Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.309 – 314

Achieving Access Control and Data Confidential by Attribute-Based-Hybrid Encryption in Cloud Computing

T.Sushmitha[1], D.Jayakumar[2]

B.E Student, Department of Computer Science and Engineering

IFET College of Engineering

suchitamil4103@gmail.com

jayakumar1988@hotmail.com

Abstract-Attribute based hybrid encryption helps to achieve access control and data confidentiality in the cloud. The data owners could adopt attribute based encryption to encrypt the data. To reduce the computing cost cloud servers mask the decryption task. As a result, attribute based encryption emerges. Still there is a problem in attribute based method because sometimes it doesn't allow the authorized users too. So it needs access control for authorized users correctly. Within these computing environments, the cloud servers can offer various data services, such as remote data storage and outsourced delegation computation etc. For data storage, the servers store a large amount of shared data, which could be accessed by authorized users. To achieve this access control, we are going to use attribute based cipher text policy of hybrid encryption delegation with verification method. The main functionality is to encrypt the original message and to do the source authentication using MAC ciphertext1.This encrypted data will be stored on the image for added security. That can be stored in cloud for decryption progress and verified by using MAC ciphertext2 after the encrypted data is retrieved from the image. Finally message may be accepted or rejected by using this process. The message could be accessed by authorized users alone.

I. INTRODUCTION

Cloud computing enables flexible, on-demand, and low-cost usage of computing resources, but the data is stored into some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the storage in cloud. However, most work focuses on the data contents privacy and the access control, while less attention is given to the privilege control and the identity privacy. The emergence of cloud computing brings a revolutionary development to the management of the data resources. Within this computing environments, the cloud servers offer various data services, like remote data storage and outsourced delegation computation. For data storage, the servers store a large amount of shared data, which could be only accessed by authorized users. For delegation computation, the servers could be used to handle and calculate various data according to the user's requests. As applications move to cloud computing ciphertext-policy-attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers.

Delegation computing is the main service provided by the cloud servers. The healthcare organizations store data files in the cloud by using CP-ABE under some access policies. The users, who want to access the data files, choose not to handle the complex process of decryption locally due to limited available resources. Instead, they are most likely to outsource part of the decryption process to the cloud server. While the untrusted cloud servers who can convert the original ciphertext into a simple one could learn nothing about the original text from the delegation. The work of delegation is promising but inevitably suffers from two problems. 1) The cloud server may change or replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext. 2) The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorize done that he/she is not eligible to access that data.

II. RELATED WORK

Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2012) [6] proposed the technique HASBE (Hierarchical Attribute-set-based Encryption).HASBE extends the ciphertext-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme by Bobba*et al.* with a hierarchical structure of system users, so as to achieve scalable, flexiblem and fine-grained access control.

Cong Wang Sherman S.M. Chow, Qian Wang (2013) [8] presents our public auditing scheme which provides a complete outsourcing solution of data—not only the data itself, but also its integrity checking. Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance.

Dijiang Huang (2015) [7] has discussed access control using Constant-size Ciphertext Policy Comparative Attribute-Based Encryption. CCP-CABE achieves the efficiency because it generates constant-size keys and ciphertext regardless of the number of involved attributes, and it also keeps the computation cost constant on lightweight mobile devices.

Jianan Hong(2015) [10] proposed that Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most attractive cryptographic techniques for data access control in cloud storage system, because of its fine-grained data access control policy and direct control of data for data owners. In CP-ABE, the user can access the content of the ciphertext, only if his/her attributes satisfy the ciphertext's preset access policy.

JieXu, Qiaoyan Wen, Wenmin Li and Zhengping Jin(2015) [9] were proposed Circuit Ciphertext-policy Attribute-ased Hybrid Encryption with Verifiable Delegation in Cloud Computing to keep data private and achieve access control. The anti-collusion circuit CP-ABE construction is used in this paper because CPABE is conceptually closer to the traditional access control methods.

III. PROPOSED WORK

We firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. On the other hand we implement our scheme over the integers. During the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly. The generic KEM/DEM construction for hybrid encryption which can encrypt messages oh arbitrary length. Based on that one time MAC will be generated. Such improved model has the advantage of achieving higher security requirements. Since the introduction of ABE has the outsourced decryption scheme to reduce the computation cost during decryption. The proposed ABE with verifiable outsourced decryption seek the guarantee of original ciphertext by using a commitment. However, since the data owner generates the commitment without any secret value about his identity, the untrusted server can then forge a commitment for a message he chooses. Thus the ciphertext relating to the message is at risk of being tampered. Further more just modify the commitments for the ciphertext relating to the message is not enough. The cloud server can deceive the user with proper permissions by responding the terminator to cheat that he/she is not allowed to access to the data.

The random encryption key is used to encrypt the message of any length and the data owner's ID are used to verify the MAC of the ciphertext. Only when the server does not forge the original ciphertext and respond a correct partial decrypted ciphertext, the user could be able to properly validate the MAC.

This can be done in 5 modules shown below

- Attribute Authority
- Encrypting PDB
- Hiding ciphertext in image
- Partial decryption
- Verifying and Accepting

Hybrid Encryption-It combines more than one cryptographic algorithm. It provides more security. It incorporates a combination of asymmetric and symmetric encryption. Secret keys depends upon attributes of the user (e.g. the country he lives, or the kind of subscription he has).Hybrid encryption consists of both encryption of secret keys and the plain data. So that, the data stored in the cloud will be very safe. The algorithm used for the encryption must be used for the decryption also. Both RSA and AES algorithm is used in the hybrid encryption. Were RSA is used for encrypting the symmetric keys and AES is used for encrypting the plain text.

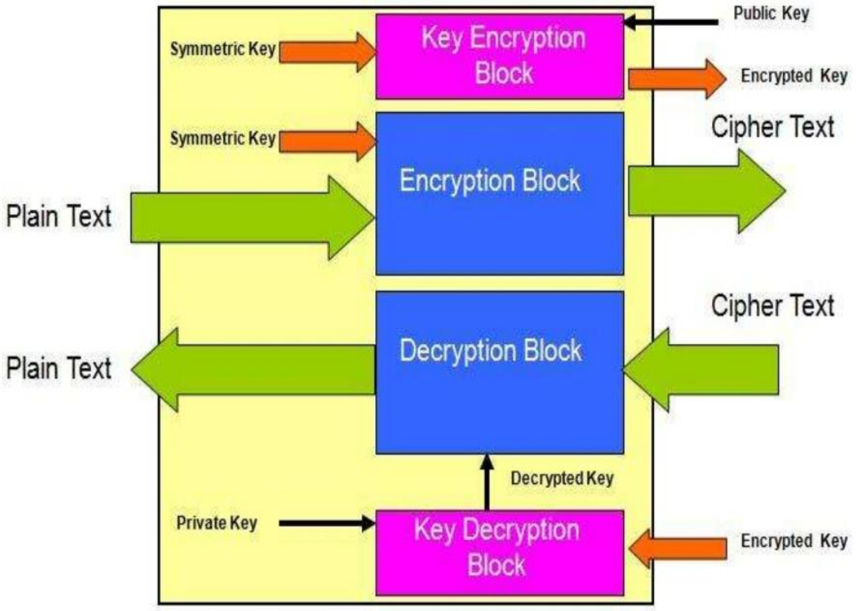

Figure. Block Diagram of hybrid crypto system

Attribute authority-Authority will have to provide the key, as per the user's key request. Every user’s request will have to be raised to authority to get access key on mail. There are two complementary forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CP-ABE). In a KP-ABE system, the decision of access policy is made by the key distributor instead of the encipherer which limits the practicability and usability for the system in practical applications.

Encrypting PDB-Data owner will have to register initially to get access to the profile. Source has destination key (PUK) i.e public key. This key is encrypted along with the text to generate the ciphertext. The key alone is encrypted and stored into the cloud for the decryption purpose. Data owner will upload the file to the cloud server in the encrypted format. Random encryption key generation is happening while uploading the file to the cloud. Encrypted file will be stored on the cloud. Plain Data Block (PDB) and Symmetric Key(SK) is the input given and Encrypted Data Block(EDB) is the encrypted output. EDB contains both the encrypted PDB(denoted by ED) concatenated with encrypted SK(denoted by ESK)

- Source has destination key(PUK)
- **Inputs**: Plain Data Block (PDB) Symmetric Key(SK)
- **Outputs**: Encrypted Data Block(EDB)

  EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK(denoted by ESK)

  EDB={ESK,ED}

Where,

ESK-Encrypted Symmetric Key

ED-Encrypted Data

EDB-Encrypted Data Block

Hiding cipher text in image-After encrypting the plain data it will be stored on the image. when the user tries to access the datas from the cloud the server initially retrieve the ciphertext from the image and then it allows the ciphertext to be decrypted.

Decryption-Cloud server will have the access to files which are uploaded by the data owner. Cloud server needs to decrypt the files available under their permission.Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer.Encrypted Data Block (EDB) is the input given for decryption.EDB contains both the encrypted PDB(denoted by ED) concatenated with encrypted SK (denoted by ESK).Plain Data Block (PDB) is the output derived after decryption which is the original text of the data owner.

Verifying and accepting-Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.If the key does not match which is send by the data owner then the data cloud not be accessed by the user.So that the key must be sent secretly.The key used for the encryption is used for decryption.

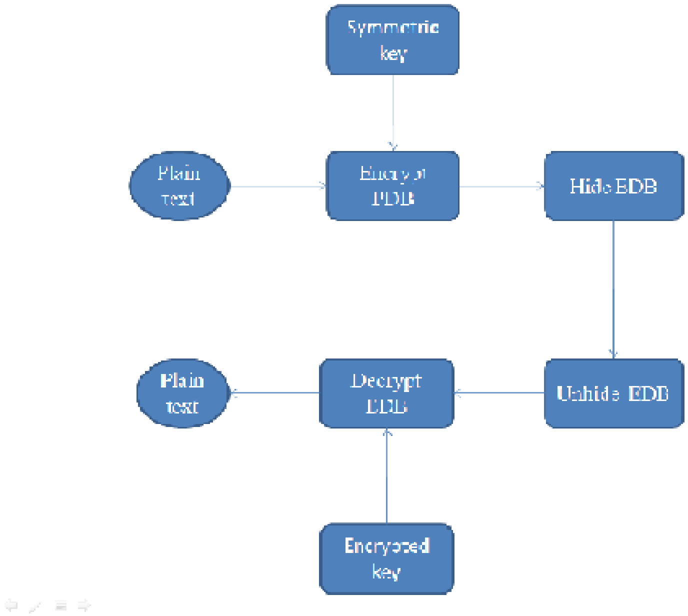

Fig.1 Data flow diagram

Initially the plain data is given as input by the data owner for the decryption.It is mentioned as plain data block(PDB).Along with the plain data block the symmetric is given for decryption.After the decryption operation has performed the ciphertext generated were hided into the image for an added security.Once the cloud receives the request from the user to access the data from it,it will check for the user authority and start for decrypting the ciphertext after unhiding the Encrypted data block(EDB) from the cloud.

IV. CONCLUSION

In this paper the proposed work is proven to be secured using the hybrid encryption concept.Encrypting the datas is done using the secret key this key is generated based on the attributes of the user.Also hiding the cipher text into the image is an added security for both the data owner and the user. The verifiable computation and encrypt-then-mac mechanism with our ciphertextpolicy attribute-based hybrid encryption, we could delegate the verifiable partial decryption.Hence breaking the original message is difficult for the attackers.Finally the end user who has the authority will access the data from the cloud after verifying it.

REFERENCES

[1] M. Green, S. Hohenberger and B. Waters, ”Outsourcing the Decryption of ABE Ciphertexts,” in Proc. USENIX SecuritySymp., San Francisco, CA, USA, 2011.

[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] Lewko and B. Waters,”Decentralizing Attribute-Based Encryption,” in Proc. EUROCRYPT, pp.568-588, Springer –Verlag Berlin, Heidelberg, 2011.

[4] Waters,”Ciphertext-PolicyAttribute-Based Encryption: an Expressive, Eficient, and Provably Secure Realization,” in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[5] Parno, M. Raykova and V. Vaikuntanathan, ”How to Delegate and Verify in Public: verifiable computation from attribute-based encryption,” in Proc. TCC, pp.422-439, Springer- Verlag Berlin, Heidelberg, 2012.

[6] Z. Wan,s J. Liu, and R. H. Deng, “HASBE: A Hierarchical attributebased solution for flexible and scalable access control in cloud computing,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[7] Zhijie Wang, Student Member, IEEE, Dijiang Huang, Senior Member, IEEE, Yan Zhu, Member, IEEE, Bing Li, Student Member, IEEE, and Chun-Jen Chung, Student Member, IEEE”Efficient Attribute-Based Comparable Data Access Control” VOL. 64, NO. 12, DECEMBER 2015.

[8] Cong Wang, Member, IEEE, Sherman S.M. Chow”Privacy-Preserving Public Auditing for Secure Cloud Storage” VOL. 62, NO. 2, FEBRUARY 2013.

[9] JieXu, Qiaoyan Wen, Wenmin Li and ZhengpingJin”CircuitCiphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing” DOI 10.1109/TPDS.2015.2392752.

[10] Jianan Hong, KaipingXue, *Member, IEEE*, andWei Li” Comments on “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems”/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems” VOL. 10, NO. 6, JUNE 2015.