Hybrid Encryption with Verifiable Delegation using Cloud Computing

Dr. Regonda. Nagaraju[1], Reddygari Aishwarya Reddy[2], S. Yamini[3], P. Mythry[4]
[1]*Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad*
[2]*UG Student, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad*
[3]*UG Student, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad*
[4]*UG Student, Department of CSE, Sreyas Institute of Engineering and Technology, Hyderabad*

***Abstract*— In the cloud, for keeping data confidential and achieving access control, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are more likely to delegate the original of the decryption task to the cloud servers to reduce the cost computing. As a result, attribute-based encryption with delegation emerges. Still, there are warning and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could damage or replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the authorized users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing cipher text-policy attribute-based hybrid encryption with verifiable delegation in the cloud has been considered in this work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the defects of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under k-multilinear Decisional & Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.**

Keywords:- Dual encryption, Malware injection attack, Random key generation, time seal.

I. INTRODUCTION

Cloud computing is the computing technique which describes the combination of logical entities like data, software which are accessible via internet. Cloud computing provides help to the business applications and functionality along with the usage of computer software by providing remote server which access through the internet. Client data is generally stored in servers spread across the globe. Cloud computing allows user to use different services which saves money that users spend on applications. Data owners and organizations are motivated to outsource more and more sensitive information into the cloud servers, such as emails, personal documents, videos and photos, company finance data, government documents, etc. To provide end-to-end data security and privacy in the cloud, sensitive data has to be encrypted before outsourcing to protect data privacy. In cloud computing, effective data utilization is a very difficult task because of data encryption, also it may contain large amount of outsourced data files. For data storage, the servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's demands. To overcome the above problem, a new technique is introduced and a technique is which used Cipher text policy attribute-based encryption.

II. RELATED WORK

Sahai and Waters introduced attribute-based encryption (ABE) as a new means for encrypted access control. In an attribute-based encryption system cipher texts are not necessarily encrypted to one particular user as in traditional public key cryptography. Instead both users' private keys and ciphertexts will be associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext if there is a "match" between his private key and the ciphertext.

The primary drawback of the Sahai-Waters threshold ABE system is that the threshold semantics are not very expressive and therefore are limiting for designing more general systems. Goyal et al. introduced the idea of a more general key-policy attribute based encryption system. In their construction a ciphertext is associated with a set of attributes and a user's key can be associated with any monotonic tree access structure. The construction of Goyal et al. can be viewed as an extension of the Sahai-Waters techniques where instead of embedding a Shamir secret sharing scheme in the private key, the authority embeds a more general secret sharing scheme for monotonic access trees.

Attribute-based encryption (ABE) is a public-keybased one-to-many encryption that allows users to encrypt and decrypt data based on user attributes Different from identity-based encryption scheme, an attribute-based encryption scheme is a scheme in

which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext. ABE comes in two forms:

1. In **Key - Policy Attribute Based Encryption (KP-ABE)** access structure is the user's private key and set of descriptive attributes are associated with the ciphertext during the encryption. To decrypt the ciphertext, the user matches his private key (access structure) with the attributes associated with the ciphertext. If it matches, then the ciphertext is decrypted otherwise not.

The disadvantage of KP-ABE [6] is that access control of the encrypted data is controlled by the set of descriptive attributes not by the access tree and also while encrypting data; the user had no control over the attributes. This reason led to the design of the cipher policy attribute based encryption (CP-ABE). Another restriction with the KP-ABE is that all attributes have to be made public as they are component of the public key.

2. **Ciphertext Policy Attribute Based Encryption (CP-ABE**) works in the reverse order of KP-ABE[6]. Instead of associating the set of attribute to the ciphertext, it associates the access structure and encrypt the message using the set of descriptive attributes (user's private key) and a user can decrypt it if and only if his private key (set of descriptive attribute) matches with the access structure associated with the ciphertext.

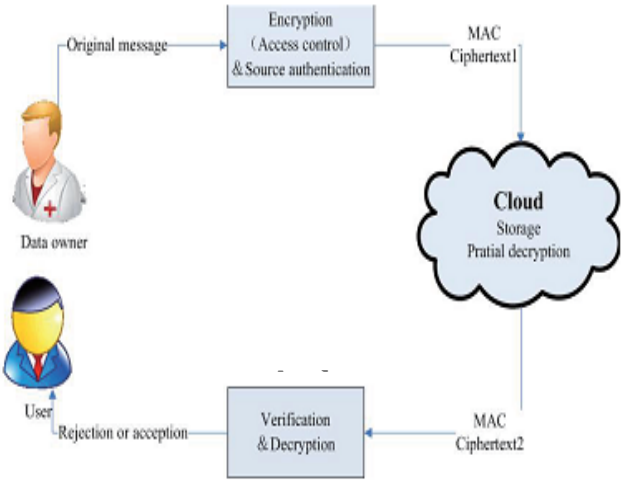
III. PROPOSED SYSTEM

Going by the requirements in the cloud, the model of CP-ABE with verifiable delegation is modified to present a concrete construction to realize circuits ciphertext-policy based hybrid encryption with verifiable delegation (VD-CPABE).

To keep data private and achieve fine grain access control, our starting point is a circuit key-policy attribute-based encryption proposed by Sahai and Waters. We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CPABE is conceptually closer to the traditional access control methods. For the main efficiency drawbacks of ABE, previous constructions provided an agile method to outsource the most overhead of decryption to the cloud.

However, there is no guarantee that the calculated result returned by the cloud is always correct. The cloud server may forge ciphertext or cheat the eligible user that he even does not have permissions to decryption[1]. To validate the correctness, we extend the CP-ABE ciphertext into the attribute based ciphertext for two complementary policies and add a MAC for each ciphertext, so that whether the user has permissions he/she could obtain a privately verified key to verify the correctness of the delegation and prevent from counterfeiting of the ciphertext.

IV. ARCHITECTURE AND MODULES



Data owner

Data owner carries the data and transmit the encrypted data to cloud service provider to store the data in cloud servers. Dual encryption of the file is to be done with the random key encryption and by the symmetric key to access the file by users, apply this theory to encrypt the data and then sync them to cloud servers to use in common with the other users.

Data Consumer

This is an entity who wants to access the outsourced data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the ciphertext and obtain the data. Data consumers are the bodies who access the encrypted data stored in cloud servers. Only the authorized users who comply with the access theory of data owner can decrypt the encrypted data to retrieve the plaintext data.

Authority

In this module, the authority login and request the key to access the file. the authority can see all the details of data owner and data consumer and ends the session by logging out.

Cloud Service

It is an entity that provides a data service. It consists of data servers and a data service manager. Data from data owners are stored in the data servers. The data service manager is in charge of controlling the accesses from outside users to the outsourced data I servers and providing corresponding contents services.

V. IMPLEMENTATION

In CP-ABE we use a hybrid variant for two reasons: one is that the circuit ABE is a bit encryption, and the other is that the

authentication of the delegated ciphertext should be guaranteed. In such a system, a circuit ciphertext-policy attribute-based encryption scheme, a symmetric encryption scheme and an encrypt-then-mac mechanism are applied to ensure the confidentiality, the fine-grained access control and the verifiable delegation.

VD-CPABE is divided into two components:

1. The CP-ABE for f and f' makes up the key encapsulation mechanism (KEM)[2] part, which encrypts a random group element and then generates a symmetric encryption key 'dk' and a one-time verified key 'vk'. Then the random encryption key 'dk' is used to encrypt the message of any length. 'vk' and the data owner's ID are used to verify the MAC[3] of the ciphertext.
2. A symmetric encryption plus the encrypt-then-mac mechanism make up the authenticated encryption mechanism[4] (AE) part.

We use a hybrid VD-CPABE scheme is defined by the following **tuple of algorithms.**

(i) Setup:

This algorithm takes as input a security parameter and it outputs the public parameters PK and a master key MK which is kept secret.

(ii) Hybrid-Encrypt(PK, M)

It is divided into two parts:

1. The KEM algorithm takes as input the public parameters PK and chooses a random string R. Then it generates KM & KR and the CP-ABE ciphertext[5] (KM, KR).
2. The AE algorithm takes as input a message M, the symmetric key KM and KR. Then it outputs the hybrid CT.

(iii) KeyGen(MK, x)

The authority generates private keys for the users. This algorithm takes as input the master key MK and a bit string x that describe the key.

It outputs a private key SK and a transformation key TK.

(iv) Transform(TK, CT)

This algorithm takes as input the transformation key TK and a ciphertext CT that was encrypted under f and f'. It outputs the partially decrypted ciphertext CT′.

(v) Verify-Decrypt(SK, CT′)

This algorithm takes as inputs the secret key SK and the partially decrypted ciphertext CT′. Then it decrypts the message.

VI. CONCLUSION & FUTURE WORK

This system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. On the other hand, we implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

In the future, it would be interesting to consider we can uploading huge data containing files (it may be video, audio or many more). Even we can go for further live video streaming files by using some good technologies like hadoop and spark. Even we can add the concept of re-encryption of encrypted file. Further we can add the concept of auto triggering SMS with OTP.

VII. REFEERNCES

[1] Jie Xu, Qiaoyan Wen, Wenmin Li and Zhengping Jin, "Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems.

[2] J. Lai, R. H. Deng, C. Guan and J. Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption," in Proc. IEEE Transactions on information forensics and security, vol. 8, NO. 8, pp.1343-1354, 2013.

[3]S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in Proc. 45th Annu. ACM Symp. Theory Comput., 2013, pp. 545–554.

[4]A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn, 2005, pp. 457–473.

[5]V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[6] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization," in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.