ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

An Efficient Scalable Data Sharing In Cloud Storage Using Key Aggregate Encryption

K Koteswara Chari #1, M Krishna #2
#1Student of M.Tech (CSE) and Department of Computer Science Engineering,
#2 Asst.Prof, Department of Computer Science and Engineering, Sir C R Reddy College of Engineering, Eluru, W.G.DIST

ABSTRACT:
In Cloud Computing data partaking is better concept on daily functions. and security is important functionality. Previously We describe public key cryptosystem . But these type crypto systems failure on maintain keys and safe keeping of keys. So the new thing is that one key of aggregation it will produced directly form cloud server instead of poll of secrete keys. So that can provides the power of all keys aggregated. In new technology we are also sending key through email for security reasons. Ensuring we are providing the security of cloud computing why because it is second major factor on clouds. In previous these type of works are defended they are not supported on multi clouds and these are destroyed the cloud services without secracy . A movement towards "Multi-Clouds", In other words "Inter-Clouds" or "Cloud-Of-Clouds" as emerged recently. This works aim to reduce security risk and better elasticity and efficiency to the user. New public key management of encryption which is called as Key aggregate encryption (KAE) is presented.

Keywords— Cloud storage, data sharing, key-aggregate encryption, Public Key Encryption.

Introduction:

Now a day's cloud is gaining popularity. The demand of data outsourcing is handled and manages of corporate data. Generally many online free space providers provides Free storage space more than 15 GB take few thousands amount more than 1 TB. The main benefit that it's not only providing elasticity and resourcability but it also provides maintainability and accessing easily data. Cloud service providers have most critical issues of data integrity and privacy because data not store on his own servers the privacy can be achieve by diving and encrypted data store on service providers with the respect of quality access data. In cloud shared commuting environments, things become even worse. Different clients can be posted on separate Virtual machines but resides on a single physical machine. For the data privacy a cryptography solution are confident. In a sharable data the number theoretic assumptions is more desirable but user is not perfectly happy. As well as the technical staff of service providers may not be trusted. Assume that Suhas puts his all documents in Google drive, and He does not want to expose to others due to data leakage possibility Suhas cannot feel protection his data. So He encrypts his data using his own keys before uploading. One day, Suhas's partners Pritam ask his to share some data for security a possible option. Suhas choose it to securely send Pritam. The secrete keys involved. Mainly , there are two ways for traditional encryption rules:

- Suhas encrypts all data with a only one encryption key.
- Suhas encrypts files with distinct keys and send s provider the Corresponding secret keys.

Example, in enterprise settings, every Client can upload encrypted data on the cloud storage server without theknowledge of the company's master-secret key.[1] Therefore, the best solution for the above problem is that Suhas encrypts files with dis tinct public-keys, but only sends Pritam a single (constant-size) decryption key. Since the decryption key should be directed through a secure channel and kept secret, small key size is always desirable. For example, we cannot guess great storage for decryption keys in the resource-constraint devices like smart phones, The smart cards or the wireless sensor nodes. Especially, these secret keys are usually stored in the tamper-proof memory, which is relatively costly [2].

II. Related Work

Symmetric-Key Encryption with Compact Key

An encryption plan which is initially proposed for succinctly transmitting substantial number of keys in show situation [3]. The development is straightforward and we quickly survey its key determination transform here for a solid portrayal of what are the attractive properties we need to accomplish. The induction 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 huge arbitrary primes. An expert mystery key is picked indiscriminately. Every class is connected with a particular prime. All these prime numbers can be put 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. Then again, 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 mystery esteem instead of a couple of open/mystery keys, it is misty how to apply this thought for open key encryption plan. At long last, we take note of that there are plans which attempt to decrease the key size for accomplishing validation in symmetric-key encryption.

A. Study of Existing Systems/ Technologies I. Identity Bases Encryption (IBE): IBE is a type of a public-key encryption. User's public key (it's a set of encryption that is Identity-String). In IBE, Master secret keys are generated by the private key generator and here on the basis on user's identity secret key is provided. Sender wants to share files. So sender will encrypt the files by making use of user identity and public parameter and sends the files. By making use of his secret key Receiver will Decrypt Files. But out of key-aggregation and IBE, Random oracles assumed by only one. .From various identity key aggregation is inhibited as key to be aggregated.[3]

Advantages

- Encryption type is public-key encryption.
- This scheme has a dependable party which will grasp secret key.
- Based on the identity, secret key will be provided. Size of decryption key is Constant .

Disadvantage

- Cipher text size is non-constant.
- Cost of storing cipher text and transmitting it expensive.

III. Proposed Method

A. Framework

The basis or outline of the key-aggregate encryption scheme consists of five polynomial-time algorithms, which are elucidated below: Setup ensures that the owner of the data can construct the public system stricture or parameter. KeyGen, as the name suggests generates a public/mastersecret (not to be confused with the delegated key explained later) key pair. By using this public and master-secret key cipher text class index he can convert plain text into cipher text via use of Encrypt. Using Extract, the master-secret can be utilized to generate an aggregate decryption key for a set of cipher text classes. These generated keys can be safely transported to the appointees by use of secure mechanisms with proper security measures adhered to. If and only if the cipher text's class index is enclosed in the single key, then every user with an aggregate key can decrypt the given cipher text provided through the use of Decrypt

B. Algorithm

1. Setup(Security level parameter, number of cipher text classes): Setup ensures that the owner of the data can construct the public system stricture or parameter he create account on cloud. After entering the input, the total of cipher text classes n and a security level parameter 1, the public system parameter is given as output, which usually skipped from the input of other algorithms for the purpose of conciseness. 2. KeyGen: it is for generation of public or master key secret pair. 3. Encrypt(public key,index,message):run any person who want to convert plaintext into cipher text using public and master-secret key 4. Extract(master key, Set): Give input as master secret key and S indices of different cipertext class it produce output aggregate key. This is done by executing extract by the data owner himself. The output is displayed as the aggregate key represented by Ks, when the input is entered in the form the set S of indices relating to the various classes and mastersecret key msk 5. Decrypt (Ks,S,i,C): When an appointee receives an aggregate key Ks as exhibited by the previous step, it can execute Decrypt. The decrypted original message m is displayed on entering Ks, S, i, and C, if and only if I belongs to the set S.

Conclusion

Clients information protection is a focal inquiry of distributed storage. Pack mystery enters in broad daylight key cryptosystems which bolster assignment of mystery keys for distinctive figure content classes in cloud capacity. Regardless of which one among the force set of classes, the delegatee can simply get a total key of steady size. In distributed storage, the quantity of figure messages for the most part becomes quickly with no limitations. So we have to save enough figure content classes for the future augmentation. Else, we have to grow general society key. Despite the fact that the parameter can be downloaded with figure writings, it would be better in the event that its size is free of the greatest number of figure content classes.

VIII. References

[1] Cheng-Kang Chu ,Chow, S.S.M, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng , — Key-Aggregate Cryptosystem forScalable Data Sharing in Cloud Storage‖ , IEEE Transactions on Parallel and Distributed Systems. Volume: 2 5, Issue: 2. Year :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, 2009, pp. 103–114

[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, vol. 15, no. 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 –CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.

[6] A. Sahai and B. Waters, —Fuzzy Identity-Based Encryption,‖ in Proceedings of Advances in Cryptology - EUROCRYPT '05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457–473.