Online-offline multi-authority CPABE with decryption outsourcing

Suneetha Y[1]

Assistant Professor, Department of Computer Science and Engineering, Kuppam Engineering College.

Prakash K[2]

Assistant Professor, Department of Computer Science and Engineering, Kuppam Engineering College.

***Abstract*—**This In order to realize attribute-based data sharing in cloud computing, multi-authority attribute-based encryption MA-ABE is extremely attractive. However, most of the existing MA-ABE schemes cannot support a fully large attribute universe and are not suitable for resource-constrained mobile data owners in that the computation cost in secret key generation and encryption is extremely heavy. To tackle the earlier challenges, we propose an online/offline MA-ABE scheme, which realizes both the online/offline secret key generation and the online/offline encryption while supporting a fully large attribute universe. In the offline phase, one global-identity authority and multiple attribute authorities do the majority of the work to issue attribute secret keys before knowing users' global identity and attributes. The data owner can perform most of the encryption computation tasks before knowing the actual message and access structure. Furthermore, the online phase can rapidly assemble the final decryption key and cipher texts when related specifications become known. Particularly, global-identity authority and attribute authorities need not to cooperate in the whole process. Our online/offline MA-ABE scheme allows the access policies encoded in linear secret sharing schemes. The formal selective security proof and extensive performance analysis indicate that our scheme is very suitable for data sharing in mobile cloud computing.

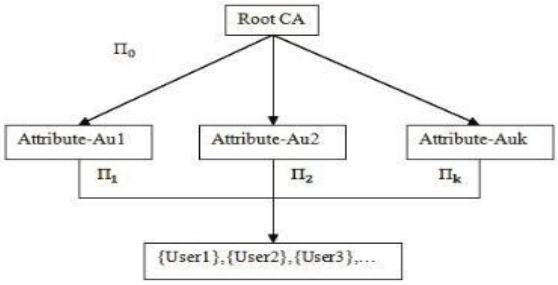
***Index Terms*—MA-ABE, Multi-authority key policy attribute based encryption, Multi-authority cipher text policy attribute based encryption, DABE**

I. INTRODUCTION

The data owner can perform most of the encryption computation tasks before knowing the actual message and access structure. Furthermore, the online phase can rapidly assemble the final decryption key and cipher texts when related specifications become known. Particularly, global-identity
This authority and attribute authorities need not to cooperate in the whole process. Our online/offline MA-ABE scheme allows the access policies encoded in linear secret sharing schemes. The formal selective security proof and extensive performance analysis indicate that our scheme is very suitable for data sharing in mobile cloud computing. All attributes of the system are managed by the single authority; Failure or corruption of the authority affects the whole system.

Chase [14] proposed a multi-authority attribute-based encryption system to overcome the drawbacks of a single authority attribute-based system. The proposed system uses a central authority (CA) and multiple attribute authorities (AAs). The problem with the Chase multi-authority attribute-based encryption system is attribute-based encryption scheme without the central authority. encryption scheme with one central authority and multiple attribute that the CA can decrypt every cipher text which reduces the user privacy and confidentiality of user data. Chase and Chow [15] proposed a multi-authority.

II. Figure 1: Multi-authority ABE system [26] Sascha Müller, Stefan Katzenbeisser, and Claudia Eckert[22,23] proposed a multi-authority ciphertext policy attribute-based encryption scheme with one central authority and multiple attribute authorities. The drawback of the scheme is that the central authority can decrypt any ciphertext in the system.
attribute-based encryption scheme without the central authority. encryption scheme with one central authority and multiple attribute that the CA can decrypt every cipher text which reduces the user privacy and confidentiality of user data. Chase and Chow [15] proposed a multi-authority.



Create _authority: The algorithm generates a private authority key SK_a.

Request_AttributePK: The algorithm generates the public attribute key of attribute A

Request_AttributeSK: The algorithm generates a secret attribute key $SK_{A,u}$ for user u.

Encrypt: The inputs of the *Encrypt* algorithm are public key, message, an access policy and the public keys associated with the attributes in the access policy. The output of the *Encrypt* algorithm is the cipher text

Decrypt: The inputs of the *Decrypt* algorithm are the cipher text produced by the Encrypt algorithm, an access policy and a key ring. Decryption is performed based on certain conditions and if the conditions are satisfied, the

Algorithm outputs the plaintext.
The advantage of the DABE scheme is that only two pairing operations are required in the decryption algorithm. Pairing operations are the most expensive operations in cryptography. The efficiency of the scheme can be improved by reducing the number of pairing operations. Only the decryption algorithm requires pairing operations. The pairing operations are not used anywhere else.

The major drawback of DABE scheme is that the overhead

Scalability, Security and Efficiency
The overhead of relying on a central authority is eliminated from the system. This ensures more scalability for the system. Without a central authority, the security and the efficiency of the system much more compares to other systems.

The authorities are working independently of each other. Therefore, the failure or malfunctioning of one authority will not affect the working of other authorities. This improves the robustness of the system.

Autonomous key generation and Collusion resistance
The system uses a hash function on the user's global identifier so that collusion resistance is ensured for multiple keys generated by different authorities.
The system uses the following five algorithms.

Global Setup: The global setup algorithm chooses a bilinear group G of order N. This N acts as a component of the global public parameter. The output of the algorithm is a description of a hash function.
Authority Setup: Each authority chooses

exponents for the attribute i. The output of the algorithm is a public key and a secret key.
Encrypt: The inputs of the *Encrypt* algorithm are a message, an access matrix, the global parameters and the public keys of the pertinent authorities. The output of the algorithm is the cipher text.
KeyGen: A key is created for the (identity, attribute) pair.

Decrypt: A hash function is applied

attribute i. The output of the decrypt algorithm is the message.

The advantage of the system is that the system provides collusion resistance; the system

robust and provides scalability.

III. COMPARISONS

The multi-authority cipher text policy attribute based encryption schemes [22,23,25] are more expressive than the multi-authority key policy attribute based encryption schemes[13,15]. However, the implementation complexity of multi-authority cipher text policy attribute based schemes are higher than the multi-authority key policy attribute based schemes.
Small Universe MA-ABE schemes: MA-ABE schemes use polynomial size attribute universe in the security parameter.
Large Universe MA-ABE schemes: MA-ABE schemes use exponential size attribute universe in the security parameter.
Unbounded MA-ABE schemes: These schemes are independent of the size of attribute universe.
Expressiveness of the MA-ABE schemes can be increased by the method of large universe construction and vice versa.
Efficiency of the MA-ABE schemes decreases considerably with the use of large universe construction and vice versa.
Large universe MA-ABE schemes can be constructed

IV.LITERATURE SURVEY

Multi-authority attribute based encryption schemes are either multi-authority key policy attribute based encryption schemes(MA-KPABE) or multi-authority cipher text policy attribute based encryption schemes.

A. Multi-authority Key Policy Attribute-Based Encryption

The notion of Multiple authority attribute based encryption scheme was first proposed by Chase[13]. The system uses the principles of trusted central authority (CA) and global identifiers (GID). The system also contains K attribute authorities. Each attribute authority is assigned a value dk. The system consists of the following five algorithms.
Setup: The algorithm generates a public key, secret key pair for each of the attribute authorities, and also outputs a

system public key and master secret key.
Attribute Key Generation: The algorithm generates a private key for the user.
Central Key Generation: The algorithm generates a central secret key for the user.
Encryption: The sender encrypts the message and outputs the cipher text.
Decryption: The user executes the decryption algorithm and decrypts the cipher text.
The scheme can provide collusion resistance against any number of colluding users. With this feature, multiauthority attribute based encryption as proposed by Chase[14] becomes one of the powerful attribute-based encryption schemes used in cloud computing.
However, each authority's attribute set must be disjoint. To overcome this problem, we can create a separate copy of each attribute for each clause.
The CA can decrypt every cipher text so that the user privacy and confidentiality of the data is less in this system.

CA-less multi-authority anonymous ABE:
Chase M. and Chow S.S.M. proposed a multi-authority attribute based scheme with user privacy [15].
Features
1. No trusted central authority
2. User privacy
3.Distributed pseudorandom functions are used in the system
4.Collusion resistance for any number of colluding users.

The scheme also defines an anonymous key issuing protocol. This protocol provides improved user privacy. Users are able to communicate with AAs via pseudonyms
• AAs are prevented from pooling their data.
The techniques from anonymous credentials are used that permits the users to get the decryption keys from the authorities.
The system uses the following four algorithms.
Setup: The authorities execute the setup algorithm by taking a security parameter and a public random string as inputs and generates an admissible bilinear group parameter. The authorities also generate a collision resistant hash function (CRHF).
Key Issuing: The key is generated for the user by executing the algorithm with each authority. The user invokes anonymous key issuing protocol. The authority issues secret key for each eligible attribute i for the user.
Encryption: The message is encrypted and the cipher text is produced.
Decryption: The input is the cipher text and the output is the message.
The advantages of the proposed system
- Trusted central authority is removed
- User privacy is protected

The disadvantage of the proposed system
- The system does not support a tree access structure

B. Multi-authority Cipher text Policy Attribute-Based Encryption (MA-CPABE) Systems
I) Distributed attribute based encryption (DABE)
The notion of multi-authority cipher text policy attribute based encryption was first proposed by Müller et al. [22,23]. The system is built up of a Central Authority (CA) and multiple attribute authorities (AAs).These attribute authorities separately maintain attributes. The major components of the scheme are master, attribute authorities and users. The duty of the master is to distribute private user keys. Attribute Authority certifies the user and distributes private attribute key to the user that can be used for decrypting the cipher text. User produces cipher text by the method of encryption technique. Whenever needed user decrypts the cipher text and retrieves the original message. A DABE scheme must be collusion resistant.
The following seven algorithms are defined in a DABE scheme.
Setup: The algorithm generates the public key of the system PK and the master key MK.
Create User: The outputs of the algorithm are a public user key PK_u and a secret user key SK_u.
Create Authority: The algorithm generates a private authority key SK_a.
Request_AttributePK: The algorithm generates the public attribute key of attribute A
Request_AttributeSK: The algorithm generates a secret attribute key $SK_{A,u}$ for user u.
Encrypt: The inputs of the *Encrypt* algorithm are public key, message, an access policy and the public keys associated with the attributes in the access policy. The output of the *Encrypt* algorithm is the cipher text.
Decrypt: The inputs of the *Decrypt* algorithm are the cipher text produced by the Encrypt algorithm, an access policy and a key ring. Decryption is performed based on certain conditions and if the conditions are satisfied, the algorithm outputs the plaintext.

The advantage of the DABE scheme is that only two pairing operations are required in the decryption algorithm. Pairing operations are the most expensive operations in cryptography. The efficiency of the scheme can be improved by reducing the number of pairing operations. Only the decryption algorithm requires pairing operations. The pairing operations are not used anywhere else.The major drawback of DABE scheme is that the overhead involved in managing the distributed authorities.

lI) Decentralized attribute based encryption
The notion of decentralized attribute-based encryption was proposed by Lewko and Waters [25]. The proposed system is a multi-authority attribute based encryption system.
Features
1. Any party can be appointed as an authority.

2. Global coordination of the authorities is required only for creating an initial set of common reference parameters.
3. To become an ABE authority, the party creates a public key and distributes private keys to users.
4. The encryption of the data is performed by the user with the help of a Boolean formula.
5. No central authority is required in the proposed system.

The Chase [14] concept of global identifiers is used in the system so that private keys issued to the same user by different authorities can be linked together.

Scalability, Security and Efficiency

The overhead of relying on a central authority is eliminated from the system. This ensures more scalability for the system. Without a central authority, the security and the efficiency of the system much more compares to other systems.

Robustness

The authorities are working independently of each other. Therefore, the failure or malfunctioning of one authority will not affect the working of other authorities. This improves the robustness of the system.

Autonomous key generation and Collusion resistance

The system uses a hash function on the user's global identifier so that collusion resistance is ensured for multiple keys generated by different authorities.

The system uses the following five algorithms.

Global Setup: The global setup algorithm chooses a bilinear group G of order N. This N acts as a component of the global public parameter. The output of the algorithm is a description of a hash function.

Authority Setup: Each authority chooses two random exponents for the attribute i. The output of the algorithm is a public key and a secret key.

Encrypt: The inputs of the *Encrypt* algorithm are a message, an access matrix, the global parameters and the public keys of the pertinent authorities. The output of the algorithm is the cipher text.

KeyGen: A key is created for the (identity, attribute) pair.

Decrypt: A hash function is applied on the identity for attribute i. The output of the decrypt algorithm is the message.

The advantage of the system is that the system provides collusion resistance; the system is more efficient, more robust and provides scalability.

V. CONCLUSION

In this paper, we review the features, advantages and disadvantages of different multi-authority attribute based encryption schemes. The ultimate goal of designing a MAABE scheme is to develope a secure, robust, expressive and efficient multi-authority attribute based encryption system. The field of MA-ABE scheme is a vast and everevolving one with its wings stretched to the areas of IoT and Social Networks.

ACKNOWLEDGMENT

Ancy George and Brighty Batley C. would like to express a wealth of gratitude to Dr. M. Newlin Rajkumar for his guidance during the project work.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data". In:
ACMCCS 2006, pp. 89-98 (2006).

[2] M. Abdalla, E. Kiltz, and G. Neven , "Generalized key delegation forhierarchical identity based encryption". In *Computer Security* ESORICS, pages 139-154, 2007.

[3] S. Al-Riyami, J. Malone-Lee, and N. Smart. "Escrow-free encryption supporting cryptographic workflow". In *Int. J. Inf. Sec.*, volume 5, pages217-229, 2006.

[4] W. Bagga, R. Molva, and S. Crosta. "Policy-based encryption schemes from bilinear pairings". In *ASIACCS*, page 368, 2006.

[5] J. Bethencourt, A. Sahai, and B. Waters. "Ciphertext-policy attributebased encryption In *IEEE Symposium on Security and Privacy*, pages321-334, 2007.

[6] D. Boneh and X. Boyen. "Efficient selective-id secure identity based encryption without random oracles". In *EUROCRYPT*, pages 223-

[7] D. Boneh and X. Boyen. "Secure identity based encryption without random oracles". In*CRYPTO*, pages 443-459, 2004.

[8] D. Boneh, X. Boyen, and E. Goh. "Hierarchical identity based random oracles". In*CRYPTO*, pages 443-459, 2004.

[9] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. "Public key encryption withkeyword search". In *EUROCRYPT*, pages 506-522, 2004.

[10] D. Boneh and M. Franklin. "Identity based encryption from the weil pairing". In *CRYPTO*,pages 213-229, 2001.

[11] D. Boneh, A. Sahai, and B. Waters. "Fully collusion resistant traitor tracing with shortciphertexts and private keys". In *EUROCRYPT*,

pages 573-592, 2006.
[12] R. Bradshaw, J. Holt, and K. Seamons. "Concealing complex
policies with hidden Credentials". In *ACM Conference on Computer and Communications Security*, pages146-157,2004.
[13] J. Camenisch and A. Lysyanskaya. "An efficient system for nontransferable
anonymous credentials with optional
anonymityrevocation", In: *EUROCRYPT*, 2001
[14] M. Chase. "Multi-authority attribute based encryption". In *TCC*,
pages 515-534, 2007.
[15] M. Chase and S. Chow. "Improving privacy and security in multiauthority
attribute- based encryption". In *ACM Conference on Computer and Communications Security*, pages 121-130, 2009.
[16] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters.
"Building efficient fully collusion resilient traitor tracing and revocation schemes". In *ACM Conference on Computer andCommunications Security*, pages 121-130, 2010.
[17] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext
policy attribute-based encryption. In *ICALP*, pages 579-591, 2008.
[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute Based
Encryption for Fine Grained Access Conrol of Encrypted Data". In
ACMconference on Computer and Communications Security, pages
89-98, 2006.
[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters.
"Fully secure functional encryption: Attribute-based encryption
and (hierarchical) inner product encryption". In