International Journal of Advanced Technology and Innovative Research

ISSN 2348–2370
Vol.08,Issue.12,
September-2016,
Pages:2291-2294

www.ijatir.org

Secure Information Retrieval in an Organized Way for Disruption Tolerant Military Networks using Ciphertext-Policy-Attribute based Encryption (CP-ABE)

B.SHALINI[1], ARUNAVARANASI[2]

[1]PG Scholar, Dept of CSE, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, India,
E-mail: shalini.bollepally@gmail.com.

[2]Professor, Dept of CSE, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, India.

Abstract: In many of the military systems during the transferring of confidential information from the source to the destination may undergo some security issues. A solution is been proposed to overcome these issues and to retrieve the confidential information efficiently and securely which is known as Ciphertext-Policy Attribute based Encryption. Ciphertext-Policy-Attribute based Encryption is a fruitful solution which deals with access control issues. In this paper, we propose secure information retrieval scheme using CP-ABE for Disruption-Tolerant-Networks in which multiple key ascendants manage their attributes seperatly.The challenges like key-escrow, attribute revocation and coordination can be resolved in the proposed scheme. The proposed method is used to explain how to manage the secure and efficient information that is distributed in the disruption-tolerant networks.

Keywords: Disruption-Tolerant Network (DTN), Attribute-Based-Encryption (ABE), Ciphertext-Policy Attribute based Encryption (CP-ABE).

I. INTRODUCTION

In the recent trends in numerous military network systems or surroundings such as battleground and a bellicose area liable to bear from intermittent network connectivity due to jamming, mobility plus patronize partitions when they are working under hostile environments. The wireless devices carried by soldiers might be disconnected due to these factors. There may be no end-to-end route between the source and the destination. The Disruption tolerant network systems are introduced which grants the nodes to interact with one another in these extreme networking admistrative situations. Normally, when there is no end-to-end transmission of data from the sender and the receiver pair the data or message need to be awaited in the intermediate storage nodes for a sufficient amount of time until the transmission is re-established. Storage nodes are deployed in the DTN [1] architecture that is used for storing and replication of confidential information which can be accessed by the specified mobile nodes quickly and securely. Most of the military systems require the confidential information to be safeguarded with the access management techniques that acryptographically implemented. In many cases, we will examine that the key authorities manage the user attributes which are differentiated by using access policies that is provided to give access services.

Suppose consider a disruption tolerant network in which a commander may store the secure data in the repository node which can be accessed by members of “Battalion 2” who are participating in the “Mission 1”.In this situation, it is desirable assumption that multiple key authorities are going to manage their attributes for soldiers who are participating in their respective regions [5]. This type of DTN architecture which uses multiple key authorities for generating and managing their attribute keys by associating with the central authority is termed as Decentralized DTN.The idea of attribute based encryption (ABE) is a hopeful approach that satisfies the needs for secure information retrieval in DTN[4]. ABE is an assured technique that permits the access services over encrypted information by making use of access policies and the attributes among private keys and ciphertext. Especially Ciphertext policy attribute based encryption (CP-ABE) which provides a mechanism which allows to link the encrypted information along with the access policy and the attribute with the keys and combine them in order to provide secure access to confidential data. So the decoder needs to possess the specified access policy and attributes in order to decrypt the ciphertext.

Therefore dissimilar clients are allowed to decode dissimilar part of information for security purpose. However the purpose of implementing the ABE to DTN’s results in some security and privacy challenges. Since some of the users may change their attributes (for e.g. moving from their region) [7], or few private keys may be compromised, key updation of each attribute is needed to make the system secure. Even then this problem is critical in ABE systems because each attribute is ultimately shared by multiple users (so we have to group such a set of users as associated attribute group). This indicates that if any update or revocation is made to any attribute or any single user in the attribute group it would affect the remaining users involved in the attribute group. For example, consider if a user enters or leaves an attribute set then the related

attribute keys need to be updated or changed and should be redistributed to the remaining users present in the same attribute set for forward/backward secrecy. During this procedure if the preceding attribute key is not updated instantly it may result in stoppage of rekeying procedure or decline in security due to windows of helplessness. The key escrow problem is another challenge.

In CP-ABE, the key authorities by utilizing their own master secret keys to user's set of attributes are responsible in generating the secret keys of users [3]. In this way every encrypted data which is determined to specific user can be decrypted by the key authorities by generating their attribute keys. If the key ascendants are conspired by opponents once they are positioned in the hostile environments this could be a major problem to the privacy or confidentiality of the data mainly when the data is more sensitive. The key escrow problem is remains as a inherent problem in multi-authority systems until every key authority involved in the system has the total rights in utilizing their own master secret information for generating their own attribute keys. Since, such a key generation technique is the general method for many of the asymmetric encryption systems such as ABE therefore removing escrow in single or multiple authority CP-ABE could be a major open problem. The last challenge deals with the coordination of the attributes which are issued from different authorities. It is a difficult task to define a fine grained access policy over attributes which are derived by different authorities when the multiple key authorities or ascendants issue and manage attribute keys to users independently by utilizing their own master secret. To understand this consider the attributes "role 1" and "region 2" are managed by authority A, and "role 2" and "region 1" are managed by authority B.So, it is not possible to generate the access policy (("role 1" OR role 2")) AND ("region 2 OR "region 1")) within the previous method because the OR logic use between the attributes issued from different attributes cannot be implemented. This can be because of the real fact that different authorities by utilizing their own master secret keys can generate their own attribute keys.

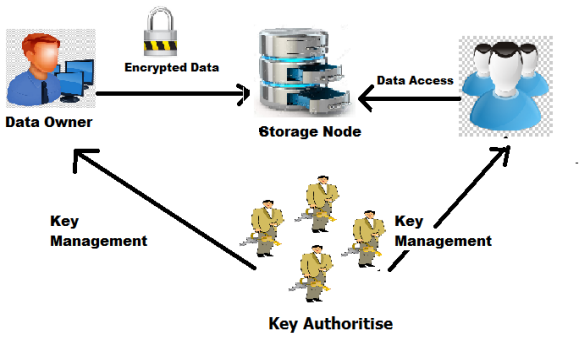

Fig.1. System Architecture.

II. METHODOLOGY

A. Existing System

The thought of attribute-predicated encryption (ABE) is a hopeful approach that consummates the requisites for secure information retrieval in DTNs.Attribute based encryption is a technique which allows a trusted single key authority to utilize their master secret information for generating the whole set of private or secret keys to users. Attribute based encryption (ABE) is of 2 types. The first one is the Key policy attribute based encryption and the second one is the Ciphertext Policy Attribute based encryption. In the key policy based encryption the encryptor will only define a ciphertext with a set of attributes; the key authority chooses a policy for each user that determines which ciphertext the user can decrypt. In the KP-ABE scheme the access structure is determined along with the private key. In the Ciphertext –Policy- Attribute based Encryption the roles of the ciphertext and keys are reversed. In CP-ABE the ciphertext is encrypted based on the access policy specified by the encryptor and a private key is simply generated by the key authority based on the user attributes. In this scheme the access structure is specified by the encryptor along with the ciphertext and not with the private key and stored in the repository node for easy access for the User.ABE is a mechanism in which a single trusted key authority will be able to generate the whole set of secret keys to User with the help of its master secret information.

B. Proposed System

In this paper to improve security for localized DTN's an attribute predicted secure information retrieval method using CP-ABE is been proposed. The proposed scheme has the subsequent achievements. First the forward/backward secrecy of confidential information is enhanced by immediate attribute revocation which reduces the windows of helplessness. Second, the encryptor may afford a fine grained access policy by using any monotone access structure utilizing the attributes generated from any picked set of key authorities. Third, the key escrow difficulty is explained by an escrow free key issuing protocol that utilizes the characteristic of the decentralized DTN architecture. By performing a secure two-party computation (2PC) protocol among the key authorities this protocol generates secret keys to users by using their own master secret information. The 2PC protocol avoids the key ascendants from retrieving any master secret information of each other such that none of them could engender the whole set of utilizing keys alone. Thus, users are not required to completely trust the ascendants entities in order to forefend their data to be shared. In the proposed scheme the information secrecy and privacy can be cryptographically implemented against any curious key authorities or data storage nodes.

III. IMPLEMENTATION

The proposed system has the following modules.

1. Login Module
2. Key Authority Module
3. Sender Module
4. Repository Node Module
5. User Module

1. Login Module: The authorized Sender or User or key authorities who possess the desired attributes (i.e. Username and Password) only can login to the system; else

an error message is displayed as invalid username or password. By this we are preventing an unauthorized user entering into the system and provide security for our project.

2. Key Authority: The key authorities are basically the key generation centers where the private/secret keys for the users are generated based on their specified attribute sets. The key authority is of two types.

3. Central key Authority: The role of the central key authority in the system is it manages all the local key authorities present in the CP-ABE system. They give access rights or permission for the local key authorities to generate the secret keys for the user using 2PC protocol. They also have the right to revocate or remove any local key authority.

4. Local Key Authority: Multiple local key authorities manage and generate the secret or private keys to User based on the User's specified attributes using the key generation protocol called 2PC(2 Party communication Protocol).The key authorities are assumed to be honest but curious.

5. Sender: Sender (e.g. a Commander) is the one who owns the confidential information or message which he/she wants to share it with the User (e.g. a Soldier).Sender will send a request to key authority for a secret key which is required for the encryption of the data. A sender will define access policy along with the ciphertext before storing it in the repository node for ease of sharing or for secure delivery of data to users in the networking environments.

6. Repository Node: The Storage Node is the intermediatory node which stores the ciphertext along with the access policy specified by the Sender. It provides access to the Users for accessing the ciphertext for decryption.

7. User: A User (e.g. a Soldier) is the one who wants to access the ciphertext that is stored in the repository node. A User who possess the set of attributes specified by the Sender and also who fulfills the access policy specified by the sender can only be able to decrypt the ciphertext using the key generated by the key authority.

V. EXPERIMENTAL WORK

Fig.2. User Registration.

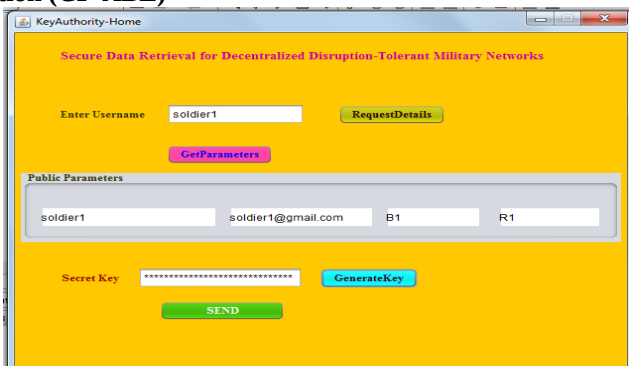

Fig.3. Secret Key Generation by the Key Authority Based on User Attributes.

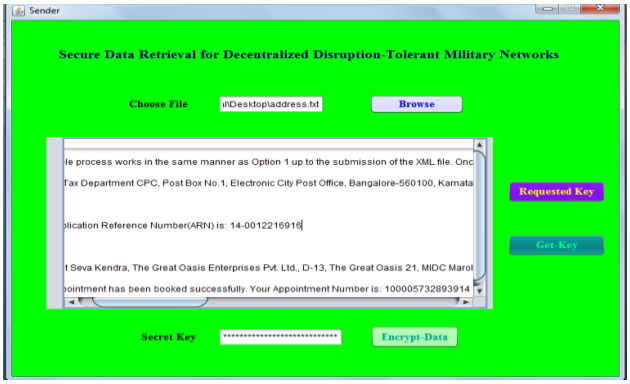

Fig.4. Sender Encrypting the Data Using the Secret Key Generated By the Key Authority.

Fig.5. User Login.

Fig.6. User Decrypting the Ciphertext Using the Secret Key Generated by the Key Authority.

VI. SECURITY

A. Data Confidentiality: Authorized users who possess enough credentials and who fulfills the access policy can only be able to access the encrypted data from the storage node. Unauthorized access from the storage node should be prevented.

B. Collusion-Resistance: The Proposed mechanism has the property of having resistance against collusion attacks. When the multiple local key authorities conspire which one another they can get the key which can be used to decrypt the encrypted data. To overcome from this issue a central authority is introduced in the system which manages all the local key authorities involved in the system. Secondly if different users conspire, they have the ability to decrypt a ciphertext by associating their attributes even if each of the users can't decrypt the ciphertext alone.

C. Backward and Forward Secrecy: In terms of CP-ABE scheme backward secrecy implies that if any user comes to hold an attribute group he ought to be avoided from retrieving the plain text of the antecedent knowledge exchanged before he holds the attribute, forward secrecy implies that if any user who drops an attribute should be averted to access the plaintext of the succeeding knowledge exchanged after he drops the attribute, until the other valid attributes that he is holding fulfills the access policy.

VII. CONCLUSION

DTN architecture is a fruitful solution which allows the mobile nodes involved in the military systems to communicate with each other and access the confidential information by utilizing the storage nodes. We propose an efficient and organized way for secure retrieval of the confidential information by utilizing CP-ABE for decentralized DTNs in which the attributes involved in the system are managed by multiple key ascendants separately. The intrinsical key escrow quandary is resolved such that the confidentiality of the stored data is ensured even under the bellicose environment where the key authorities involved in the system might be compromised or not plenarily trusted. And also each attribute group will undergo a fine grained key revocation. We illustrate how the confidential information is dispersed in the disruption tolerant network and how the proposed scheme is applied in order to manage the confidential information securely and efficiently.

VIII. REFERENCES

[1]Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", member IEEE, ACM, Feb 2014.

[2]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.

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

[4]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.

[5]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.

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

[7]J. Bettencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.