ENHANCING CLOUD STORAGE SECURITY: EFFICIENT REVOCABLE MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION

[1]Mr. P. NAVEEN SUNDAR KUMAR , M.Tech,(Ph.D), Assistant Professor
[2]KALLA RAKSHAK, MCA Student
Department of Master of Computer application,
Rajeev Gandhi Memorial College of Engineering and Technology
Nandyal, 518501, Andhra Pradesh, India.

ABSTRACT

As is known, attribute-based encryption (ABE) is usually adopted for cloud storage, both for its achievement of fine-grained access control over data, and for its guarantee of data confidentiality. Nevertheless, single-authority attribute-based encryption (SA-ABE) has its obvious drawback in that only one attribute authority can assign the users' attributes, enabling the data to be shared only within the management domain of the attribute authority, while rendering multiple attribute authorities unable to share the data. On the other hand, multi-authority attribute-based encryption (MA ABE) has its advantages over SA-ABE. It can not only satisfy the need for the fine-grained access control and confidentiality of data, but also make the data shared among different multiple attribute authorities. However, existing
MA-ABE schemes are unsuitable for the devices with resources-constraint, because these schemes are all based on expensive bilinear pairing. Moreover, the major challenge of MA-ABE scheme is attribute revocation. So far, many solutions in this respect are not efficient enough. In this paper, on the basis of the elliptic curves cryptography, we propose an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage. The security analysis indicates that the proposed scheme satisfies indistinguishable under adaptive chosen plaintext attack assuming hardness of the decisional Diffie-Hellman problem. Compared with the other schemes, the proposed scheme gets its advantages in that it is more economical in computation and storage.

1. INTRODUCTION

CLOUD storage is an application pattern of cloud computing [1] to store massive data, so more and more individuals and organizations shift their data from local computers to cloud. However, this new paradigm poses a serious threat to the privacy of their owners, since the data might be accessed and analyzed by the cloud server providers for illegal or monetary purposes.

To solve this problem, people have figured out a variety of approaches. One common way is to resort to the traditional public key encryption technology to encrypt data, but the data owners fail to have fine-grained access to their data flexibly. Accordingly, Sahai and Waters [2] advanced

a new way of encryption, attribute-based encryption (ABE). It used to be considered one of the most promising technologies for cloud storage, since it ensures the data owners to enjoy non interactive and fine-grained control over encrypted data.

Since then, many single-authority attribute-based encryption (SA-ABE) schemes [2-9] have been put forward. In these schemes, it is required that only one trusted attribute authority administers the attributes and distributes the corresponding secret keys of attributes to the data consumers. This mechanism may not meet the practical requirements in cloud storage, when data consumers' attributes are distributed by multiple different attribute authorities. For example, when a data owner intends to share the data with a targeted data consumer holding the attribute "Professor" from a university and the attribute "Engineer" from a research institution, obviously SA-ABE scheme can not be applied to this scenario. To deal with this problem, many researchers [10-24] turn to multi-authority attribute-based encryption (MA-ABE), so that secret keys of attributes are issued to data consumers with the corresponding privileges for different attribute authorities respectively. There exists two kinds of multi authority ABE schemes, namely centralized multi-authority ABE and decentralized multi authority ABE, the difference between them is whether the key is distributed by center authority. When the key is distributed by central authority, we can consider it as centralized multi-authority ABE scheme [10]. When the key is distributed by attribute authority, we can consider it as decentralized multi-authority ABE scheme [2-9,11-23,25-26].

From the perspective of practical application, the following challenges should be solved before applying MA-ABE in cloud storage system. One of the major challenges is the highly computational overhead, since the existing MAABE schemes [10-23] are all based on the expensive bilinear pairing operations, hinders the further development of MA-ABE schemes on the resource constrained devices. The other challenge is the attribute revocable, since multiple data consumers may share the same attribute, and each data consumers may possess multiple different attributes, result in that revocation for anyone attribute may influence the other data consumers in the cloud storage system. Although re encrypting the data is a method [19] to solve this problem, it will generate high computation cost. Another technology [24] is to introduce a timestamp into every attribute, but it is not achieved immediate revocation. This paper involves the construction of an efficient RMAABE scheme for cloud storage. Our main contributes are as follows: _

First, based on the elliptic curve cryptography (ECC), an efficient RMA-ABE scheme is proposed for cloud storage, so that bilinear pairing operations will be no longer needed. In the proposed scheme, we use the linear secret sharing schemes (LSSS) to boost the expressiveness of access policy and add version key to attribute to realize immediate attribute revocation. _

Second, the security analysis indicates that under the decisional Diffie-

Hellman (DDH) assumption, the proposed RMA-ABE scheme achieves the in distinguish ability against the choose plaintext attack (IND-CPA), and satisfies collision resistant and forward secrecy.

Finally, the performance evaluation of the scheme indicates lower the computation cost and lower storage overhead than other schemes.

The rest of this paper is organized as follows. Section II introduces the related work. Preliminaries are given in Section III. The concrete RMA-ABE scheme is described in Section IV. In Sections V and VI, the security and performance analysis of the proposed scheme is shown, respectively. In Section VII, this paper is concluded.

2. LITERATURE SURVEY

The ABE scheme is introduced by Sahai and Waters [2]. With ABE, data owner can share his/her data encrypted with the targeted data consumers, with no knowledge of their public keys or identities, ensuring ABE schemes to achieve finegrain and flexible access control in cloud storage. The notion of key-policy attribute-based encryption (KP-ABE) was put forward by Goyal et al. [3], that the data consumers' secret keys are relevant to access structures, and the ciphertext is related to certain attributes. Then, Bethencourt et al. [4] introduced the concept of ciphertext-policy attribute-based encryption (CP-ABE), that data consumers' secret keys are relevant to some attributes, and ciphertexts are relevant to access structures. The CP-ABE scheme is more applicable to access control, since data owners can determine access structures. Thus many scholars pay attention to CP-ABE schemes [5-9]. In ABE schemes [2-9], there is only one attribute authority administering all attributes. However, problem arises as attributes are distributed by multiple attribute authorities, so Chase [10] proposed MA-ABE scheme. According to Chase's scheme several different attribute authorities issue attributes and secret keys of attributes to data consumers.

Nevertheless, the privacy of data owner is not been protected because the central authority can decrypt all the ciphertexts. Then, Chase and Chow [11] introduced the MA-ABE scheme without the trusted authority, but the data consumers need at least one attribute from every attribute authority, so this scheme is not practical enough. Lewko and Waters [12] devised a CP-ABE scheme with fully decentralized multiauthority, needing no cooperation among the attribute authorities, so from every attribute authority, data consumers can possess any number of attributes. The majority construction of the above MA-ABE [10-12] schemes involves bilinear pairing operations scaling with the attribute number, resulting in exorbitant computational overhead in both encryption and decryption phases. To lower the computation overhead at encryption phase, Zhang et al. [13] offered an MA-ABE scheme in mobile cloud by using the technique of offline/online encryption. According to this scheme, all major encryption computation can be shifted to the offline phase, so the data owners only perform a few online computations. To reduce the computation cost at decryption phase, data consumers can outsource the decryption computing to the third-party servers.

Yang et al. [14] presented a supporting decryption outsourcing multi-authority CP-ABE scheme, where data consumers do not need to perform any complex bilinear pairing operations in decryption phase. To guarantee the security of data, data consumers must be able to examine the correctness and completeness of the received ciphertext partially decrypted. Then, Li et al. [15] proposed a securely outsourcing MAABE scheme with checkability, without the need of a trusted central authority, and it can check the correctness and completeness of outsourcing decryption.

Xu et al. [16] put forward a decentralized ABE scheme for cloud computing. It can provide both online/offline encryption and outsourcing decryption, and its security is guaranteed in the random oracle model (ROM).

Belguith et al. [17] introduced the outsourcing MA-ABE scheme for cloud assisted IoT, in which users' privacy can be protected by hiding access policy. Sethi et al. [18] constructed the MA-ABE scheme, supporting both white-box traceability and policy updating, as well as outsourcing decryption over large attribute universe. Although the MA-ABE schemes [14-18] are effective by reducing encryption or decryption computational overhead, these schemes do not support attribute revocation. For MA-ABE systems, when data consumer's attributes are changed, the access permission for the data consumer also ought to be altered timely and effectively. Therefore, efficient attribute revocation is necessary for MA-ABE schemes.

3. EXISTING SYSTEM

The ABE scheme is introduced by Sahai andWaters [2].With ABE, data owner can share his/her data encrypted with the targeted data consumers, with no knowledge of their public keys or identities, ensuring ABE schemes to achieve finegrain and flexible access control in cloud storage. The notion of key-policy attribute-based encryption (KP-ABE) was put forward by Goyal et al. [3], that the data consumers' secret keys are relevant to access structures, and the ciphertext is related to certain attributes. Then, Bethencourt et al. [4] introduced the concept of ciphertext-policy attribute-based encryption (CP-ABE), that data consumers' secret keys are relevant to some attributes, and ciphertexts are relevant to access structures. The CP-ABE scheme is more applicable to access control, since data owners can determine access structures. Thus many scholars pay attention to CP-ABE schemes [5-9].

In ABE schemes [2-9], there is only one attribute authority administering all attributes. However, problem arises as attributes are distributed by multiple attribute authorities, so Chase [10] proposed MA-ABE scheme. According to Chase's scheme several different attribute authorities issue attributes and secret keys of attributes to data consumers. Nevertheless, the privacy of data owner is not been protected because the central authority can decrypt all the ciphertexts. Then, Chase and Chow [11] introduced the MA-ABE scheme without the trusted authority, but the data consumers need at least one attribute from every

attribute authority, so this scheme is not practical enough. Lewko and Waters [12] devised a CP-ABE scheme with fully decentralized multiauthority, needing no cooperation among the attribute authorities, so from every attribute authority, data consumers can possess any number of attributes.

The majority construction of the above MA-ABE [10-12] schemes involves bilinear pairing operations scaling with the attribute number, resulting in exorbitant computational overhead in both encryption and decryption phases. To lower the computation overhead at encryption phase, Zhang et al. [13] offered an MA-ABE scheme in mobile cloud by using the technique of offline/online encryption. According to this scheme, all major encryption computation can be shifted to the offline phase, so the data owners only perform a few online computations. To reduce the computation cost at decryption phase, data consumers can outsource the decryption computing to the third-party servers. Yang et al. [14] presented a supporting decryption outsourcing multi-authority CP-ABE scheme, where data consumers do not need to perform any complex blinear pairing operations in decryption phase.

Disadvantages

- The proposed system implemented MAABE schemes which are all based on the expensive bilinear pairing operations.
- There is no Data Integrity Proof on outsourced data.

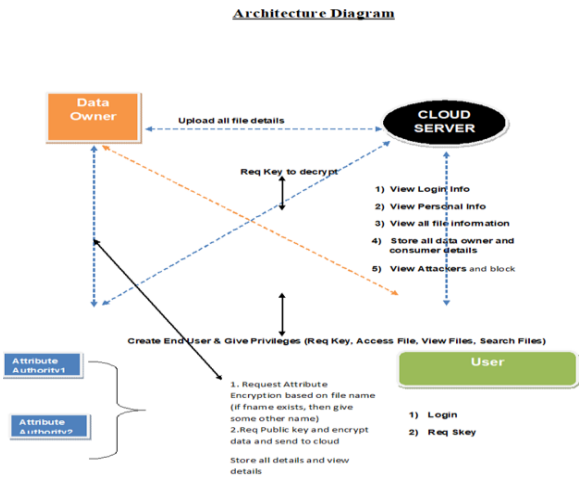
4. PROPOSED SYSTEM

This paper involves the construction of an efficient RMAABE scheme for cloud storage. Our main contributes are as follows:
First, based on the elliptic curve cryptography (ECC), an efficient RMA-ABE scheme is proposed for cloud storage, so that bilinear pairing operations will be no longer needed. In the proposed scheme, we use the linear secretsharing schemes (LSSS) to boost the expressiveness access policy and add version key to attribute to realize immediate attribute revocation.
Second, the security analysis indicates that under the decisional Diffie-Hellman (DDH) assumption, the proposed RMA-ABE scheme achieves the indistinguishability against the choose plaintext attack (IND-CPA), and satisfies collision resistant and forward secrecy.
_ Finally, the performance evaluation of the scheme indicates lower the computation cost and lower storage overhead than other schemes.

Advantages

- The proposed system is very effective due to presence of Attribute revocation which will give more security on cloud data for the data owners.
- The system is more effective due to presence of COLLISION RESISTANCE on outsource data of the cloud users.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

DATA OWNER

In this module, data owner register to the cloud server. To upload the file data owner has to login and then he will be having the permission to upload the file. Data owner selects the file and he get attributes key for that particular file. Attribute key consist of owner, file name, secret key, date, time, area and content. After getting the attribute key he will encrypt the file and upload to the cloud server.

ATTRIBUTE AUTHORITY

It consist of owner, file name, secret key, date, time, area and content called attribute keys, After getting the attribute key he will encrypt the file and upload to the cloud server.

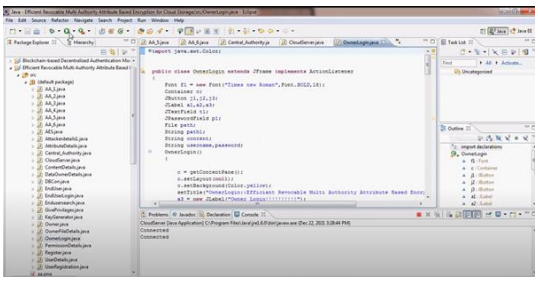
CLOUD SERVER

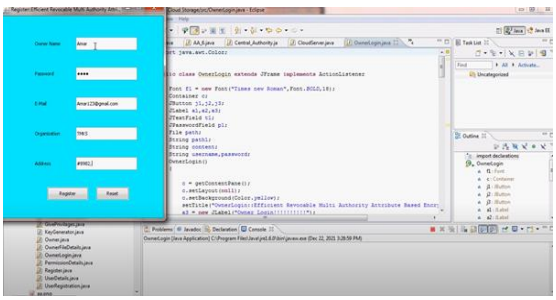
In this module when data owner upload file to the cloud server It matches with all the attribute key and for that particular file. Cloud server gives the access to data owner and data owner details will be stored in the cloud server, When data owner uploads the file, the details of the file will be stored in cloud server. Data consumers details will be stored in the cloud server when he wants to download the file, cloud server gives permission to the data consumer to access. If data consumer enters wrong secret key he will be sent to the attackers list and data consumer will be blocked.

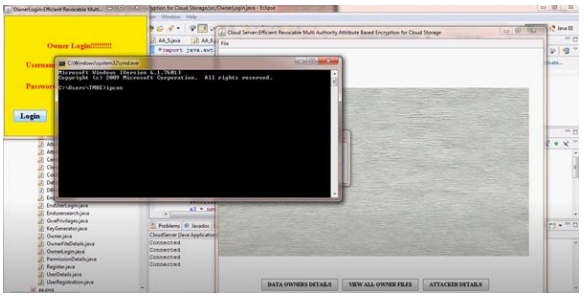
End User

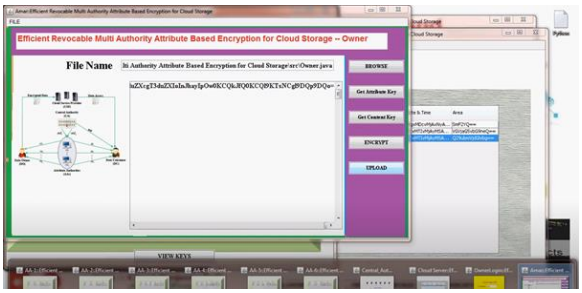
Data consumer gets register to cloud server and then login to the cloud server to download the file. Before downloading the file data consumer has to get the attribute key and then he has request to the cloud server to search the file. If file is present in the cloud server encrypted file will be decrypted and downloads the file..Data consumer trying to attack the file means he will be blocked in the cloud server and he wont be having to permission to download any other file in the cloud.

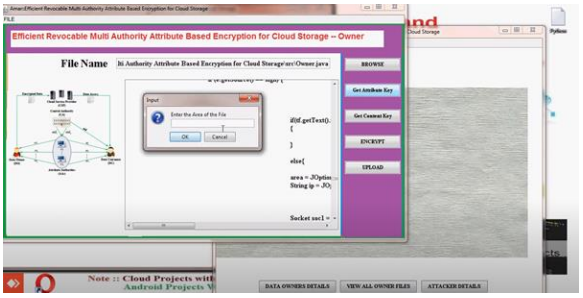
7. SCREEN SHOTS

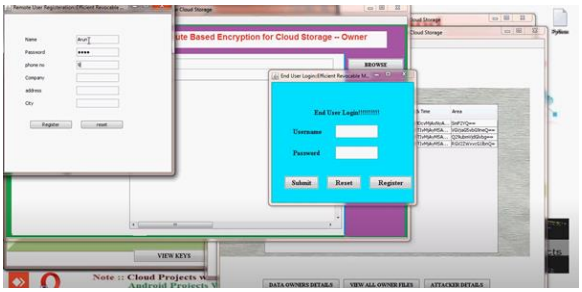


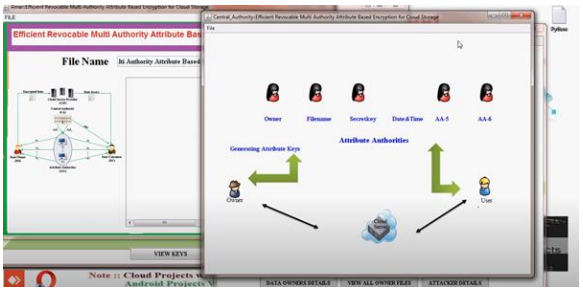


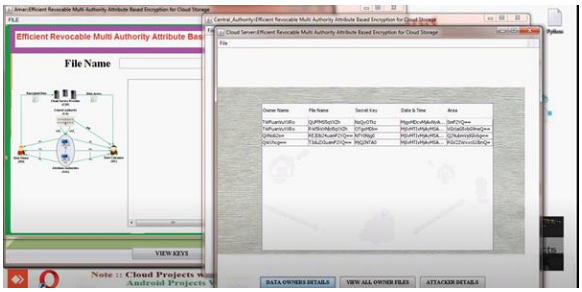

Owner Login!!!!!!!!
Login
DATA OWNERS DETAILS
VIEW ALL OWNER FILES
ATTACKER DETAILS

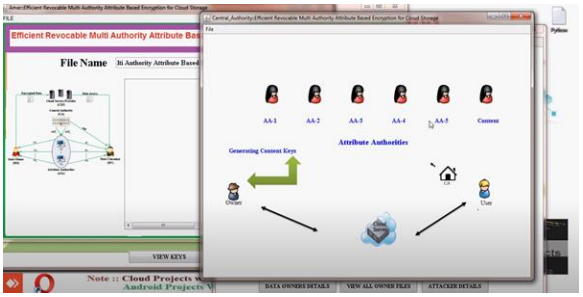

Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage -- Owner
File Name
BROWSE
Get Attribute Key
Get Content Key
ENCRYPT
UPLOAD
VIEW KEYS


Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage -- Owner
File Name
BROWSE
Get Attribute Key
Get Content Key
ENCRYPT
UPLOAD
DATA OWNERS DETAILS
VIEW ALL OWNER FILES
ATTACKER DETAILS

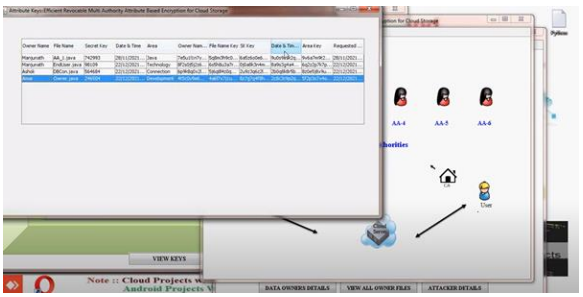

Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage -- Owner
End User Login!!!!!!!!
Username
Password
Submit
Reset
Register
VIEW KEYS

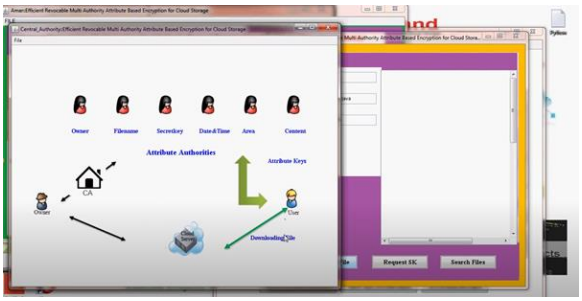

Efficient Revocable Multi Authority Attribute Based
File Name
Owner
Filename
Secretkey
Date&Time
AA-5
AA-6
Attribute Authorities
Generating Attribute Keys
VIEW KEYS

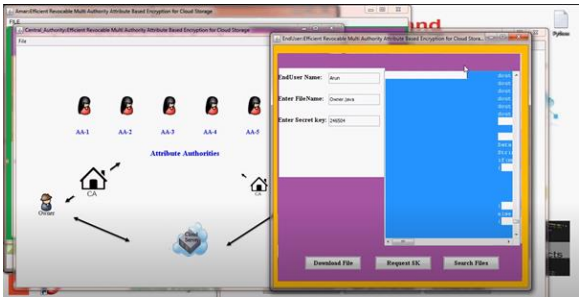

Efficient Revocable Multi Authority Attribute Bas
File Name
VIEW KEYS
DATA OWNERS DETAILS
VIEW ALL OWNER FILES
ATTACKER DETAILS

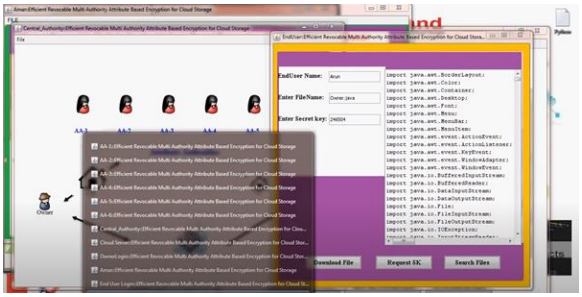

Efficient Revocable Multi Authority Attribute Bas
File Name
AA-1
AA-2
AA-3
AA-4
AA-5
Content
Attribute Authorities
Generating Content Keys
VIEW KEYS


Owner
Filename
Secretkey
Date&Time
Area
AA-6
Attribute Authorities
Attribute Keys
Requesting Keys
Request EK
Search Files


AA-4
AA-5
AA-6
VIEW KEYS







8. CONCLUSION AND FUTURE ENHANCEMENT

This project proposes an efficient RMA-ABE system for cloud storage, which is on the basis of the elliptic curve cryptography. The proposed scheme will not need any bilinear pairing operations any more. The version key is introduced into the attribute to achieve the attribute revocation. Security proof demonstrates that the proposed scheme enjoys the confidentiality. In addition, by using the unique identity uid tied to the secret keys of attributes, collusion resistant is realized. It is showed in the performance analysis that the proposed scheme is high-efficiency in storage as well as computation cost.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Computer Security, pp. 267-269, 2009.

[2] A. Sahai and B.Waters, "Fuzzy identity-based encryption," in Advances in Cryptology-EUROCRYPT. Berlin, Heidelberg: Springer, pp. 457-473, Jan. 2005.

[3] V. Goyal, O. Pandey, A. Sahai, and B Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM Conference on Computer and Communications Security, ACM, Alexandria, pp. 89-98, Jan. 2006.

[4] J. Bethencourt and A. Sahai, "Ciphertext-policy attribute-based encryption," in Proc. of IEEE Symposium on Security and Privacy, IEEE, California, pp. 321-334, 2007.

[5] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," IEEE T. Parall. Distr., vol. 22, no. 4, pp. 673-686, Apr. 2011.

[6] Z. Wan, J. Liu, and R. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE T. Inf. Foren. Sec., vol. 7, no. 2, pp. 743-754, Apr. 2012.

[7] K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE T. Parall. Distr., vol. 26, no. 12, pp. 3461-3470, Dec. 2015.

[8] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute based encryption with keyword search function for cloud storage," IEEE T. Ser. Comput., vol. 10, no. 5, pp. 715-725, Dec. 2017.
[9] J. Li, X. Lin, Y. Zhang, and J. Han, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," IEEE Syst. J., vol. 12, no. 2, pp. 1767-1777, Feb. 2018.
[10] M. Chase, "Multi-authority attribute based encryption," in Proc. of Theory of Cryptography Conference. Berlin, Heidelberg: Springer, pp. 515-534, Feb. 2007.
[11] M. Chase and S. Chow, "Improving privacy and security in multi-authorityattribute-based encryption," in Proc. of ACM Conference on Computer and Communications Security, ACM, NY, pp. 121-130, Jan. 2009.
[12] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology-EUROCRYPT. Berlin, Heidelberg: Springer, pp. 568-588, May 2011.
[13] Y. Zhang, D. Zheng, Q. Li, J. Li, and H. Li, "Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing," Security and Communication Networks, vol. 9, no. 16, pp. 3688-3702, Aug. 2016.
[14] K. Yang, X. Jia, and K Ren, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," IEEE T. Inf. Foren. Sec., vol. 8, no. 11, pp. 1790-1801, Nov. 2013.
[15] J. Li, X. Huang, X. Chen, and Y. Xiang, "Securely outsourcing attributebased encryption with check-ability," IEEE T. Inf. Foren. Sec., vol. 8, no. 8, pp. 1343-1354, Aug. 2014.