Open access Journal International Journal of Emerging Trends in Science and Technology
Impact Factor: 2.838 DOI: http://dx.doi.org/10.18535/ijetst/v3i05.07

Exploration Encryption Mechanism Using Single Key for Public Cloud Storage

Authors
Abhilash T P[1], Pranathi P[2], Shalini P M[3]
[1,2,3]PG Student, Dept of Computer Science & Engineering, SSIT, Tumakuru, Karnataka, India

Abstract
Sharing of Data is an main functionality in cloud Computing. In this system, we show how to share data in securely, flexibly, efficiently, and with others in cloud computing. Cloud storage is a bulk of information online in cloud which is able to access from various and associated assets. Cloud storage can give great openness and reputability, solid assurance, disaster recuperation, and most minimal expense. Cloud storage having significant usefulness i.e. safety, productively, adaptable offering information to others. New public–key encryption which is called as Enhanced Searchable cryptosystem (ESE) is presented. ESE produce steady size ciphertexts such that effective authorization of decipherment rights for any arrangement of ciphertext are conceivable. Any set of secrete keys can be aggregated and make them as single key, which incorporates force of the considerable number of keys being aggregated. This aggregate key can be sent to the others for decipherment of ciphertext set and remaining encoded records outside the set are stays secret.

Keywords— *Searchable Encryption, SSE key, public-key encryption.*

Introduction

Distributed computing has changed the way associations approach IT, empowering them to end up more coordinated, present new plans of action, give more administrations, and diminish IT costs. Distributed computing advancements can be executed in a wide assortment of architectures, under various administration and organization models, and can exist together with different innovations and programming outline approaches.

Information insurance beat the rundown of cloud concerns today. Nonetheless, while getting a charge out of the comfort of sharing information through distributed storage, clients are likewise progressively worried about unintentional information spills in the cloud. Such information spills, brought on by a malevolent foe or an acting up cloud administrator, can as a rule lead to genuine breaks of individual protection or business mysteries (e.g., the late prominent episode of big name photographs being spilled in iCloud). To address clients' worries over potential information spills in distributed storage, a typical methodology is for the information proprietor to scramble all the information before transferring them to the cloud, such that later the encoded information might be recovered and decoded by the individuals who have the unscrambling keys. Such a distributed storage is frequently called the cryptographic distributed storage. On the other hand, the encryption of information makes it trying for clients to seek and after that specifically recover just the information containing given watchwords. A typical arrangement is to utilize a searchable encryption (SE) plan in which the information proprietor is required to scramble potential catchphrases and transfer them to the cloud together with encoded information, such that, for recovering information coordinating a watchword, the client will send the comparing catchphrase trapdoor to the cloud for performing look over the scrambled information. In spite of the fact that consolidating a searchable encryption plan with cryptographic distributed storage can accomplish the essential security prerequisites of a cloud capacity, actualizing such a framework for expansive scale applications including a large number of clients and billions of documents might at present be impeded by functional issues including the productive administration of encryption keys, which, to the best of our insight, are to a great extent overlooked in the writing. Above all else, the requirement for specifically offering encoded information to various clients (e.g., offering a photograph to specific companions in an interpersonal organization application, or imparting a business record to specific associates on a cloud drive) for the most part requests diverse encryption keys to be utilized for various documents. Be that as it may, this suggests the number of keys that should be disseminated to clients, both for them to look over the encoded records what's more, to decode the records, will be corresponding to the quantity of such documents such an expansive number of keys.

Related Works:

Enaloh et al. [2] exhibited an encryption plan which is initially proposed for briefly transmitting substantial number of keys in broad scenario [3]. The development is straightforward and we quickly audit its key generation process here for a solid portrayal of what are the alluring properties we need to accomplish.

The determination of the key for an arrangement of classes (which is a subset of all conceivable ciphertext classes) is as per the following. A composite modulus is picked where p and q are two expansive random primes. An expert mystery key is picked aimlessly. Every class is connected with a particular prime. All these prime numbers can be placed in people in general framework parameter. A consistent size key for set can be produced. For the individuals who have been designated the entrance rights for S' can be created. In any case, it is intended for the symmetric-key setting. The substance supplier needs to get the comparing mystery keys to scramble information, which is not suitable for some applications. Since technique is utilized to produce a secrete key as opposed to a couple of open/mystery keys, it is hazy how to apply this thought for open key encryption plan. At last, we take note of that there are plans which attempt to diminish the key size for accomplishing verification in symmetric-key encryption, e.g., [4]. Be that as it may, sharing of unscrambling force is not a worry in these plans.

Identity based encryption:

Identity based encryption (IBE) (e.g., [5], [6], [7]) is an public key encryption in which user in general key of a user can be set as a identity-string of the client (e.g., an email address, portable number). There is a private key generator (PKG) in IBE which holds an master secrete key and issues a secrete key to every client regarding the user personal information. The data provider can take people in general parameter and a user identity to scramble a message. The beneficiary can decode this ciphertext by his mystery key. Guo et al. [8], [9] attempted to fabricate IBE with key collection. In their plans, key collection is obliged as in all keys to be aggregated must originate from various identity divisions‖. While there are an exponential number of personalities and along these lines secrete keys, just a polynomial number of them can be aggregated.[1] This altogether expands the expenses of putting away and transmitting ciphertexts, which is not practical as a rule, for example, shared cloud storage. As Another approach to do this is to apply hash capacity to the string meaning the class, and continue hashing more than once until a prime is acquired as the yield of the hash function. [1] we specified, our plans highlight consistent ciphertext size, and their security holds in the standard model. In fluffy IBE [10], one single minimized mystery key can decode ciphertexts encoded under numerous characters which are close in a specific metric space, however not for a discretionary set of identities and accordingly it doesn't coordinate with our concept of key aggregation.

Attribute Based Encryption:

ABE has demonstrated its promising future in fine-grained access control for outsourced touchy information [11], [12], [13]. Normally, data are encrypted by the owner under a set of parameters. The gatherings getting to the information are doled out access structures by the owner and can unscramble the information just if the access structures coordinate the information traits.

Mate [11] proposed a scheme which is aim for suitable for access control to data stored in the cloud. For this reason, we focus on giving to the encryption full control over the entrance rights, giving practical key administration even in the event of numerous free powers, and empowering reasonable client denial, which is fundamental by and by.

Cheng-Chi Lee [12] made review five distinctive characteristic based encryption plans: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, and HABE, and delineate their plans and look at them. These plans can be ordered by access approach. The entrance strategy in the client's private key is KP-ABE, and the entrance approach in the encoded information is CP-ABE. Plus, we can discover these plans that are difficult to fulfill client responsibility. In addition, the entrance structure is pre-characterized in these plans; if another client needs to get to information and his qualities are not in the entrance structure, these encoded information will be re-produced.

Considering above issues, in this paper presented an efficient approach which utilizes searchable encryption.

Proposed System:

We propose the novel methodology of Enhanced searchable encryption (ESE) as an improved solution, as portrayed in Figure 1, in ESE, user1 necessities to issue a solitary aggregate key, rather than $\{k_i\}m_i = 1$ for sharing m documents with user2, and smash needs to issue a solitary aggregate trapdoor, rather than $\{ Tr_i \}m_i = 1$, to the cloud server. The cloud server can use this aggregate trapdoor and some open information to complete catchphrase seek and return to the outcome to user2. As a result, in ESE, the delegation of keyword search can be accomplished by sharing the single aggregate key.

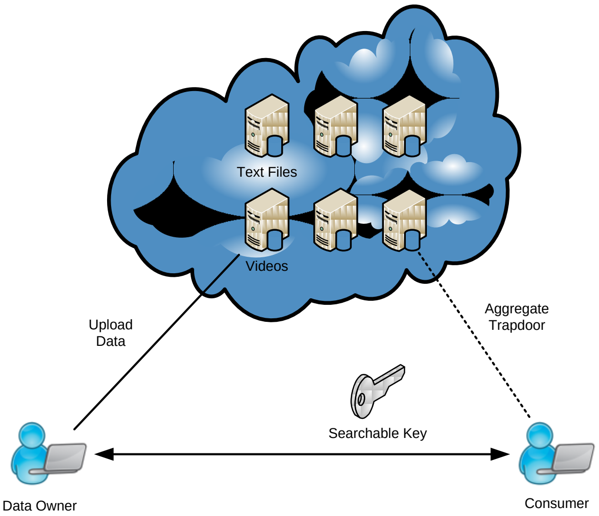


Figure 1: Overview of Proposed system

The ESE development is made out of a few algorithms. Exceptionally, to set up the strategy, the cloud server would produce public parameters of the system in Setup phase, and these open parameters can be further process by different data owners to disperse their documents. For every data owner, they ought to create a public/master-secret key pair through the Key generation algorithm. Keywords of every document can be encrypted through the Encrypt algorithm with the restrictive searchable encryption key. All things considered, the information proprietor can apply the expert mystery key to create a total searchable encryption key for a gathering of chose reports through the Extract calculation. The total key can be spread safely to affirm clients who need to get to those records. After that, as appeared in Figure 2, an ensured client can generate a keyword trapdoor by means of the Trapdoor algorithm utilizing this aggregate key, and submit the trapdoor to the cloud. After the trapdoor is accessible, to complete the keyword search over the specific set of data, the cloud server will run the Adjust algorithm to create the privilege trapdoor for every archive, and after that run the Test algorithm to test whether the data consists the keyword.

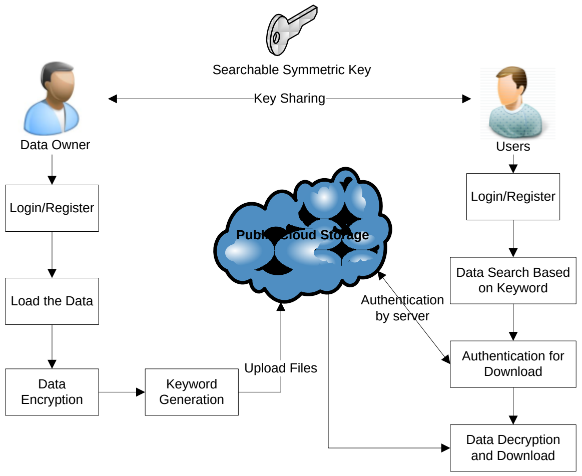


Figure 2: Architecture of ESE framework

Users:

Data Owner

Cloud Data owner is a data uploader. For uploading data must register to cloud. Data owner can do several functionalities such as follows:

Key generation:

Here a random key pair (p_k, ms_k) will be generated with irrespective of size of the data.

Data Encryption:

This process is achieved before uploading the n files into the cloud storage. To encrypt the i^{th} document and generate its keywords' ciphertext, for each document, this algorithm will create a delta Δ_i for its searchable encryption key k_i. Using the public key p_k and the file index i , this algorithm results ciphertext and keyword ciphertext C_i.

Searchable Symmetric Key Generation:

To share the particular set of data to user data owner needs to generate key for the set of documents. It takes input as owner's master-secrete key ms_k and a set of documents which will be shared to users.

Data Consumer

Data consumer can download the single data or set of data from the cloud using the SSE key shared by the data owner. For each set of files a keyword w will be generated.

Cloud Server

Cloud server is responsible for the tracking the cloud users and cloud functionality. Which includes proper authentication when registration of users and downloading data from the cloud storage.

Result and Discussion:

The proposed system is implemented on eclipse. Here data owner can upload single file or multiple files. When uploading files to cloud an SSE key will be generated. Based on SSE key user can download the number of files as shown in below Figures. Generation of SSE key reduces the time consumption and improves the access performance.

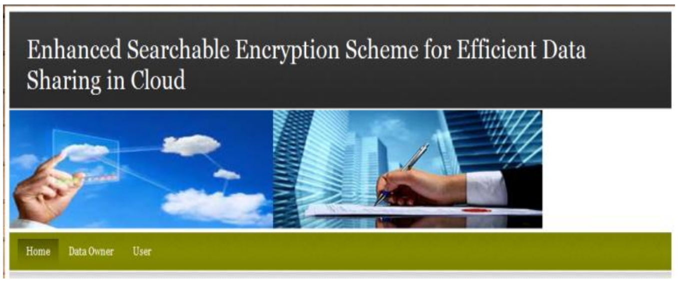
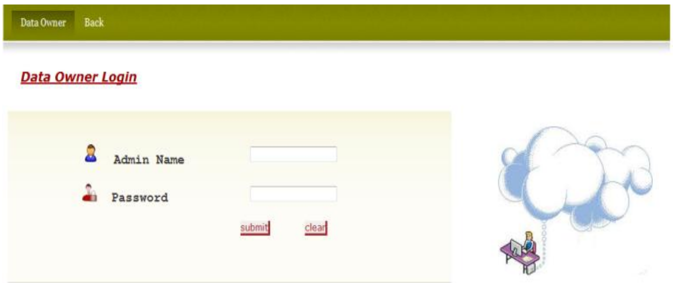

Enhanced Searchable Encryption Scheme for Efficient Data Sharing in Cloud

Figure 3: Home Page

A home page or index page is the initial page of a website. Home page includes the option home, dataowner and user from that the further pages will be operated.



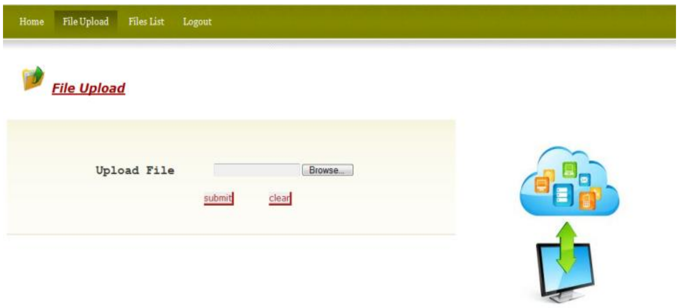
Data Owner Login

Admin Name

Password

Figure 4: Data Owner Login Page

It is the page where the dataowner will login to the page. It contains admin name and password from this page the addmin can login and select the flies and encrypt the files.

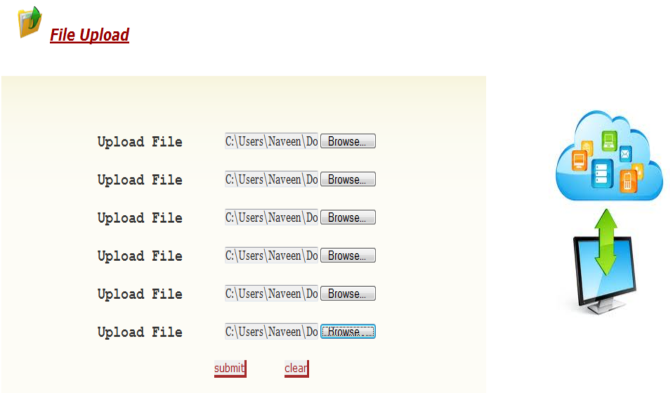


File Upload

Upload File

Figure 5: Upload Single File

After the dataowner login and select the page he will upload the file to the cloud.it may be of single file or multiple file.

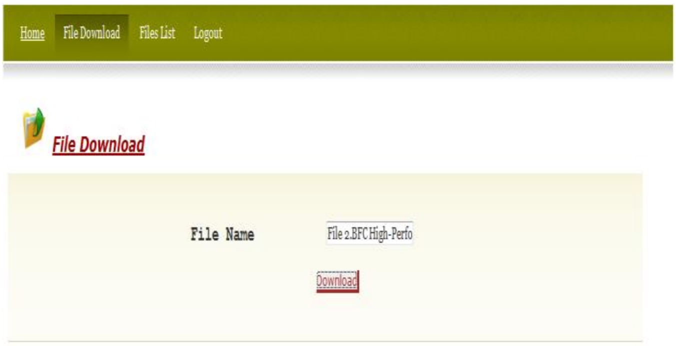

File Upload

Upload File C:\Users\Naveen\Do Browse...
Upload File C:\Users\Naveen\Do Browse...
Upload File C:\Users\Naveen\Do Browse...
Upload File C:\Users\Naveen\Do Browse...
Upload File C:\Users\Naveen\Do Browse...
Upload File C:\Users\Naveen\Do Browse...

submit clear

Figure 6: Upload Multiple File

In this page dataowner will upload multiple files to the cloud and it must be of encrypted file.


Home File Download Files List Logout

File Download

File Name File 2.BFC High-Perfo

Download

Figure 9: Downloading File

In his page the user will dowload the file which is uploaded by the dataowner.

Conclusion

Considering the sensible issue of security ensuring information sharing system in light of public cloud storage which needs data provider to appropriate an extensive number of keys to customers to permit them to get to the records, in this proposed thought of Enhanced searchable encryption (ESE) and build up a strong ESE approach. It can give a profitable response for building valuable information sharing system in light of public cloud storage. In this approach, the data owner needs to share a single key to a customer (data consumer) while contributing an extensive measure of data with the customer, and the customer need to exhibit a secrete trapdoor when they doubt general records shared by the same data owner.

In future work we can integrate aggregate key generation with searchable encryption.

References

1. Cheng-Kang Chu, Chow, S.S.M, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, Volume 25, Issue: 2, 2014.
2. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records”, in Proceedings of ACM Workshop on Cloud Computing Security (CCSW ’09). ACM, pp. 103–114, 2009.
3. J. Benaloh, “Key Compression and Its Application to Digital Fingerprinting”, Microsoft Research, Tech. Rep., 2009.
4. B. Alomair and R. Poovendran, “Information Theoretically Secure Encryption with Almost Free Authentication”, J. UCS, Volume 15, Issue 15, pp. 2937–2956, 2009.
5. D. Boneh and M. K. Franklin, “Identity-Based Encryption from the Weil Pairing”, in Proceedings of Advances in Cryptology, Volume 2139. Springer, pp. 213–229, 2001.
6. Sahai and B. Waters, “Fuzzy Identity-Based Encryption”, in Proceedings of Advances in Cryptology, Volume. 3494, Springer, pp. 457–473, 2005.
7. S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, “Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions”, in ACM Conference on Computer and Communications Security, pp. 152–161, 2010.
8. F. Guo, Y. Mu, and Z. Chen, “Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key”, in Proceedings of Pairing-Based Cryptography, Volume 4575. Springer, pp. 392–406, 2007.
9. F. Guo, Y. Mu, Z. Chen, and L. Xu, “Multi-Identity Single-Key Decryption without

Random Oracles", Information Security and Cryptology, Volume 4990. Springer, 2007, pp. 384–398.

10. S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions", in ACM Conference on Computer and Communications Security, pp. 152–161, 2010.
11. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data", in Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98, 2006.
12. M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.
13. Mate Horvath, "Attribute-Based Encryption Optimized for Cloud Computing", Springer, pp. 566-577, 2013.
14. Cheng-Chi Lee, Pei-Shan Chung and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Volume15, Issue4, pp. 231-240,2013.
15. Bharti Ratan Madnani and Sreedevi N, "Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation", International Journal of Innovative Research in Computer and Communication Engineering, Volume 1, Issue 3, May 2013.