Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

CP-ABE in Decentralized Disruption-Tolerant Military Networks for Secure Retrieval of Data

Sneha
M.Tech Student
Computer Network Engineering
Srinivas Institute of Technology,
Mangaluru, India

H. Harshavardhan
Associate Professor
Department of Computer Science
Srinivas Institute of Technology,
Mangalusru, India

Abstract— **In this rapidly growing world, communication involves transfer of confidential information across the globe within a short amount of time. This kind of technical communication involves network of communicating devices. These devices will be carrying the confidential data across the devices which may be far apart. In military environment, communication disruption can occur because of intermittent network connectivity. Solution found for these kinds of disruption is the Disruption Tolerant Network (DTN) technology. This technology allows the soldiers to reliably access the data by using the capacity of the external storage nodes. Most challenging issue found in this DTN technology is enforcement of authorization policies and update of policies for the retrieval of confidential data. CP-ABE is one such cryptographic method which provides the solution to the access control issues. But there exists several problems with regard to key escrow, attribute revocation and coordination of attributes which are issued by different key authorities when applying CP-ABE in decentralized DTNs. In this paper, more secured method for the retrieval of confidential data using CP-ABE for decentralized DTNs is proposed where sets of attributes will be generated and managed by multiple authorities independently and addresses several existing problem**

Keywords— Disruption Tolerant Network (DTN), Attribute Based Encryption (ABE), Ciphertext-Policy Attribute Based Encryption (CP-ABE), Key escrow, Attribute Revocation, Access control, Secure data retrieval.

I. INTRODUCTION

Communication is a way of transferring information between the peoples who are present across the globe. In technical concept, communication is done by means of either wired or wireless devices. Military environment is one such area where soldiers will be mainly depending on wireless mobile devices for communication. Connection between these wireless devices sometimes may or may not get connected because of environmental issues or the mobility. In such cases communication between soldiers doesn't occur.

Disruption Tolerant Network (DTN) is one technology where it makes possible of communication when there is no end-to-end connection between wireless devices. Here in DTN technology the message from source to destination will be stored in one intermediate node when there is destruction in the path between source and destination.

Many routing algorithms are present in order to route the data from source to destination. Data in military application are confidential ones. These data's must only be accessed by authorized groups of user and unauthorized users must be denied from access. So some form of security must be given to these confidential data.

Methods based on cryptographic are introduced which provided more protection to confidential data's. These methods will be having different access policies for different users. So that only those users with correct access policies can access the particular data. Hence these methods will be providing secured retrieval of data. Recently Ciphertext Policy Attributed Based Encryption in decentralized DTNs has been introduced. But this scheme faced many security related problems like Key escrow, Attribute revocation and Coordination of attributes issued from different authorities.

To solve the aforementioned problem a proper method has to be introduced which will be capable of generating and managing the attribute from multiple key authorities individually. Here an Multi-authority CP-ABE scheme has been proposed where local authorities will be issuing attributes for the user by performing secure 2PC protocol with central authority. Hence users attribute key can be updated individually.

II. RELATED WORK

In Military environment, soldiers communicate with each other using wireless devices. The connection between these wireless devices may get damaged and the communication between the soldiers may not be possible. Disruption Tolerant Network(DTN) is one such technology which provides successful solution. This technology allows the wireless devices to communicate with each other even in the case where there is no end-to-end connection between wireless devices [1]. When the path between source and destination is not connected data from the source must be stored in intermediate node.

Chuah[2] and Roy [3] introduced a method in which messages from source is stored or replicated in external node. These external nodes could be accessed only by authorized user in an efficient manner and must be quickly accessible. Military application will involving the transfer of confidential data. Hence protection to these data must be given. Many cryptographic methods have been proposed which provided controlled access to these data. It is efficient to provide the access policies based on user attributes or roles to access the data which will be managed by key authorities. In DTN architecture, where multiple key authorities issue and manage their own attributes keys independently are referred as decentralized DTN.

For the retrieval of data in secure manner in DTN, attribute based encryption has be introduced [4]. Attribute based encryption is based on the concept of public key encryption. ABE is a method in which encrypted data is allowed to decrypt by a particular user only. It is an successful scheme which

addressed the problem of more secure data sharing and access control. It achieves one-to-many encryption than one-to-one as in public key encryption. Ciphertext-Policy Attribute Based Encryption (CP-ABE) is one type of method in ABE which provides an scalable way of encrypting the data [5]. Applying CP-ABE to DTN introduces many security problems. One such problem is Key escrow problem. Key escrow is an inherent problem even in multiple-authority systems if key authorities has privilege to generate their own attribute keys with their own master secrets. Another problem faced in CP-ABE is Key revocation. Soldiers in military environment may be continuously changing their attributes. So revoking of keys in efficient manner is necessary for the system to be secure. Last problem found in applying CP-ABE in DTN is the coordination of attributes issued from different authorities. It will be difficult to define the fine-grained access policy over the attributes which are defined and managed by the different key authorities for each user.

A. Contribution

In this paper, an attributed based secure data retrieval scheme using CP-ABE for decentralized DTNs has been proposed. The proposed system has got the following key features. Firstly, it reduces chances of vulnerability to the confidential data by enhancing backward/ forward secrecy through immediate attribute revocation. Second, Sender who encrypts the data will be defining access policy using access structure which is formed by the attributes issued by chosen set of authorities. Third, escrow-free key issuing protocol is used to solve the problem of key escrow. It will be generating secret keys to the user by performing a secure two-party computation (2PC) protocol among key authorities. Hence this system ensures the full protection for confidential data of the user which can be shared without fully trusting the authorities.

III. SYSTEM ARCHITECTURE

In this section, architecture of the DTN is been defined. Fig. 1 shows the overall architecture of proposed system.

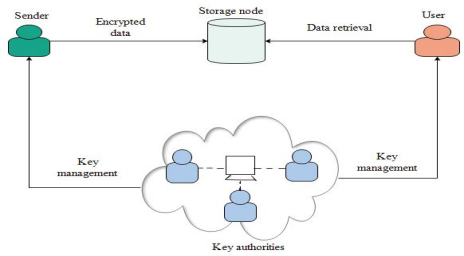

Fig. 1 Overall system architecture of proposed system

1) Sender: This is an entity who has got confidential data and stores them in the storage node. This storing of data in external node helps in accessing of data in extreme networking environment. Sender will be issuing access policy based on attribute and encrypts the data under policy and then stores the encrypted data to the storage node.

2) Key authorities: This is a key generation center where public/secret parameters are generated which is needed for encryption/decryption. In this module we have one main central authority and multiple local authorities. We assume that the communication channels between a central authority and each local authorities is secure and reliable. Here each local authorities will be issuing attributes keys based on their own attributes set which will be managed independently. These will be granting differential access rights to each individual users based on their attributes. It is assumed that key authorities are honest but curious as they will be doing the assigned task honestly and curious because they would like to learn information regarding encrypted data.

3) Storage nodes: This is an entity which can be mobile or static. It is used to store the encrypted data by the sender. These are the external storage nodes.

4) Users: This is an entity who access the data from the storage node. User can only decrypt the data stored in the storage node only if his/her set of attributes satisfies the access policy of ciphertext. If it doesn't satisfy then the user cannot decrypt the encrypted data.

Here key authorities should be denied from accessing the plaintext but they should be still able to issue the secret keys. To satisfy this requirement central authority and local authorities will be performing 2PC protocol with master secret keys of their own and will be issuing independent keys for users. Here 2PC protocol will not allow the key authorities to know each other master secrets.

IV. EXPERIMENTAL SETUP

Proposed system is implemented using Eclipse IDE and coding is done using Java language. To store the information we use MySql database. The experiment is carried out using three different systems. One main system will be implementing Sender, Key authorities and Storage module and the rest two system is considered as Users.

Sender module has got four different options. First is the Browse option which allows to browse the file. Second is the Encrypt option. On clicking this option the browsed file gets encrypted. Third option Get key from KA which gets the secret key from key authorities and the last option is Upload

option which uploads the ciphertext to the storage node.

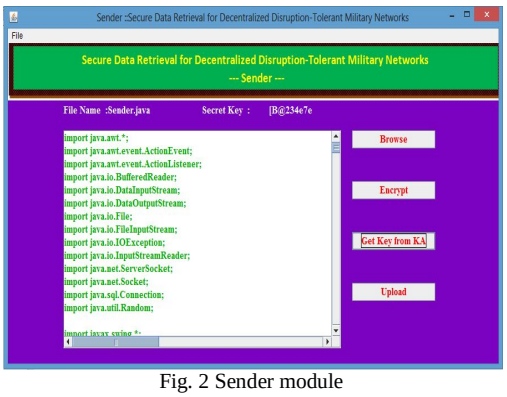

Fig. 2 Sender module

Second module is key authorities module. Here we are considering total of three key authorities. Each of the key authorities has got four option i.e. View user, View Privileges, View keys and Exit. View user option allows the key authorities to view the registered users along with the password. View privileges option shows the list of the user with the download privilege and View key displays the secret key generated.

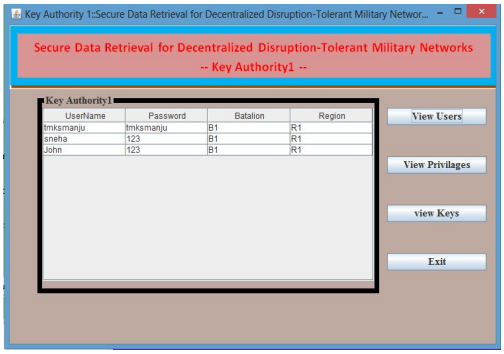

Fig. 3 Key authority module

Third module is the Storage node module. Here it has the facility to view the files uploaded in the storage node and also view the list of attackers who attempted to access the stored data without the proper access permission.

Fig. 5 Storage module

Last module is the User module which has an option of Receive and Save decrypted file.

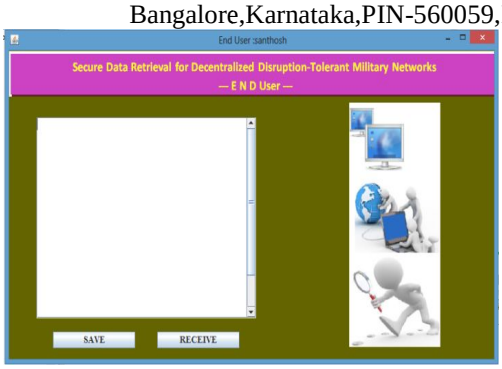

Fig. 6 User module

V. CONCLUSION

In this paper, a secure data retrieval scheme based on CP-ABE for decentralized DTNs has been proposed where multiple key authorities manage their attributes independently. 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 protocol among the key authorities with their own master secrets. The fine-grained key revocation can be done for each attribute group.

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

[3] 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.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Eurocrypt, 2005,pp. 457-473.

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

