International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

Searchable Encryption using Key Aggregate for Data Sharing in Cloud Storage

1.**Abhishek Dubey**
B.E Student
Department of Computer Engineering

2.**Nilesh Gherde**
B.E Student
Department of Computer Engineering

3. **Shubhangi Gavade**
B.E Student
Department of Computer Engineering

4.**Abhijeet Deshmukh**
Professor
Department of Computer Engineering

***Abstract*—*Data sharing is an important functionality in a cloud storage. We propose a searchable encryption using key aggregate for data sharing in cloud storage. In this if user wants to access some information, data or files in cloud storage then the user send request to the authorized person. Then authorized person send one registration form to the user. The user fills the registration form and send to the authorized person. Then the authorized person checks which type of access like public or private information or files. If user wants to access public information or files then they can directly search in cloud storage and access data or information. In this user can not modify and delete data on cloud storage, users can only view and download these data. In the other hand, if the user wants to access private Information in cloud storage, then the authorized person sends the aggregate key to the user through an E-mail. In this we provides features like Integrity, Security, Encryption, Decryption and Searchable encryption. If the authorized person sends key to user to access the information or file and if user share these key to another user. In such a situation we provide OTP and time stamp for extra level of security.*

1.INTRODUCTION

Cloud storage has emerged as a conforming solution for providing ubiquitous, user convenient, and on-demand accesses to large amounts of data shared over the Internet. Today, lots of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being impressed by cloud storage due to its various benefits, including lower cost, greater activity, and better resource utilization. However, while enjoying the convenience of sharing data via cloud storage, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious non-observance of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in iCloud). To address users' concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such a cloud storage is often called the cryptographic cloud storage [6]. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable encryption (SE) scheme in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, such that, for retrieving data matching a keyword, the user will send the corresponding keyword trapdoor to the cloud for performing search over the encrypted data. Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, implementing such a system for large scale applications involving millions of users and billions of files may still be hindered by practical issues involving the efficient management of encryption keys, which, to the best of our knowledge, are largely ignored in the literature. First of all, the need for selectively sharing encrypted data with different users (e.g., sharing a photo with certain friends in a

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

social network application, or sharing a business document with certain colleagues on a cloud drive) usually demands different encryption keys to be used for different files. However, this implies the number of keys that need to be distributed to users, both for them to search over the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keys must not only be distributed to users via secure channels, but also be securely stored and managed by the users in their devices. In addition, a large number of trapdoors must be generated by users and submitted to the cloud in order to perform a keyword search over many files. The implied need for secure communication, storage, and computational complexity may render such a system inefficient and impractical.

2. LITERATURE SURVEY

Attribute Based Encryption for Fine Grained Access Control of Encrypted Data" presented a technique called Key-Policy Attribute Based Encryption .

Sahai and Waters, "Fuzzy Identity-Based Encryption" presented a new type of identity-based encryption that called fuzzy IBE.

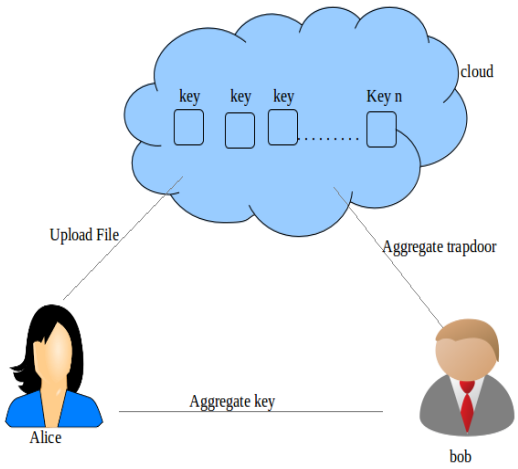
i. EXISTING SYSTEM

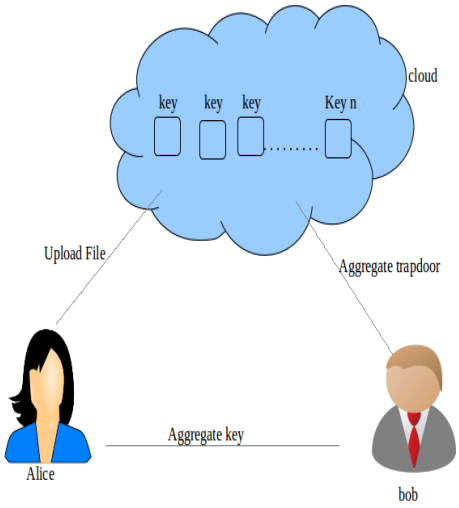
Traditional way-To enforce the access control

Unauthorized user Expose data

The costs and complexities involved generally increase with the number of the decryption keys to be shared.

The encryption key and decryption key are different in public key encryption.





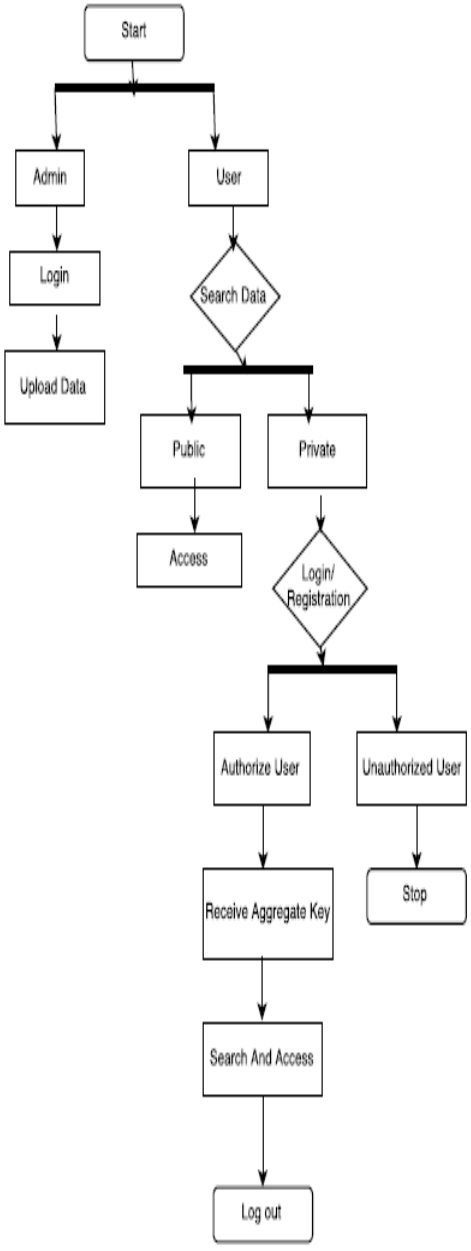
- Cloud
- Public & private
- Searchable Encryption
- Privacy
- Integrity
- Encryption And Decryption

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate machines but reside on a single physical machine. Data in a target could be stolen by instantiating another co-resident with the target one. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owner's anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality. A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the or the honesty of the technical staff. These users are motivated to encrypt their data with their own keys before uploading them to the server.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

Searchable Encryption

Generally speaking, searchable encryption schemes fall into two categories, i.e., searchable symmetric encryption (SSE) and public key encryption with keyword search (PEKS). Both SSE and PEKS can be described as the tuple SE= (Setup, Encrypt, Trapdoor, Test):



_ **Setup**(1_): this algorithm is run by the owner to set up the scheme. It takes as input a security parameter 1_, and outputs the necessary keys.

_ **Encrypt**(k;m): this algorithm is run by the owner to encrypt the data and generate its keyword ciphertexts. It takes as input the data m, owner's necessary keys including searchable encryption key k and data encryption key, outputs data ciphertext and keyword ciphertexts Cm.

_ **Trpdr**(k;w): this algorithm is run by a user to generate a trapdoor Tr for a keyword w using key k.

_ **Test**(Tr, Cm): this algorithm is run by the cloud server to perform a keyword search over encrypted data. It takes as input trapdoor Tr and the keyword ciphertexts Cm, outputs whether Cm contains the specified keyword.

For correctness, it is required that, for a message m containing keyword w and a searchable encryption key k, if (Cm **Encrypt**(k;m) and Tr **Trpdr**(k;w)),then **Test**(Tr, Cm)=true.

ACKNOWLEDGMENT

This work is a part of graduation project done by students of computer engineering. We thank everyone who supported and motivated us. And special thanks to our guide Prof. Abhijeet Deshmukh. Assistant Professor (Computer Engineering).

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 multiowner 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.
[16] J. Li, K. Kim. "Hidden attribute-based signatures without anonymity revocation", Information Sciences, 180(9): 1681-1689, Elsevier, 2010.
[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-
525, 2012.
[22] D. Boneh, C. Gentry, B. Waters." Collusion resistant broadcast encryption with short ciphertexts and private keys", Advances in CryptologyCCRYPTO 2005, pp. 258-275, 2005.
[23] D. H. Phan, D. Pointcheval, S. F. Shahandashti, et al. "Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts", International journal of information security, 12(4):
251-265, 2013.
[24] D. Boneh, B. Lynn, H. Shacham. "Short signatures from the Weil pairing", Advances in Cryptology ASIACRYPT 2001, pp. 514-532, 2001.
[25] L. B. Oliveira, D. F. Aranha, E. Morais, et al. "Tinytate: Computing the tate pairing in resource-constrained sensor nodes", IEEE Sixth IEEE International Symposium on Network Computing
and Applications, pp. 318-323, 2007.
[26] M. Li, W. Lou, K. Ren. "Data security and privacy in wireless body area networks", Wireless Communications, IEEE, 17(1): 51-58, 2010.
[27] D. Boneh, C. Gentry and B. Waters. "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", CRYPTO'05, pp. 258C275, 2005.
[28] R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption".Cryptology ePrint Archive, Report 2013/508, 2013.