International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A SURVEY PAPER ON SECURE DATA RETRIEVAL FOR DECENTRALIZED DISRUPTION-TOLERANT MILITARY NETWORKS

C.VASUKI[1] , K.SABANA[2]

[1] *Assistant Professor Department of Information Technology*
Sri Adi Chunchanagiri Women's College, Cumbum.(India)
[2] *Research Scholar, Department of Computer Science,*
Sri Adi Chunchanagiri Women's College Cumbum.(India)

ABSTRACT

Frequent partitions and stopping network connectivity hampers the mobile nodes, e.g. in military areas. DTN's (Disruption Tolerance Networks) like technologies are found to be emerging as successful solutions for wireless devices which are carried by soldiers. Here by exploiting external storage nodes, these devices are used for communicating with each other and access the secret information. Limitationsare enforcement of policies authorization and policies update for safe data retrieval. To handle control issues CP-ABE (Ciphertext-Policy Attribute-based Encryption) is promising cryptographic solution. With the involvement of CP-ABE in decentralized DTNs privacy and security problem a rises. Attribute revocation, coordination of attributes issued by various authorities and key escrow. Review or survey is done on the data retrieval scheme using CP-ABE for decentralized DTNs.

Keywords: Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multi authority, secure data retrieval

I.INTRODUCTION

In many military network models, connections of wireless devices carried by soldiers. These connections may be disconnected by hampering some factors, jamming or mobility, particularly when it works in a hostile environment. Where the links in between intermediate nodes may be opportunistic, unsurprisingly connectable, or occasionally connected, there does not always exist an end-to-end path between a host and a destination spot. The research community has future architecture to allow nodes to communicate with each other in these extreme networks in environments, are known as DTNs (Disruption-Tolerant Networks). Several DTN techniques [2] [3] [5] have been projected. Typically, the source node's message may need to wait in the intermediate nodes for an extensive amount of time when there is no connection to the final destination. After the connection is ultimately established, the message is delivered to the destination node. Other regular users (mobile node) can access the necessary information quickly and efficiently because there are some storage nodes" that is also called as the

mobile node in the network where valuable data is stored or replicated. So that it is very necessary in many military applications to increase requirements, protecting confidential data. To protect and important the confidential data stored in the storage nodes or routed through the network some security-critical application is to design. In many cases, it is enviable to provide differentiated access services in a way that information/data approach policies are defined over user attributes or rules, which are managed by key authorities. For example, in a DTN (military), a commander can store secret information in the node, which should be accessed only by members of "Battalion 6" or a participant in Area3". In this case, this is area reasonable assumption that multiple or various key authorities are likely to manage their dynamic attributes (own Dynamic attributes) for soldiers in their deployed echelons (region), which could be frequently changed (e.g., attribute representing the current location of moving soldiers) [1] [3] [4]. Several current solutions follow the some traditional cryptographic-based approach, here contents before being stored are encrypted in storage nodes, and the decryption keys are distributed to the user (authorized user) We refer to this DTN architecture where multiple authorities issue and manage their attribute (own attributes) keys inside. Thus, to provide fine-grain access control, we need to design a scalable solution. In this paper, we describe a CP-ABE based encryption method that provides fine-grained access control. A CP-ABE scheme, each user is associated with a set of attributes. Attribute depends encryption an Encryptor will associate encrypted information with a set of attributes. An authority will issue users different private key. Where user's private key is associated with an access a structure over attributes. If the key authority is adjusted by adversaries when deployed in the enemy environments, it could be a potential risk (threat) to the information (Data) secrecy or privacy especially when the data is highly confidential. Even in the multiple-authority systems as long as each key authority has the whole privilege to generate their attribute keys with their own master confidence. Since such a key generation mechanism based on the single or particular master secret is the basic method for most of the asymmetric encryption systems such as the attribute-based encryption protocols, and also identity based encryption protocol, CP-ABE is a pivotal open problem of removing escrow in single or multiple-authority. The last challenge is the coordination of attributes issued by different authorities. It is very hard to define fine-grained access policies over attributes issued by different authorities as users get their own master secrets by various authorities since they manage and issue attribute keys to users independently. The different authorities generate their attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as 'n-out-of-m' logic, cannot be expressed in the previous schemes, which is a very implementable and generally required access policy logic.

II. LITERATURE SURVEY

It is necessary to decide the time factor, economy n company strength before developing the tool. After these things 'r' satisfied, then next steps is to decide which language and operating system can be used for developing the tool. In the above consideration 'r' taken into account for before developing proposed system. Attribute-

based encryption comes in two flavours following area: (I). Key-Policy ABE (KP-ABE). (II).CiphertextPolicy ABE (CP-ABE).

- KP-ABE (Key-policy ABE): In KP-ABE allows to the Encryptor simply gets to label a ciphertext with a set of attributes. The key authority selects a policy for each user that decides which cipher-texts he can decrypt and issues the key to each user by embedding the policy into the user's key.
- CP-ABE (Cipher-text policy Attribute-based encryption): In CP-ABC keys and ciphertexts are reversed. The Encryptor choose an access policy to encrypt the cipher-text, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE since it enables encryptors such as a commander to choose an access policy on attributes and to encrypt secret data under the access structure via encrypting with the corresponding public keys or attributes.

2.1 ATTRIBUTE REVOCATION:

Solutions proposed to distribute a new set of keys to valid users after the expiration and append to each attribute an expiration date (or time). Two main limitations with periodic attribute revocable ABE schemes. The security degradation problem in conditions of the backward and forward secrecy. The users such as soldiers may change their attributes frequently that scenario must considerable. Example attributes like position or location move are must consider. The other problem is scalability. All of the non-revoked users can update their keys when the key authority periodically announces a key renew material by unicast at each time-slot. This outcome in the '1_affects' issue. Wholly non-revoked users who distribute the attributes, are affected by this particular update on attribute. This could be a restricted access for both the key authority and all non-revoked users. The immediate key revocation can be done by recalling users using ABE that supports negative clauses. To do so,user identities recalled one just adds conjunctively the AND of negation. But this solution still is fairly lacking efficiency performance. This system will cause the overhead O(R) group elements1 additively to the size of the ciphertext and O (log M) multiplicatively to the size of private key over the original CP-ABE system of Bethencourtet al. [8], where is the highest size of revoked attributes set. Golle et al. [10] system only works when the number of attributes related to a ciphertext is exactly fifty percent of the universe size which a user revocable KP-ABE scheme.

2.2 KEY ESCROW:

Generally of the existing ABE schemes are constructed in the structural design where a single trusted authority has the authority to generate the whole private keys of users with its master secret information [11] [12] [2] [9]. Accordingly, the key escrow difficulty is ingrained such that the key authority has right to decrypt every ciphertext addressed to users in the system by generating their secret keys at any instance. A scattered KP-ABE scheme proposed solves the key escrow difficulty in a multi authority system. In this approach, all (put out of joint) attributes authorities are participating in the key generation protocol in scattered way such that they can't pull their data and link multiple attribute sets, belong to the same user. The performance degradation the

limitation of this fully distributed approach. Since there is no admin authority with master secret information, all attributes authorities need to communicate with each other in the system to generate a user's secret key.

2.3 DECENTRALIZED ABE:

Huang et al.[7] and Roy et al. [6] For decentralized CP-ABE schemes, multi - authority network environment is used. They achieved a gathered access policy over the attributes issued by different authorities by simply encrypting data several times. The limitation of these approaches is effective and self-expression of access policy. For example, when a commander encrypts a top secret mission to soldiers under the policy ('Battalion 2' AND ('Area 3' OR 'Area 4')), it cannot be expressed while each "Area" attribute is managed by different authorities, since simply multi encrypting approaches can by no means express any general" n-out-of-m " logics (1-out- of- m).

III. DISCUSSIONS

The concept of attribute-based encryption (ABE) 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. 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. 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.

3.1 DISADVANTAGES

The process of applying ABE technique involves several security and privacy challenges. In order to make the system secure key revocation is done in the system.

However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, he refer to such a collection of users as an attribute group)

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.

The last 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 finegrained access policies over attributes issued from different authorities.

CP-ABE (Ciphertext Policy Attribute-Based Encryption)

Multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bethencourt et al. [13], dozens of CPABE schemes have been proposed. The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model. A cipher text policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Key Generation, Encryption and Decryption.

3.1.1 Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

3.1.2 Key Generation (MK, S): The key generation algorithm takes as input the master key MK and a set of attributes So that describe the key. It outputs a private key SK.

3.1.3 Encrypt (PK, A, M): 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. Assume that the ciphertext implicitly contains

3.1.4 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.

IV.ADVANTAGES OF CP-ABE

4.1 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.

4.2 Collusion-resistance:

If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.

4.3 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.

V.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. 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. In CP-ABE, A ciphertext is associated with the access structure and the user secret key is associated with a set of attributes.

REFERENCES

[1] 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.*

[2] M. Chuah and others. Enhanced disruption and fault tolerant network architecture for bundle delivery (EDIFY). *In Proceedings of I IEEE Infocom, 2006*.

[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] 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.*

[5] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," *In Proc. ASIACCS, 2009.*

[6] J. Burgess and others. Maxprop: Routing for vehiclebased disruption tolerant networks. *In Proceedings of IEEE Globecom, 2005.*

[7] A. Lewko and B. Waters, "Decentralizing attribute-based encryption", *Cryptology Print Archive: Rep. 2010/351, 2010.*

[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] 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.*

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

[12] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption*," In Proc. ASIACCS, 2009.*