AN EFFICIENT CLOUD SECURITY SYSTEM USING DOUBLE SECRET KEY DECRYPTION PROCESS

Ms.B.Narmada[1], Ms.G.Gunadharshini[2],Ms.A.Jese Owens[3],Ms.R.Kalpanachawla[4], Ms.R.Keerthika[5]

[1]Assistant Professor, Department of Computer Science & Engineering, Dhirajlal Gandhi College of Technology, Salem, Tamilnadu, India

[2,3,4,5] UG Scholar, Department of Computer Science & Engineering, Dhirajlal Gandhi College of Technology, Salem, Tamilnadu, India

---

Abstract - Internet technology is growing quickly, and people can process, store, or share with their data by using its ability. Cloud shares infrastructure between several organizations and it is managed internally or by a third-party. The user stores the data in an encrypted format. ABE is an encryption scheme used by the user to store the data in the cloud. ABE is a public-key based one to many encryption techniques which allows users to encrypt and decrypt data based on user attributes. Access control of encrypted data stored in the cloud is, by using access polices and ascribed attributes associated with private keys and cipher texts. In existing ABE schemes decryption has expensive paring operations and the complexity of the access policy is proportional to the number of attributes. An ABE system with outsourced decryption eliminates the decryption overhead. Here user provides data to the cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied with the user's attributes or access policy into a simple cipher text. In this project, use the security model of ABE with verifiable outsourced decryption by providing the verification key at the time of output decryption. Then using user revocation scheme to overcome the key leakage problems. We can implement this approach in real time cloud environments.

***KeyWords*:** Attribute Based Encryption(ABE), Outsourced decryption, cloud security

1.INTRODUCTION

While the storage of corporate data on remote servers is not a new development, current expansion of cloud computing justifies a more careful look at its actual consequences involving privacy and confidentiality issues. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. The overhead of using cloud storage should be minimized as much as possible, such that user does not need to perform too many operations to use the data.To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent cloud storage server to audit the outsourced data when needed [2]. As more sensitive data is shared and stored by third-party across many sites on the internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level. The drawbacks of the standard ABE schemes are their relatively large cipher text size and high decryption cost and also it requires many number of pairing operations in decryption. These pairing operations are usually more expensive than exponentiation. To overcome this problem green et.al suggested outsourcing decryption in attribute based encryption. This scheme provides no guarantee on the correctness of the transformation done by the cloud server. There are two schemes that are associated with the Attribute Based Encryption with verifiable decryption is: 1) Cipher-Text Policy Attribute Based Encryption (CP-ABE). 2) Key Policy Attribute Based Encryption (KP-ABE). Attribute Based Encryption with Verifiable Outsourced Decryption is a public key based encryption technique, in which the encrypted content that is known as cipher-text is associated with the access policy and the attributes of the user [1]. Attribute Based Encryption with Verifiable Outsourced Decryption is a challenging application that serves as public key based encryption that allows the user for the encryption and the decryption of the file/ data based on their own attributes. This application also provides the user's data in terms of security saying no malicious cloud will be able to learn about the encrypted file and also provides fully security against the key being compromised by the cryptanalyst.

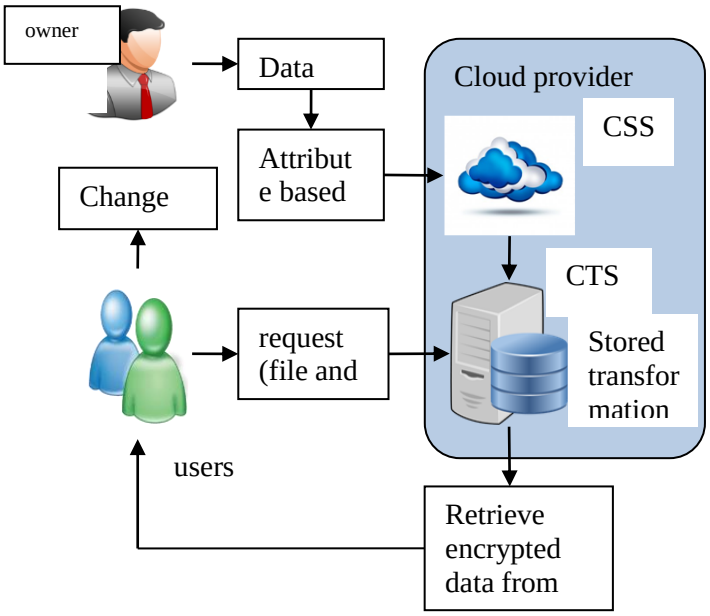
2. Body of Paper

Existing System: As a lot of sensitive information is shared and hold on by third-party sites on the net, there'll be a desire to cipher information hold on at these sites. One disadvantage of encrypting information is that it will be by selection shared solely at a coarse-grained level (i.e., giving another party your personal key). And proposed a scheme for fine-grained sharing of encrypted information that it has the tendency to developed Key-Policy Attribute-Based coding. In that, attributes and personal keys are related to access structures that manage the cipher texts that the user is ready to rewrite. It didn't hide the set of attributes underneath that the information is encrypted. Then proposed a cipher text policy attribute-based coding (CP-ABE), every secret key is associated with a set of attributes, and each cipher text is associated with access structure on attributes. Secret writing is enabled if and only if the user's attribute set satisfies the cipher text access structure. This provides fine-grained access management on shared information in several sensible settings, likewise as secure databases and secure multicast. It gifts a variant with well smaller cipher texts and faster encryption/decryption operations. The most arrange is to form a hierarchy of attributes, so fewer cluster components square measure required to represent all attributes within the system. This economical variant is proven to be controller secure and also proposed the first attribute-based encryption (ABE) schemes allowing for truly expressive access structures and with constant cipher text size.

Proposed System: The verifiability of the cloud's transformation and a technique to verify the correctness of the transformation is provided. Initially it modifies the original model of ABE with outsourced decryption then the existing to permit for verifiability of the transformations. Once describing the formal definition of verifiability, we tend to propose a new ABE model and supported this new model construct a concrete ABE theme with verifiable outsourced decryption. Abe scheme with verifiable outsourced decryption and recoverability consists of seven algorithms namely Setup, KeyGen, Encrypt, Decrypt, GenTkOut , Transformout, and DecryptOut. A trusted Party uses the SetUp algorithmic rule to come up with the general public parameters and a master secret key, and uses KeyGenOut to come up with a non-public key. Encrypt algorithmic rule uses the general public parameters and access structure to cipher the message. In Outsourced Decryption the user uses the GenTkOut algorithmic rule to come up with the transformation key and the retrieving key. The user sends the transformation key to the cloud. Taking as input the transformation key given by a user and a cipher text, the cloud will use the algorithmic rule Transformout to rework the cipher text into a straightforward ciphertext. If the user's attribute satisfies the access structure related to the cipher text; then the user uses the DecryptOut algorithmic rule to recover the plaintext from the transformed cipher text. It takes input as cipher text, public parameters and therefore the transformed cipher text. The hashed blocks of original message are compared with the hashed blocks of retrieved message; if any change within the block then we can confirm that the remaining blocks are original. User splits the original message in to fixed size blocks, and for each block sha1 algorithm is applied. The resultant random hashed blocks can be stored in the user side. After retrieving the data from the cloud the verification operation is performed. If the verification results the data is modified then to identify the modified block and recover the remaining content Random hash function is applied to the retrieved data.

work and provide (potentially) superior scalability possibilities. Unlike the blockchain, a distributed ledger does not necessarily need to contain a data structure in blocks.

3.SYSTEM DESIGN



In a CP-ABE scheme, every cipher text is associated with a set of attributes and every user's private key is associated with an access policy on attributes. A user is able to decrypt a cipher text only if the set of attributes associated with cipher text satisfies the access policy associated with the user's private key. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped from what they described for CP-ABE [3]. One of the main efficiency drawbacks of the most existing ABE schemes is that
decryption is expensive for resource-limited devices due to pairing operations and the number of pairing operations required to decrypt a cipher text grows with the complexity of the access policy. Attribute Based Encryption with Verifiable Outsourced Decryption is a public key based encryption technique, in which the

encrypted content that is known as cipher-text is associated with the access policy and the attributes of the user.

4.COMPONENTS

A. Cloud Entities

Cloud computing is computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Clouds can be classified as public, private or hybrid. Cloud server is responsible for store the data in cloud storage. It contains two sub servers such as Ciphertext transformation server (CTS), Cloud storage server (CSS)

- Data owner is the owner of storage system. They are stored data in cloud and also download the data from cloud without any authorization
- Cloud users are access the data from cloud using the attribute and use data based on access control mechanism.

B. Key generation and key distribution

The owner generates the public key and the secret key based on the user attributes and the access control assigned with the them. All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services. However, the cloud server is not involved in any attribute management and the creation of secret keys that is associated with attributes. The owner divides the secret key into transformation key (denoted by TK) and El Gamal-type secret key (denoted by DK). DK is kept secret in user side. TK is transferred from user to CTS server.

C. Security model

The cloud server stores the owners' data and provides data access service to users. It generates the decryption token of a cipher text for the user by using the secret keys of the user issued by the CTS. User Revocation starts with the intuition of the user revocation operation as follows. Whenever there is a user to be revoked, the data owner first determines a minimal set of attributes without which the leaving user's access structure will never be satisfied. Next, they updates these attributes by redefining their corresponding system master key components [5]. Mechanism (KEM) setting approach where the ABE cipher text hides a symmetric session key. The formal definition of attribute-based KEM with outsourced decryption is exactly the same as that of ABE with outsourced decryption, except that the encryption algorithm of ABE is replaced by an encapsulation algorithm, which doesn't take a message as an input.

D. Secure data sharing

Each user is assigned with CTS. Each user can freely get the cipher texts from the server in secure manner. To decrypt a cipher text, each user may submit their secret key TK issued by some CTS together and kept the key DK in user side and ask it together at the time of decryption token for some cipher text. Upon receiving the decryption token, the user can decrypt the cipher text by using its DK. Only when the user's attributes satisfy the access policy defined in the cipher text, the server can generate the correct decryption token. The secret keys and the global user's public key can be stored on the server; subsequently, the user Data owner not need to submit any secret keys if no secret keys are updated for the further decryption token generation. It aims to allow the users with eligible attributes to decrypt the entire data stored in the cloud server. However it cannot limit the users from accessing the data's which are not accessible to them. That is it cannot limit the data access control to the authorized users.

E. Evaluation Criteria

This module evaluates the performance of the system using the performance metrics such as storage overhead, communication cost and computation efficiency. The storage overhead is one of the most significant issues of the access control scheme in cloud storage systems. In their scheme, besides the storage of attributes, CTS also needs to store a public key[9] and a secret key for each user in the system. Thus, the storage overhead on CTS in their scheme is also linear to the number of in the system. The communication cost of the normal access control is almost the same. The communication cost of attribute revocation is linear to the number of cipher texts which contain the revoked attribute. They compare the computation efficiency of both encryption and decryption in two criteria: the number of authorities and the number of attributes per authority.

5.CONCLUSIONS

This project proposes a novel framework of achieving grained access control for sharing personal data. Considering partially trustworthy cloud servers, it argues that to fully realize the concept, patients shall have complete control of their own privacy through encrypting their files to allow fine-grained access. The framework addresses the unique challenges brought by multiple data owners and users, in that greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. It utilizes ABE to encrypt the cloud data, so that user can allow access not only by personal users, but also various users from public Data owner mains with different professional roles,

qualifications, and affiliations. We considered a new requirement of ABE with outsourced decryption: Verifiability. It is used to modify the original model of ABE with outsourced Decryption. This ABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .Our scheme does not rely on random oracles. A flexible access control for encrypted data stored in cloud is provided. It eliminates Decryption overhead for users according to attributes .This Data transformation is guaranteed to store in cloud. This secure attribute based cryptographic technique for robust data security that's being shared in the cloud.

6.FUTURE ENHANCEMENTS

In future, we can extend our work to implement various algorithms to provide improved security in cloud environments and also analyze the various attributes to encrypt the data.

7.REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACMConf. Comput. Commun. Secur., 2006, pp. 89–98.

[2] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.

[3] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," Theoretical Comput. Sci., vol. 422, pp. 15–38, Mar. 2012.

[4] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. ForensicsSecurity, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[5] K.-M. Chung, Y. Kalai, and S. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 483–501.

[6] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632, K. G. Paterson, Ed. Berlin, Germany: Springer-Verlag, 2011, pp. 129–148.

[7] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Advancesin Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 465–482.

[8] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, "Secure delegation of elliptic-curve pairing," in Smart CardResearch and Advanced Application (Lecture Notes in Computer Science), vol. 6035, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 24–35.

[9] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proc. ACMConf. Comput. Commun. Secur., 2013, pp. 463–474.

[10] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 4,pp.2201–2210,Aug.2014.[Online].