International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 1, No 3, 2015. ISSN: 2348-6600
Reference ID: IJCS-085 PAGE NO: 486-490.

Efficient Management of Confidential Data in Disruption-Tolerant Military Networks

V.KOTESWARA RAO(M.Tech),Dept of Computer Science and Engineering.SRM University,CHENNAI
Mrs T.MANORANJITHAM, Asst Prof, Dept of Computer Science and Engineering.SRM University,CHENNAI
[1]koti0937@gmail.com
[2]manoranjitham.t@ktr.srmuniv.ac.in

***Abstract*— In today's world of growing commercial environment, transmitting secure data has become a great challenge. Portable nodes in military environments are prone to experience irregular system network and frequent partitions. A methodology called Disruption-tolerant network (DTN) permits remote devices to speak with one another and access the confidential data or secret data by abusing outside capacity nodes or storage nodes. This system provides efficient scenario for authorization policies and policies update for secure data retrieval. One of the most promising cryptographic solutions introduced to control the access issues is Cipher text Policy Attribute Based Encryption (CP-ABE). However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network.**

***Index Terms*— key generated, backward secrecy, fine-grained**

I. INTRODUCTION

The design of the current Internet service models is based on a few assumptions such as (a) the existence of an end to-end path between a source and destination pair, and (b) low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Some examples are: (i) battlefield ad-hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped with wireless modems and have intermittent RF connectivity with one another. In this paper, we propose a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt. Our scheme can provide not only fine-grained access control to each content object but also more sophisticated access control antics. Cipher text-policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a few securities and protection challenges as to the property disavowal, key escrow, and coordination of characteristics issued from distinctive powers.

II RELATED WORK

ABE is of two types; key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the cipher text is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes [6], [7], [8].
Bethencourt *et al.* [9] and Boldyreva *et al.* [10] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 3, 2015. ISSN: 2348-6600
Reference ID: IJCS-085 PAGE NO: 486-490.

revocable ABE schemes [11], [12], [13], [14] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy [15]. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering these as attributes [6], [16]. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is re encrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). We call this uncontrolled period of time windows of vulnerability. The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the nonrevoked users can update their keys. This could be a bottleneck for both the key authority and all nonrevoked users.

III.DATA ENCRYPTION

System Setup: At the initial system setup phase, the trusted initializer[2] chooses a bilinear group G_o of prime order p with generator g according to the security parameter. It also chooses hash functions $H: \{0, 1\}^* \; G_0$ from a family of universal one-way hash functions. The public parameter *param* is given by (G_o, g, H). For brevity, the public parameter *param* is omitted below.

Key Generation: In CP-ABE, user secret key components consist of a single personalized key and multiple attribute keys. The personalized key is uniquely determined for each user to prevent collusion attack among users with different attributes. The key generation protocol is composed of the personal key generation followed by the attribute key generation protocols. It exploits arithmetic secure 2PC protocol to eliminate the key escrow problem such that none of the authorities can determine the whole key components of users individually.

During the key generation phase using the 2PC protocol, the proposed scheme (especially 2PC protocol) requires $(3m + 1)C_0$ messages additively to the key issuing overhead in the previous multi authority ABE schemes in terms of the communication cost, where m is number of key authorities the user is associated with, and C_0 is the bit size of an element in G_0. However, it is important to note that the 2PC protocol is done only once during the initial key generation phase for each user. Therefore, it is negligible compared to the communication overhead for encryption or key update, which could be much more frequently performed in the DTNs.

Data Encryption: When a sender wants to deliver its confidential data M, he defines the tree access structure T over the universe of attributes L, encrypts the data under T to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm chooses a polynomial q_x for each node x in the tree T. These polynomials are chosen in a top down manner, starting from the root node R. For each node x in the tree T, the algorithm sets the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node. For the root node R, it chooses a random $s \; Z^*_p$ and sets $q_R(0) = s$. Then, it sets d_R other points of the polynomial q_R randomly to define it completely. Let Y be the set of leaf nodes in the access tree. To encrypt a message M G_1 under the tree access structure T, it constructs a cipher text *(CT)* using public keys of each authority as given in equation

IV DATA DECRYPTION

When a user receives the cipher text CT from the storage node, the user decrypts the cipher text with its secret key. The algorithm performs in a recursive way. We first define a recursive algorithm *DecryptNode (CT, SK, x)* that takes as inputs a cipher text CT, a private key SK, which is associated with a set of attributes, and a node x from the tree T. It outputs a group element of G. The *DecryptNode (CT, SK, x)* algorithm is given by equation 2.

$$DecryptNode\ (CT, SK, x) = e(g, g)^{rt,qx(0)}$$

The decryption algorithm begins by calling the function on the root node R of the access tree. We observe that $DecryptNode\ (CT, SK, x) = e(g, g)^{rt,qx(0)}$ if the tree T is satisfied by . When we set $A = DecryptNode\ (CT, SK, x) = e(g, g)^{rt,qx(0)}$, the algorithm decrypts the cipher text by computing M.

V .ANALYSIS

In this section, we first analyse and compare the efficiency of the proposed scheme to the previous multi authority CP-ABE schemes in theoretical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation in terms of the communication cost.

A .Efficiency

The authority architecture, logic expressiveness of access structure that can be defined under different disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme. In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [12] such that the access

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 3, 2015. ISSN: 2348-6600
Reference ID: IJCS-085 PAGE NO: 486-490.

policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [16] and RC [6] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be set to the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

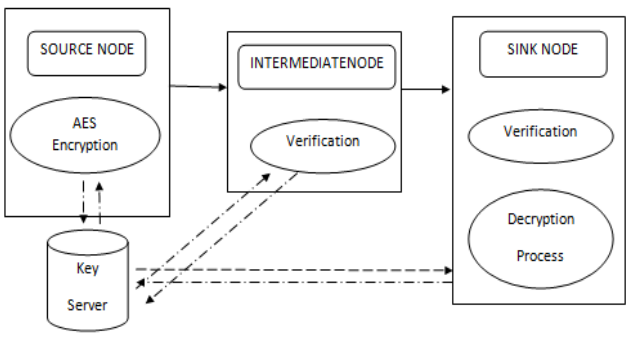
B .Simulation

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar [26] demonstrated the group behaviour in the Internet's multicast backbone network (MBone). They showed that the number of users joining a group follows a Poisson distribution with rate, and the member ship duration time follows an exponential distribution with a mean duration 1/ . Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behaviour distribution [32].

The total communication cost that the sender or the storage node needs to send on a membership change in each multi authority CP-ABE scheme. It includes the cipher text and rekeying messages for nonrevoked users. It is measured in bits. In this simulation, the total number of users in the network is 10 000, and the number of attributes in the system is 30. The number of the key authorities is 10, and the average number of attributes associated with a user's key is 10. To achieve an 80-bit security level, we set $C_0 = 512$, $C_p = 160$. C_T is not added to the simulation result because it is common in all multi authority CP ABE schemes. As shown in Figure 4.1, the communication cost in HV is less than RC in the beginning of the simulation time (until about 30 h). However, as the time elapses, it increases

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW [12]	Single	-	yes	Periodic attribute revocation
HV [16]	Multiple	AND	Yes	Periodic attribute revocation
RC [6]	Multiple	AND	Yes	Immediate system level user revocation
Proposed	Multiple	Any monotone access structure	no	Immediate system level user revocation

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryption defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy.While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems After authentication there is a file sharing. In existing technology, file sharing is done with less security.



4.2 Architecture of proposed system architecture

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 3, 2015. ISSN: 2348-6600
Reference ID: IJCS-085 PAGE NO: 486-490.

After encryption,public,key will received from the Key Authorities and send the message after receiving message key and save the data.Data should be encrypted successfully and receiver will receive the sender data and private key will receive from the message storage and message will decrypted

1. Key Authorities
2. Storage Nodes
3. Securely Formatting the Storage Nodes
4. Confidential Data Provider
5. Trusted curious User

1 Key Authorities :

They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities.We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible. Key authorities needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

2 Storage node

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted that is honest-but-curious,The storage node generates a new header message with such that a set of attribute group members including a new joining user (for backward secrecy) or excluding a leaving user (for forward secrecy) can decrypt the data

3 Securely Formatting the Storage Nodes

The "homomorphic" part of a fully homomorphic encryption scheme can also be described in terms of category theory. If C is the category whose objects are integers (i.e., finite streams of data) and whose morphisms include addition and multiplication, then the encryption operation of a fully homomorphic encryption scheme is an endo functor of C. The categorical approach allows for a generalization beyond the ring structure (finitary composition of addition and multiplication) of the integers

4 Confidential Data Provider

This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets.The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually

5 Trusted curious User

This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the cipher text and obtain the data.Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme. When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy,respectively.

IV CONCLUSIONS

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 1, No 3, 2015. ISSN: 2348-6600
Reference ID: IJCS-085 PAGE NO: 486-490.

information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed 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. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

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, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.
[4] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *Proc.*
[6] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309 323.
[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.
[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334
[10] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.