Secure Attribute-Based Encryption with Valid Outsourced Decryption

Ms. Surya Suresh[1] Mrs. Sherin Peter[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]MBCCET Peermade, Idukki, Kerala, India

Abstract— Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing. Cloud users data security is very essential need of the cloud computing. The technique of cryptography provides the way for data security in cloud. Attribute based encryption is a special kind of encryption that supports complex access control over encrypted data. But the decryption using personal devices increase complexity. Outsourcing the encrypted data to a third party will overcome this problem. Even though the outsourcing reduces complexity, it is not possible to trust the third party. So security of the data used for outsourcing is important. This paper uses the concept of partial outsourced decryption. It allows the proxy (third party) only to perform the partial decryption. The receiver can do the remaining decryption by simple operations. Thus the proxy does not learn anything about the encrypted message. It is very essential that the correctness of outsourced decryption must be verified. RCCA-secure and CPA-secure are two systems used for verifying the correctness of the outsourced decryption. Even though the system is secure there may be chances of attack that unauthorized user attempts to access files. This paper introduces a blocking mechanism that blocks the one who perform unauthorized access.

Key words: Attribute Based Encryption, Outsourced Decryption, Verifiability

I. INTRODUCTION

Cloud computing had made revolutionary changes in networking, in which computation and storage are moved far from terminal gadgets to the cloud. This new and well known worldview brings vital transformations and makes bold innovations for the manner in which enterprises and people oversee, disseminate, and share content. By outsourcing their data innovation capacities to some cloud specialist organizations, cloud clients may accomplish significant cost savings.

Since the popularity of cloud computing has increased more and more users began to explore it. So it is very essential to ensure the security of user data. The data that is outsourced will be very confidential and must be accessed only by the authorized person. It is very essential scenario while using cloud storage. Cryptography is the technology that can be used to achieve this goal. Attribute Based Encryption Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes.

Depending on how to deploy the access control policy there are two various types of ABE frameworks. That is, Key-Policy Attribute-Based Encryption (KP-ABE) Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In a CP-ABE conspire, each ciphertext is related with an entrance strategy, and each client's private key is related with an arrangement of attributes. While in a KPABE plot, ciphertext are named with sets of attributes and access strategies over these attributes are related with clients' private keys. In an ABE framework, decoding task requires that the arrangement of attributes should coordinate the entrance strategy. However, in most existing ABE schemes, one of the main efficiency downsides is that the span of the ciphertext and the unscrambling overhead (computational cost) develop with the multifaceted nature of the entrance arrangement. ABE framework with outsourced unscrambling, the key calculation is modified to create two keys for a client.

In order to reduce the overhead of decryption the concept of outsourced decryption is used. Outsourced decryption is done by a proxy, which is considered to be untrusted. The proxy is a third party who may exploit the confidential data. Thus only partial decryption is allotted to proxy and remaining is done by the authenticated user. In order to verify the correctness of outsourced decryption two systems called CPA-secure and RCCA-secure [12] is introduced. They are efficient mechanisms that checks whether the decrypted data is same as the original one or not based on the hash value generated during uploading a file. Proposed system enables broadcasting a file to many users. A user may find many files in his account may be related to his firm or organisation. If he tries to access, a file that he has no privilege to access, greater than three times proxy get alert and the proxy has the privilege to block him. If the blocked user proves his genuinely to the proxy then the proxy can unblock him. The proposed system mainly finds application in an organization or firm.

II. RELATED WORK

Sahai and Waters work [1] first introduced the concept of Attribute Based Encryption. They proposed very efficient encryption mechanism in which the encryption is performed based on the attributes of the receiver. The attributes are used as the key for encryption. The main advantage of this scheme is that it enables the broadcasting an encrypted message to a set of receivers. Goyal et al. [3] proposes a new cryptosystem for fine-grained sharing of encrypted data called Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Bethencourt et al. [4] proposed the first CP-ABE scheme. In this system the encrypted data can be kept confidential even if the storage server is untrusted; moreover, it is secure against collusion attacks. These two [3] [4] ABE schemes are based on monotone access structures. There are a large number of papers that proposed various ABE schemes. In [2], Cheung et al. presented a secure CP-ABE scheme and a novel key management schemes that allow users whose attributes satisfy a certain access control policy to derive the group key. This scheme efficiently supports rekeying operations when

the group changes due to joins or leaves of group members. In [5], Waters proposed several very efficient CP-ABE constructions. These constructions work for any access policy that can be expressed in terms of a linear secret sharing scheme (LSSS) matrix. This allow any encrypt or to specify access control in terms of any access formula over the attributes in the system. Ostrovsky et al. [6] proposed a KP-ABE scheme that allows a user's private key to be expressed in terms of any access formula over attributes. KP-ABE and CP-ABE schemes with non-monotone access structures was proposed by Okamoto and Takashima [7]. Many papers employed ABE to realize fine-grained data access control. Chase Multi-authority ABE which allows any polynomial number of independent authorities to monitor attributes and issue secret keys was proposed by Chase at el. [8]. His proposal uses the concepts of a trusted central authority and global identifiers. Chow and Chase [9] (somewhat) removed the trusted central authority by using a distributed pseudorandom function. Lekwo and Waters [10] proposed a new decentralized multi-authority ABE system. Many of the papers presented different ABE schemes. But a complete secure model could not found by any paper.

III. Problem Formulation

A. Problem Definition

There are two fundamental drawbacks with current Attribute based encryption scheme. They are cipher text size and decryption overhead. Decryption using resource limited devices like mobile phones makes the decryption more complex and time consuming. Users always require quick access with least resource utilization. It is the fundamental problem with attribute based encryption.

ABE-schemes mainly proposed for firm or organizations. So there may be chances of inside attacks. If an unauthorized person tries to access any confidential file must be alerted to the proxy. Those tries to access unauthorized files must be revoked. The proxy must have the privilege to revoke the users. So a mechanism is required to enable revoking and invoking the user.

B. Existing System

Cloud computing had made revolutionary changes to networking. People find many advantages such as memory, cost and time savings by using cloud technology. They began to store even their confidential data in cloud. So security of user data is a significant problem. Cryptography is a power full tool that provides security for user data. Sahai and Water [1] proposed a new encryption scheme named Attribute Based Encryption as a technique to provide security for cloud computing. There are two ABE-schemes such as Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) based on the access structure. The main problems with ABE scheme are cipher text size and decryption overhead. Complete decryption using mobile phones or computers create more overhead to users. Memory and time are the basic limiting factors. While decrypting large files these factors are becoming critical barriers in resource-limted devices. Inorder to overcome the decryption overhead the concept of outsourced decryption has been proposed.

The ABE scheme with outsourced decryption encountered some problems: the ill-disposed proxy wants to save computing cost, the proxy may undergo malicious attack or other system failures. During such situations, the data receiver must verify the correctness of outsourced decryption. CPA-secure and RCCA-secure are two systems introduced to check whether the outsourced transformation is done correct or not. In these methods an encryption of an extra random message and a checksum value are added to the ciphertext, which is computed with a random message and the actual plaintext. This checksum value plays a role of the commitment to the actual plaintext and is used to check whether the transformation is indeed done correctly. Even though the system is not secured. So it is very essential to find out a more efficient manner and secure mechanism to provide the verifiability of outsourced decryption for ABE systems with outsourced decryption, especially in the standard model. The proxy that we use for outsourcing is considered to be untrusted. So we need a mechanism to do the outsourcing in more secure way.

IV. Proposed System

The third party that we use for outsource decryption is not trusted. So in this paper it proposes the concept of partial decryption. Since the proxy is untrusted allow him only the partial decryption of the ciphertext. Remaining was done by the user. Thus the proxy does not learn anything from the message. This system have 'decrypt then verify' flavor. That is, after receiving a partially-decrypted ciphertext transformed by a proxy, the data receiver first decrypts it using some simple operations and then verifies the correctness of the outsourced decryption. In this paper the CPA system is constructed in a different way. In this method a message and a random value together is encrypted and then committing to the message by using the random value. It also enables to verify the correctness of outsourcing.

This proposed model is more helpful in the broadcasting of the messages or data. It is designed mainly of institutions or organization. While uploading the file the sender can decide the receiver. The sender chooses attributes of the receivers and the message is encrypted using these attributes. Based on the content of files hash values are generated which is unique for each file. This hash values help in the verification phase. The verification is performed by CPA-secure and RCCA-secure systems using the hash value. Based on the attributes used for encryption an access structure is created. Those who satisfy this access structure will only be able to download the file. User may find many files. If he found a legitimate file for him then he can send it to the proxy. The proxy does the partial decryption and returns it to user. The user can perform the remaining decryption using single operations. A set of algorithms are executing in background for these activities. The user may found many files. If he tries to access a file on which he have no privilege to access then the proxy get alert on this attack. Thus the proxy had authority to block him. In this paper the proxy was provided with a privilege to block the users that tries to access a confidential file.

A. Proposed Implementation Scheme

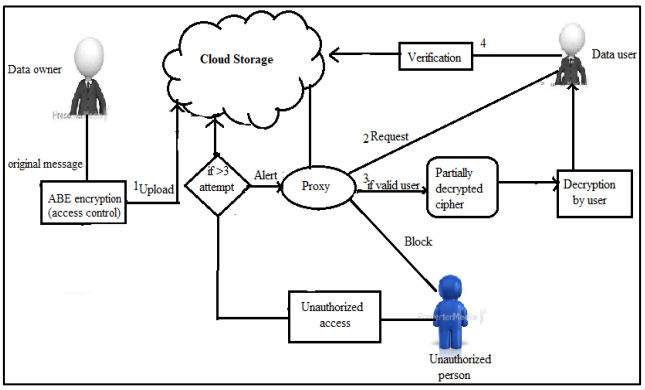

Fig. 1: Proposed System Architecture

The data owner can upload files to the cloud storage. User can choose the required attributes of the receiver for encryption. Based on attribute based algorithm the encryption will be taken place. Thus actually the encrypted file will be uploaded to the cloud. The registered users can access the file from cloud if his credentials satisfy the attributes used for encryption of the file.

The user may find different file, he can choose the required file. Thus the proxy will perform the partial decryption and return the file to the user. User can download the file and the partial decryption intended for user will run in the background. The user can verify the correctness of decryption with the help of proxy. CPA-secure and RCCA-secure are two systems that are used for verification. The proposed system implements a system to block an attacker. The system is secure by Attribute based encryption. But there is no mechanism to block the unauthorized users. So in the proposed system if an unauthorized user tries to access a file that he has no privilege to access, then the system will block that user if he attempts more than three times. The blocking authority is proxy. The proxy also has authority to unblock a user. If the blocked user proves his innocents then the proxy will unblock him.

V. CONCLUSION

This paper proposes an efficient attribute based encryption mechanism for secure data transmission across cloud storage. In order to overcome the problem of decryption overhead the concept of outsourced decryption is introduced. The proxy used for outsourcing is not trusted. Thus the proxy used only for partial decryption and the remaining is done by the user. This mechanism provides more security to data in cloud storage. The systems to verify the correctness of outsourced decryption is also proposed. Any unauthorized access to a confidential file will cause the proxy to block that attacker. While using cloud computing to store and retrieve data the proposed system will enable high degree of security.

REFERENCES

[1] R. Zha A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 457–473.

[2] L. Cheung, J. A. Cooley, R. Khazan, and C. Newport, "Collusion resistant group key management using attribute-based encryption," Group-Oriented Cryptographic Protocols, p. 23, 2007.

[3] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[5] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography, ser. PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[6] R. Ostrovsky, A. Sahai ,and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser.CCS '07. New York, NY, USA: ACM, 2007, pp. 195–203.

[7] T.Okamoto and K.Takashima,"Fully secure functional encryption with general relations from the decisional linear assumption," in Proceedings of the 30th Annual Conference on Advances in Cryptology, ser. CRYPTO'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 191–208

[8] M. Chase, "Multi-authority attribute based encryption," in Proceedings of the 4th conference on Theory of cryptography, ser. TCC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 515–534.

[9] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and communications security, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 121–130.

[10] Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology, ser. EUROCRYPT'11. Berlin, Heidelberg: Springer Verlag, 2011, pp. 568–588.

[11] J. Lai, R. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.

[12] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in Advances in Cryptology CRYPTO '99, ser. Lecture Notes in Computer Science, M. Wiener, Ed. Springer Berlin Heidelberg, 1999, vol. 1666, pp. 537–554.

