of Technology and Sciences, affiliated to JNT University, Kakinada in the year 2013. His area of interest include Cloud Computing and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. B. Srinivas, M.Tech (CSE) from jntuk is working as Assistant Professor , Department of Computer science engineering , Srinivasa Institute of Engineering an Technology .He has 7 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals . His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems andother advances in computer Applications.