IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Secure Access of Multimedia Data at Cloud storage using Key-Cipher Policy-Based ABE Algorithm

[1]Kavyasri M N, [2]Ramesh B,

[1]Assistant Professor, [2]Professor
[1]Department of Computer Science & Engineering,
[1]Malnad College of Engineering, Hassan, India

Abstract: The era of cloud computing is evolving around the globe. More and more users are attracted to it. Many of the applications are hosted on it, due to which the number of users increased and placed their data on it. The security of multimedia data stored in the cloud is of significant concern today. There are many access control policies available in the market today but they lack scalability, flexibility, and efficiency in performance and do not support a wide range of attributes. We propose a scheme called key-cipher policy-based ABE which is capable of addressing the issues like scalability, flexibility, and efficiency. We implement the scheme and perform security and performance analysis in this paper.

***Index Terms* - Key-cipher-policy based ABE, Data User, Data owner, tree access structure, Symmetric cryptographic systems, Asymmetric cryptographic systems.**

I. Introduction

Cloud computing is a prominent and vital area of technology. Cloud provides various services to the users. With the advancement of technology, Multimedia has become increasingly significant in today's environment. Multimedia is an effective means of communication. Multimedia data involves animation, music, video, and more. Multimedia can be stored in CDROMS, pen drives, etc. With the introduction of cloud computing, many of the companies are opting for Storage-as-a-service (A service of Cloud Computing). As Storage-as-a-Service is an essential service of Cloud service provider. A collection of multimedia data is stored at the storage on the cloud. Most of the data placed in cloud storage are confidential, and we need to secure the personal data. There are various existing research approaches to ensure confidentiality few of them are: Only data owners should be able to view their data, Before uploading a customer's data to a cloud storage server, transfer the customer's data location, Cryptographic access control can be implemented by making use of different keys to encrypt data. Different formats for various types of contents can be used to store and handle data at different locations. Implement role-based access controls. All of these approaches can be used to protect user’s sensitive data. In this research, we propose a hybrid solution to maintaining the confidentiality and security of user data called Key-Cipher-Policy based ABE.. In this approach, before outsourcing the data to the cloud server customer needs to encrypt the data. To protect data confidentiality, Encryption seems to be a good solution. On the other hand, traditional public-key encryption schemes or identity-based encryption schemes will not provide users to selectively share their fine-grained encryption of data efficiently. Two major types of Attribute-Based Encryption are. Key-policy attribute-based encryption (KP-ABE),in which fine-grained access control can be high if re-encryption technique is added to it, higher efficiency if used for the broadcast type of system and has much of computational overhead and cipher text-policy attribute-based encryption (CP-ABE), access control is done at a fine-grained level, it is not suitable for modern enterprise environment and has average computational overhead. We propose a novel approach of Key-Cipher Policy-Based ABE, which involves the combination of CP-ABE and KP-ABE approaches to provide secure access of multimedia data at the storage centers of the cloud. The remaining contents are organized as follows, we discuss related work in section II, we discuss on proposed work in section III, construction of work in section IV, performance analysis of proposed work in Section V and finally conclusion with advantage and future work.

II. Related Work

Hybrid key-attribute based encryption was introduced by Sangeetha M and P VijayKarthik [2]. The access structure tree, as well as user attributes, will be detailed in this work. This eliminates the disadvantage of KP-ABE and reduces the time it takes to encrypt and generate keys. This concept works well with traditional approaches, but it fails to deliver satisfactory outcomes with today's systems. Stefan G. Weber suggested a hybrid attribute-based encryption system that encrypts data using expressive policies with dynamic attributes. He combines ciphertext-policy of attribute-based encryption, symmetric AES encryption, the location-based approach in his work. This model provides safe cooperation based on location and can be used to deliver end-to-end secure attribute-based communications and identity management, and it enables secure collaboration based on location.

Based on CP-ABE, Win-Bin Huang and Wei-Tsung Su suggested an identity-based access control solution for digital content[5]. This method requires less storage to distribute digital files with several users. When compared to a typical access control list, this model performs well. This model has more minor security features.

III.METHODOLOGY

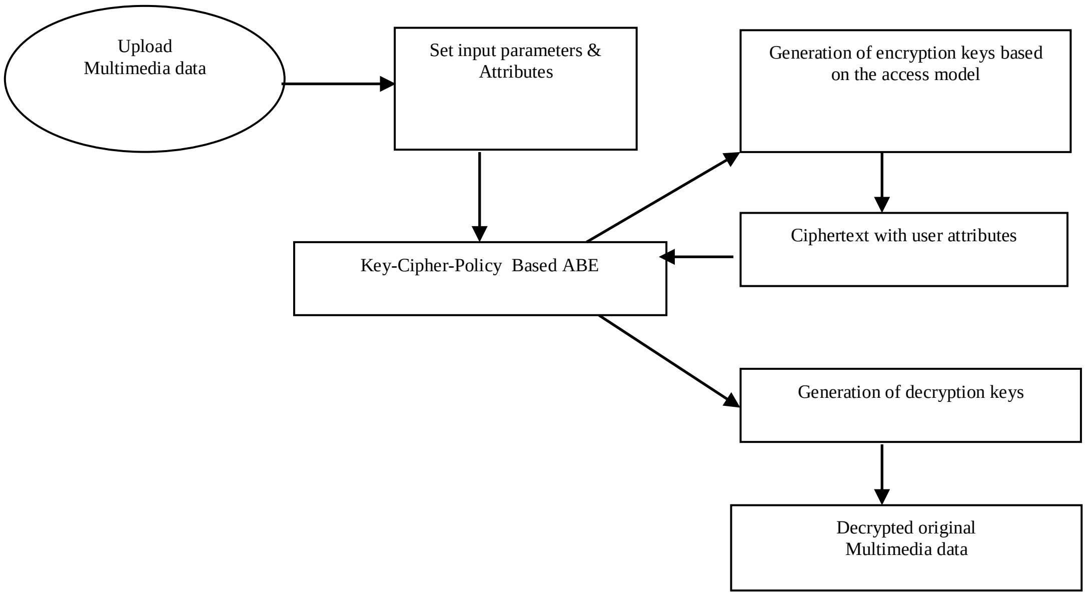
KP-ABE has efficient access control but lacks flexibility and scalability, whereas CP-ABE has efficiency in key generation and encryption but lacks efficiency in granting access controls. We proposed a model where two approaches of ABE, KP-ABE and CP-ABE, combined in order to attain secure access control and to reduce the time taken to generate a key and time to encrypt. We named the model Key-Cipher-PolicyABE. Key-Cipher-Policy based ABE has four algorithms.

Setup: This technique employs a security parameter as K has input and outputs a master key McCabe and a public key Okabe. Message senders use Pkabe to encrypt their messages. McCabe helps users in generating a secret key.

Encryption: This algorithm accepts a message McCabe, an access tree Ta, and returns ciphertext CT as an output.

Key generation: The algorithm receives access tree structure associated with user attributes and the message Mkabe as input and generates a secret key Skabe. This secret key used decrypts the message encrypted using encryption algorithm under access structure Tabe.

Decryption: This algorithm takes ciphertext CTabe and secret key Skabe for attributes set. It gives the decrypted message as output only if it satisfies the access structures of ciphertext CTabe.


Upload
Multimedia data
Set input parameters &
Attributes
Generation of encryption keys based
on the access model
Ciphertext with user attributes
Key-Cipher-Policy Based ABE
Generation of decryption keys
Decrypted original
Multimedia data

IV.CONSTRUCTION

Setup (Babe, McCabe): Let The bilinear group of prime of order P is considered to be Gp. g bet the Generator of Gp.
Consider eabe:GixGj→Gp represents bilinear map, and K, which is a security parameter, represents group size. It uses two hash **functions**, which are Habe:{0,1}*→Gi, H1abe: Gj→{0,1}log p. It publishes a public parameter Pk(eabe, g, Gp, Y. Tiabe | i∈u) and uses master key Mkabe as: (y, ti |i∈u).

Key generation: It creates private keys or users by executing KeyGen(M_{cCabe}, Sk_{abe}). This algorithm receives the message(M_{abe}) and attributes sets (S_{abe}) is considered to be the input and outputs a secret key that holds attributes in S(set of attributes)
Input: public key(Pk_{abe}), message (M_{cCabe}), attribute-associated access structure (Ta_{nabe}).

$$Skut = (Dabe = g(\alpha + ri)/\beta, \quad \forall \lambda j \in Sabe \qquad (1)$$

$$Djabe = gri.H'abe(\lambda j)rj) \qquad (2)$$

It selects two random input exponents RI ∈ RZp* and RJ ∈ RZp* where ri and RJ are unique secret keys to the user Ui and Uj, respectively ∈S_{abe}. Then it provides a private key to the user.

Data encryption: The tree access structure, based on the user attributes(Tabe), an encryption algorithm is used to encrypt messages. Let Tabe's leaf nodes are referred to as Kabe. The data owner computes Sy_{abe}=$(e(g^{\beta})^{\alpha}$, $H_{abe}(\lambda y))$ for all y ∈Y in the leaf node of the access tree and then calculates $H1_{abe}(Sy_{abe})$. With the tree access structure T_{abe} coupled with user attributes, message M is encrypted by the encryption method. For each of the nodes in the tree T_{abe}, which includes leaves, the algorithm begins by choosing a polynomial qx_{abe}; each node is represented as x_{abe}. Starting with the node considered to be the root R_{abe}, using the topdown approach, the polynomials are chosen. Set the polynomial qx_{abe}'s degree dx_{abe} which is less than the threshold value of $kx_{abe.}$ Of each node x_{abe} in the tree, that is, $dx_{abe} = kx_{abe}-1$. Beginning with R_{abe}, the algorithm selects a random attribute set S, Zp and will set $qR_{abe}(0) = S$. Then, to completely define the polynomial qR_{abe}, it chooses dR_{abe} and other points at random from QR, polynomial. It sets

$$qxabe(0) = qabeparent(xabe)(index) \qquad (3)$$

for any other node x_{abe}.

$$CTabe = T ; \qquad (4)$$

$$C'abe = Me(g,g')\alpha sabe; \qquad (5)$$

$$Cabe = hSabe , \quad \forall\ y \in Y; \qquad (6)$$

$$Cyabe = g\,qyabe(0); \qquad (7)$$

$$C'yabe = Habe(att(y))qyabe \qquad (8)$$

Decryption: decryption procedure is chosen to be recursive. First, the recursive algorithm executes Decrypt(CTabe, Skabe, x). It takes ciphertext as the input CTabe = (Tabe , C′abe, Cabe, ∀y ∈Y: Cyabe, C′yabe) and a private key Skabe associated with a attributes set S and a node x_{abe} from T_{abe}.

If node x_{abe} is considered to be a leafy node, then $i=att(x_{abe})$, and if $i \in S_{abe}$ then,

$$Decrypt(CT_{abe},Sk_{abe},x_{abe}) = \frac{e_{abe}(Di_{abe,}Cx_{abe}}{e_{abe}(D'i_{abe,}C'x_{abe})}$$

$$= \frac{e_{abe}(gr\cdot H_{abe}(i)ri\ ,hqx_{abe}(0)}{e_{abe}(gri\ ,Habe(i)qxabe(0))}$$

$$= e_{abe}(g,g).rqx_{abe}(0) \qquad (9)$$

X_{abe} from T_{abe}. If node x_{abe} is considered to be a leafy node, then $i=att(x_{abe})$, and if $i \notin S_{abe}$ then

$$Decrypt(CTabe, Skabe, xabe) = \perp \qquad (10)$$

The algorithm decrypts by calculating

$$C'_{abe}/(e_{abe}(C_{abe},D_{abe})/A) = C'_{abe}/(e_{abe}(hs_{abe},g(\alpha+r)\ /\beta)\ /e_{abe}(g,g)\ rs) = M_{abe} \qquad (11)$$

V .PERFORMANCE ANALYSIS

Performance analysis of key-cipher policy attribute-based encryption is carried out with respect to three aspects, 1. Security,2. Space complexity, 3. Time complexity. The analysis environment includes authority, one data owner, and multiple data users.

A. Security Analysis

Security analysis is performed on confidentiality, authentication, and authorization.

1. *Confidentiality*

Confidentiality is one of the key concerns in cloud storage. Consider an image-sharing service as an example. When the user erases the image in the application, the image will be erased in the application also, but there are a lot of third-party service providers that may or may not provide security and can save the user's image.

But in this work, all the multimedia content is encrypted before outsourcing to the cloud, and even-if third-party service providers can access the multimedia data if and only if it is decrypted with the user attributes.

2. *Authentication*

In Key-Cipher-Policy ABE, the user could obtain secret keys only with the help of access trees associated with user attributes.

3. Authorization

In Key-Cipher-Policy ABE the user decrypts the multimedia message M only when attributes described in secret keys satisfy the access structure. Thus admission control can be enabled.

*B. **Space complexity***

The space complexity is compared with encryption approaches symmetric, asymmetric cryptosystems, and Key-Cipher-Policy ABE as shown in Figure 3. Following analysis is made by considering the sizes of key and messages p and q.

In the symmetric crypto-based system approach, each user must possess a unique secret key corresponding to the data owner. The data owner should store available secret keys, which are of size np. The multimedia message should be encrypted uniquely with each data user. Thus the data owner should keep the messages of the size of nq. The total storage size will be np+nq.

In the asymmetric crypto based system. The data owner should store the public keys of size np with all data users. All data users store the private keys of size np. The message should be encrypted with the public key of each user. Finally, the data owner must keep all the messages with the size of nq. The total storage size is 2np+nq.

In Key-Cipher-Policy ABE. The data owner must store the public key with size np, and the data user needs to encrypt the message only once because the secret key is derived from the access structure associated with user attributes. Thus the data owner should store a copy message with size q. Hence total storage will be np + q.

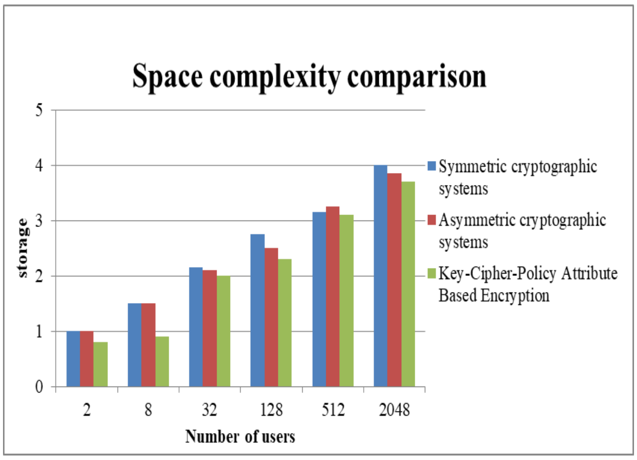


Figure 3. Space Complexity Comparison

C. *Time complexity:*

The time complexity of Key-Cipher-Policy ABE is calculated based on enormous distribution, single-user licensing, single-user revoking. Among symmetric-based approach, asymmetric-based approach, and Key-Cipher-Policy ABE. The comparison result is shown in the table 1.

*1. **Enormous distribution:***

In symmetric cryptographic systems and asymmetric cryptographic systems approaches data owner needs to encrypt the multimedia data per data user, so for enormous distribution, the time complexity is defined to be O(n) per data user. In Key-Cipher-Policy ABE the data owner needs to encrypt multimedia data only once for distributing the data among n data users. The time complexity with enormous distribution to n data users is 0(1).

*2. **Single-user licensing.***

Following discussion of enormous distribution in symmetric cryptographic systems and asymmetric cryptographic systems, data owners need to encrypt multimedia data for distributing to a fresh user. So time complexity of the individual user will be 0(1). Whereas in Key-Cipher-Policy ABE, If attributes of the data user satisfy the access structure, then no need to encrypt separately. If the user attribute does not satisfy the access structure, then encryption needs to be performed. So time complexity for single-user licensing is 0 or 0(1).

*3. **Single user revoking***

In symmetric cryptographic systems and asymmetric cryptographic systems, data owners need to remove the protected content for revoking a user. The time complexity of user revocation is 0. In Key-Cipher-Policy Attribute-Based Encryption, a new access structure is required to re-encrypt the data with a new access structure. The time complexity of single-user revoking is 0(1).S

	Enormous distribution	Single user licensing	Single user revocation
Symmetric cryptographic systems	0(n)	0(1)	0
Asymmetric cryptographic systems	0(n)	0(1)	0
Key-Cipher-Policy ABE	0(1)	0(1)	0(1)

Table 1. Time complexity Comparison table

VI. Conclusion

The primary concern of our work is the implementation of the Key-Cipher-Policy ABE algorithm. Compared to the existing algorithms, we can keep the multimedia data secure and confidential using this algorithm. We used the hybrid approach where KP-ABE and CP-ABE algorithms were combined to provide secure access to multimedia data at cloud storage centers. Based on the Performance analysis of the system regarding security space and time complexity, our work outperformed the traditional access control methods and encryption-based access control methods. The future enhancement of this work is to improve the key generation time and encryption time in order to provide fine-grained access control to the user data.

References

[1]. M Vignesh, R Naresh, “Exploration of Attribute-Based Encryption schemes on cloud computing",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020

[2]. Sangeetha M, P VijayaKarthik, “To Provide a Secured access control using combined hybrid Key-Ciphertext Attribute-based encryption (KC-ABE). IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing. 2017.

[3]. Nurmamat Hell, Kaysar Rahman, "CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy", Security and Communication Networks, vol. 2017, Article ID 2713595, 13 pages, 2017. https://doi.org/10.1155/2017/2713595

[4]. Edema K, Jang B, Kim JW CESCR: CP-ABE for efficient and secure sharing of data in collaborative ehealth with revocation and no dummy attribute
(2021) CESCR: CP-ABE for efficient and secure sharing of data in collaborative ehealth with revocation and no dummy attribute. PLOS ONE 16(5): e0250992. https://doi.org/10.1371/journal.pone.0250992.

[5]. Win-Bin Huang, Wei-Tsung Su, "Identity-based access Control for Digital Content based on Ciphertext-Policy Attribute-Based Encryption. ICON 2015.

[6] Shulan Wang, Kaitai Liang, Joseph K Liu, “Attribute-Based Data Sharing Scheme Revised in Cloud Computing" IEEE Transactions of Information forensics and security, Volume 11, No8, August 2016.

[7]. B. Waters, “Ciphertext-Policy attribute-based encryption:An expressive, efficient, and provably secure realization," in proc 14th Int. Conf.Theory Public Key Cryptography Conf. Theory Cryptograph. 2012.

[8]. Sahai A, Waters B, et al. Fuzzy identity-based encryption[C]//Proc of EUROCRYPT’2005. LNCS 3494, 2005, pp.457–473. Springer, Heidelberg.

[9]. Bethencourt J, Sahai A, et al. Ciphertext-Policy attribute-Based Encryption[C]//Proc of IEEE Symposium on Security and Privacy 2007. 2007, pp.321-334.

[10]. S Yu, K Ren, et al. Attribute-Based Content Distribution with Hidden Policy[C]//Proc Of NPSEC'08. Orlando, Florida,USA, 2008, pp.39-44.