isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 1 Jul,2016,ISSN_NO: 2321-3337

SHIELDED DATA REGENERATION FOR DECENTRALIZED INTERRUPTION – ENDURED MILITARY WEB

Mrs SanthiPonraj[1],Prashanthy.S[2],Sangamithra.A[3],Saranya.M[4]

Asst.Professor[1], Dept of Computer Science, Sri Muthukumaran Institute of Technology, Chikkarayapuram, Chennai – 600 069 India.

UG Scholars[2,3,4],Dept of Computer Science, Sri Muthukumaran Institute of Technology, Chikkarayapuram, Chennai – 600 069 India.

ABSTRACT: *In military networks, the soldiers carry wireless devices that may be temporarily disconnected by environmental factors, especially when they are used in hostile environments. For this, Disruption-Tolerant Network (DTN) is a profitable solution that helps 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 need of authorization polices and the policies redesign for secure information recovery. Cipher text- Policy Attribute–Based Encryption (CP-ABE) is a guaranteeing cryptographic solution to the access control issues. In any case, the problem of applying CP-ABE in decentralized DTNs provides a several security and protection challenges such as property revocation, key escrow, and co-ordination of characteristics (attributes) issued from different authorities. In this case a secure data retrieval scheme is proposing a safe information recovery plan obtaining CP-ABE for decentralized DTNs where numerous key authorities deal with their attributes autonomously. The proposing mechanism demonstrates to deal the secured information dispersed in the Disruption-Tolerant Military Network safely and efficiently. And also demonstrates secret file sharing among the key authorities.*

Keywords: **Disruption Tolerant Network, CP-ABE, Key escrow.**

I. INTRODUCTION

In military network, soldiers carry the wirelessdevices that may be temporarily disconnected byenvironmental factors, especially when they used in hostileenvironments. For this, there is a profitable solutions that allows a node to communicate with one another in thesenetworking environments is a Disruption-tolerant network(DTN) [10][11]. Source anddestination pair provides an end-to-end path between them. A message sent from the source node will be stored in the intermediate node and it may need to wait until an end-to-end path will be established. Storage nodes inDTNs were introduced where, data stored can be sent fromsource node such that data can quickly and efficiently accessonly by authorized person[1][12].

A purpose of somesecurity-critical applications is to design an access controlsystem to protect the secure data stored in the storagenodes or contents of the confidential messages passedthrough the network. For example, in a disruption-tolerantmilitary 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 thiscase, it is a valuable assumption that multiple keyauthorities are likely to manage their own dynamic attributesfor soldiers in their deployed

regions or echelons, whichcould be frequently changed (e.g., the attribute representingcurrent location of moving soldiers)[1].
It is an DTN architecture where attribute keys manageindependently by multiple authorities as a decentralizedDTN.

II. IMPLEMENTATION OF MODULES

I. 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.

II. 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.

III. Storage Service:

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).

IV. User:

The 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.

V. *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 ofAttributesL 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 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.

III. SYSTEM ANALYSIS

The idea of attribute-based encryption (ABE) is aguaranteeing approach that satisfies the necessities for secureinformation recovery in DTNs. The main feature of ABE isthat empowers a right to gain access control over scrambledinformation (encrypted data) utilizing the access policies andattribute qualities among private keys and cipher texts.

Key-policy ABE (KP-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 ciphertext [4]. Consequently, multiple users are permitted todecrypt different sets of data per the security policy.

Limitations of Existing System:

I. When ABE approach is applied to DTNs, it willintroduce a few security and protection (privacy)challenges. Since at some point, few users maychange their related attributes or compromise some private keys, in order to make framework secure key repudiation for each one attribute isnecessary.However, this issue is more troublesome,particularly in ABE framework, since multiple users will share their attributes.

II. Another challenge is the key escrow issue. In, KP-ABE,by applying the powers expert secrets keys strides related set of attributes key authority or powergenerates a private keys of users.

III. Next is the coordination of attributes issuedfrom multiple powers(authorities).With their ownexpert secrets, different authorities willindependently manage and issue attributes keys toclients(users),the fine-gained access policies istricky to characterize over attributes issued fromdifferent powers or authorities.

IV. MAIN FEATURES

a) Information Secrecy: Unauthorized or unapproved users who don't have enough accreditationsfulfilling 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.

b) Collusion-safety: If different users get 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.

c) 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 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.

V. IMPLEMENTATION OF ATTRIBUTE BASED ENCRYPTION

A property based secure information recovery plan utilizing CP-ABE for decentralized DTNs is proposed. 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.

VI. SYSTEM ARCHITECTURE

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

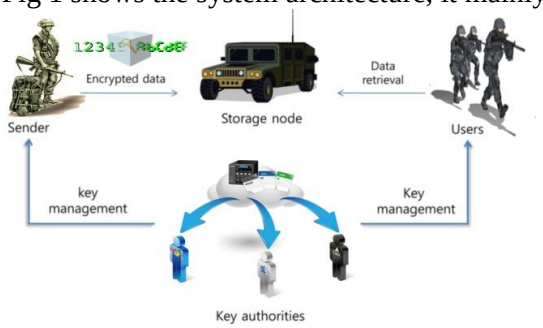

Fig 1.System Architecture

VII. CONCLUSION

Disruption-tolerant network (DTN) is a profitable 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.

VIII. 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

IX. REFERENCES

#1. 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. A. Lewko and B. Waters, "Decentralizing attributebasedencryption", Cryptology e-Print Archive:Rep.2010/351, 2010.
#4.A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryptionwith Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.
#5.R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and
Comm. Security, pp. 195-203, 2007.
#6.V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM
Conf. Computer and Comm. Security, pp. 89-98, 2006.
#7.P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp.Identity Trust Internet, 2008,pp. 26–35.
#8.L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in Proc. ACM Conf. Comput.Communication Security, 2007, pp. 456– 465.
#9.D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," AdHocNetw., vol. 7, no. 8, pp. 1526–1535, 2009.
#10.Sergio M. Tornell, Carlos T, Calafate, Juan-Carlos Cano, Pietro Manzoni "Assessing the Effectiveness of DTN Techniques Under Realistic Urban Environments "in Proc IEEE 38th Conference on Local Computer Networks, 2013, pp. 573-580.