International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

AN ENHANCED CIRCUIT CIPHERTEXT IN CLOUD BASED EFFICIENT USER REVOCATION MECHANISM ON TOP OF ANONYMOUS ABE

P. Lavanya [#1] and K. Kishore Raju [*2]

[#] *M.Tech. Student, Information Technology, SRKR Engineering College, Bhimavaram India*

[*] *Assistant Professor, Information Technology, SRKR Engineering College, Bhimavaram India*

***Abstract*— Cloud services are attaining its popularity day-by-day. Due to its increasing popularity users are showing interest to store their data or files in cloud servers. However, there are some drawbacks in cloud service provider. The cloud server sometimes doesn't allow even authorized users to access the file due to its high computational cost. To avoid this, Attribute Based Cipher Policy of Hybrid Encryption and Delegation with Verification methods is proposed. The main functionality of proposed method is that the owner encrypts the data using hybrid encryption. In hybrid encryption it incorporates a combination of asymmetric and symmetric encryption, both RSA and AES algorithms are used. RSA is used for encrypting the symmetric keys and AES is used for encrypting the plain text. The data consumer decrypts data by verifiable delegation to verify whether data is original or not, by using the key sent by the attribute authority. With this proposed method confidentiality and verifiability are implemented for the data owner and data consumer.**

***Index Terms*—Cloud, hybrid encryption, data security**

I. Introduction

The emergence of cloud computing brings a revolutionary innovation to the management of the information resources. In side this computing setting, the cloud servers can give numerous information services, like remote information storage and outsourced delegation computation, etc. For information storage, the servers store an oversized quantity of shared information that may well be accessed by licensed users. For delegation computation, the servers may well be accustomed handle and calculate various information in step with the user's demands. As applications move to cloud computing platforms, cipher-text policy attribute-based encryption and verifiable delegation area unit accustomed make sure the information confidentiality and also the verifiability of delegation on dishonest cloud servers. Taking medical information sharing as associate, with the increasing volumes of medical pictures and medical records, the care organizations place an oversized quantity within the cloud for reducing data storage prices and supporting medical cooperation. Since the cloud server might not be credible, the file cryptographic storage is an efficient methodology to forestall non-public information from being taken or tampered. With in the meantime, they will get to share information with the one who satisfies some necessities. In access policy, information sharing can be accomplishable, attribute based encoding is applicable.

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. 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 un-trusted cloud servers who can convert the original cipher text 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 cipher text for malicious attacks, and then respond a false transformed cipher text. 2) The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed cipher text to an unauthorized user, he could cheat an authorize one that he/she is not eligible to access that data.

II. LITERATURE SURVEY

A. A Berkeley View of Cloud Computing

A.Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica et al, has provided certain obstacles are overcome, we believe Cloud Computing has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. The economies of scale of very large-scale datacenters combined with ``pay-as-you-go" resource usage has heralded the rise of Cloud Computing. It is now attractive to deploy an innovative new Internet service on a third party's Internet datacenter rather than your own infrastructure, and to gracefully scale its resources as it grows or declines in popularity and revenue. Expanding and shrinking daily in response to normal diurnal patterns could lower costs even further. Present an economic model that quantifies the key buy vs. pay-as-you-go decision offer a spectrum to classify Cloud Computing providers.

B. Outsourcing the Decryption of ABE Cipher texts

M. Green et al, has proposed that Attribute-based encryption is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attributes. For example, a user can create a cipher text that can be decrypted only by other users with attributes satisfying. Given its expressiveness, ABE is currently being considered for many cloud storage and computing applications. However, one of the main drawbacks of ABE is that the size of the cipher text and the time required to decrypt it grows with the complexity of the access formula. In this work, we propose a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE cipher texts are stored in the cloud.

C. Attribute-Based Encryption with Verifiable Outsourced Decryption

J. Lai et al, has proposed that Attribute-based encryption is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an un-trusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher-text satisfied by that user's attributes or access policy into a simple cipher-text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher-text.

D. Decentralizing Attribute Based Encryption

A.Lewko et al, has proposed a Multi-Authority Attribute-Based Encryption system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components of a user's private key by randomizing the key. However, in this system each component will come from a potentially different authority, where we assume no coordination between such authorities. Here creates new techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

E. Cipher-text-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization

B.Waters et al, has proposed a new methodology for realizing Cipher-text-Policy Attribute Encryption (CP-ABE) under concrete and non-interactive cryptographic assumptions in the standard model. Our solutions allow any encrypted to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption.

III. PROBLEM STATEMENT

Privacy-preserving decentralized key-policy ABE scheme where each authority can issue secret keys to a user independently without knowing anything about his GID. Therefore, even if multiple authorities are corrupted, they cannot collect the user’s attributes by tracing his GID. Access control mechanism using cipher text-policy attribute based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute based encryption and selective group key distribution in each attribute group.

A. IMPLEMENTATION PLANSARCHITECTURE

To provide the confidentiality and verifiability on data for the data owner and data consumer the proposed framework is implemented in 4 modules as follows:

a. Data owner
b. Cloud Server
c. Attribute Authority
d. Data Consumer

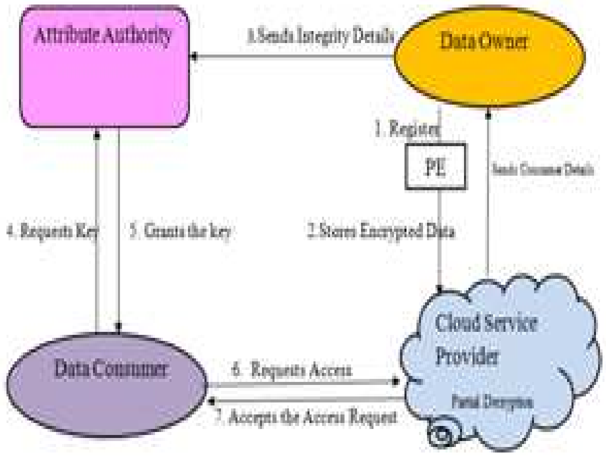

Fig.1. Architecture for Attribute Based Encryption.

1) Data Owner

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 cipher-text. 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.

2) Cloud Server

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.

3) 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. Attribute authority checks whether the user satisfies all the constraints mentioned by the data owner. If true then attribute authority sends the decryption key to data consumer.

4) Data Consumer

Data consumer requests attribute authority for decryption key. If user satisfies all the constraints mentioned by data owner then attribute authority sends the encrypted symmetric key to the user. Then data owner gives another key to the user to decrypt the symmetric key. With the decrypted symmetric key the data consumer decrypts the data that is provided by the cloud server.

5) Hybrid Encryption

It combines more than one cryptographic algorithm. It provides more security. It incorporates a combination of asymmetric and symmetric encryption. Secret keys depend upon attributes of the user. 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.

6) 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 data from the cloud the server initially retrieve the cipher text from the image and then it allows the cipher text to be decrypted.

B. ALGORITHMS

Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

F (K) → (PK, MK)
K – Implicit security parameters

Encrypt (PK, M, A): The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the cipher text implicitly contains A.

E (PK, M, A) → CT (CT → CT +A)

Key Generation (MK, S): The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

K (MK, S) → SK

Decrypt (PK, CT, SK): The decryption algorithm takes as input the public parameters PK, a cipher text CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the cipher text and return a message M.

D (PK, CT, SK) → M

Delegate (SK, ˜ S): The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S˜ ⊆ S. It output a secret key S˜K for the set of attributes ˜ S.

De (SK, ˜ S) → S˜K **S˜ ⊆ S**

IV. EXPECTED RESULT

Our design should allow the user to verify the Correctness, Completeness, and Freshness of returned search results. The main idea behind our scheme is to let cloud server return the accurate search results according to requested search query. The cloud server grants access to authorized users only, it rejects the access for unauthorized users. Data owner stores encrypted Symmetric key at Attribute Authority and encrypted data in cloud server. Data owner uses RSA algorithm for encryption of Symmetric key and AES for encryption of data.

RSA Encryption:
Mechanism used for Encrypting symmetric key:
Let key be 10
Choose two prime numbers P=7 Q=17
Then n=7*17=119
(P-1)*(Q-1) = 6*16=2*3*2*2*2*2
Now choose public E = 5[coz 5 is not a factor of (P-1)*(Q-1)]
D is private key. This must satisfy the following equation:
(D*E) mod (P-1)*(Q-1) =1
Let D = 77
Now we obtain cipher text as follows,
CT = PT^E mod n
CT = 10^5 mod 119 = 40
Now 40 will be the encrypted symmetric key
For Decryption the data consumer uses
PT=CT^D mod n
PT= 40^77 mod 119 = 10

AES Encryption:
Mechanism used for Encrypting the plain text:
Let the 16 byte key is,
Key – XXXXXXXXXXXXXXXX
Convert to 128 bit –
X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 X_9 X_{10} X_{11} X_{12} X_{13} X_{14} X_{15} X_{16} X_{17} X_{18} X_{19} X_{20} X_{21} X_{22} X_{23} X_{24} X_{25} X_{26} X_{27} X_{28} X_{29} X_{30} X_{31} X_{32}
Now convert this as follows:
W[0] =(X_1 X_2,X_3 X_4,X_5 X_6,X_7 X_8)

- .
- .
-

W[3] = (X_{25} X_{26},X_{27} X_{28},X_{29} X_{30},X_{31} X_{32})
W[5] = W[i-1] XOR W[i-4] (when i is not a multiple of 4)
Consider W[4] (when i is multiple of 4)
Temp=W[3]
Temp=substitute(rotate(temp)) XOR const[i/4]
W[4]=W[4-4] XOR temp
Overall encryption mechanism for first round:
Shift rows(substitute bytes(add roundkey(mix column)))
For rest of the rounds the mechanism is as follows:
Substitute bytes(shift rows(mix column(add roundkey)))
Now decryption is as follows:
Inv mix column(add roundkey(inv substitution bytes(inv shift rows)))

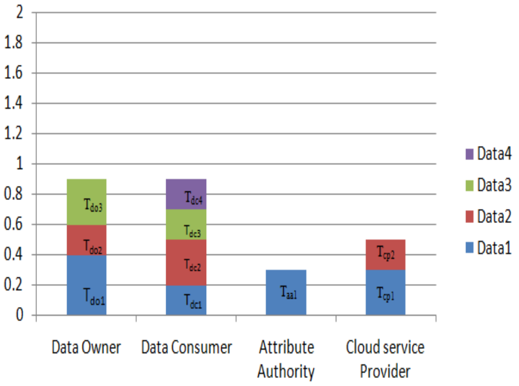

Fig.2. Users time graph for Attribute Based Encryption.

As per the graph:
T_{do1}: Time taken to encrypts the data
$T_{do2:}$ Sends the key to attribute authority
$T_{do3:}$ Sends the data to Cloud service provider
$T_{do4:}$ Sends the key to Data Consumer
$T_{dc1:}$ Requests the Attribute Authority for key
$T_{dc2:}$ Decrypts the key
$T_{dc3:}$ Requests the Cloud to access the data
$T_{dc4:}$ Download the data
$T_{aa1:}$ Checks and sends the key
$T_{cp1:}$ Partially decrypts the data
$T_{cp2:}$ Accepts the Consumer request

Firstly, the data owner encrypts the data (T_{do1}): [T_{do1}[E(PT)→CT]] and then sends the key used for encryption to the attribute authority (T_{do2}): [T_{do2}[E_k →AA]] and then places the data in the cloud service provider (T_{do3}): [T_{do3}[CT→CP]]. Data consumer requests the attribute authority for key (T_{dc1}).Attribute authority checks & sends the key (T_{aa1}).Now Data consumer decrypts the key send by the attribute authority

T_{dc1}+T_{aa1}+T_{dc2} = Symmetric key(encrypted key)

When data consumer requests attribute authority for key to decrypt the data in cloud, if the user is authorized attribute authority sends key to the data consumer by verifying certain attributes of data consumer and the encrypted key will be automatically decrypted with the combination of attributes and encrypted key itself.

T_{aa1}+ T_{dc3}+ T_{dc4}=PT

V. CONCLUSION

In this paper, we firstly present a circuit cipher-text policy attribute-based hybrid encryption with verifiable delegation scheme. Combined verifiable computation and encrypt-then-MAC mechanism with our cipher-text policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secure-based on *k*-multi-linear Decisional Diffie-Hellman assumption. 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.

REFERENCES

[1] M. Green, S. Hohenberger and B. Waters, ”Outsourcing the Decryption of ABE Ciphertexts,” in Proc. USENIX Security Symp., 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] A.Lewko and B.Waters, “Decentralizing Attribute-Based Encryption,” in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[4] 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.

[5] B. 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 attribute based 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 “Circuit Ciphertext-policy Attribute-based Hybrid Encryption with Verifiable Delegation in Cloud Computing” DOI 10.1109/TPDS.2015.2392752.

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

[11] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A.Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M.Zaharia, ”Above the Clouds: A Berkeley View of Cloud Computing, “University of California, Berkeley, Technical Report, no. UCB/EECS-2009-28, 2009.

[12] S. Yamada, N. Attrapadung and B. Santoso,”Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication,” in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.