Cipher text policy Attribute Based Encryption for Secure Data Retrieval in DTNs

Vishwajeet I. Mete[1], Ms. Deepali B. Gothawal[2]

[1]*Department of Computer Engineering*
D.Y.Patil College of Engineering & Research Center
Akurdi, Pune, India
vishwajeet.mete@gmail.com
[2]*Department of Computer Engineering*
D.Y.Patil College of Engineering & Research Center
Akurdi, Pune, India
dgohil.1519@gmail.com

---***---

Abstract - *Mobile nodes connecting one device to another devices sometimes face some network connectivity problem in common environment. In military environment that is in battle field they should not suffer from network connectivity problem because of confidential data. Disruption- Tolerant Network (DTN) technologies are the solution to overcome network connectivity problems by using external storage nodes. Attribute-based encryption (ABE) gives the way for data delivery securely in Disruption Tolerant Networks. Thus concept of applying ABE in DTNs introduces security and privacy problems with regard to Attribute revocation, Key escrow, Coordination of attributes issued from different authorities. This scheme provides confidential data transformation using CP-ABE in decentrailzed Disruption Tolerant Networks(DTNs). CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. Ciphertext-policy Attribute based encryption (CP-ABE) uses the way of encrypting data that encryptor have to give detail about attribute set and decryptor have to possess such that to decrypt the ciphertext.*

Key Words*: Access control, attribute-based encryption (ABE), disruption-tolerant network, multiauthority, secure data retrieval*;

1. INTRODUCTION

Currently the military environment is a hostile and a turbulent one therefore applications running in this environment needs more security to protect their data, access control and their cryptographic methods. For communication to takes place securely, a node must be created and a connection must be established between the node and the neighbor nodes in this hostile networking environment, but if there is no connection between the source and the destination the message from the source node may have to wait until the connection will be eventually established. This refers to as a DTN architecture. where multiple key authorities issue and manage their own attribute keys independently.

In this paper, it describes a CP-ABE based encryption scheme that provides fine grained access control. In a CP ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes matches the access policy are able to decrypt. The concept of attribute-based encryption (ABE) is a promising approach that fulfills 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 cipher texts. Especially, cipher text-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 cipher text. 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. 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. 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 in critical region. In order to realize the goals of CP-ABE the key authority makes use of master's secret keys and private keys of which the users apply by requesting it from the key authority. When a user keyed in some attributes that matches or corresponds with the one in the access policy, it is updated to match with the group attributes which provides security for group members.

2. LITERATURE SURVEY

ABE comes in two types called key-policy ABE (KP-ABE) and Cipher text-policy ABE (CP-ABE). The concept of attribute-based encryption (ABE) [11]–[14] is a promising approach that fulfils the requirements for secure data retrieval in DTNs. ABE features that enables an access control over encrypted data using access policies and main IP parameters, like source IP address, source destination pair, hop count, next protocol field and combination of multiple attributes. A cryptographic technique that enables the tracing of attack source in provided in the intelligent router based hardened network which is proposed in [5]. A hop count based technique where received IP packet is plunged if huge difference exists between its hop count & the estimated values is proposed in [6]. P ascribed attributes among private keys and cipher texts. Especially, Cipher text-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 Cipher text [13]. In KPABE, the encryptor only gets to label a Cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the Cipher text 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 and useful 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 [5], [9], [15].

2.1 Attribute Revocation

Bethencourt *et al.* [13] and Boldyreva *et al.* [16] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions were 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 [13], [16], [17], [18] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy [19]. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g. position or location moves when considering these as attributes [5], [20]. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the new attribute or until the data is reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). 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). He called 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-m" problem, which means that the update of a single attribute affects the whole non revoked users who share the attribute [21]. This could be a bottleneck for both the key authority and all non revoked users.

2.2 Key Escrow

Most of the existing ABE schemes are constructed on the architecture where a single trusted key authority has the privilege to generate the whole private keys of users with its master secret information [11], [13], [14]. Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text 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.

2.3 Decentralized ABE.

A Junbeom Hur and Roy *et al.* [5] 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 "*n*-out-of-*m*" logics (e.g., OR, that is 1-out-of- m).

.

3. PROPOSED SYSTEM

In this paper proposed 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. Second, encryptors can define a fine-grained access policy using any access structure under attributes issued from any chosen set of authorities Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol prevents the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

3.1 CP-ABE Scheme FOR DTN

In KP-ABE, the encryptor only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key.

In CP-ABE the cipher text 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.

3.2 Advantages of proposed system

- **Data confidentiality:** Unauthorized users who do not have enough attributes or 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.
- **Collusion-resistance:** If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.
- **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.

4. PERFORMANCE ANALYSIS

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

4.1 Modeling

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

- **Key Authorities**: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.
- **Storage node:** This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semi trusted, that is honest-but-curious.
- **Sender:** This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the data storage node for easy 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.
- **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 cipher text and obtain the data.

4.2 Design

Fig. 1 shows the architecture of the DTN.

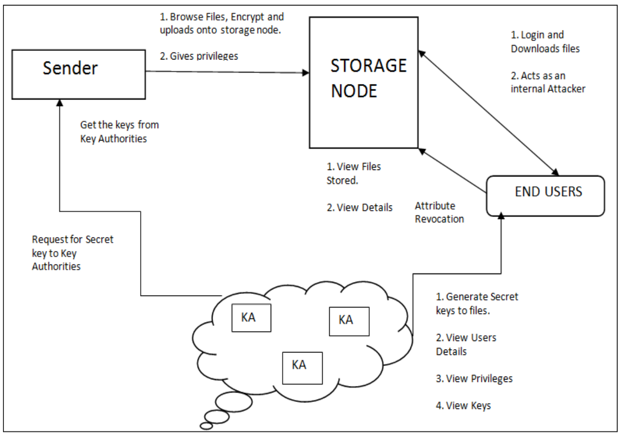
1. Browse Files, Encrypt and uploads onto storage node.
2. Gives privileges
Sender
STORAGE NODE
1. Login and Downloads files
2. Acts as an internal Attacker
Get the keys from Key Authorities
1. View Files Stored.
2. View Details
Attribute Revocation
END USERS
Request for Secret key to Key Authorities
KA
KA
KA
1. Generate Secret keys to files.
2. View Users Details
3. View Privileges
4. View Keys

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

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. In order to realize this somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, it takes an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

4.3 Results

The aim is to enhance the system performance and to send the message securely in the DTNs network. In Fig. 2 it shows the total communication cost that the sender or the storage node needs to send on a membership change in each multi authority CP-ABE scheme. It includes the ciphertext and rekeying messages for non revoked users. It is measured in bits. In this simulation, the total number of users are 20, and the number of attributes in the system is 2. The number of the key authorities is 5, and the average number of attributes associated with a user's key is 2. For a fair comparison with regard to the security perspective, It sets the rekeying periods in HV as $1/\lambda$ min. the communication cost in HV is less than RC in the beginning of the simulation time (until about 30 min). However, as the time elapses, it increases conspicuously because the number of revoked users increases accumulatively. The proposed scheme requires the least communication cost in the network system since the rekeying message in is comparatively less than the other multi authority schemes. It can seen that the total computation time to encrypt data by a sender in the proposed scheme is the same as BSW, while decryption time by a user requires exponentiations in G.

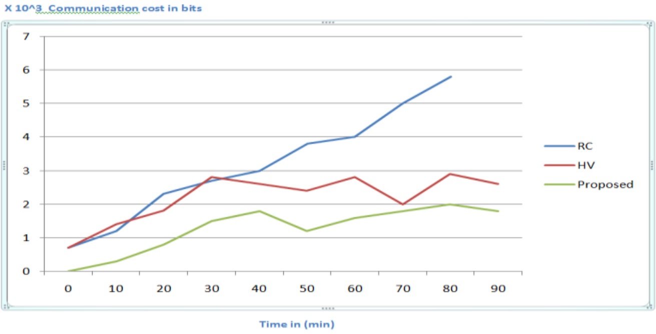

Fig 2 Communication cost Vs Time of revocation in mins

These exponentiation operations are to realize the fine-grained key revocation for each attribute group. Therefore, it can be observed that there is a tradeoff between computational overhead and granularity of access control, which is closely related to the windows of vulnerability. However, the computation cost for encryption by a sender and decryption by a user are more efficient compared to the other multi authority schemes.

Table 1 shows the authority architecture, logic expressiveness of access structure that can be defined under different disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme.

Table -1: Comparison based on Expressiveness, Key Escrow, and Revocation analysis.

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW	Single	--	Yes	Periodic attribute revocation
HV	Multiple	AND	Yes	Periodic attribute revocation
RC	Multiple	AND	Yes	Immediate system level user revocation
CP-ABE	Multiple	Any monotone access structure	NO	Immediate system level user revocation

In this scheme, the logic can be very expressive as in the single authority system like BSW [13] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be set to the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

5. CONCLUSION AND FUTURE SCOPE

DTN technologies are fast becoming popular and successful solutions in military applications that permit or enable wireless devices in the network to communicate with each other and access the confidential data in secure or in a trustworthy manner by utilizing the storage nodes. The ABE scheme provides access controls mechanism over an encrypted data with its policies and attributes over private and master keys, and cipher texts (CP-ABE). Scalability is provided by CP-ABE for data encryption and decryption. The approach used in this paper, is an efficient and effective way for securing data using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. In order to realize the goals of CP-ABE the key authority make use of mater secret and private keys of which the users apply by requesting it from the key authority .

As a future work, it can extend it to investigate the feasibility of incorporating value compare and predicates in policy tree in the future so that the sender can control the lifetime of attributes also it can be extends user validation for set of attribute in authentication of multi authority network environment.

REFERENCES

[1] "M. Chuah and others. Enhanced disruption and fault tolerant network architecture for bundle delivery (EDIFY). In Proceedings of IEEE Globecom, 2005".

[2] 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.

[3] Junbeom Hur and Kyungtae Kang, Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks, IEEE/ACM transactions on networking, vol. 22, no. 1, february 2014.

[4] M. M. B. Tariq, M. Ammar, and E. Zequra, “Mesage ferry route design for sparse ad hoc networks with mobile nodes,” in Proc. ACM MobiHoc, 2006, pp. 37–48.

[5] S. Roy and M. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

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

[7] 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.

[8] A. Harrinton and C. Jensen. Cryptographic access control in a distributed file system. In Proceedings of ACM SACMAT, 2003.

[9] 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.

[10] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” Cryptology ePrint Archive: Rep. 2010/351, 2010

[11] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Eurocrypt, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

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

[14] 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.

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

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

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attributebased systems,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.

[18] 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.

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

[20] D. Huang and M. Verma, “ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks,” Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

BIOGRAPHIES

Vishwajeet I. Mete pursuing Master's in Computer Engineering from DY Patil College of Engineering. His area of interest is Networking and Information Security.

Ms. Deepali Gothawal completed her Master's in Computer Engineering from DY Patil College of Engineering and have UG and PG teaching experience of 10 years. Guided 13 ME students and have 11 publications in conferences and journals of National and International repute. Her area of interest is Networking.