ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

A Secured Cryptographic Technique for Protecting Online data in the Cloud

[1] Ashish Ladda, [2] Sandhya Mekala
[1][2] Assistant Professor in CSE Dept, Balaji Institute of Technological Sciences

***Abstract* - Cloud computing may be an in style space of analysis for inventors. And it's important in information sharing applications. On cloud the info being shared should be secure. The pliability and therefore the potency of the info is rely upon the protection parameter. To attain purpose we tend to outline new algorithms that is rely upon public key cryptography and outline constant size cipher text by exploitation these key we are able to decode cipher text. The opposite encrypted files except this cipher stay personal. The survey depicts some encoding schemes introduced during this information privacy for firmly and economical sharing of confidential information over a secure channel. Recently analysis concentrate on aggregation of keys of the keys in signal aggregation key that is assistance on load of network information sharing being vital practicality in cloud storage implement show to firmly, expeditiously, and flexibly share information with others.**

Keywords: Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

INTRODUCTION

Cloud storage is turning to be an important feature today. [1]In enterprise settings, we tend to see the increase in demand for information outsourcing that edges within the field of company information and its management. It's conjointly helpful as a core technology for various on-line technologies for individual applications. Cloud computing is thought as another to [2] ancient technology because of its higher resource-sharing and low maintenance capabilities. the most aim of cloud computing is to produce high performance energy of computing for varied field like military and analysis organization for playacting billions of computations at every second. it's conjointly utilized in client bound areas like portfolios to transfer guidance. [3]In cloud computing, the cloud service suppliers, like Amazon, area unit ready to offer varied services to users with the assistance of powerful information servers. Moving the native information management systems into cloud servers, users will make the most of high-quality services and store vital investments on their native infrastructures. However, whereas sharing information through cloud storage, users area unit at the same time privy to the info leakages within the cloud. One amongst the foremost basic services delivered by cloud service suppliers is information storage. Take into account a knowledge application. There's a corporation which allows its staffs within the same cluster or department to store and share documents or files within the cloud. Exploitation the cloud, the staffs will be absolutely discharged from the native information storage and maintenance. However, it conjointly creates a major risk to the confidentiality of these hold on documents. Specifically, the cloud servers controlled by cloud suppliers aren't absolutely believed by users whereas the documents hold on within the cloud is also s confidential, like business ideas. Identification of privacy is most significant drawback for wide development of cloud computing. While not the proof of identity privacy users aren't able to utilize the cloud services as a result of they don't need to show their real identity. To take care of information privacy, a basic plan is to encode files, so transfer the encrypted information into the cloud. During this paper, we tend to demonstrate crypto logical situations for the matter of looking out on encrypted information and supply results of security for the ensuing crypto systems. The storage within the cloud has materialized as a capable account appropriate and on-demand accesses to large amounts of data shared over the net. Business user's area unit being attentive by cloud storage because of its many edges, together with lower value, higher gracefulness, and improved resource utilization. Everyday users are sharing personal information, like photos and videos, with their friends through social network applications supported cloud. On the opposite hand, whereas profiting from the advantage of sharing information through cloud storage, users are bit by bit troubled concerning accidental information reveal

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

by the cloud. Such information revealing, are performed by malicious opponent or a mischievous cloud operator, will routinely direct to severe violation of personal information or confidential information concerning business. [4]In this paper, we tend to propose the novel thought of key mixture searchable encoding (KASE), and instantiating the thought through a concrete KASE technique. The planned KASE theme relates to any cloud storage that supports the searchable cluster information sharing feature, which suggests any user could value more highly to distribute a bunch of files that area unit selective with a bunch of designated users, whereas allowing the ultimate to hold out keyword search on top of the sooner. to take care of searchable cluster information sharing the most wants for economical key management area unit double. Primarily, a knowledge owner needs to portion one mixture key (instead of a bunch of keys) to a user for sharing any variety of files. Subsequent, the user must submit one mixture trapdoor to the cloud for playacting keyword search over any amount of shared files. KASE theme will assure each requests.

II. LITERATURE SURVEY

Existing System

A. Predefined Hierarchy using Cryptographic Keys:Cryptographic key assignment main aim is to minimize the expense in storing and managing secret keys for cryptographic use. Utilizing a tree structure, the keys of its descendant nodes can be derived using a key for a given branch. Advanced cryptographic key assignment scheme (e.g., [1], [2], [3], [4]) support access policy that can be modelled by cyclic graph or acyclic graph

B. Symmetric-Key Encryption using Compact Key:An encryption scheme is originally proposed for concisely transmitting large number of keys in broadcast scenario [5]. Finally, we see that there are many types which try to minimize key size for getting authentication in symmetric-key encryption, e.g., [6]. Hence sharing of decryption power is not a problem in these schemes. C. Identity-Based Encryption (IBE) using Compact Key IBE is one of the types of public-key encryption where the public-key of a user can be used as an identity string of the user. (e.g., [7], [8], [9])There is a trusted party known as private key generator in IBE which holds master-secret key and issues a secret key to each and every user with respect to the user identity. The encryption can take the public parameter and an user identity to encrypt a message. Recipient can decrypt this cipher-text by his secret key. D. Attribute-based encryption (ABE) ABE permits each cipher text to be associated with an attribute, [10], [11]and master secret key holder extract a secret key for a policy of these attributes so that cipher text can be decrypted by this key its associated attribute observe to the policy. E. Primitive is proxy re-encryption (PRE) to delegate decryption power of cipher texts without sending the secret key to the delegate, a useful primitive is proxy re-encryption (e.g [11], [12]). It allows sender to delegate to the server the ability to convert cipher text encrypted under the public-key into ones for receiver.

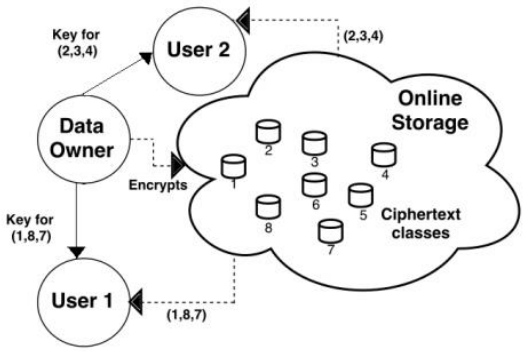

Fig 1: Key-Aggregate Cryptosystem for Online Storage

III. PROPOSED METHODOLOGIES

Multiuser Searchable Encryption

A rich literature has been available on searchable encryption. Including SSE schemes and PEKS schemes. Contradictory to those existing work, in the control of cloud storage keyword search under the multi tenancy setting is a more common scenario. [3]In such a scenario, the data owner would like to share a document with a group of authorized users and the user who has access right can provide a trapdoor to perform the keyword search over the shared document namely the "Multi user searchable encryption" scenario. Some recent work, focus to such a MUSE scenario. Though they all adopt single key combined with access control to achieve the goal. In,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Muse scheme are constructed by sharing the document's searchable encryption key with all users who can access its and broadcast encrypting is used to achieve coarse joined access control. In, attributes based encryption is applied to achieve line grained access control aware keyword search as shown in Fig.1. The main problem in MUSE has been to control users who can access documents, In order to reduce the number of shared keys and trapdoors are not considered. Key aggregate searchable encryption can provide the solution for the latter and it can make MUSE more efficient and practical. B. Multi Key Searchable Encryptions [13]In multi user application the number of trapdoors are proportional to the number of documents to search over different provides to the server a keyword trapdoor under each key which have to be matched and document can be encrypted firstly introduces the concept of multi key searchable encryption (MKSE) and places forward the first feasible scheme in 2013 MUSE enables a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoor's keyword in documents encrypted with different keys. KASE is altogether different from MKSE. KASE delegates the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system while the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user. C. Key Aggregate Encryption For Data Sharing Data sharing system based on closed storage has much priority now days. In particular, how to reduce the number of distributed data encryption keys sharing different document with different encryption keys with the same user the data owner will need to distribute all such keys to him/her in a traditional approach which is usually impractical. [16]In order to resolve this problem key aggregate encryption (KAE) scheme for data sharing is proposed to generate an aggregate key for the user to decrypt all the documents. A set of documents encrypted by different keys to be decrypted with a single aggregate key so that user can encrypt a message both under a public key and under the identifier of each documents The construction is inspired by the broadcast encryption key The data owner can be regarded as the broadcaster who has public key pk and master key MSK Every document with identifier's can be regarded as a receiver listening to the broadcast channel and a public information used in decryption is designed to be relevant to both the owner's MSK and the encryption key the message encryption process has resemblance with data encryption using symmetric encryption in BE but the key aggregation and data encryption are regarded as mathematical transformation of BR Encrypt algorithm and BE Decrypt algorithm respectively.

Algorithms:

- Setup(1λ): This algorithm is run by the owner to set up the scheme. It takes as input a security parameter 1λ and outputs the necessary keys. Encrypt(l;n): This algorithm is run by the owner to encrypt the data and generate its keyword ciphertexts. It takes as input the data n, owner's necessary keys including searchable encryption key l and data encryption key, outputs data ciphertext and keyword ciphertexts Cn.

- Trpdr(l;x): This algorithm is run by a user to generate a trapdoor Trd for a keyword w using key l.

- Test(Trd, Cn): This algorithm is run by the cloud server to perform a keyword search over encrypted data. It takes as input trapdoor Trd and the keyword ciphertexts Cn, outputs whether Cn contains the specified keyword. For exactness, it is required that, for a message n containing keyword x and a searchable encryption key l, if (Cn◊Encrypt(l;n) and Tr◊Trpdr(l;x)), then Test(Trd, Cn)=true.

Table 1: NIST recommended key sizes

Symmetric algorithm (bit)	RSA and DH (bit)	ECC (bit)
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

3.2 Elliptic Curve Cryptography In 1985, Neal Koblitz and Victor Miller independently proposed using elliptic curves to design public key cryptographic systems. In the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

late 1990`s, ECC was standardized by a number of organizations and it started receiving commercial acceptance. Nowadays, it is mainly used in the resource constrained environments, such as ad-hoc wireless networks and mobile networks. Elliptic curves are used to construct the public key cryptography system. The private key d is randomly selected from [1, n-1], where n is integer. Then the public key Q is computed by dP, where P,Q are points on the elliptic curve. Like the conventional cryptosystems, once the key pair (d, Q) is generated, a variety of cryptosystems such as signature, encryption/decryption, key management system can be set up. ECC requires significantly smaller key size with same level of security. Benefits of having smaller key sizes are faster computations need less storage space. ECC ideal for constrained environments such as Pagers, PDAs, Cellular Phones, Smart Cards.

IV. CONCLUSION AND FUTURE WORK

How to shield users' information privacy may be a central question of cloud storage. With a lot of mathematical tools, crypto logical schemes are becoming a lot of versatile and infrequently involve multiple keys for one application. During this article, we tend to take into account the way to "compress" secret keys in public-key cryptosystems that support delegation of secret keys for various cipher text categories in cloud storage. Despite that one of the facility set of categories, the delegate will perpetually get AN mixture key of constant size. Our approach is a lot of versatile than graded key assignment which might solely save areas if all key-holders share an analogous set of privileges. A limitation in our work is that the predefined sure of the amount of most cipher text categories. In cloud storage, the amount of cipher texts typically grows speedily. Therefore we've got to order enough cipher text categories for the longer term extension. Otherwise, we want to expand the public-key as we tend to delineated though the parameter will be downloaded with cipher texts, it might be higher if its size is freelance of the most variety of cipher text categories. On the opposite hand, once one carries the delegated keys around in an exceedingly mobile device while not exploitation special trusty hardware, the secret's prompt to escape, coming up with a escape resilient cryptosystem [22], [34] nevertheless permits economical and versatile key delegation is additionally a motivating direction.

REFERENCES

[1] S. G. Akl and P. D. Taylor, ―Cryptographic Solution to a Problem of Access Control in a Hierarchy,‖ ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239–248, 1983.

[2] G. C. Chick and S. E. Tavares, ―Flexible Access Control with Master Keys,‖ in Proceedings of Advances in Cryptology – CRYPTO '89, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322.

[3] W.-G. Tzeng, ―A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy,‖ IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188, 2002.

[4] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, ―Provably-Secure Time-Bound Hierarchical Key Assignment Schemes,‖ J. Cryptology, vol. 25, no. 2, pp. 243–270, 2012.

[5] 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

[6] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS ‟07). ACM, 2007, pp. 185–194.

[7] L. Hardesty, "Secure computers aren‟t so secure," MIT press, 2009, http:// www. physorg. com/news 176107396.html.

[8] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2,

pp. 362–375, 2013.

[9] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[10] G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in Proceedings of Advances in Cryptology – CRYPTO ‟89, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322.

[11] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188, 2002.