International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

SECURE DATA RETRIEVAL FOR DECENTRALIZED DISRUPTION-TOLERANT MILITARY NETWORKS USING CP-ABE

Bhavyashree H D[1], M S Maheshan[2]
[1]Student, [2]Assistant Professor,
Dept of IS&E, SJCE, Mysuru, India

Abstract: In many military networks, the soldiers carry wireless devices that may be temporarily disconnected by environmental factors, especially when they used in hostile environments. For this, Disruption-Tolerant Network (DTN) is a fruitful solution that allows a node to communicate with one another and access the confidential information by exploiting outside storage services. Probably the most difficult issues in this situation are the requirement of authorization polices and the policies redesign for secure information recovery. Cipher text-Policy Attribute–Based Encryption (CP-ABE) is a guaranteeing cryptographic answer to the access control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a several security and protection challenges as to the property revocation, key escrow, and co-ordination of characteristics (attributes) issued from different authorities. Here, a secure data retrieval scheme is proposed a safe information recovery plan utilizing CP-ABE for decentralized DTNs where numerous key authorities deal with their attributes autonomously. The proposed mechanism demonstrates how to safely and efficiently deal the confidential information dispersed in the Disruption-Tolerant Military Network. And also demonstrates how secret file will share among the key authorities.

Keywords: Disruption Tolerant Network, CP-ABE.

I. INTRODUCTION

In many military network, soldiers are carried the wireless devices that may be temporarily disconnected by environmental factors, especially when they used in hostile environments. For this, there is a fruitful solutions that allow a nodes to communicate with one another in these networking environments is a Disruption-tolerant network (DTN) [10][11]. An end-to-end path between a source and a destination pair may not always exist, message from source node will be stored in intermediate and it may need to wait until end-to-end path will be established. Storage nodes in DTNs were introduced where, data stored can be sent from source node such that data can quickly and efficiently access only by authorized person[1][12]. A requirement in some security-critical applications is to design an access control system to protect the confidential data stored in the storage nodes or contents of the confidential messages routed through the network. For example, in a disruption-tolerant military network, a storage node may have some confidential information which should be accessed only by members of "Battalion 2" who are participating in "Region 3". In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers)[1]. That is a DTN architecture where attributes keys are issue and manage independently by multiple authorities as a decentralized DTN. The idea of attribute-based encryption (ABE) [3][13] is a guaranteeing approach that satisfies the necessities for secure information recovery in DTNs. The main features of ABE are that empowers a right to gain access control over scrambled information (encrypted data) utilizing the access policies and attributed qualities among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) give an adaptive method for scrambled information such that encryptor characterizes the characteristic set that decryptor needs to have a specific end goal to unscramble the cipher text [4]. Consequently, multiple users are permitted to decrypt different sets of data per the security policy.

II. PREVIOUS WORK

The idea of attribute-based encryption (ABE) is a guaranteeing approach that satisfies the necessities for secure information recovery in DTNs. The main feature of ABE is that empowers a right to gain access control over scrambled information (encrypted data) utilizing the access policies and attributed qualities among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) give an adaptive method for scrambled information such that encryptor characterizes the characteristic set that decryptor needs to have a specific end goal to unscramble the cipher text [4]. Consequently, multiple users are permitted to decrypt different sets of data per the security policy.

Limitations of Existing System:

- When ABC approach apply to DTNs, it will introduce a few security and protection (privacy) challenges. Since at some point, a few users may change their related attributes or compromised the some private keys, in order to make framework secure key repudiation for each one attribute is necessary.
- However, this issue is more troublesome, particularly in ABE framework, since multiple users will shared their attributes.
- Another challenge is the key escrow issue. In, CP-ABE, by applying the powers expert secrets keys to users related set of attributes key authority or power generates a private keys of users.

- The last test is the coordination of attributes issued from multiple powers(authorities).With their own expert secrets, different authorities will independently manage and issue attributes keys to clients(users),the fine-gained access policies is tricky to characterize over attributes issued from different powers or authorities.

III. BACKGROUND

We first give formal definitions for the security of ciphertext policy attribute based encryption (CPABE). Next, we give background information on bilinear maps. we define an access structure and use it in our security definitions. However, in these definitions the attributes will describe the users and the access structures will be used to label different sets of encrypted data.

Definitions

Definition 1 (Access Structure [1]) Let{P1, P2, . . . , Pn} be a set of parties. A collection A ⊆ 2{P1,P2,...,Pn} is monotone if ∀B,C : if B ∈ A and B ⊆ C then C ∈ A. An access structure (respectively,monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {P1, P2, . . . , Pn}, i.e., A ⊆ 2{P1,P2,...,Pn}\{∅}. The sets in A are called the authorized sets, and the sets not in A are called the unauthorized sets. In our context, the role of the parties is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. We restrict our attention to monotone access structures. However, it is also possible to (inefficiently) realize general access structures using our techniques by having the not of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. From now on, unless stated otherwise, by an access structure we mean a monotone access structure.

Definition 2(Bilinear Maps)

We present a few facts related to groups with efficiently computable bilinear maps.

Let G0 and G1 be two multiplicative cyclic groups of prime order p. Let g be a generator of G0 and e be a bilinear map, e : G0 × G0 → G1. The bilinear map e has the following properties:

1. Bilinearity: for all u, v ∈ G0 and a, b ∈ Zp, we have e(ua, vb) = e(u, v)ab.

2. Non-degeneracy: e(g, g) = 1.We say that G0 is a bilinear group if the group operation in G0 and the bilinear map e : G0 × G0 → G1 are both efficiently computable. Notice that the map e is symmetric since e(ga, gb) = e(g, g)ab = e(gb, ga).

Definition 3(Access tree T) . Let T be a tree representing an access structure. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. If numx is the number of children of a node x and kx is its threshold value, then 0 < kx ≤ numx. When kx = 1, the threshold gate is an OR gate and when kx = numx, it is an AND gate.Each leaf node x of the tree is described by an attribute and a threshold value kx = 1.

To facilitate working with the access trees, we define a few functions. We denote the parent of the node x in the tree by parent(x). The function att(x) is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. The access tree T also defines an ordering between the children of every node, that is, the children of a node are numbered from 1 to num. The function index(x) returns such a number associated with the node x. Where the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

Satisfying an access tree. Let T be an access tree with root r. Denote by Tx the subtree of T rooted at the node x. Hence T is the same as Tr. If a set of attributes γ satisfies the access tree Tx, we denote it as Tx(γ) = 1. We compute Tx(γ) recursively as follows. If x is a non-leaf node, evaluate Tx′ (γ) for all children x′ of node x. Tx(γ) returns 1 if and only if at least kx children return 1. If x is a leaf node, then Tx(γ) returns 1 if and only if att(x) ∈ γ.

IV. Proposed work

Here proposes a property based secure information recovery plan utilizing CP-ABE for decentralized DTNs. The main features of proposed scheme have following achievements. First, backward/forward secrecy of secret information enhanced by attribute revocation by lessening the windows of helplessness. Second, by utilizing any monotone access structure, encryptor can characterize a fine-grained access policy under the attributes that will be provided from any picked set of authorities. Third, escrow-free key issuing protocol resolved the key escrow problem that adventures the normal for the decentralized DTN architecture. With their own master secrets, key issuing protocol produces and issues an user secret keys by performing a protected two-party computation (2PC) convention or protocol among the key authorities. The 2PC convention deflects the key authorities from getting any master secret information of one another such that none of them could produce the entire set of user's keys alone. Subsequently, to protect their shared data users are not needed to completely trust the authorities. In the proposed plan, the information privacy and security can be cryptographically implemented against any curious key authorities or information storage node.

Advantages:

- Information Secrecy: Unauthorized or unapproved users who don't have enough accreditations fulfilling the access policy should be prevented from getting to the plain information in the storage node. Likewise, unauthorized or unapproved access from the storage node or key authorities should also be prevented.
- Collusion-safety: If different users are collude, they may have the capacity to decrypt a ciphertext by consolidating their attributes regardless of the fact that each of the users can't decrypt the ciphertext alone.
- Backward and forward Secrecy: Backward secrecy implies that any user who comes to hold a characteristic that is attribute(that fulfills the right to gain the access policy)should be kept from getting to the plaintext of the previous information

exchanged before he holds the characteristic. Forward secrecy implies that any user who drops a characteristic should be kept from getting to the plaintext of the consequent information exchanged after he drops the characteristic; unless the other substantial attributes that he is holding that fulfill the access policy.

System Architecture

Figure 1 shows the system architecture , it mainly consist of five modules, they are

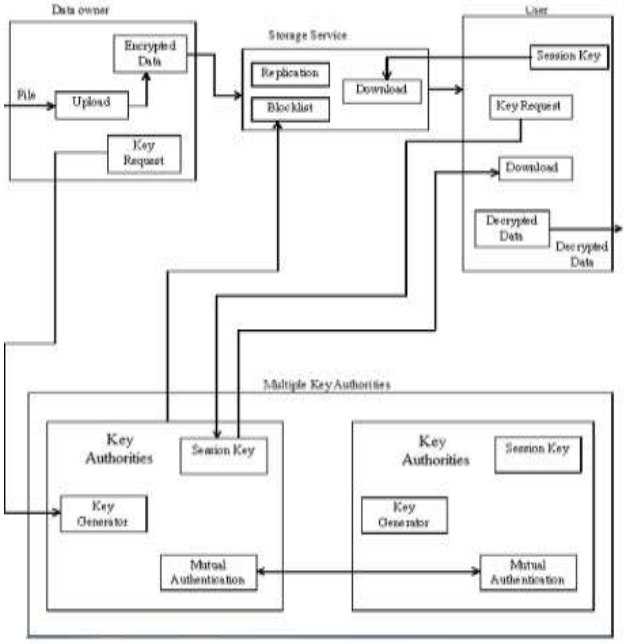

Figure 1.System Architecture

Key Authorities:

They are key era focuses that create public/secret parameters for CP-ABE. During initial key setup and generation phase, assume that there are secure and dependable correspondence channels between the two authorities and each local authority. Each local authority oversees different characteristics (attributes) and issues relating attribute keys to users. They give a differential access rights to individual users focused around the users attributes. The key authorities are thought frankly however inquisitive. That is, they will sincerely execute the allotted tasks in the framework; however they might want to learn information of scrambled (encrypted) contents as much as could reasonably be expected.

Data Owner:

In the extreme networking environment, data owner having confidential message or information and for easy sharing to user he will store the data in external storage node. A data owner is in charge of characterizing the session key and authorizing it all alone information by scrambling (encrypting) the information under the key before putting away it to the storage service.

Storage Service:

This is the node that stores the information from the data owners and gives a comparing access to user. It might be portable or static. Assume that the storage node is to be semi-trusted that is fair yet inquisitive (that is honest-but-curious).

User:

This is a node that needs to get to the information put away at the storage services (e.g. a fighter).In the event that a user has a set of properties fulfilling right to gain session key of the encoded information characterized by the sender, and it is not revoked in any of the qualities (attributes), then he will have the capacity to decode the cipher text and get the information.

Algorithm:

The CP-ABE consists of following algorithms

Setup: It will take implicit security parameter and output public parameter PK and master key MK.

KeyGen (MK,L): The key generation algorithm runs by CA. It takes as input the master key of CA and the set of attributes L for user, then generate the secret key SK.

Encrypt(PK,M,A): The encryption algorithm takes as input the message M, public parameter PK and access structure A over the universe of attributes. Generate the output such that only those users who had valid set of attributes that satisfy the access policy can only able to decrypt. Assume that CT implicitly contains access structure A.

Decrypt(PK,CT,SK): The decrypt algorithm run by user takes input the public parameter, the cipher text CT contains access structure A and the secret key SK contain of user attribute set S. If S satisfies the access tree then algorithm decrypt the CT and give M otherwise gives null.

V. IMPLEMENTATION

Secret Sharing (Shamir's Secret Sharing):

In cryptography, secret sharing refers to method for distributing a secret among for distributing amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. Standard definition of a (k, n) threshold scheme will be use to share the secret where k is the number of shares and n is the number of parties or participants.

Step by step procedure for secret sharing algorithm

Step 1: Use (k , n) threshold scheme to share the secret S where k<n.

Step2:Choose at random (k-1) coefficients $a_1, a_2, a_3 \ldots\ldots a_{k-1}$,and let S be the a_0

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}{}^{k-1}$$

Step 3: Construct n points (i , f(i)) where i=1,2…..n

Step 4: Give any subset of k of these pairs, find the coefficients of the polynomial by interpolation, and then evaluate a_0=S, which is the secret.

VI. CONCLUSION

Disruption-tolerant network (DTN) is a fruitful solution in military applications that allows a node to communicate with one another and access the confidential information by exploiting outside storage nodes. CP-ABE (cipher text attribute based encryption) is an efficient solution for access control and secure data retrieval problem. By using CP-ABE, where different key authorities deals with their qualities autonomously. The inherent key escrow problem is resolved such that the confidentiality data is obtained 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. And also, demonstrate how to apply the proposed mechanism to safely and efficiently deal the confidential information dispersed in the Disruption-Tolerant Military Network.

VII. FUTURE WORK

The future work is how to construct a ciphertext-policy attribute-based encryption scheme which would have both: the flexible delegation and attribute revocation properties, without involving a Mediator in the system Architecture

REFERENCES

[1] S. Roy and M. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs", Lehigh CSE Tech. Rep., 2009.

[2] D.HuangandM.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, "Cipher text-policy attribute based encryption", inProc. IEEE Symp. Security Privacy, 2007, pp.321–334.

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

[6] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication",Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.

[7] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system", inProc. Symp. Identity Trust Internet, 2008, pp. 26–35.

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

[9] M. Chase, "Multi-authority attribute based encryption", inProc. TCC, 2007, LNCS 4329, pp. 515–534.

[10] J. Burgess, B. Gallagher, D. Jensen, and B. N .Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks", inProc.IEEE INFOCOM,2006,PP.1-11.

[11] M. M B. Tariq, M. Ammar,and E. Zequra, "Message ferry route design for sparse adhoc networks with mobile nodes",inPoc.ACM MobiHoc,2006,pp.37-48.

[12] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks", inproc.IEEE MILCOM,2006,PP.1-6.

[13] R. Ostrovsky, A. Sahai,and B. Waters, "Attribute-based encryption with non-monotonic access structures", inproc.ACM Conf.Comput.Commun. Security,2007,pp.195-203.

