"DESIGN DATA GROUP SHEARING SYSTEM IN CLOUD USING KEY-AGGREGATE SEARCHABLE ENCRYPTION"

[1]MISS RASHMI Y. PATIL
Department of Computer Science & Engineering, V. M. Institute of Engineering & Technology, Nagpur, India
rashmipatilbe@gmail.com

[2]PROF. GURUDEV B. SAWARKAR
Head, Department of Computer Science & Engineering, V. M. Institute of Engineering & Technology, Nagpur, India

ABSTRACT: *Today the world has accepting the cloud computing and raising several issues about treatment of data in the cloud. Now a day's Cloud computing is a buzz word and it is still in its beginning in terms of its implementation at all levels due the limitations it suffers. Most of the security techniques need a basic level of trust between the data owner and cloud provider, when this trust is breached either intentionally or unintentionally it is the data and its owner that suffers. Thus, we suggest techniques where the trust from service provider is not required. The security of data will be in control of the data owner solely. It would mainly contain a tool that would allow the owner of the data to decide about the access rights of his/her data, revocation if any, and notification if any security breaches are in place. In this paper we are trying to design a secure system that data owner needs only single key to a user for sharing a huge number of documents or information.*

***Keywords*:** cloud computing, Searchable encryption, data privacy, cloud storage

1. INTRODUCTION

Cloud storage is a solution for sharing and accessing large amounts of data, which is shared for various users by means of internet. 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, 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. 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 this paper we are trying to design a secure system that data owner needs only single key to a user for sharing a huge number of documents or information.

2. LITURATURE SURVEY OF RELATED WORK

Prajakta Solapurka [1] focused on reducing key-size by generating a single aggregate key, but does not provide searchable encryption, which is required for flexible data sharing. The proposed scheme addresses this issue by enabling a patient to distribute a single constant-size aggregate key to a data user for sharing a large number of documents and then user submits a single aggregate trapdoor to the cloud for searching over authorized encrypted documents. The novelty of this scheme lies in submitting a single trapdoor for keyword search over documents encrypted with different keys as opposed to traditional methods requiring submission of multiple trapdoors. Performance evaluation confirms that our proposed scheme is practically efficient and also reduces storage overhead by reducing both the number of keys and key-size without affecting security-level, which is highly desired in the resource constraint devices like smart phones.

Ya-ling Zhang et. al. [2] proposed a new multi-users and keyword-based searchable encryption scheme in which document encryption key is not shared among users, which is based on bilinear pairings, and its security in query privacy, query unforgeability and user revocability is proved according to the security definitions. Compared with the previous schemes, the proposed scheme possesses a good overall efficiency, meanwhile needs less storage space.

Rongmao Chen et. al. [3] presenting the practical and applicable treatment on the security vulnerability by formalizing a new PEKS system named Server-Aided Public Key Encryption with Keyword Search (SA-PEKS). In SA-PEKS, to generate the keyword ciphertext/trapdoor, the user needs to query a semi-trusted third party called Keyword Server (KS) by running an authentication protocol and hence security against the off-line KGA can be obtained. They introduce a universal transformation from any PEKS scheme to a secure SA-PEKS scheme using the deterministic blind signature. To illustrate its feasibility, Author presenting the

first instantiation of SA-PEKS technique by utilizing the FDH-RSA signature and the PEKS scheme proposed by Boneh et al. in Eurocrypt 2004. Finally, author describes how to securely implement the client-KS protocol with a rate-limiting mechanism against on-line KGA and evaluate the performance of our solutions in experiments.

Kaitai Liang et. al. [4] proposed a new privacy-preserving functional encryption which is based on search mechanism over encrypted cloud data. A main advantage of new primitive compared to the existing public key based search systems is that it supports an extreme expressive search mode, regular language search. Author shows the security and performance analysis of proposed system is provably secure and more efficient than some searchable systems with high expressiveness.

3. PROPOSED SYSTEM

The design of our KASE scheme draws its insights from both the multi-key searchable encryption scheme and the key-aggregate data sharing scheme. Specifically, in order to create an aggregate searchable encryption key instead of many independent keys, we adapt the idea presented in. Each searchable encryption key is associated with a particular index of document, and the aggregate key is created by embedding the owner's master-secret key into the product of public keys associated with the documents. In order to implement keyword search over different documents using the aggregate trapdoor. The cloud server can use this process to produce an adjusted trapdoor for every document. We propose a concrete Architecture of Key-Aggregate Searchable Encryption (KASE) scheme as follows.

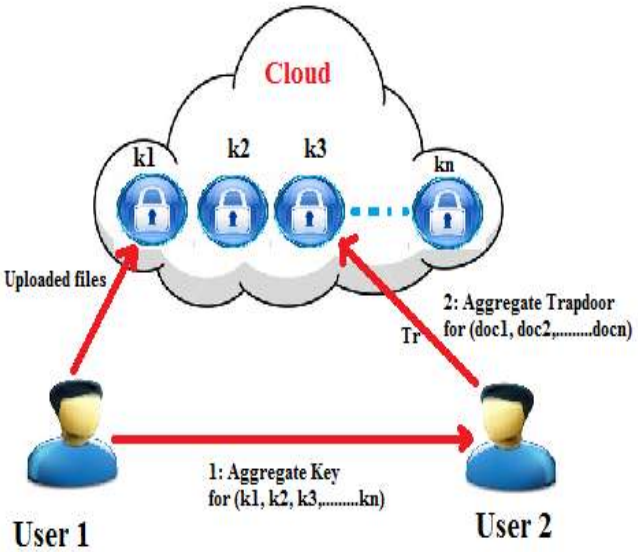

Figure 1: Architecture of Key-Aggregate Searchable Encryption

4. PROPOSED ALGORITHM

Setup (1λ, n): the cloud server will use this algorithm to initialize system parameters as follows:

- Generate a bilinear map group system B= (p, G, G1, e (·, ·)), where p is the order of G and $2\lambda \le p \le 2\lambda+1$.
- Set n as the maximum possible number of documents which belongs to a data owner.
- Pick a random generator $g \in G$ and a random $\alpha \in Zp$, and computes $gi = g(\alpha i) \in G$ for $i = \{1,2,\cdots,n,n+2,\cdots,2n\}$.
- Select a one-way hash function $H: \{0, 1\} * \rightarrow G$. Finally, cloud server publishes the system parameters prams = (B, Pub, H), where Pub = (g, g1, ⋯, Gn, Gn+2... g2n) ∈G2n+1.2)

Keygen: Data owner uses this algorithm to generate his/her key pair. It picks a random $\gamma \in Zp$, and outputs: pk = v = gγ, msk = γ.

Encrypt (pk, i): Data owner uses this algorithm to encrypt data and generate its keyword cipher texts when uploading the i-th document. To generate the keyword cipher texts, this algorithm takes as input the file index $i \in \{1... n\}$, and:

- Randomly picks a $t \in Zp$ as the searchable encryption key ki of this document.
- Generates a delta Δi for ki by computing: c1 = gt, c2 = (v·gi) t
- For a keyword w, outputs its cipher text cw as: cw = e(g,H(w))t/e(g1,gn)t. Note that c1,c2 are public and can be stored in the cloud server.

Extract (msk, S): data owner uses this algorithm to generate an aggregate searchable encryption key. For any subset $S \subseteq \{1, \cdots, n\}$ which contains the indices of documents, this algorithm takes as input the owner's master-secret key msk and outputs the aggregate key kagg by computing: kagg = Πj∈sgγ n+1−j. To delegate the keyword search right to a user, data owner will send kagg and the set S to the user.

Trapdoor (kagg, w): the user uses this algorithm to generate the trapdoor to perform keyword search. For all documents which are relevant to the aggregate key kagg, this algorithm generates the only one trapdoor TR for the keyword w by computing: TR = kagg ·H (w) Then, the user sends (TR, S) to the cloud server.

Adjust (params, i, S, TR): the cloud server uses this algorithm to produce the right trapdoor. For each document in the set S, this algorithm takes as input the system public parameters params, the document index $i \in S$ and the aggregate trapdoor Tr, outputs the right trapdoor Tri by computing: Tri = Tr·Πj∈s,j6=ign+1−j+i Then, the cloud server will use Test algorithm to finish the keyword search.

Test (Tri, i): the cloud server uses this algorithm to perform keyword search over the i-th document. For the i-th document, this algorithm takes as input the adjusted trapdoor Tri, the Δi= (c1, c2) relevant to its searchable encryption ki and the subset S, outputs true or false by judging: cw? == E (Tri, c1)/e (pub, c2) where pub = $\Pi j \in sgn+1-j$. Note that for efficiency consideration, the pub for the set S can be computed only once.

5. CONCLUSION & FUTURE ENHANCEMENT

Taking into consideration of the realistic problem of privacy preserving data sharing system based on public cloud storage which is need a data owner to allocate a large number of keys to users to permit them to access the documents, In this proposed concept of key-aggregate searchable encryption (KASE) and construct a concrete KASE scheme. It can provide an efficient solution to building practical data sharing system based on public cloud storage. In a KASE scheme, the owner needs to distribute a single key to a user when contributing a lot of documents with the user, and the user needs to submit a single trapdoor when they queries over all documents shared by the same owner. On the other hand, if a user wants to question over documents shared by multiple owners, that user must produce multiple trapdoors to the cloud. The future enhancement for this proposed work is to find out how to decrease the number of trapdoors under multi-owners setting by attaining the security.

6. REFERENCES

[1] Prajakta Solapurkar, "Secure Sharing of Personal Health Records on Cloud Using Key-Aggregate Cryptosystem", IEEE, International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.

[2] Ya-ling Zhang, Li-jun Liu, Shang-ping Wang, "Multi-user and Keyword-based Searchable Encryption Scheme", IEEE,12th International Conference on Computational Intelligence and Security, 2016.

[3] Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo, Xinyi Huang, Xiaofen Wang and Yongjun Wang, "Server-Aided Public Key Encryption with Keyword Search", IEEE Transactions On Information Forensics And Security, 2016.

[4] Kaitai Liang, Xinyi Huang, Fuchun Guo, and Joseph K. Liu, "Privacy-Preserving and Regular Language Search over Encrypted Cloud Data", IEEE Transactions on Information Forensics and Security, 2016.

[5] Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo and Xiaofen Wang, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage", IEEE Transactions On Information Forensics Security, 2015.

[6] ZHANG Yaling, JIA Zhipeng,WANG Shangping, "A Multi-User Searchable Symmetric Encryption Scheme for Cloud Storage System", IEEE, 5th International Conference on Intelligent Networking and Collaborative Systems, 2013.

[7] Robert Koletka, Andrew Hutchison, "An Architecture for Secure Searchable Cloud Storage", IEEE, 978-1-4577--1483-2/11/$26.00 ©2011.

[8] Sarika Gupta, Sangita Rani Satapathy, Piyush Mehta, Anupam Tripathy, "A Secure and Searchable Data Storage in Cloud Computing", IEEE, 978-1-4673-4529-3/12/$31.00 c 2012.

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

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

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

[12] 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.

[13] 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.

[14] J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689, Elsevier, 2010.

[15] 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.