International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-11 Issue-1, May 2022

Key-Cipher-Policy based ABE with Efficient Encryption of Multimedia Data at Data Centers of Cloud

Kavyasri M N, Ramesh B

Abstract: ***Cloud computing is relatively one among the new technologies that is attracting moreclients to adopt cloud storage for easy and convenient online data storage and sharing. Because of its efficient computations, it has attracted the attention of both industry and academia. Companies began outsourcing confidential data to cloud service data centres. These data storage applications have security concerns about data confidentiality and privacy. When data is moved to the cloud, the customer loses control of the data and must rely on the cloud service provider. To protect their data, clients must first guarantee that it is encrypted. Encryption is a promising method for keeping data private in the cloud. ABE is a potential technique for dealing with security challenges in data center cloud storage. The key benefit is that it allows flexible one-to-many encryption. We present a model termed key-Cipher-policy-based ABE in this study. It allows optimized and more secure access to data stored at the data centers of cloud. with optimized encryption and less encryption time.***

Keywords: ***Key-Cipher-Policy Based Abe, Access Policy, Data Owner, Tree Access Structure.***

I. INTRODUCTION

Cloud computing is a new technology in which cloud service providers deliver various services over the internet on a pay-per-use basis. It is a hybrid of distributed and parallel computing technologies in which work is done on multiple units parallelly. The provider of cloud services will rent resources to the user, who will not have to deal about maintenance and can concentrate on the task. Multimedia has become increasingly significant in today's environment as technology advances. Multimedia is an effective means of communication. Animation, music, video, and other forms can be found in multimedia. Multimedia can be saved on CDROMs, flash drives, and other storage devices; but, with the introduction of Cloud Computing, many businesses are turning to storage services. Storage-as-a-Service is one of the most crucial services provided by a Cloud service provider. As a result, a collection of multimedia material is stored on the cloud. Multimedia data comprises animations, well-choreographed presentations, high-definition audio and video, and collaborative multimedia papers.

Manuscript received on 20 September 2021.
Revised Manuscript received on 12 April 2022.
Manuscript published on 30 May 2022.
* Correspondence Author
Kavyasri M N*, Assistant Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan (Karnataka), India.
Dr. Ramesh B, Professor, Department of Computer Science and Engineering, Malnad College of Engineering, Hassan (Karnataka), India.

It's kept on a cloud-based data storage server. The data storage server suffers personal privacy and security issues when storing and accessing multimedia data. We are concentrating on work-related to security concerns. The majority data which is stored in cloud storage is very sensitive, and we must protect it. To ensure security of the users data , Secure access of multimedia data stored at data centres of cloud is the major concern. When it comes to protecting sensitive data from unwanted access, data encryption is the most effective. Encrypted data have to be encrypted by single user in traditional public key encryption which is also known as identity-based encryption approaches . Regrettably, this does not have the features for advanced data exchange. To address this issue, Sahai and Waters [10] proposed an algorithm which is attribute-based encryption (ABE). This system, instead of encrypting to specific users, an access policy is added in the ciphertext or key used for decryption. As a result of the encryption, Cryptography makes data access self-enforcing. ABE algorithm is a development of the encryption concept which is based on identity , in which set of descriptive features are used to define the user's identity rather than individual string. ABE has a significant advantage over identity-based encryption [11] in that it offers flexible one-to-many encryption rather than one-to-one encryption. It is considered to be the potential solution for solving the challenge of fine-grained , safe, and secure data sharing and decentralised access control. There are two main types of attribute-based encryption. Key-policy attribute-based encryption (KP-ABE), If re-encryption technique is added to it results in high fine grained access control, 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 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 efficient encryption for secure access of multimedia data at the storage centres of cloud.

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 sufficient 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, location-based approach of 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 less security features.

III. KEY CIPHER POLICY BASED ABE

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 time taken to generate a key and time to encrypt. We named the model as Key-Cipher-PolicyABE. Key-Cipher-Policy ABE has four algorithms.

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

Encryption: This algorithm accepts a message Mkabe, an access tree Ta, and returns cypher text 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 decrypted message as output only if it satisfies the access structures of cipher text CTabe.

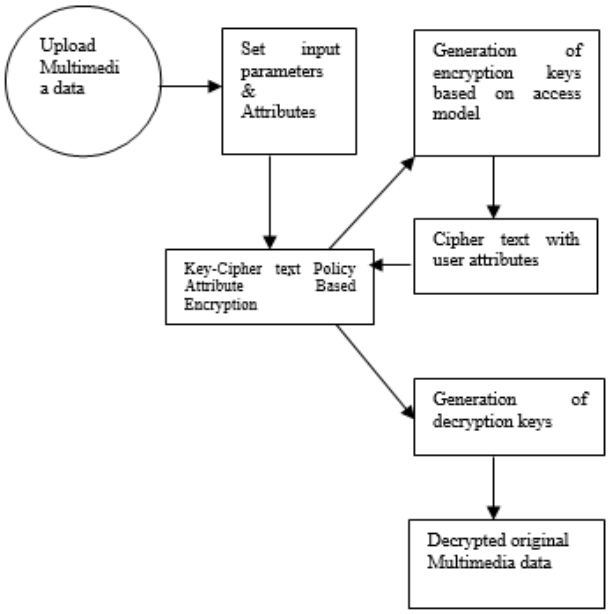

Fig. 1. Block diagram of Key Cipher Policy based ABE

Table: 1 Notation

Notation	Definition
Pk_{abe}	Public key of data owner
Mk_{abe}	Master key of data ower
Sk_{abe}	Secret key of data user
T_{abe}	Access tree structure
Ta	Attributes associated with access tree
M_{abe}	Multimedia data

IV. CONSTRUCTION

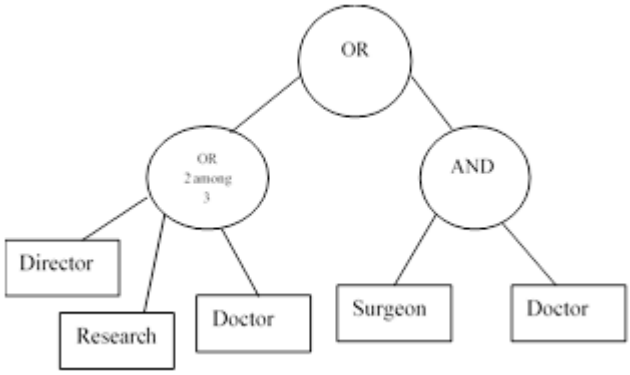

Fig. 2. Key generation using key-cipher-policy based ABE

Set of attributes

T a= {a1 = "Director", a2= "Research", a3= "Doctor", a4= "Surgeon",……}

Our Access model

Ta= {(2 of ("Director", "Research", "Doctor")) or ("Surgeon" and "Doctor")}

Setup (P_{abe},Mk_{abe}): Let The bilinear group of prime of order P is considered to be Gp. g bet the Generator of Gp. Consider e_{abe} :GixGj→Gp represents bilinear map and K which is a security parameter represents group size. It uses two hash functions, which are H_{abe}:{0,1}*→Gi, $H1_{abe}$: Gj→{0,1}$^{\log p}$. It publishes a public parameter Pk(e_{abe}, g, Gp, Y. T_{iabe} | i∈u) and uses master key Mk_{abe} as: (y, ti |i∈u).

key generation: It creates private keys or users by executing KeyGen(Mk_{abe}, Sk_{abe}). This algorithm receives 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 (Mk_{abe}), attribute-associated access structure (Ta_{abe}). It selects two input random 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 private key to the user.

Skut=(D_{abe}=g(α+ri)/β, ∀ λj∈S_{abe}

Dj_{abe}= gri.H′$_{abe}$(λj)rj).

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^{β})$^{\alpha}$, H_{abe}(λy)) for all y ∈Y in the leaf node of access tree and then computes $H1_{abe}$(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 node in the tree T_{abe}, which includes leaves, 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 top-down 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}, 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 $qx_{abe}(0) = q_{abe}parent(x_{abe})(index)$ for any other node x_{abe}.

$CT_{abe} = T$,

$C'_{abe} = Me(g,g') \alpha s$,

$C_{abe} = hS_{abe}$, $\forall \quad y \in Y$:

$Cy_{abe} = g\, qy_{abe}(0)$,

$C'y_{abe} = H_{abe}(att(y))\, qy_{abe}(0)$.

Decryption: decryption procedure is chosen to be recursive. First, recursive algorithm executes Decrypt(CTabe, Skabe, x). It takes cipher text 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,

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

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

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

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

$$Decrypt(CT_{abe}, Sk_{abe}, x_{abe}) = \perp$$

The algorithm decrypts by calculating

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

V. RESULT AND DISCUSSION

The time taken to the key generation method will be proportional to the attributes number connected to issue the key. Because the time taken to run encryption algorithm is almost exactly linear in relation to the leafy nodes number in the policy defined by access structure, both solutions will be feasible for the most severe problem cases. The performance of the decryption technique is more interesting; the time it takes to decrypt a collection of attributes is heavily influenced by the access tees. The decryption algorithm was tested on a set of cypher texts that is encrypted using policy trees generated randomly with the policy trees of varied sizes. Starting with root nodes, the trees are created by attaching the child to a node which is randomly selected repeatedly until adequate leaf nodes was created. For each internal node, a random threshold was set. The amount of time it takes to decrypt is also determined by the quantity of attributes accessible. For each run, a key is chosen uniformly and randomly from available keys that meet the policy's requirements. This is achieved by considering random attributes subsets on the tree's leaves in an iterative manner. Based on attributes present in a key which is based on leaves in a policy, key generation and key encryption take a predictable amount of time. The efficiency obtained by decryption algorithm is determined by the attributes present in the private key of specific access tree.

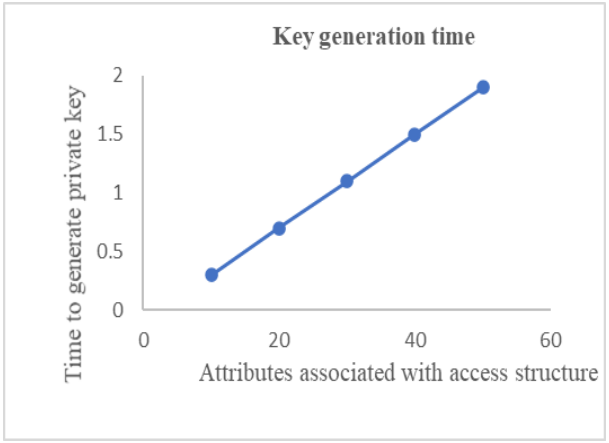

Fig. 3. Key generation time in key-cipher-policy based ABE

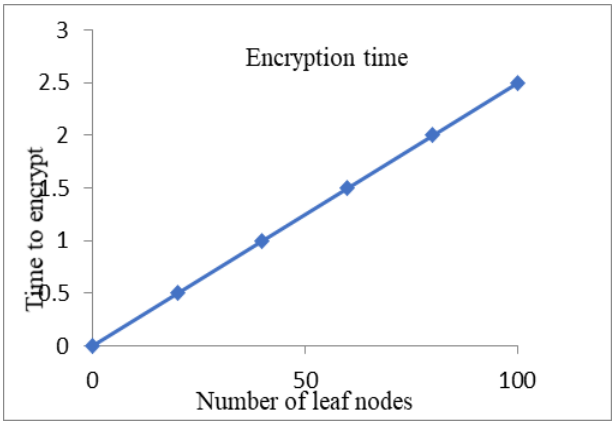

Fig. 4. Encryption time in key-cipher-policy based ABE

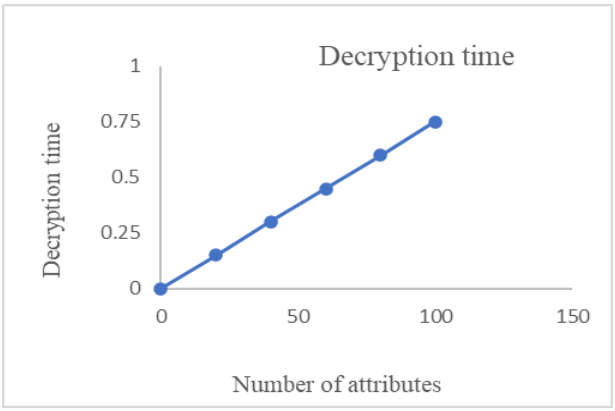

Fig. 5. Decryption time in key-cipher-policy based ABE

VI. CONCLUSION

Our work centered on execution of Key-Cipher-Policy Attribute Based Encryption algorithm. Compared to the existing algorithms we can keep the multimedia data secure and confidential. We used the hybrid approach where KP-ABE and CP-ABE algorithms were combined to provide secure access of multimedia data at the storage centers of cloud.

Based on attributes present in a key which is based on leaves in a policy, key generation and key encryption take a predictable amount of time. The efficiency obtained by decryption algorithm is determined by the attributes present in the private key of specific access tree. Thus proposed algorithm has efficient encryption and decryption techniques along with key generation time, resulting in providing secure access of multimedia data at data centers of cloud.

REFERENCES

1. M Vignesh, R Naresh, “Exploration of Attribute Based Encrypt ion 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). International Conference on Intelligent Techniques in Control, Optimization and Signal Processing. IEEE, 2017.
3. Nurmamat Helil, 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. Edemacu 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.
5. Win-Bin Huanh, Wei-Tsung Su, “Identity-based access Control for Digital Content based on Ciphertext-Policy Attribute-Based Encryption. ICOIN 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, “Ciphettext-Policy attribute-based ecryption:An expressive, efficient, and provably secure realization,” in proc 14th Int. Conf.Theory Public Key Cryptography Conf. Theory Cryptograph. 2012.
8. Sahai and B. Waters, “Fuzzy identity based encryption,” in Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494 of Lecture Notes in Computer Science, pp. 457–473, Springer, 2005
9. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing,” in Proceedings of the Annual International Cryptology Conference (CRYPTO '01), vol. 2139 of Lecture Notes in Computer Science, pp. 213–229, Springer, 2001.

AUTHORS PROFILE

Kavyasri M N, is currently working Assistant Professor in the Department of Computer Science and Engineering, Malnad College of Engineering, Hassan. She is currently pursuing her research in Cloud COMPuting, Her major area of research includes Cloud Computing, soft Computing, Computer Networks. She has presented ten papers in the international journals and conferences

Dr. Ramesh B, is currently working as Professor in the Department of Computer Science and Engineering, Malnad College of Engineering, Hassan. He Received his Ph.D degree in Mobile Adhoc etwork from Computer Science and engineering from Anna University, Tamilnadu. His research interests include Computer Networks, Multimedia Computing, Mobile AdHoc Networks, Cloud Computing and Network Security. He is been awardes as the Best Citizens of India Award 2013 from yhe international Publishing House.