International Journal of Science Engineering and Advance Technology

Efficient Solution For Searchable Data Sharing In Public Cloud

[1]G.S.Aswini, [2]B.Santhi Sri
[1,2]Dept. of CSE, K.I.E.T(w) College of Engineering & Technology, Korangi.East Godavari District,AP,India

ABSTRACT:

Cloud storage providing more facilities like on demand access and convenient Sharing of data by internet. This cloud storage suffers from security as well as data leakage. The main challenging problem is designing effective mechanisms to encrypt any group of documents with encryption keys and share these documents along with search keywords to any users with decryption keys which leads secure communication, storage and computation complexity. We present a novel technique named as key aggregate searchable encryption with AES-256 bit algorithm for data file encryption and decryption, in this data owner shares a single key to a user for large documents and receiver only issued the shared single along with single trapdoor for documents deriving. Proposed Approach shows efficiency in terms of secure communication, storage and computation.

KEYWORDS: Searchable encryption, data sharing, cloud storage, data privacy

I. INTRODUCTION:

Despite the fact that joining a searchable encryption plot with cryptographic cloud storage can accomplish the fundamental security necessities of a distributed storage, executing such a framework for extensive scale applications including a great many clients and billions of records may in any case be blocked by viable issues including the effective administration of encryption keys, which, to the best of our insight, are generally overlooked in the writing. Above all else, the requirement for specifically offering encoded information to various clients (e.g., imparting a photograph to specific companions in ansocial network application, or imparting a business record to specific partners on a cloud drive) regularly asks for particular encryption keys to be used for different archives. In any case, this surmises the amount of keys that ought to be flowed to customers, both for them to look for over the mixed archives and to unscramble the records, will compare to the amount of such records. Such a broad number of keys must not simply be spread to customers by method for secure channels, also be securely secured and administered by the customers in their gadgets. Besides, must be made by customers and submitted to the cloud with a particular true objective to play out a watchword look for over various reports. The induced necessity for secure correspondence, stockpiling, and computational multifaceted nature may render such a system wasteful and unrealistic.

LITERATURE SURVEY:

[1], secure provenance that records possession and process history of information items is crucial to the accomplishment of information crime scene investigation in distributed computing, yet it is still a testing issue today. In this, to handle this unexplored territory in distributed computing, we proposed another protected provenance conspire in light of the bilinear matching systems. As the fundamental bread and margarine of information crime scene investigation and post examination in distributed computing, the proposed plan is portrayed by giving the data privacy on delicate reports put away in cloud, mysterious validation on client get to, and provenance following on questioned records. With the provable security systems, we formally exhibit the proposed plan is secure in the standard model.

[2], with the character of low support, distributed computing gives a sparing and effective answer for sharing gathering asset among cloud clients. Sadly, sharing information in a multi-proprietor way while saving information and character security from an untrusted cloud is still a testing issue, because of the successive change of the participation. In this paper, we propose a safe multi-proprietor information sharing plan, named Mona, for element gathers in the cloud. By utilizing bunch signature and element communicate encryption strategies, any cloud client can secretly impart information to others. In the interim, the capacity overhead and encryption calculation cost of our plan are free with the quantity of revoked clients.

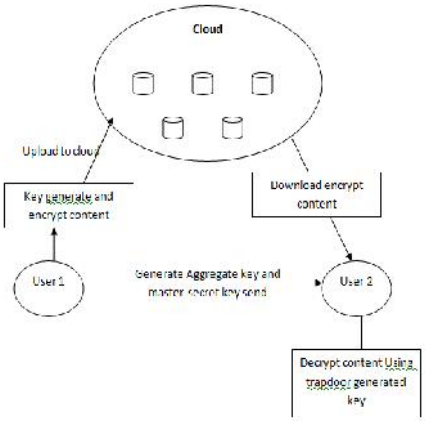
PROBLEM DEFINITION

The encryption of information makes it trying for clients to inquiry and afterward specifically recover just the information containing given keywords. In MUSE, the primary issue is the means by which to control which clients can get to which records, while how to decrease the quantity of shared keys and trapdoors is not considered. The key total encryption plot permits effectively designating the decoding rights to different clients, yet it doesn't bolster any pursuit over the encrypted information.

PROPOSED APPROACH

The proposed upgraded KASE conspire applies to any distributed storage that backings the searchable gathering information sharing usefulness, which implies any client may specifically impart a gathering of choose documents to a gathering of choose clients, while permitting the last to perform keyword search over the previous. To bolster searchable gathering information sharing the primary necessities for efficient key administration are to fold. Initial, an information proprietor just needs to circulate a solitary total key (rather than a group of keys) to a client for sharing any number of documents. Second, the client just needs to present a solitary total trapdoor (rather than a group of trapdoors) to the cloud for performing keyword search over any number of shared documents.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

DATA OWNER:

In this module we executed by the data owner to setup an account on an untrusted server. On input a security level parameter 1^{λ} and the number of ciphertext classes n (i.e., class index should be an integer bounded by 1 and n), it outputs the public system parameter param, which is omitted from the input of the other algorithms for brevity.

Organize STORAGE (DROP BOX):

With our answer, Alice can essentially send Bob a solitary total key by means of a protected email. Sway can download the scrambled photographs from Alice's Dropbox space and afterward utilize this total key to unscramble these encoded photographs. In this Network Storage is untrusted outsider server or dropbox.

Encoded AGGREGATE KEY AND SEARCHABLE ENCRYPTED KEY TRANSFER:

The information proprietor sets up people in general framework parameter through Setup and creates an open/ace mystery key combine by means of KeyGen. Messages can be scrambled by means of Encrypt by any individual who additionally chooses what ciphertext class is connected with the plaintext message to be encoded. The information proprietor can utilize the ace mystery to create a total decoding key for an arrangement of ciphertext classes by means of Extract. The produced keys can be passed to delegates safely (by means of secure messages or secure gadgets) at long last; any client with a total key can unscramble any ciphertext gave that the ciphertext's class is contained in the total key through Decrypt

TRAPDOOR GENERATION

This trapdoor era calculation is controlled by information client and performs watchword seeking by creating trapdoor. On account of hunting down coordinating pertinent records by utilization of single total searchable key. One and only single total trapdoor is created for a solitary catchphrase which is utilized for seeking. Than information client sends this produce single trapdoor and subset of coordinated reports.

Record USER:

The produced keys can be passed to delegates safely (by means of secure messages or secure gadgets) at long last; any client with the Trapdoor watchword era process can decode any ciphertext gave that the figure content's class is contained in the Encrypted total key and Searchable Encrypted key by means of Decrypt.

Calculation:

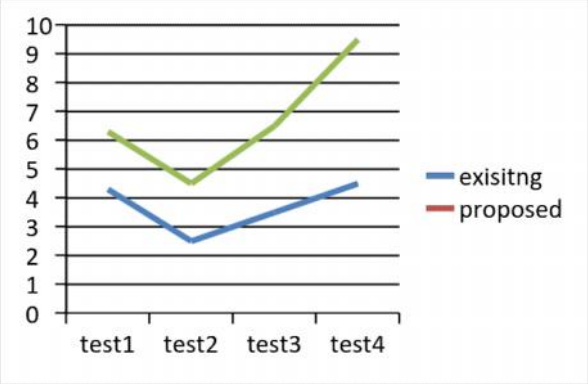
Upgraded KASE FRAMEWORK:

The outline of our KASE conspire draws its experiences from both the multi-key searchable encryption plot and the key-total information sharing plan. In particular, with a specific end goal to make a total searchable encryption key rather than numerous autonomous keys, we adjust the thought introduced. Each searchable encryption key is connected with a specific file of report, and the total key is made by installing the proprietor's lord mystery enter into the result of open keys connected with the records. Keeping in mind the end goal to actualize watchword look over changed records utilizing the total trapdoor, we utilize a comparable procedure as in. The cloud server can utilize this procedure to create a balanced trapdoor for each archive.

INPUT: F,PK,SK,FI,T,SK,TGK
STEP1: new account setup by the data owner with cloud service provider.
STEP2: data owner is authorized by the cloud service provider.
STEP3: data owner generates the master-secret key abd public key for file uploading.
STEP4: data owner encrypt the data file along with keyword by using AES-256BIT algorithm.

STEP5: data owner extracts aggregate searchable key from master-secret key that is shared to users.
STEP6: user issues keyword along with aggregate key for download data file.
STEP7: cloud server checks the aggregate key along with trapdoor for data file forwading to user.
STEP8: after verification user decrypts the data file.
OUTPUT: decrypted data file.

RESULTS:



The result graph indicates the performance of proposed approach compared to earlier approach in terms of communication and computation overhead.

CONCLUSION:

We interestingly propose the idea of key-aggregate searchable encryption (KASE) and build a solid KASE conspire. Both investigation and assessment comes about affirm that our work can give a compelling answer for building functional information sharing framework in light of open distributed storage. In a KASE scheme, the proprietor just needs to disseminate a solitary key to a client when offering heaps of archives to the client, and the client just needs to present a solitary trapdoor when he questions over all reports shared by similar proprietor. Not with standing, if a client needs to inquiry over archives shared by different proprietors, he should produce numerous trapdoors to the cloud.

FUTURE WORK:

The most effective method to lessen the quantity of trapdoors under multi-proprietors setting is a future work. In addition, unified mists have pulled in a ton of consideration these days, yet our enhanced KASE can't be connected in this case specifically. It is additionally a future work to give the answer for enhanced KASE on account of combined mists

REFERENCES:

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multi owner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182- 1191.

[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.

[8] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.

[10] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

[11] J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypted data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.

[12] C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114- 127, 2011.

[13] C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.

[14] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.

[15] J. W. Li, J. Li, X. F. Chen, et al. "Efficient Keyword Search over Encrypted Data with Fine-Grained Access

Control in Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490- 502, 2012.

Mrs. G.S. Aswini is a student of K.I.E.T(w) College of Engineering & Technology, Korangi. Presently she is pursuing her M.Tech [computer science engineering] from this college and she received her B.Tech from Aditya Engineering college,affiliated to JNT University, Kakinada in the year 2014. Her area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mrs.B.Santhisri received M.Sc. in computer science from Andhra University and M.Tech. (CSE) from Acharya Nagarjuna University, Guntur is working as Associate Professor in Department of Computer Science Kakinada Institute of Engineering and Technology for Women, Korangi. She has 10 years of teaching experience. There are a few of publications both national and International Conferences / Journals to her credit. Her area of interest includes Information Security, Computer Networks, Cloud Computing and other advances in Computer Applications.