International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-3, February 2017

A Novel Algorithm for Multiple Data Sharing Via Cloud Storage

Krishna Samalla

Abstract: ***As the way that computing concepts gives the cloud computing, which permits once needed and low maintenance usage of resources, but the information is shares to some cloud servers and numerous privacy connected considerations emerge from it .Various schemes like primary based on the attribute based encoding are developed to secure the cloud storage. Most of the work looking at the information privacy and therefore the access management, while less attention is given to the privilege management and the privacy. An economical scientific discipline approach for information sharing wherever information is shared among a bunch of users as information. How to firmly and with efficiency share a group of information associated with any subject areas with others in cloud storage. Development of new novel concept of Key Aggregate Searchable cryptography (KASE). This concept is enforced through development of a concrete key-aggregate searchable cryptography framework theme. This scheme is delineate as wherever knowledge an information owner solely has to generate and distribute one mixture key to a data user for sharing an outsized variety of documents and on the opposite aspect user solely has to submit one mixture trapdoor to the cloud server, so that he/she will question over the shared documents by the assistance of generated single mixture trapdoor. Advanced Key sharing system based on hint text methodology is created to share the information safely. Once the data sharing is completed then the key combination differs from its actual kind. So the user cannot guess the key combination cryptosystem and this method provides economical answer than the prevailing ones.***

Index Terms*: Data Security, Cloud, Integrity, Bulk Request, Bulk Response, Dynamic Keys.*

I. INTRODUCTION

Cloud storage is a solution for sharing and accessing large Today, a number of users are mainly sharing a large number of various kinds of documents, which are considered to be under various categories like photos, amounts of data, which is shared for various users by means of internet., videos and documents via various social networking based applications on daily basis. There are huge benefits of using cloud storage like lower cost, greater agility and better resource utilization has add more attraction from plenty number of business users toward using the cloud storage. Cloud computing which is built on parallel, distributed computing, utility computing and service-oriented architecture. Generally, speaking about cloud storages, we all are enjoying the comfort of sharing all kinds of data.

Manuscript published on 28 February 2017.
***** Correspondence Author (s)
Dr. Krishna Samalla, Professor, Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad (Telangana). India. E-mail: krishna.oume@gmail.com

But all users are more bothered about the data leaks which usually happen in the cloud storage. Such type of data leaks occur due to reason like an untrusted cloud provider and by hackers who decrypt the files using various types of software. A common approach usually used is to encrypt all the types of data available with him/her. Which are to be uploaded to the cloud by the data owner. The encrypted data obtained shall be retrieved and then performing decryption by persons who have right set of access keys. This type of cloud storage is known as Cryptographic cloud storage.

In cloud computing, the cloud service providers (CSP), like Amazon, are able to provide various services to users with the help of powerful data servers. Moving the local data management systems into cloud servers, users can take advantage of high-quality services and store important investments on their local infrastructures. However, while sharing data through cloud storage, users are simultaneously aware about the data leakages in the cloud [5]. One of the most fundamental services delivered by cloud service providers is data storage. Consider a data application. There is a company which permits its staffs in the same group or department to store and share documents or files in the cloud. Using the cloud, the staffs can be fully released from the local data storage and maintenance. However, it also creates a significant risk to the confidentiality of those stored documents. Specifically, the cloud servers controlled by cloud providers are not fully believed by users while the documents stored in the cloud may be s confidential, such as business ideas. Identification of privacy is most important problem for wide development of cloud computing.Without the proof of identity privacy users are not ready to utilize the cloud services because they dont want to expose their real identity.To maintain data privacy, a basic idea is to encrypt files, and then upload the encrypted data into the cloud. In this paper, we demonstrate cryptographic scenarios for the problem of searching on encrypted data and provide result of security for the resulting crypto systems [4].

Original of all, the require for selectively distribution encrypted information with dissimilar users Ex: distribution a photo with persuaded friends in a social network demand, or distribution a business article with convinced generation on a cloud constrain] more often than not anxiety dissimilar encryption keys to be used for poles apart files. On the other hand, this involves the numeral of keys that require to be disseminated to users, both for them to investigate over the encrypted files and to decrypt the files, will be relative to the number of such files.

Such a great amount of keys have got to not only be disseminated to users via protected channels, but also be steadily stored and administered by the users in their campaigns. In adding up, an outsized quantity of trapdoors have got to be produced by users and put forward to the cloud in arrange to carry out a keyword investigate in excess of many documentations. The indirect necessitate for protected announcement, storage space, and computational complication may cause to be such a scheme incompetent and not practical. In this paper, we speak to this confront by propose the novel concept of Key Aggregate Searchable Encryption [KASE], and instantiating the concept through a tangible KASE method. The planned KASE proposal is relevant to any cloud storeroom that ropes the searchable collection information distribution functionality, which means any user can selectively go halves a assembly of elected files with a assemblage of preferred users, while consent to the latter to carry out keyword investigate over the previous. To hold up searchable collection information allocation the main requirements for well-organized key administration are double. Foremost, a information proprietor only requirements to deal out a on its own aggregate input [in its place of a assembly of keys] to a user for distribution any amount of documentations. Subsequent, the user only desires to put forward a solitary collective trapdoor [as an alternative of a cluster of trapdoors] to the cloud for the theater keyword rummage around over several quantities of communal documentations. To the most excellent of our information, the KASE method projected in this paper is the primary known proposal that can make happy together necessities [the key collective cryptosystem [2], which has stimulated our effort, can gratify the first prerequisite but not the succeeding.

II. RELATED EXISTING WORK

The concept of ABE for Fine Grained Access Control of Encrypted Data in 2006. He introduces the new cryptosystem for fine grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption (KPABE). In cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Secret-sharing schemes (SSS) are used to divide a secret among a number of parties. Matthew Pirretti and Brent Waters introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. A performance analysis of ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, demonstrates that the attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. Decryption decrypts a cipher text encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the cipher text in order to obtain the AES and HMAC key. John Bethencourt, AmitSahai, Brent Waters introduces Ciphertext-Policy Attribute-Based Encryption in 2008. They employ a trusted server to store the data and mediate access control. In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In addition, they provide an implementation of the system and give performance measurements. The primary challenge in this line of work is to find new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrates the basic principles on which architecture for combining access control and cryptography can be built. Then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. It also described an approach for policy evolution that takes into account the main features of the scenario and is able to guarantee in most cases confidentiality of the information in the presence of significant policy updates, clearly identifying the exposure to collusion when this risk may arise. Other issues to be investigated include the integration with the Web paradigm, and the efficient execution of queries. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Bjorn Tackmann, Daniele Venturi introduced Anonymity-preserving PublicKey Encryption: A Constructive Approach where publickey cryptosystems with enhanced security properties have been proposed. it investigate constructions as well as limitations for preserving receiver anonymity when using public-key encryption (PKE). They use the constructive cryptography approach by Maurer and Renner and interpret cryptographic schemes as constructions of a certain ideal resource (e.g. a confidential anonymous channel) from given real resources (e.g. a broadcast channel) and defined appropriate anonymous communication resources and show that a very natural resource can be constructed by using a PKE scheme which fulfills three properties that appear in cryptographic Literature. Results do not only support the trust in existing schemes and constructions; they also show that the simpler and more efficient weakly robust schemes can be used safely. Junbeom Hur, Dong Kun Noh introduces the concept of Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The other extra function is the ReEncrypt(CT;G) which is a reencryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it. R.Ranjith and D.Kayathri Devidescribes the concept of Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication in 2013. It is implemented with secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination.

Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches. Mr. ParjanyaC.A and Mr. Prasanna Kumar describe the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in March 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

III. METHODOLOGY

Through the concrete KASE scheme we address the challenges by proposing the new concept of key aggregate searchable encryption (KASE). By applying proposed KASE scheme to any cloud storage any user may selectively share group of selected files with a group of selected users. User revocation is used in the proposed system. In user revocation forward secrecy and backward secrecy is used. User revocation is used for the key updation in the cloud storage. Forward secrecy means if any user is added into the group theaggregate is forward to the new member of the group. Backward secrecy is if any group member is leaves from the group the aggragate key is updated in the server.And the new aggregate key is informed to the existing group members. Because ofthe user revocation the data is more secure in the cloud. In the concrete KASE scheme user only needs to submit a single trapdoor to the cloud for querying the shared documents. And data owner only needs to distribute a single key to user for sharing a large number of documents Maintaining aggregate key is easy in server and for the group members. KASE alice only need to distribute a single aggregate key instead of multiple keys. It is an efficient public-key encryption scheme which supports flexible delegation. In this work we uses the AES algorithm for the encryption and decryption of data

IV. PROPOSED METHOD

This system will be secure as encryption technique is involved. Also it is efficient as aggregate key for multiple documents are shared with group of user. Which is not case in existing system Decryption key should be sent via a secure channel and kept secret e.g. email hence data will be secure. This system will be efficient public-key encryption scheme which supports flexible delegation for searching also. Searching over encrypted data is performed efficiently since important public information is retrieved and mapped with the document in encryption format. searching is performed based on the index . Similarity search is performed on the number of document. It reduces the searching time and then retrieve the document. Various phases are use to design system like setup, key generation, encrypt, search, decrypt, share key phase. In this scheme user only need to share single key over the number of document and decrypt document using that single key.

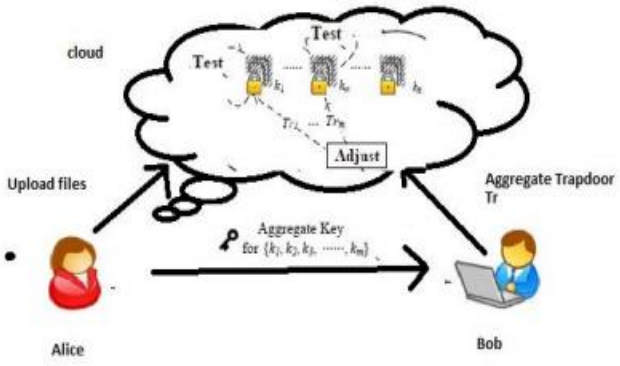

Fig 1: Aggregate Key Sharing Mechanism

Our work is flexible in the sense that this constraint is eliminated, that is, no special relation is required between the classes. The technique of bilinear aggregate signature is used to achieve key auditing. Key auditing reduces the computation overhead. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We introduce the concepts of similarity relevance and scheme robustness to formulate the privacy issues in encryption schemes, and then solve the insecurity problem by proposing a random key encryption scheme. Novel technologies in the cryptography community and information retrieval community are employed. Merits of Proposed System: To achieve better robustness and improve efficiency.ϖ This scheme fulfills the secure multi-keyword top-k retrieval over encrypted data.ϖ Specifically, for the first time we employ relevance score to support multi-keyword top-k retrieval.ϖ Thorough analysis on security demonstrates the proposed scheme guarantees high data privacy. Furthermore,ϖ performance analysis and experimental results show that our scheme is efficient for practical utilization.

V. KEY-AGGREGATE SEARCHABLE ENCRYPTION (KASE)

Development of KASE scheme ideas is adapted from papers like key-aggregate cryptosystem scheme [7] for scalable data sharing and Multi-key searchable encryption scheme [31]. This was done to generate a single aggregate encryption key in replacement of many numbers of individual independent keys for each documents uploaded by the data owner.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Defining this scheme each key which is used for searching is connected with a particular index of uploaded document. Creation of aggregate key is done by using the data owner's master-secret key with product of his/her public keys used for encryption. Keyword based searching is performed by generation of aggregate trapdoor mechanism. This is implemented by adjusting process [31]. Than cloud server can use single adjusted aggregated trapdoor which was created for each set of document. 3.0.4 KASE Scheme Description. KASE Framework was described in the above section, this KASE scheme consists of seven algorithms:

(1) Setup: This algorithm is run by cloud server to setup all system parameters. Generate a bilinear mapping based group sharing system, set the maximum possible number of documents available with the data owner. Two operations are computed which are random generator calculation and selecting a oneway hash function. Cloud server broadcast the generated system parameter and public key.

(2) Keygen: This algorithm is run by data owner to generate his/her key pair which will be used for document encryption by the Encrypt algorithm. In this stage, we have public key and master secret key along with the generated key pair.

(3) Encrypt: This algorithm is run by data owner to perform data encryption and also generate corresponding ciphertexts for all the documents which will be uploaded. For the creating the keyword ciphertexts, it takes the document file index, randomly picks a searchable encryption key for each document and generates a delta information. It will produce a ciphertext for a keyword, this generated ciphertexts are stored under cloud server.

(4) Extract: This algorithm is run by data owner and generating an aggregate searchable encryption key and this key is send to all authorized users via a secure communication channel. This algorithm takes input as master secret key and generates an aggregate key as output. Data owner than send this aggregate key to data users, so that they can perform keyword searching over the shared documents.

(5) Trapdoor: This algorithm is run by data user and performs keyword searching by generating trapdoor. In the case of searching for matching relevant documents by use of single aggregate searchable key. Only one single aggregate trapdoor is generated for a single keyword which is used for searching. Than data user sends this generate single trapdoor and subset of matched documents.

(6) Adjust: This algorithm is run by cloud server and creating right set of trapdoor. It accepts input as system publicly available parameters, all documents index in the set and also single aggregate trapdoor. It performs adjusting process on the single aggregate trapdoor and output a new right single trapdoor. This produced trapdoor will be used for next Test algorithm for performing keyword search over the shared collection of documents.

(7) Test: This algorithm is run by the cloud server. Cloud server does a series of keyword searching by using the input, which is adjusted trapdoor and creates the delta information which is relevant to subset by using searchable encryption key. Output produced will be binary, i.e. true or false values after performing various computations.

VI. CONCLUSION

In this paper, practical problems of sharing data among a set of users is considered, without data leaks which usually occurs in the cloud storage. Normal method performed is to share a large number of keys to all authorized data users from data owner through a secure communication channel, which gives the authorized user to access the relevant set of documents shared to him/her. Development of new concept involving the key-aggregate searchable encryption (KASE) and also constructing a KASE scheme. Results based on various comparison and analysis confirm that KASE work can give a better and more efficient solution for building a more secure data sharing system based on public cloud storage available on internet. Description of KASE scheme, the data owner generates a single aggregate key which will be used for encryption process and send this key to the entire authorized user. On the other end, data user creates and query through generated single aggregate trapdoor, this trapdoor produced is used to query over collection of documents shared by the same data owner. Comparison of various methodologies is done and performed pairing computation analysis on system and mobile phone. However, future work of this is concerned over the data shared under multiple owners and how to decrease the number of trapdoor generation.

REFERENCES

1. Cloud-Storage,http://www.thetop10bestonlinebackup.com/cloudstorage.
2. Amazon Web Services (AWS), http://aws.amazon.com.
3. Google App Enginehttp://code.google.com/appengine/.
4. 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..
5. 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.
6. 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.
7. X. Song, D. Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
8. 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.
9. P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.
10. 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.
11. D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.
12. 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.
13. J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypt-ed data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.
14. C. Bosch, R. Brinkma, P. Hartel. "Conjunctive wildcard search over encrypted data", Secure Data Management. LNCS, pp. 114-127, 2011
15. C. Dong, G. Russello, N. Dulay. "Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.

16. 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.
17. 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.
18. J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681- 1689, Elsevier, 2010.
19. X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. "Secure Outsourced Attribute-based Signatures", IEEE Trans. on Parallel and Distributed Systems, DOI.ieeecomputersociety.org/10.1109/TPDS.2013.180, 2013.
20. J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014. [22] Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), IEEE, pp. 249- 255, 2013.
21. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", Proc. IEEE INFOCOM, pp. 525-533, 2010.
22. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Intl Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.
23. D. Boneh, C. Gentry, B. Waters. "Collusion resistant broadcast encryption with short ciphertexts and private keys", Advances in Cryptology CCRYPTO 2005, pp. 258-275, 2005.

Dr. Samalla Krishna so far has successfully guided many post graduate students in the fields of Signal and Image Processing, Neural Networks and Pattern Recognition while several other students are being supervised by him in a wide variety of other fields like DSP, Medical Image Processing and Object Recognition in addition to this he supervised many electrical and other disciplinary engineering students .He served as an academic supervisor to more than 300 Bachelor Degree dissertations towards the award of Undergraduate Degree ,and He has published more than 35 research papers in reputed International Journals. He shared his research experience more than many podiums like conferences, workshops, seminars and symposia. And currently he is working as a professor of ECE in Sreenidhi Institute of Science and Technology, Hyderabad. He has 12 years of experience in the teaching and research field. His many research articles are cited by scholars and research institutions.