ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Multi Point Encryption In Clod Data Transmission

[1] K.N.Ashwini Jayamma, [2] Dr.R.Karthikeyan
[2] Professor, Department Of Computer Science And Engineering, BIHER
[1] Student , Department Of Computer Science And Engineering ,BIHER

Abstract: ***A re-encryption scheme of public key cryptography is proposed for secure data sharing in public cloud. The re-encryption scheme offers owner to securely store his data in cloud by encrypting the data over an asymmetric data encryption and symmetric data encryption is further encrypted by the public key of data owner which is also stored in the cloud and is made available to all the legitimate recipients in accordance with the access control. The cloud maintained here is a public cloud and is a semi-trust as because it does not allow the owner. Data owner's stores encrypted data in the cloud to ensure security for his data in the cloud computing environment and issues decryption key to only authorized user to access the data from cloud. When user is revoked, data owner as to re-encrypt the data so that revoked user cannot access the data again .To perform this operation he will issue re-encryption command to cloud so that data in cloud gets re-encrypted. Once re-encryption is done there is a need for generation of new decryption keys to valid user, so that they can continue to access the data.***

I. INTRODUCTION

A public cloud is one based on the standard cloud computing paradigm, where a cloud service provider makes numerous resources like servers and storage, available globally over the web. Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organizations hoping to gain profit. People love to share information with one another. Due to all these advantages of the public cloud many of the organizations are now use the pubic cloud to store the data. But there are some problems with this public cloud. The most challenging problem faced by the public cloud is the confidentiality of its sensitive data. But the major drawback of this system is the key management. In order to avoid this drawback this system introduced a mediated certificate less encryption method for the secure data sharing. But this system doesn't assure the confidentiality of the data. It only guarantees the protocol will work properly. So here a new approach is introduced to assure the confidentiality of the sensitive data in the cloud.

II. EXISTING SYSTEM

A mediated CL-PKE was found to be insecure against partial decryption attack, since this security model did not consider the capabilities of the adversary in requesting partial decryptions. Attribute based encryption (ABE) is a more expressive predicate encryption with a public index. Key Policy ABE (KP-ABE) and Cipher-text Policy ABE (CP-ABE) are two popular extensions of ABE. An ABE based approach supports expressive Access Control Policies (ACPS). Whenever the group dynamic changes, the re keying operation requires to update the private keys given to existing members in order to provide backward/forward secrecy.CL-PRE scheme only achieves CPA (Chosen Plaintext Attack) security which is not sufficient to protect real-world applications. All existing systems suffer from the key escrow problem.

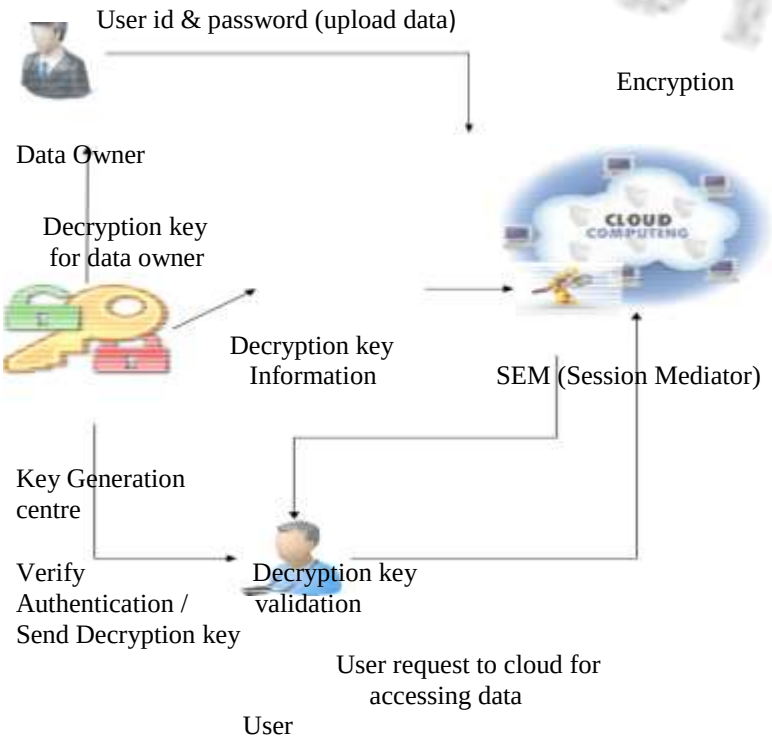
III. PROPOSED SYSTEM

In this project the proposed scheme architecture is divided into three main parts: (1) Owner, (2) Cloud and (3) User. Cloud is further divided into three sub parts; Encrypted Storage (ES), Decryption Center (DC) and Key Generation

Center (KGC).The proposed technique Elliptic Curve Cryptography (ECC) is providing the better enhancement in compare to the existing technique. The ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The proposed technique is generating the encryption and decryption key for both user and Data owner respectively by the key generation center. Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the data with public key and the user will decrypt its private key. The session mediator is proving the intermediate key for the encrypting and decrypting the data over the cloud and doing a perfect management for validating the key validation time within the side of data owner and user. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements. Reduce cost of computation Reduce the computation time.

IV. OVER ALL ARCHITECTURE

The popularity and widespread use of Cloud have brought great convenience for data sharing and collection. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. The shared data must be strongly secured from unauthorized accesses. The common approach to ensure confidentiality is to encrypt the data before uploading it to the cloud. Many encryption mechanisms support fine-grained encryption based access control. In our proposed scheme, first data owner register on cloud. Then data owner upload data on cloud. Cloud receives the data and put ECC encryption on data. Elliptic Curve Cryptography (ECC) is providing the better enhancement in compare to the existing technique. Protection of data is achieved by this step. After successful encryption key generation center sent the decrypt key to Data Owner. Now the user process will start. In that first user register on cloud and request the cloud to access data. Once cloud gets the request from user it validates the user by the user information. If user is validate person, key generation center sends decrypt key to user at the same time it send decryption key information and data information to Session Mediator (SEM Keys). Session Mediator is responsible for maintains the user session and provides the security on data. Users can decrypt the data using the decryption key. Users can using the data depend on the type of data. Because session mediator gives the accessibility to users depend on the data. If user time limit is exceeds session mediator close the connection of user session. In this proposed system we achieve the data security and validation of users.



V. SYSTEM IMPLEMENTATION

Cloud Set Up

The KGC runs the SetUp operation of the ECC scheme and generates the master key *MK* and the system parameters *params*. It should be noted that this setup operation is a one-time task.

The mediated certificateless public key encryption scheme is a 7-tuple ECC=(SetUp, SetPrivateKey, SetPublicKey, SEM-KeyExtract, Encrypt, SEM-Decrypt, USER-Decrypt).

The cloud consists of two main services: an encrypted content storage and a security mediation server (SEM), which acts as a security mediator for each data request and partially decrypts encrypted data for authorized users. The cloud is trusted to perform the security mediation service and key generation correctly, but it is not trusted for the confidentiality of the content and key escrowing.

User registration with KGC and KGC key generation

Initially the users register with the KGC with his ID and access list. The KCG verifies user and uses ECC algorithm to generate two pair of keys. The kgc takes two prime numbers p, q and uses ECC algorithm to generate two keys

Data Owner get KCG key of user

The data owner obtains the KGC-keys of users from the KGC in the cloud. The data owner then symmetrically encrypts each data item for which the same access control policy applies using a random session key *K* and then the data owner encrypts *K* using the KGC-keys of users. The encrypted data along with the access control list is uploaded to the cloud. The encrypted content is stored in the storage service in the cloud and the access control list, signed by the data owner, is stored in the SEM in the cloud.

The data owner uses ECC key to encrypt the data

The plain text is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to log2(n); in practice, the block size is 2k bits, where $2k<n<=2k+1$.

Data Decryption

When a user wants to read some data, it sends a request to the SEM to obtain the partially decrypted data. The SEM first checks if the user is in the access control list and if the user's KGC-key encrypted content is available in the cloud storage. If the verification is successful, the SEM retrieves the encrypted content from the cloud and partially decrypts the content using the SEM-key for the user. The partial decryption at the SEM reduces the load on users. The user uses its SK and U-key to fully decrypt the data.

VI. CONCLUSION

The proposed technique elliptic curve cryptography (ECC) provides an efficient secure sharing of data in public clouds. The service is being provided by the cloud is not much secure with the existing technique, to overcome on the existing problems, Elliptic Curve Cryptography (ECC) within the session mediator and Key Generation Center is proposed. The proposed technique is providing a better output over cloud security. The data is being securely share with the users and the privacy of the data is containing with the data owner. The ECC security key is not a lengthy process; it is providing a short and sufficient secret key for

the encryption and decryption process of the data. The Session mediator is providing different key for the every request to access the stored data in cloud by user. This project proposes a re-encryption scheme for secure data sharing with public cloud. Re-encryption scheme in cloud makes the data in cloud secure, flexible and a robust system. The proxy re-encryption is certificate less as the owner and recipient need not authenticate themselves through providing certificates, the owner and recipient are validated to the cloud that they opt to choose. The solution to Achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, so the data remain information secure against the Cloud provider and other malicious users It is given as a secure way of data sharing. Thus, in this project, we have presented a survey of different techniques used for secure data sharing in public clouds.

VII. REFERENCES

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," in Proc. Crypto '98, H. Krawczyk Ed. Springer-Verlag, LNCS 1462.

[2] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," ACM TISSEC, volume 5, no. 3, paper 290–331, 2002.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. 2007 IEEE Symposium SP, Taormina, Italy, pp. 321–334.

[4] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," *ACM Trans. Internet Technol.*, vol. 4, no. 1, pp. 60–82, Feb. 2004.

[5] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th TCC*, Amsterdam, The Netherlands, 2007, pp. 535–554.

[6] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in Proceedings of 16th ACM Conference CCS, New York, NY, USA, 2009, paper 131–140.

[7] X. W. Lei Xu and X. Zhang, "CL-PKE: A certificate less proxy re encryption scheme for secure data sharing with public cloud," in ACM Symposium on Information and Computer Communication Security, 2012.

[8] Seung-Hyun Seo, Xiaoyu Ding and Elisa Bertino "An Efficient

Certificateless Encryption for Secure Data Sharing in Public Clouds". IEEE Trans. Knowl. Data Eng.,, vol. 26, no. 9, Sept 2014

[9] C. Yang, F. Wang, and X. Wang,"Efficient mediated certificates public key encryption scheme without pairings," in AINAW, Niagara Falls, ON, May 2007, pp. 109–112.