Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

CP-ABE Secure Data Retrieval

Salini K[1], Sruthy Manmadhan[2]
Dept of Computer Science & Engineering,
NSS College of Engineering, Palakkad ,Kerala

Abstract— Partitions in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity. Disruption-tolerant network DTN technologies are true and easy solutions. DTN is a Disruption-tolerant network. Thus a new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). The Attribute-based encryption scheme fulfills the requirements for secure data retrieval in DTNs. The concept is Cipher text Policy ABE), it gives an appropriate way of encryption of data. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. The encryption includes the attribute set that the decryption needs to possess in order to decrypt the cipher text. Hence, many users can be allowed to decrypt different parts of data according to the security policy.

Keywords— Military Networks, Encryption, Decryption, DTN, CP-ABE, Removing escrow, Distributed trust computation.

I. INTRODUCTION

The recent development of the Internet service models design is based on a few assumptions such as the end to-end path between a source and destination pair and low round-trip latency between any node pair. Attribute based encryption technique determines decryption`s capability on bases of uses attributes. This introduce us with the new public key primitive knows as Attribute based Encryption.ABE gives authority to user in such a way that encryptor to define set of attribute over a whole place of attribute that a decryptor should possess in order to decrypt the cipher text. One example is that battlefield ad hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections. In the above example, an end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic, predictably connectable, or periodically connected. If a user sends through the access request to the sharing, the sharing will return to the same cipher text data user a user to decrypt the data using private key. But this matter would lead to some problems they are, the data owner needs to obtain the data user's public key to complete this then a lot of storage overhead would spend because of the same plaintext with different public keys. In order to overcome these limitations Attribute based encryption came into existence.ABE first identify user`s properties. ABE has advantage over traditional public key cryptography, as it favors with one too many encryption instead of one to one.ABE as a set of attribute, is used to encryption and decryption of data.

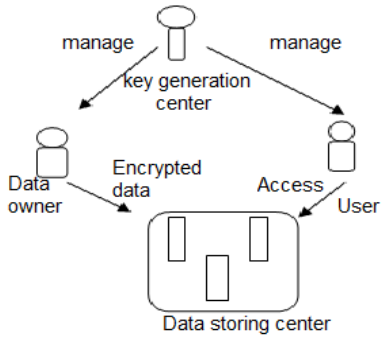

Fig 1: Architecture of Security Method.

Roy and Chuah [1] introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can

access the necessary information quickly and efficiently. The cipher text policy attribute-based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text, and enforce it on the contents.

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 [2]. Thus, different users are allowed to decrypt different pieces of data per the security policy.

This paper, describes about 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 match the access policy are able to decrypt. 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 (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.

II. RELATED WORKS

Since the introduction of ABE in implementing fine-grained access control systems, a lot of works have been proposed to design flexible ABE schemes. There are two methods to realize the fine-grained access control based on ABE: KP-ABE and CP-ABE. They were both mentioned in [3] by Goyal et al. In KP-ABE, each attribute private key is associated with an access structure that specifies which type of cipher texts the key is able to decrypt, and cipher text is labeled with sets of attributes. In a CP-ABE system, a user's key is associated with a set of attributes and an ecrypted cipher text will specify an access policy over attributes. The first KP-ABE construction [4] realized the monotonic access structures for key policies. Bethencourt et al. [2] proposed the first CP-ABE construction. The construction is only proved secure under the generic group model. To overcome this weakness, Cheung and Newport [4] presented another construction that is proved to be secure under the standard model. A store-and-forward approach has been already been implemented for delivering messages in disruption tolerant networks. Recently, several approaches have been proposed for unicast routing in disruption-prone networks.

Mobile Nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery scenarios. Disruption Tolerant Network (DTN) technologies are designed to enable nodes in such environments to communicate with one another. Several application scenarios require a security design that provides fine grain access control to contents stored in storage nodes within a DTN or to contents of the messages routed through the network. Here introducing a new scheme is described below.

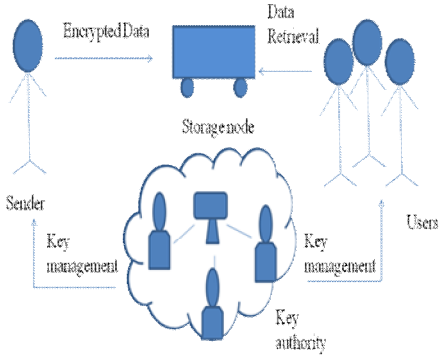

Fig 2: Syatem architecture

Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. Cipher

text-policy 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 de-crypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. 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 from different authorities. Proposing a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. Demonstrate that how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

A. Attribute-Based Encryption Scheme

Attribute-based encryption (ABE) offers this desired ability to encrypt without exact knowledge of the receiver set. It enforces access policies, defined on attributes, within the encryption procedure. This idea was first introduced by Sahai and Waters (SW) as an application of their fuzzy IBE scheme [3], where both cipher texts and secret keys are associated with sets of attributes. Decryption is enabled if and only if the cipher text and secret key attribute sets overlap by at least a fixed threshold value d. Two variants of ABE were subsequently proposed. In the key policy variant (KP-ABE) of Goyal, Pandey, Sahai and Waters (GPSW) [2], every cipher text is associated with a set of attributes, and every user secret key is associated with a threshold access structure on attributes. Decryption is enabled if and only if the cipher text attribute set satisfies the access structure on the user secret key. In the cipher text policy variant (CP-ABE) of Bethencourt, Sahai and Waters (BSW) [2], the situation is reversed: attributes are associated with user secret keys and access structures with cipher texts. Sahai and Waters proposed an attribute based encryption scheme in 2005. There are authority, data owner (also be called sender) and data user (also be called receiver) in this scheme, and authority's role is to generate keys for data owners and users to encrypt or decrypt data. In this scheme, the authority generates keys according to attributes; and these attributes of public key and master key, which are generated by the authority, should pre- define (means that it will list attributes which will be used in the future). If any data user who wants to add to this system, and he owns to attributes don't include pre- defined attributes. The authority will re-define attributes and generate a public key and master key again. And data owner's role in this scheme is to encrypt data with a public key and a set of descriptive attributes. A data user's role is to decrypt encrypted data with his private key sent from the authority, and then he can obtain the needed data. In an ABE system, a user's keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. The cryptosystem of Sahai and Waters allowed for decryption when at least *k* attributes overlapped between a ciphertext and a private key. While this primitive was shown to be useful for error-tolerant encryption with biometrics, the lack of expressibility seems to limit its applicability to larger systems.

The primary drawback of the Sahai-Waters [8] threshold ABE system is that the threshold semantics are not very expressive and therefore are limiting for designing more general systems. Goyal et al. introduced the idea of a more general key-policy attribute-based encryption system. In their construction a ciphertext is associated with a set of attributes and key can be associated with any monotonic tree access structure. The construction of Goyal et al. can be viewed as an extension of the Sahai-Waters techniques where instead of embedding a secret sharing scheme in the private key, the authority embeds a more general secret sharing scheme for monotonic access trees. Goyal et. al. also suggested the possibility of a ciphertext-policy ABE scheme, but did not offer any constructions. The key-policy attribute-based encryption (KP-ABE) was first introduced in 2006 by Goyal et al. [3] In this cryptography system, cipher text are labeled with sets of attributes. Private keys, on the other hand, are associated with access structures A. A private key can only decrypt a cipher text whose attributes set is authorized set of the private key's access structure. KP-ABE is a cryptography system built upon bilinear map and Linear Secret Sharing Schemes. In a multi-authority ABE system [5], consists of many attribute authorities, and many users. There are also a set of system wide public parameters available to everyone (either created by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the cipher text. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

B. CP-ABE Policy

In the CP-ABE scheme described in [1], each user is associated with a set of attributes and her private key is generated based on these attributes. When encrypting a message *M*, the encryptor specifies an access structure which is expressed in terms of a set of

selected attributes for *M*. The message is then encrypted based on the access structure such that only those whose attributes satisfy this access structure can decrypt the message. Unauthorized users are not able to decrypt the ciphertext even if they collude. In [1], the access structure is sent in plaintext. A CP-ABE scheme consists of the following four algorithms:

1) *Setup:* This is a randomized algorithm that takes a security parameter as input, and outputs the public parameters *PK* and a master key *MK*. *PK* is used for encryption and*MK* is used to generate user secret keys and is known only to the central authority.
2) *Encryption:* This is a randomized algorithm that takes as input a message *M*, an access structure *T*, and the public parameters *PK*. It outputs the ciphertext *CT*.
3) *KenGen:* This is a randomized algorithm that takes as input the set of a user (say *X*)'s attributes *SX*, the master key *MK* and outputs a secret key *SK* that identifies with *SX*.
4) *Decryption*: This algorithm takes as input the ciphertext *CT*, a secret key *SK* for an attribute set *SX*. If *SX* satisfies the access structure embedded in *CT*, it will return the original message *M*.

In Cipher text Approach Quality based Encryption plot, the encryptors can alter the arrangement, who can decode the scrambled message. The strategy could be structured with the assistance of characteristics. In CP-ABE, access arrangement is sent alongside the cipher text. Proposing a system in which the right to gain entrance approach require not be sent alongside the cipher text, by which the capacity safeguard the security of the encryptor. This methods encoded information might be kept classified regardless of the fact that the stockpiling server is un trusted; besides, the techniques are secure against intrigue assaults. Past Characteristic Based Encryption frameworks utilized credits to portray the encoded information and incorporated arrangements with client's keys; while in the framework ascribes are utilized to depict a client's qualifications, and a gathering encoding information decides an arrangement for who can unscramble. Cipher text-policy attribute-based encoding (CP-ABE) could be a promising cryptanalytic resolution to the access management problems. However, the matter of applying CP-ABE in suburbanized DTNs introduces many security and privacy challenges with relevance the attribute revocation, key escrow, and coordination of attributes issued from completely different authorities.

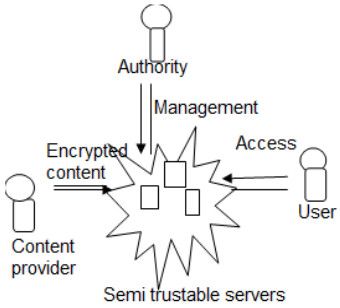

Fig 3: An example application scenario of sharing.

So one factor is a tendency to do all time is store the files on remote servers. There are varieties of reasons why do that tendency to do this. The tendency to might want to supply scalable access to that files to others victimization further resources on the market elsewhere. Have a tendency to might want a lot of dependability just in case of failures. During this case there is a tendency to might want to duplicate that files totally different information centers or with different organizations. However that would like security. Having a tendency to could have needs on World Health Organization will access that files. The fascinating factor is, there's a tension between security and therefore the alternative properties. The lot of tendency to replicate the files, and also having a tendency to introduce potential points of compromise and therefore the lot of trust having a tendency to need. It's this tension that makes this type of drawback fascinating, and provides a context within which CP-ABE is also helpful.

III. PROPOSED SYSTEM

In this paper, proposing 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 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 deters 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.

Advantages are: 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. 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.

Efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. 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 or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group.

A. Data Storage Soldier Trust Evaluation

Trust computations consist of three components: ‘experience’, ‘recommendation’ and ‘knowledge’. The ‘experience’ component of trust for each node is directly measured by their immediate neighbors and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as ‘recommendation’ part of the trust. At a regular interval, the previously evaluated trust is included in the current ‘knowledge’ component of total trust. Now either these three components individually or a combination of them can be used in computing the trust.

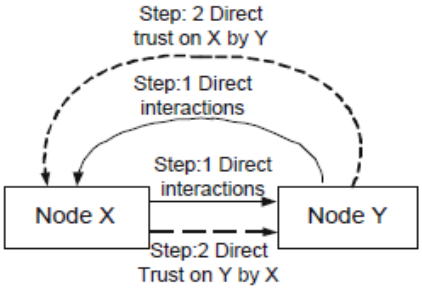

Fig 4: Trust Computation

B. Neighbour sensing (Direct Trust)

Distributed trust computation based on neighbour soldier sensing is illustrated in Fig. 3, where every soldier observes neighbour soldiers for their event reports and stores the reports in ‘knowledge’ cache. A trustor soldier (trust measuring soldier) will compare its own observation report on event with the observation report it received from the storage node (storage node whose trust need to be measured) and also from other close by neighbor soldiers. Trust factor will be determined based on amount of deviations between the observation reports.

IV. CONCLUSIONS AND FUTURE WORK

The project is not the unique one, but is an endeavour attempt to have a precise scenario of what the terms “secure data retrieval for decentralized disruption tolerant network” is meant to be and its implementation as well on currently working. As stated before, the proposed system can enhance the security of military network by using CP-ABE mechanism. CP-ABE is a scalable cryptographic

solution to the access control and secures data retrieval issues. In this paper, proposing an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. 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 or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. Demonstrate that how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network. 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 or not fully trusted. In addition, the finegrained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

V. ACKNOWLEDGEMENT

The authors would like to thank professors of NSSCE, Palakkad for suggestions and support on this paper.

REFERENCES

[1] 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.
[2] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
[3] 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.
[4] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
[5] M. Chase and S. S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in CCS ’09, 2009, pp. 121–130.
[6] 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.
[7] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in Proc. IEEE MILCOM, 2006, pp.1–6.
[8] 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.
[9] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.
[10] 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.