USE OF ATTRIBUTE BASED ENCRYPTION FOR SECURE DATA ACCESS CONTROL IN MOBILE CLOUD COMPUTING - A CASE STUDY

U. Sujatha[1], U. Saranya[2] and C.P. Boopathy[3]

[1,2]Department of Master of Computer Applications, Dr. Mahalingam College of Engineering and Technology, India
[3]Department of Electrical and Electronics Engineering, SVS College of Engineering, India

Abstract

Cloud Computing has become an important paradigm that has attracted many users in industry and academia. Many people use the cloud every day without knowing its technology. All versions of email, drives, access to the applications that are not physically installed on the local system they utilize the features of the cloud. Mobile Cloud Computing (MCC) provides cloud-based services to users through mobile devices. The data shared/uploaded with mobile devices to public data storage increases productivity, but on the other side introduces security vulnerabilities as well. In the Attribute-based Encryption (ABE) scheme, attributes are dynamically collected from the mobile devices. It plays a vital role in generating a public key for encrypting data and control user access policy. The authors review ABE methods that provide secure data access control for Mobile cloud computing environment.

Keywords:

Security, Encryption, Multiple Dynamic Attributes

1. INTRODUCTION

Cloud Computing delivers highly scalable and elastic computing services, storage services on pay-per-use model. Many organizations are now moving their data from in-house data centers to the Cloud Storage Providers [10] [12].

According to Cisco global cloud index forecast, by 2020 with the growth of global data center and cloud-based services 92 % of workloads will be processed by cloud data centers, while 8% will be processed by traditional data centers [3].

Nowadays, the usage of mobile devices has been increasing in the areas of the education system, health care management [24], online transactions and marketing. But the mobile device has limited resources in terms of battery lifetime, storage, and processing capacity, to overcome these limitations cloud computing can be accessed into the mobile environment i.e., Mobile Cloud Computing (MCC) where computation resources and data to other services provided on demand.

In MCC, the resource-intensive tasks can be offloaded to a remote cloud for processing and the result will come back to the mobile device. The mobile devices are connected to the remote cloud with the help of 3G (or) LTE networks. So it is possible to access the stored data using mobile devices from Cloud Service Provider (CSP) anywhere, anytime. As the data has to travel in the network there different types of attacks and threats are possible.

Data confidentiality is not guaranteed in cloud computing and the data of user may be leaked by a third party, if data is stored in its original configuration. To overcome this issue, many researchers proposed various scheme to store encrypted data in public servers [4].

2. ATTRIBUTE BASED ENCRYPTION

ABE is a type of public-key encryption system. It generates the secret key of a user and the ciphertext are dependent upon static and dynamic attributes. It uses the user’s identity as attributes and these sets of attributes were used to encrypt and decrypt data. The ABE scheme solves the problem that the data owner needs to use every authorized user’s public key to encrypt data [3] [9].

ABE provides the fine-grained access control policy for encrypted data in the cloud. In traditional approaches, Public Key Infrastructure (PKI) is used as the access control algorithms for the encryption and decryption process. It starts with the sender requesting a public key from the Key Distribution Center (KDC). Then PKI signs the public key and sends it to the requester. The sender uses the public key to encrypt the message for the receiver. The receiver uses the private key to decrypt the message encrypted by the sender. This has certain limitations like, to communicate with the receiver, the sender has to communicate with the PKI [2].

ABE is mainly used to prevent unauthorized users from accessing the confidential data in cloud. In the traditional cryptography methods, it combines the public key cryptography and symmetric cryptography, which is inefficient for wireless environment [25]. ABE can be used for access control in distributed and wireless environment. In the current ABE schemes [1] [3] [7] [11] rely on pairing-based a group that creates more computational overheads and implies high cost for the encryption and decryption process. To overcome this limitation in sharing keys in the common medium, in ABE access policy is being associated with the attributes of the user. Many researchers proposed modified ABE Methods to increase the efficacy of the system [21]. The Table.1 summarizes the merits and demerits of the above methods [6] [10] [26].

3. ABE TYPES

User can decrypt the cipher-text when they meet the required attributes, which makes is suitable for cipher-text based access control and broadcast encryption [25].

There are mainly two types of ABE schemes: Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher text-Policy Attribute-Based Encryption (CP-ABE) [10] as shown in the Fig.1.

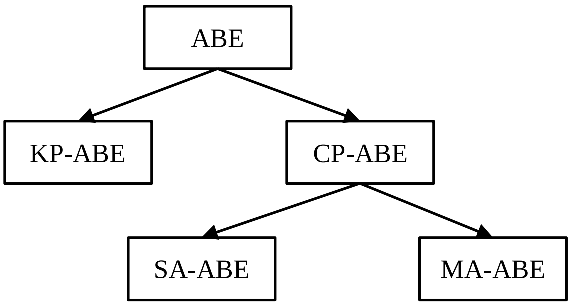

Fig.1. Types of ABE

In KP-ABE, private keys of users are associated with policies and ciphertext is labelled by sets of attributes. The user's private key in KP-ABE is identified with an access-tree structure, where the user's attributes are located in the nodes of the tree. The interior nodes of this access-tree are the threshold gates which are described by their children and a threshold value. A user can decrypt a cipher text with a given key if and only if the data access structure is satisfied by the attributes associated with a ciphertext. It ensures the confidentiality of outsourced data [5] [11].

CP-ABE is a cryptosystem in which ciphertext are associated with policies, whereas the user's private key is associated with a set of descriptive attributes. An encryptor has to specify a policy that private keys must satisfy to decrypt the message by using an access tree structure. A user will be able to decrypt a ciphertext with a given key, if and only if the attributes satisfy the policy of the respective ciphertext. Policies may be defined over attributes using conjunctions, disjunctions threshold gates [9]. Wang et al. [22] proposed a searchable encryption algorithm with attribute update in cloud storage. It uses AND-gate access policy with version number for each attribute, when the version number of revocation attributes changes.

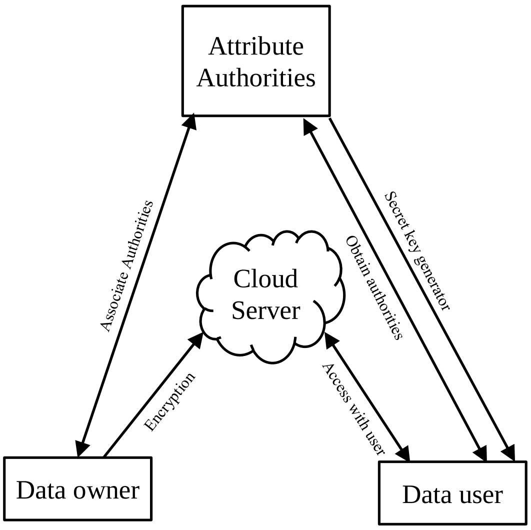

Fig.2. ABE Architecture

ABE is further classified into Single Authority-ABE (SA-ABE) and the Multiple Authorities-ABE (MA-ABE). In SA-ABE, only one authority is involved, which monitors all the attributes and assigns the encryption or decryption credentials to the data owner and user. When attacker knows all the attributes, they can decrypt the data; it leads to user data privacy breach issues. In MA-ABE multiple independent authorities monitor the distribution of encryption or decryption credentials which avoids collisions and attacks [1]. The Fig.2 explains the general architecture of ABE where multiple attributes decides the access control of data [20] [23].

4. RELATED WORK

Cloud service providers to secure their cloud platform and provide better services to user, adopts different security technologies. Much research work has been carried out for secure access control in the mobile cloud computing platform.

Agrawal et al. [1] put forwarded an access control policies associated with the multiple dynamic attributes collected from mobile devices like spatial or temporal attribute, application usage, unlock failures, location and proximity details are used to curb the access of data.

In cloud computing data is stored and processed in third-party service providers. Personal data may be leaked by a third party, if data is stored in its original configuration. Access control through encryption is employed to achieve confidentiality and to prevent unauthorized access to personal data [11].

The authors proposed CP-ABE cryptographic method, where the data owner stores encrypted data using fine-grained access policies; hence the users who fulfil the access constraints can only access the data. To overcome the delays in the communication and frequent disconnection, two mobile agents Client-Side Agent (CSA) and Server-Side Agent (SSA). CSA will run at the user's mobile device while, SSA will run within the wired network is used.

The data owner request for a certificate from Certificate Authority (CA) by providing their ID if authorized the data owner request Attribute Authorities (AA) for the encryption credentials. Each AA generates the global parameters, a public key and a private key using bilinear pairing. If the dynamic attributes collected by each AA is valid, Lagrange interpolation is applied to generate a combined secret key. With the use of the secret key, the data owner can encrypt with the static and dynamic attributes and store it in the cloud or access the encrypted data. It also provides uninterrupted communication between the clients and the cloud storage server by using the pairs of mobile agents. Since multiple attribute authorities involved the anonymity of the user is also maintained.

Koe et al. [3] proposed an efficient decentralized multi-authority attribute-based scheme for mobile cloud data storage. It solves the key escrow problem by removing the central authority with CP-ABE, without making use of any global user identity and reduces the communication overheads with cloud user assistant on the user side. It serves as the gateway for the mobile user during interactions with the multiple attribute authorities. A Cloud User- Agent (CUA) [13] is a semi-trusted and cloud-based entity to alleviate computation and communication overhead on the data user.

When the user requested to access the data stored in the CSP, Data Owner (DO) with the security parameter, runs a key generation algorithm to produce the Public key (PK), Master Key (MK) with the use of bilinear groups. DO maintain a list of user for local authentication and access policy for the data that are uploaded to CSP. If the user successfully authenticated, with inputs of PK and MK, DO generates the DO_key and sent both PK and DO_key to the user via a secure medium. DO will send the secret parameter to the different AA through secure communication channel [14].

After the successful acquisition of requested attributes from AA, plain message is encrypted with PK, with the access policy. The corresponding ciphertext which will is uploaded to CSP [16].

Once the CUA has received a request for the user attributes, it sends the request for attribute secret keys to the solicited AA managing those attributes. Once CUA has received the PK and attributes from various AA, the CUA will aggregate all to produce a unified key. The user key generation stage performed by the user after having received both the DO secret key and the CUA secret key. The data user will then run the key generation to generate its secret key [17]. The data user now having its secret key, request the partially decrypted cipher text from the cloud to recover the plain text.

Zhang et al. [7] Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing proposes a novel technique called match-then-decrypt, which introduces a matching phase before the decryption process. It embeds special components in cipher texts, which used to perform the test. If the attribute private key matches the hidden access policy in cipher texts without decryption, then only the decryption process will be carried out, thus improves the efficiency of the decryption process.

It uses Canetti–Halevi–Katz transformation through which the decryptor can test data before complete decryption and the subsequent decryption procedures are performed if and only if the test passes.

During system initialization, AA chooses a security parameter and runs the algorithm of anonymous CP-ABE to generate PK and MK for the system. Then AA publishes PK and keeps MK as a secret key. When a user with an attribute list L wants to join the system, AA runs the algorithm of anonymous CP-ABE to obtain an attribute secret key SKL and gives it to the user. Whenever the Data owner wants to outsource a file to CSP, the user defines an access policy *W* for this file. Then, DO randomly pick a symmetric key *K* from the key space and encrypts the file using a standard symmetric encryption algorithm such as AES [12] [21] to obtain the ciphertext.

DO anonymously encrypts the symmetric key with respect to access policy with anonymous CP-ABE and generates, and the ciphertext is CTK, where the access policy is hidden. Finally, CTK is anonymously outsourced to CSP with the access policy hidden [15] [19].

When the user wants to get an outsourced file of his/her interests, he/she downloads the ciphertext from CSP and anonymously decryption has to be carried out. First, the user performs the Matching Phase based on his/her attribute secret keys to check message under a ciphertext policy is matches with secret key SKL associated with an attribute list *L*, or not. Only if the attribute match is successful, the user performs the Decryption Phase and anonymously decrypts CTK, to get the symmetric key by running the algorithm of anonymous CP-ABE and retrieves the file. The Table.2 summarises the above approaches [18] [20].

Table. 1. Comparison of ABE Types

Type	KP-ABE	CP-ABE
Association of Attributes	Data is associated with access policy	Cipher text is associated with access policy
Attribute support	Supports user with dis similar attributes based on key policy	Users different attributes in single set
Encryption	It cannot decide who can encrypt data.	Decrypt key only support user attribute that are organized logically
Computation Overheads	High	Average
Collision Resistance	Average	Good

Table.2. Comparison of MA-ABE methods

Parameters	Trustworthy Agent-based Encrypted Access control Method	Decentralized Multi-Authority Attribute based Encryption	Attribute Privacy Protection and Fast Decryption
ABE-TYPE	CP-ABE with multiple AA	CP-ABE with multiple AA	CP-ABE with multiple AA
Use of Agents	Both at user side and CSP	Agents only at user side	No Agents
Encryption	RSA Cryptographic Algorithm	Decisional bilinear Diffie-Hellman	Decisional bilinear Diffie-Hellman
Decryption Efficiency	Average	Good	Good
User Revocation	Yes	Yes	No
Collusion Resistance	Yes	Yes	Yes
Data Confidentiality	Yes	Yes	Yes
Solution for Network disconnection issues	Yes	No	No
User Anonymity	Yes	Yes	Yes

5. CONCLUSIONS

The above study concludes the scope of workspace available in MA-ABE access control method for the mobile cloud environment.

The observation of this study shows the data owner authorizes with dynamic attributes along with static attributes for data encryption and also the users must satisfy these attributes to access the stored data. This study illustrates and compares the different techniques that reduce computation and communication overhead between the user and multiple attribute authorities. It needs to study more on the usage of mobile agents that can reduce the overheads and increase the speed of encryption and decryption.

REFERENCES

[1] Neha Agrawal and Shashikala Tapaswi, "A Trustworthy Agent-based Encrypted Access control Method for Mobile Cloud Computing Environment", *Pervasive and Mobile Computing*, Vol. 52, pp. 13-28, 2019.

[2] Cheng-Chi Lee1 , Pei-Shan Chung and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", *International Journal of Network Security*, Vol. 15, No. 4, pp. 231-240, 2013.

[3] Voundi Koe Arthur Sandor, Yaping Lin, Xiehua Li, Feng Lin and Shiwen Zhang, "Efficient Decentralized Multi-Authority Attribute based Encryption for Mobile Cloud Data Storage", *Journal of Network and Computer Applications*, Vol. 129, pp. 25-36, 2019.

[4] Neha Agrawal and Shashikala Tapaswi, "Access Control Framework using Dynamic Attributes Encryption for Mobile Cloud Environment", *Progress in Advanced Computing and Intelligent Engineering*, Vol. 13, No. 1, pp. 611-621, 2018.

[5] Balamurugan and P. Venkata Krishna, "Extensive Survey on Usage of Attribute Based Encryption in Cloud", *Journal of Emerging Technologies in Web Intelligence*, Vol. 6, No. 3, pp. 263-272, 2014.

[6] Mehdi Sookhaka, F. Richard Yu, Muhammad Khurram Khan, Yang Xiang and Rajkumar Buyya, "Attribute-Based Data Access Control in Mobile Cloud Computing: Taxonomy and Open Issues", *Future Generation Computer Systems*, Vol. 72, pp. 273-287, 2017.

[7] Yinghui Zhang, Xiaofeng Chen, Jin Li, Duncan S.Wong, Hui Li and IlsunYou, "Ensuring Attribute Privacy Protection and Fast Decryption for Outsourced Data Security in Mobile Cloud Computing", *Information Sciences*, Vol. 379, pp. 42-61, 2017.

[8] Maha Tebaa and Said El Hajii, "Secure Cloud Computing through Homomorphic Encryption", *International Journal of Advancements in Computing Technology*, Vol. 5, No. 16, pp. 1-12, 2013.

[9] Peddi Kishor and N. Divya, "Efficient Attribute based Signature Scheme for User Access Control in Database Environment", *International Journal of Advanced Research and Innovation*, Vol. 8, No. 1, pp. 123-128, 2015.

[10] Jiang Zhang, Zhenfeng Zhang and Hui Guo, "Towards Secure Data Distribution Systems in Mobile Cloud Computing", *IEEE Transactions on Mobile Computing*, Vol. 16, No. 11, pp. 3222-3235, 2017.

[11] Mengting Li, Joseph K. Liu, Xinyi Huang and Li Xu, "GO-ABE: Group-Oriented Attribute-Based Encryption", *Proceedings of 8th International Conference on Network and System Security*, pp. 260-270, 2014.

[12] M. Garg and R. Nath, "Cloudlets in Mobile Cloud Computing", *International Journal of Innovations and Advancement in Computer Science*, Vol. 7, No. 4, pp. 235-241, 2018.

[13] Payal Patel, Rajan Patel and Nimisha Patel, "Integrated ECC and Blowfish for Smartphone Security", *Proceedings of International Conference on Information Security and Privacy*, pp. 11-14, 2015.

[14] Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham and Sangoh Jeong, "Securing Elastic Applications on Mobile Devices for Cloud Computing", *Proceedings of International Workshop on Cloud* Computing, pp. 1-6, 2009.

[15] Merve Bayramustaa and V. Aslihan Nasirb,"A Fad or Future of IT?: A Comprehensive Literature Review on the Cloud Computing Research", *International Journal of Information Management*, Vol. 36, No. 4, pp. 635-644, 2016.

[16] S. Wang, K. Guo and Y. Zhang, "Traceable Ciphertext-Policy Attribute-Based Encryption Scheme with Attribute Level User Revocation for Cloud Storage", *PLOS ONE*, Vol. 13, No. 10, pp. 1-12, 2018.

[17] J.K. Liu, T.H. Yuen, P. Zhang and K. Liang, "Time-Based Direct Revocable Ciphertext-Policy Attribute-Based Encryption with Short Revocation List", *Proceedings of International Conference on Applied Cryptography and Network Security*, pp. 516-534, 2018.

[18] B. Faber, G. Michelet, N. Weidmann, R.R. Mukkamala and R. Vatrapu, "A Blockchain-based Personal Data and Identity Management System", *Proceedings of the 52nd Hawaii International Conference on System Sciences*, pp. 6855-6864, 2019.

[19] Jin Sun, Lili Ren and Xiaomin Yao, "Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage", *IEEE Access*, Vol. 7, pp. 66655-66667, 2019.

[20] Huiling Qian, Jiguo Li, Yichen Zhang and Jinguang Han, "Privacy-Preserving Personal Health Record using Multi-Authority Attribute-Based Encryption with Revocation", *International Journal of Information Security*, Vol. 14, No. 6, pp. 487-497, 2014.

[21] Baodong Qin, Robert H. Deng, Shengli Liu and Siqi Ma, "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption", *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 7, pp. 1384-1393, 2015.

[22] Yujiao Song, Hao Wang, Xiaochao Wei and Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud", *Security and Communication Networks*, Vol. 2019, pp. 1-9, 2019.

[23] Hao Wang, Zhihua Zheng, Lei Wu and Ping Li, "New Directly Revocable Attribute-based Encryption Scheme and its Application in Cloud Storage Environment", *Cluster Computing*, Vol. 20, No. 3, pp. 2385-2392, 2017.

[24] Cheng Guo, Ruhan Zhuang, Yingmo Jie, Yizhi Ren, Ting Wu and Kim-Kwang Raymond Choo, "Fine-Grained Database Field Search using Attribute-Based Encryption for

E-Healthcare Clouds", *Journal of Medical Systems*, Vol. 40, pp. 235-243, 2016.

[25] Xuanxia Yao, Zhi Chen and Ye Tian, "A Lightweight Attribute-based Encryption Scheme for the Internet of Things", *Future Generation Computer Systems*, Vol. 49, pp. 104-112, 2015.

[26] Umashankar. "A Review on Attribute Based Encryption (ABE) and ABE Types", *International Journal of Computer Science and Mobile Computing*, Vol. 5, No. 5, pp. 142-146, 2016.