National Conference on Emerging Trends in Computing
March 2015, PP. 58 - 63

Attribute-Based-Encryption in Disruption Tolerant Military Networks to secure data access

[1]Sonia.M, [2]Hemakumar.V

Department of Computer Science & Engineering

GKM College of Engineering & Technology
G.K.M.Nagar, New Perungalathur (Near Tambaram), Chennai-600063, TamilNadu , India.
Contact no. : [1]09952051209, [2]09841411732
[1]imsonia1993@gmail.com
[2]hemu.be1989@gmail.com

***Abstract*—Wireless devices carried by soldiers in hostile areas or battle fields are likely to suffer the threats of information leaks and disruptions in connectivity. Disruption-tolerant network (DTN) technologies allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued by authority. The existing system says about key generation using multiple authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for DTNs where key generation is done by automated scheme. The admin(Sender of message) generates a random one-time-key for the user based on the attributes, which solves the problems of forward secrecy and backward secrecy. In addition it solves key escrow problem since central authority is not explicitly involved in key generation. We describe how to apply the proposed mechanism.**

***Keywords*-security, CP-ABE, Military Networks, Disruption Tolerant Network, One-time-key**

I. INTRODUCTION

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments [1]. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. Roy [2] and Chuah [3] introduced storage nodes in DTNs where data is stored such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced [4], [5]. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 2."

II. CURRENT METHODOLOGY

In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers) [2], [6]. Multiple authorities issue and manage their own attribute keys independently as a decentralized DTN. The challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities.

A. Issues

The concept of attribute-based encryption (ABE) [7]–[9] is a promising approach that fulfils the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext [8]. Thus, different users are allowed to decrypt different pieces of data per the security policy.

However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute-based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B. Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys.

B. Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the ciphertexts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes[2],[5],[10].

1) Attribute Revocation: Bethencourt *et al.* [8] and Boldyreva *et al.* [11] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes [6], [8], [11], [12] have two main problems.

The first problem is the security degradation in terms of the backward and forward secrecy [13]. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering these as attributes [2]. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time t_i, a ciphertext is encrypted with a policy that can be decrypted with a set of attributes a_i (embedded in the users keys) for users with a_i . After time , say t_j , a user newly holds the attribute set . Even if the new user should be disallowed to decrypt the ciphertext C for the time instance t_j , he can still decrypt the previous ciphertext C until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute a_i at time t_j , he can still decrypt the ciphertext of the previous time instance unless the key of the user is expired and the ciphertext is reencrypted with the newly updated key that the user cannot obtain. We call this uncontrolled period of time windows of vulnerability.

The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the non-revoked users can update their keys. This results in the "1-affects- " problem, which means that the update of a single attribute affects the whole non-revoked users who share the attribute . This could be a bottleneck for both the key authority and all non-revoked users.

The immediate key revocation can be done by revoking users using ABE that supports negative clauses [2], [9]. To do so, one just adds conjunctively the AND of negation of revoked

user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. This scheme will pose overhead O(R) group elements additively to the size of the ciphertext and O(log M) multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt *et al.* [8], where M is the maximum size of revoked attributes set . Golle *et al.* [14] also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the universe size.

2) Key Escrow: Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information [7], [8], [9], [15]–[17]. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Chase *et al.* presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. This results in $O(N_2)$ communication overhead on the system setup and the rekeying phases and requires each user to store $O(N_2)$ additional auxiliary key components besides the attributes keys, where N is the number of authorities in the system.

3) Decentralized ABE: Huang *et al.* and Roy *et al.* [2] proposed decentralized CP-ABE schemes in the multi authority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multi encrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let $A_1,\ldots,A_N$ be the key authorities, and $a_1,\ldots,a_N$ be attributes sets they independently manage, respectively. Then, the only access policy expressed with $a_1,\ldots,a_N$ is a_1 AND … AND a_N, which can be achieved by encrypting a message with a_1 by A_1 , and then encrypting the resulting ciphertext c_1 with a_2 by A_2 (where c_1 is the ciphertext encrypted under), and then encrypting resulting ciphertext c_1 with a_3 by A_3 , and so on, until this multi encryption generates the final ciphertext c_N . Thus, the access logic should be only AND, and they require N iterative encryption operations where N is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require O(N) computation and storage costs. Chase [18] and Lewko *et al.* [10] proposed multi authority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

III. NETWORK ARCHITECTURE

In this section, we describe the DTN architecture and define the security model.

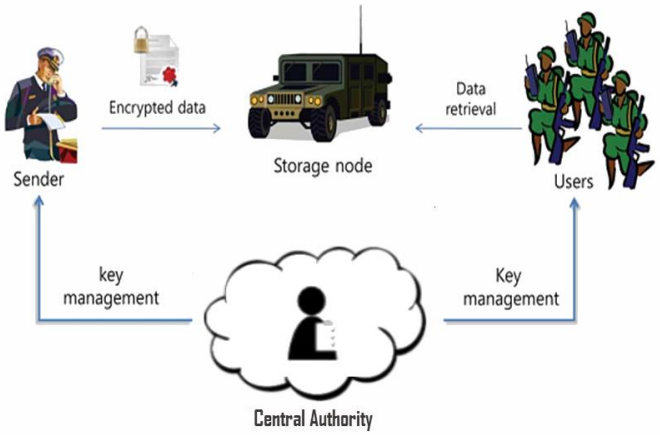

Fig 1: Architecture of secure data retrieval in a disruption-tolerant military network.

A. System Description and Assumptions

Fig. 1 shows the architecture of the DTN. As shown in Fig. 1, the architecture consists of the following system entities.

1) Central Authority(Key Authority): The role of central authority is to track the reliability of the key and message generated and reaching the users at the exact time.

2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [2], [3]. Similar to the previous schemes, we also assume the storage node to be semi-trusted, that is honest-but-curious.

3) Sender(Admin): This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node. The sender generates the one-time key for the particular user and passes it through the central authority.

4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a

set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users.

B. Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data into a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

1) What data should be given as input?
2) How the data should be arranged or coded?
3) The dialog to guide the operating personnel in providing input.
4) Methods for preparing input validations and steps to follow when error occur.

C. Contribution

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by restricting the functionality of central authority. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the Central Authority and the Sender. The role of the Central Authority is limited to passing the key generated by the admin to the corresponding users. The Central authority has to maintain the reliability in the system. The 2PC protocol deters the Central authority from obtaining any master secret information such that he could not determine the key generated for user. Thus, users are not required to fully trust the authority in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authority or data storage nodes in the proposed scheme.

D. Analysis

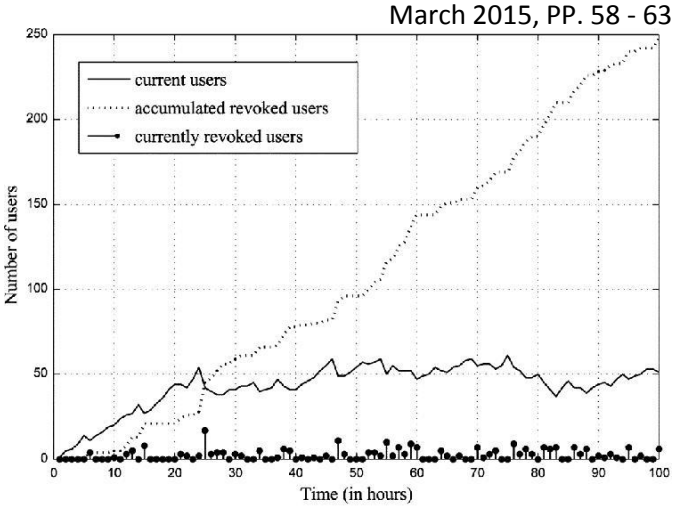

Fig. 2. Number of users in an attribute group.

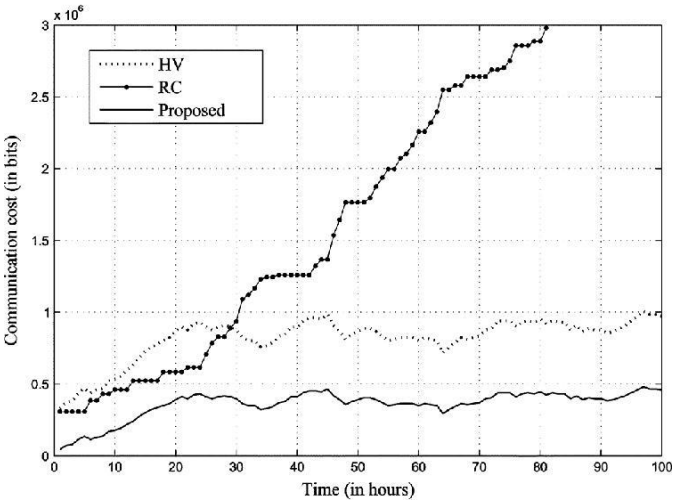

Fig. 3. Communication cost in the multi authority CP-ABE systems.

IV. PROPOSED SCHEME

An ciphertext-policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, KeyGen, and Decrypt.

i) *Setup(λ,U):* takes as input a security parameter and attribute universe description U. It outputs the public parameters PK and a master key MK.

ii) *Encrypt(PK,M,A):* The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

iii) *KeyGeneration(MK, S):* The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

iv) *Decrypt(PK,CT, SK):* The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

A. Mathematical Model

1) Encryption

i. Input: Attribute Value (Attr).

ii. Get Byte []($B1$) of that Attr.

iii. Generate Public Key(Pk).

iv. Perform Encryption on B1.

v. Convert B1 into string(EAttr).

2) Decryption

i. Input: Encrypted attribute value(EAttr)

i. Convert EAttr into byte []($B2$).

ii. Generate Private Key.

iii. Perform Decryption on B2.

iv. Convert B2 into string(DAttr).

V. SECURITY

In this section, we prove the security of our scheme with regard to the security requirements discussed in Section II.

A. Collusion Resistance

In CP-ABE, the secret sharing must be embedded into the ciphertext instead to the private keys of users. There are less chances of collusion between the keys generated for the soldiers with the same attributes or with different attributes since the algorithm deals with random generation. It is hard to find two inputs that hash to the same output; that is, two inputs a and b such that $H(a) = H(b)$, and $a \neq b$.

B. Data Confidentiality

Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented. Data confidentiality on the stored data against unauthorized users can be trivially guaranteed. If the set of attributes of a user cannot satisfy the access tree in the ciphertext, he cannot recover the desired value during the decryption process, where is a random value uniquely assigned to him. In order to decrypt a node for an attribute , the user needs to pair from the ciphertext and from its private key.

C. Backward and Forward Secrecy

In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

D. Reliability

Since the entire key generation process is governed by admin or sender of message , there are less chances of information leak. The central authority is responsible for rendering the key to the user on time.

VI. SUGGESTIONS

i) *Deal with Break-glass Access*- Sender may need to have temporary view at the data stored in Storage Node in case when the Sender System is hacked. The Sender may want to analyse the effects of the acts by intruder. Break-glass provides temporary access under emergency scenarios.

ii) *Serialization in storage node*- By the serialization, the size of the data becomes very small which reduces the overheads required in Storage Node.

iii) *Constant-sized keys*- Lightweight devices, such as radio frequency identification tags, have a limited storage capacity, which has become a bottleneck for many applications, especially for security applications. A novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes can be used with size as small as 672 bits.

VII. CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for centralized DTNs where central authority and sender manage the key generation using automated scheme that generates random one-time-key based on attributes. This solves the problem of forward secrecy and backward secrecy. It also solves Key Escrow problem since central authority is not explicitly involved in key generation. In addition, the system promotes reliability since the central authority keeps tracking

on when message was sent and received and also about key reaching the soldier in time. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised. In addition, the fine-grained key revocation can be done for each attribute group. This ABE(Attribute-Based-Encryption) method can be further used in other hostile networks and private concerns like Hospitals , Research Centre to preserve data.

ACKNOWLEDGEMENT

I express my sincere thanks to my project guide **Asst. Prof. V.Hemakumar** and **Head Of Department, Dr.S.Selvakumar** of Computer Science Engineering Department at GKM College of Engineering & Technology, for their valuable guidance, suggestion and support through the project work, who have given co-operation for the project with personal attention in spite of their busy schedule. I would like to thank ETIC-2015 team , Department of Computer Science and Engineering , S.A. Engineering College for providing me this opportunity.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc.IEEE INFOCOM*, 2006, pp. 1–11.

[2] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[3] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *Proc.Conf. File Storage Technol.*, 2003, pp. 29–42.

[5] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[6] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[9] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

[11] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[12] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.

[13] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Comput. Surv.*, vol. 35, no. 3, pp. 309–329, 2003.

[14] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in *Proc. Symp. Identity Trust Internet*, 2008, pp. 26–35.

[15] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[16] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

[17] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. ASIACCS*, 2009, pp. 343–352.

[18] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.