The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 5 || Pages || PP.01-05 || 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Secure and efficient management of confidential data in the decentralized disruption-tolerant militery networks

[1,] Seema S Balappanavar, [2,] Prof. Arati Shahapurkar
[1, 2,] *Department of Computer Science and engg, GIT Belgaum*

ABSTRACT

Mobile Nodes in some difficult areas subjected to intermittent network property and frequent partitions for e.g. battlefield. Disruption Tolerant Network (DTN) technologies are designed to specific situations wherever it will tolerate noise, attacks etc which means that nodes will get confidential information with none loss. Many application situations need a security for data that has secure access to information hold on in storage nodes at intervals a DTN or to contents of the messages routed through the network. Here, we have a tendency to use a way that allows secure access of data that is referred to as Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach. There are many problems during this state of affairs. Some of those are control of policies needed for correct authentication of user and therefore the policies to retrieve the information. Therefore we have a tendency to use a promising solution i.e. Ciphertext-policy attribute-based encoding (CP-ABE) to resolve the problem of accessing information. But, by applying CP-ABE in decentralized DTNs results into many security and privacy challenges with reference to the attribute revocation, key escrow, and coordination of attributes issued from multiple authorities. Here, we have a tendency to propose a secure and efficient management of data within the decentralized Disruption Tolerant Network (DTN) wherever multiple key authorities severally manage their attributes.

KEYWORDS *- Access Control, Attribute-Based Encryption (ABE), Disruption Tolerant Network (DTN), Multiauthority System, Secure Data Retrieval*

Date of Submission: 11-May-2015 Date of Accepted: 30-May-2015

I. INTRODUCTION

The design of the current Internet service models is based on a few assumptions such as (a) an end-to-end path that exists between a source and destination, and (b) delay between any node pair. Anyway, these assumptions do not hold in some networks. Some examples are: (i) in battlefield networks where soldiers carry wireless devices those operate in hostile environments where network jamming, environmental conditions and mobility of node may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are used with wireless modems and have intermittent connectivity with one another. In the above scenarios, there may not exist an end-to-end path between a source and a destination pair always. Inorder to communicate the nodes with each other in such networking environments, the research community has introduced a new architecture called the disruption tolerant network (DTN) recently. Several DTN routing approaches have been proposed. Sometimes, the message sent by the source node may need to queued in the intermediate nodes for some amount of time, when connection to the intended destination has not been established. After the connection is established, the message is delivered to the destination node.

Later, storage nodes are introduced in DTNs, where data is stored and will be replicated such that only authorized users (or mobile nodes) can access the necessary information securely and quickly. Many military applications require high level protection of confidential data including methods to access data that are cryptographically enforced. In several scenarios, it is required to provide services to access data such that the policies are defined over user attributes or roles to access data by authentic users and the attributes are managed by the key authorities. For example, in a disruption-tolerant military network, a major (or commander) may store confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 1." In this case, it is to be assumed that multiple key authorities are going to manage their own attributes for soldiers who are participating in their regions. We call this type of architecture as DTN (disruption tolerant network) architecture(i.e..,[1]), where multiple authorities are involved and generate their attribute keys by interacting with central authority which is referred as decentralized DTN(disruption tolerant network)

The method attribute-based encryption (ABE)(i.e..,[2]) is an approach that is appropriate for secure retrieval of data in DTNs(i.e..,[3]-[7]). ABE provides a mechanism where encryption is done based on attributes provided by users and defines policies over encrypted data. In ciphertext-policy ABE (CP-ABE) approach, it provides an encryption approach such that some attribute sets are defined by encryptor and the decryptor needs to possess those in order to decrypt the ciphertext. Thus, different users are allowed to decrypt data after satisfying the policies that are defined by data owner (or encryptor).

However, by applying the ABE (i.e..[8])to DTNs introduces several security and privacy challenges(i.e.[10]-[12]). First challenge is attribute revocation. some users may change their associated attributes at some point, or some private keys might be compromised by key authorities, since each attribute is shared by multiple users. This implies that any changes that made to attribute set by a single user affect the other users in the group.

Another challenge is the key escrow [i.e..,6] problem. In CP-ABE, the multiple key authorities make use of master keys and generate private keys of users. Thus, the key authority can generate the attribute keys of users and can decrypt every ciphertext belonging to specific users (i.e..[9]).

II. PROBLEM FORMULATION

To improve the security for decentralized disruption tolerant military networks, Ciphertext-policy Attribute-based Encryption (CP-ABE) algorithm can be used. CP-ABE is a promising cryptographic solution that solves the problem of accessing data. 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. To achieve data confidentiality, collusion resistance we use CP-ABE algorithm.

III. LITERATURE SURVEY.

S.Roy and M.chuah proposed CP-ABE system for DTNs. They used two types of encryption techniques along with CP-ABE. In the first technique, the data will be encrypted using symmetric key encryption. Then the result will be subjected to CP-ABE encryption .In the second technique, the data will be encrypted using a key encryption key (KEK) and then KEK will be encrypted using CP-ABE. They also extended CP-ABE method to support static and dynamic attributes [1].

D. Huang and M. Verma, proposed a scheme in the multi authority network environment known as decentralized Ciphertext-policy Attribute-based Encryption (CP-ABE). They achieved a combined access policy by encrypting the data multiple times over the attributes issued from multiple authorities [2].

A. Lewko and B. Waters proposed multi-authority attribute based encryption method. This method consists of multiple authorities that they manages different attributes of user. They do not require the central authority [3].

J. Bethencourt, A. Sahai, and B. Waters proposed a secure data access control method called as Ciphertext-policy attribute based encryption. In previous techniques like in case of Attribute based encryption method the policies are defined with secret keys of users and the data will be stored in the storage nodes are highly insecured.But here, after encrypting data, the data owner will define some policies over encrypted data and it will be stored in the storage node. Inorder to get encrypted data which is stored in the storage node, the decryptor needs to satisfy the policies [4].

A. Boldyreva, V. Goyal, and V. Kumar proposed a method that is an alternative to the public key encryption method called as Identity based encryption technique. Here the encryption will be done based on the identity of users by using trusted authority. The main advantage of this technique is the users do not need to have public keys and is secure technique [5].

Chase and S. M. Chow presented a distributed key-policy Attribute-based Encryption (KP-ABE) scheme that solves the key escrow problem in a multi authority system. In this scheme, multiple authorities are participating to generate attribute keys using the key generation protocol in a distributed way such that they cannot collect their data and get attribute sets that are belonging to the same user [6].

Chase proposed multi authority key-policy Attribute-based Encryption (KP-ABE).Here multiple authorities involved in generating the private keys of users and user uses key-policy technique where policies are defined over the private keys of user for enforcement of encrypted data and hence this method provides reliable access of data to data users [7].

IV. WORKING PROCESS OF THE SYSTEM

Our system uses CP-ABE (Ciphertext policy-attribute based encryption) in decentralized disruption tolerant networks (DTNs).The system architecture is shown below.

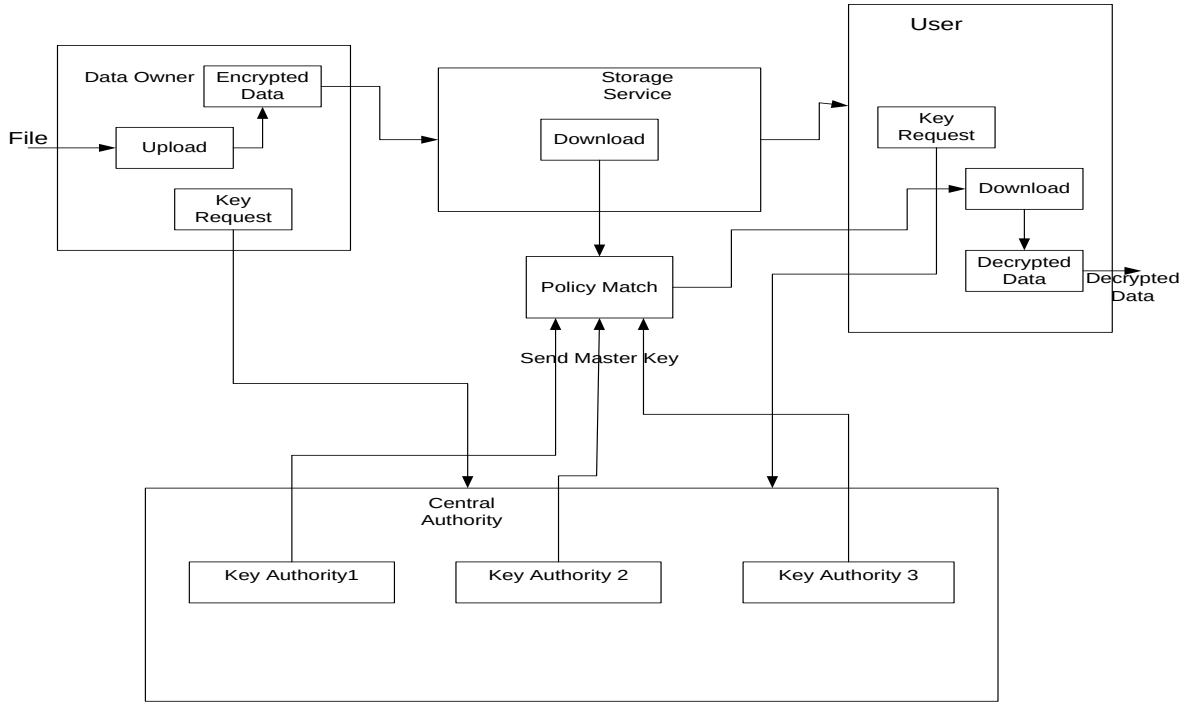


Fig4.1. Block diagram

In above Fig4.1, the System architecture consists of four components. They are

1) Sender
2) Key authorities
3) Storage node
4) Users

1) **Sender**: sender requests key to key authority required to encrypt the confidential message.

2) **Key authorities**: There are two types of authorities.

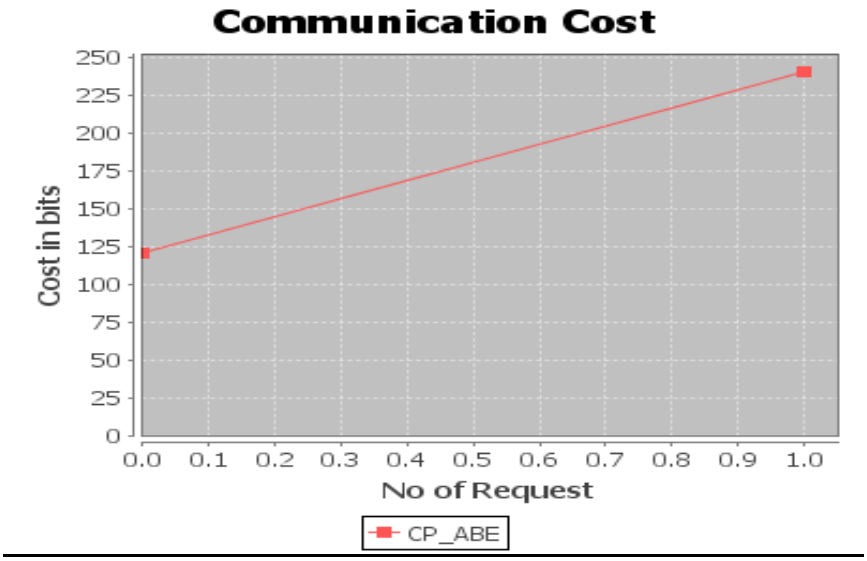
a) **Central authority**: This authority manages all local authorities and in which 2pc protocol has been used.

b) **Local authority**: multiple local authorities generate key based on set of attributes provided by sender using key generation protocol called as 2PC protocol.

3) **Storage node**: sender will encrypt message using key and will be stored it into storage node provided with access policies.

4) **Users**: After satisfying policies, Users retrieve encrypted data and request key from key authority and decrypt the data using key.

V. INTERPRETATION OF RESULT



Here, the graph is drawn No of request vs cost and the cost is measured in bits. Here, X-axis contains No_of_request and Y-axis contains Cost in bits. From the graph it is observed that the cost is going to be increased as number of user requests increased which is very low.

VI. SECURITY

Our system provides security in terms of following

1) Collusion resistance:

Our system provides protection against two types of collusions. one is collusion against multiple local key authorities. When local key authorities collude among themselves they can get a key required to decrypt the ciphertext. Hence our system consists of central key authority that manages all the local key authorities and hence provide collusion protection among users. another is collusion against users. if multiple users collude they can get ciphertext without requiring key. hence our system provide protection against collusion among users also.

2) Data confidentiality:

In our system data confidentiality can be achieved by providing external storage nodes.

V.CONCLUSION AND FUTURE SCOPE

Disruption Tolerant Network (DTN) technologies are designed to specific applications such as military applications where soldiers use wireless devices to communicate with one another and access the confidential information reliably by using external storage nodes. We use a cryptographic solution i.e. Ciphertext-policy attribute-based encryption (CP-ABE) to solve the problem of accessing data i.e. data owner (encryptor) defines policies and decryptor needs to satisfy the policies to get ciphertext from storage node. In this paper, we proposed an efficient and secure management of data using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. Here we solved key escrow problem such that the confidentiality of the stored data is not violated even under the extreme situations such as key authorities might be compromised. In addition, key revocation problem can be done for each attribute group. The future scope of proposed system can be extended to block unauthorized users and it can also be extended to encrypt and decrypt videos and other forms of data.

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] 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

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

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

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

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.

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

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

[9] 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.

[10] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-basedencryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.

[11] 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.

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