IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

Multi Secured Data Recovery from Disruption –Tolerant Military Networks

R.Dhivya[1] ,Ms.K.P.RamyaRani.M.E[2]

[1]Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, Tamil Nadu.
[2]Assistant Professor, Department of Computer Science and Engineering IFET College of Engineering, Villupuram, Tamil Nadu.

ABSTRACT:Disruption Tolerant Network technology are becoming successful solution that allow wireless devices are carried by soldier to access the secret data or command reliably by abusing external storage node .CP-ABE in the Decentralized Networks allow central authority and multiple local authority in which act autonomously with regards to the attribute key revocation.And also security and privacy challenginghave issues regards to attribute revocation, key escrow and coordination problem lead to collusion attack. CP-ABE with proxy re-encryption is encryption method used for encrypt log with attribute on recipients, this cryptography solution provide more security and privacy access policy. The re-encryption is full securely manage the information without collusion attack in the disruption tolerant network.

Keywords:CP-ABE,proxy re-encryption(PRE),privacy access policy.

I.INTRODUCTION

Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject tofrequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. The storage nodes are introduced in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require secure data exchange between mobile nodes including access control methods that are cryptographically enforced. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over soldier attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node, which should be accessed by members of “Troop 1” who are participating in “Region 2.”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. To refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN[6].

ISSN 2348 – 7968

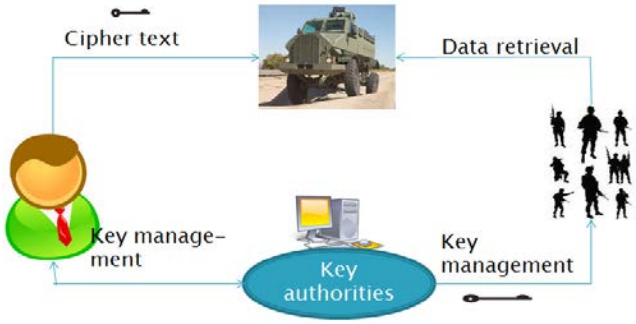
1.1.Scope Of The Study

Attribute Based Encryption (ABE) provides normal encryption and extra access control function. ABE is more efficient, flexible and suitable than other cryptographic techniques and may be a lightweight security solution .With this approach, confidentiality of information can be achieved even if control is lost during transmission.

The HASBE scheme seamlessly incorporates a hierarchical structure of system soldiers by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient soldier revocation because of multiple value assignments of attributes. HASBE based on the security of CP-ABE and implemented the scheme, and conducted comprehensive performance analysis and evaluation[3].

II.PROPOSED ARCHITECTURE

In this section ,describe the DTN architecture and security model.



2.1 System Description

Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE and PRE. We assume that there are protected 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 soldiers.They grant differential access rights to individual soldiers based on the soldiers' 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.

Storage node: This is an entity that stores data from senders and provide corresponding access to soldiers. It may be portable or fixed. Similar to the previous schemes, we also assume the storage node to be semi trusted, that is truthful-but-questioning.

Sender: This is an person 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 unfailing delivery to soldiers in the extreme networking environments. A sender is responsible for defining (attributebased) access policy and carry out it on its own data by encrypting the data under the policy before storing it to the storage node.

Soldier: This is a mobile node who wants to right to use the facts stored at the storage node (e.g., a soldier). If a soldier holds a set of attributes satisfying the access policy of the encrypted data

ISSN 2348 – 7968

defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the information.

III.DEFINITION AND IMPLEMENTATION

In this paper, Given some basic definitions, and then provide an overview of proxy re-encryption (PRE) scheme and hierarchical attribute-based encryption (HABE).

PRE

Let G be a multiplicative group of prime order q, and g be a random generator of G. The PRE scheme is consisted of the following algorithms:

Key Generation: Alice can choose a random element a $a \varepsilon Z_q^r$as her secret key SK_A, and her public key $PK_A$is $g^a \varepsilon$ G. In the same way, Soldier's public/secret key pair (SK_B, PK_B) are (b, g^b). The PRE key $RK_{A\rightarrow B} = b/a$ (mod q) is used to transfer a ciphertext that is encrypted under $PK_A$to the ciphertext that can be decrypted with SK_B, and vise versa.

Encryption: To encrypt a message $m \varepsilon$ G to Alice, the sender randomly chooses
$r\varepsilon Z_q^r$and generates ciphertext
$C_A = (C_{A1}, C_{A2}) = (g^r m, g^{ar})$.

Decryption: Given the ciphertext $C_A=(C_{A1,}C_{A2})$, Alice can recover message m with her secret key a by calculating $CA1/(CA2)^{1/a}$.

Re-encryption: Given $RK_{A\rightarrow B}$, the mail server can convert $C_A$to $C_B$that can be decrypted by Soldier as follows:
$C_{B1} = C_{A1}$and $C_{B2} = (C_{A2})$ $C_{B2}=(C_{A2})^{RKa\rightarrow b.}$
Given the cipher text (C_{B1}, C_{B2}), Soldier can recover message m with his secret key b by calculating $C_{B1}/(C_{B2})^{1/b}$.

HABE

Definition (BDH Problem): Given a random element P $\in$ G1, as well as aP, bP, and cP, for some a, b, c $c \in Zq^*$, compute $e(P, P)^{abc} \in$ G2.

Definition (BDH Assumption): If IG is a BDH parameter generator, the advantage that an algorithm has in solving the BDH problem is defined to be the probability that outputs $e(P,P)^{abc}$on inputs q, $G1$, G2, e, P, aP, bP, cP, where $<q,G1,G2,e>$are the outputs of IG for a sufficiently large security parameter K, P is a random element $\in$ G1, and a, b, c are random elements of Z_q^*. The BDH assumption is that is negligible for any efficient algorithm.

PRE SCHEMA CONSTRUCTION

Setup(K,UA)→ (PK,MK,s) :The commander takes a sufficiently large security parameter K as input to generate the system public key PK, the system master key MK, and the root secret key s. The system public key will be published, the system master key will be kept secret, and the root secret key will be sent to the trusted party.

GenKey (PK, MK, s, PKu, a, Tu) Suppose that soldier u with public key PKu is eligible for attribute a and his access right is effective in time Tu. The commander uses the system public key PK, the system master key MK, the root secret key s,soldier public key PKu, attribute a, and

ISSN 2348 – 7968

effective time period *Tu* to generates soldier identity secret key (UIK) *SKu* and time-based soldier (soldier)attribute secret key (UAK) *SKu,aTu* for *u.*

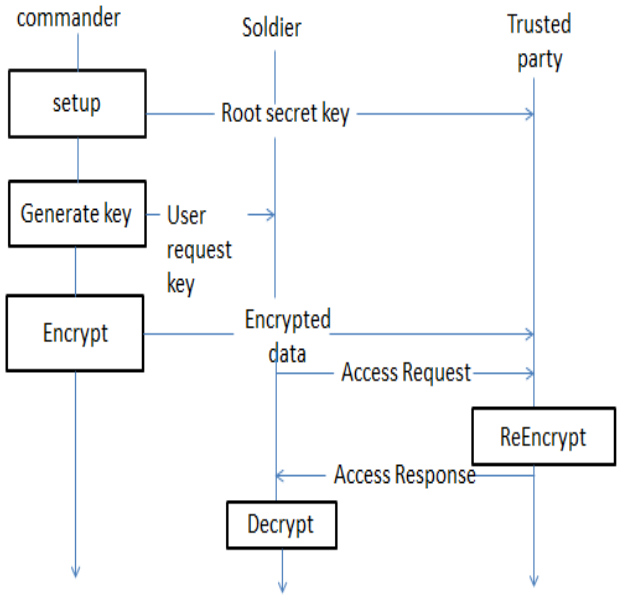


Fig 2: process of Proxy Re Encryption

Encrypt (PK,A,F)→ (CA) : The commander takes a DNF access structure A, a data *F*, and system public key *PK*, e.g., initial public keysof all attributes in the access structure *{PKa}a&A* as inputs to output a ciphertext *CA..ReEncrypt (CA,PK,s,t)* : Given a ciphertext CA with structure A, the tursted storage node first uses the system public key *PK* and the root secret key *s* to generate PRE keys on all attributes in the access structure A based on the access time *t*, and then uses these PRE keys to re-encrypt the original ciphertext CA to C_A^t.
Decrypt:Soldier*u*,whose at-tributes satisfy the access structure A,and whose effective time period *Tu* satisfy the access time *t*, can use *SKu* and C_A^t.

IV.SECURITY ANALYSIS

We evaluate the security of our work by analyzing the fulfillment of the security requirements.
A.Fine-grained Data Access Control To provide fine-grained data access control, the proposed scheme should provide a strategy that is able to define and enforce complex access policies for sensor data of various types or security levels. In FDAC, the access structure embedded in each soldier's secret key is able to represent complicated predicates such as disjunctive normal form (DNF),conjunctive normal form (CNF), and threshold gates. The combination of these predicates are able to represent sophisticated access structures. In fact, our scheme is able to support non monotonic (general) access structures if we define the *NOT* of each attribute as a separate attribute,which in turn will double the number of attributes in our system In our basic scheme,

ISSN 2348 – 7968

the master key is actually encrypted under the standard key-policy attribute-based encryption (KP-ABE) scheme which is provably secure. Our advanced scheme, to achieve efficient soldier revocation, makes some enhancement to the standard KP-ABE when encrypting the master key. The enhanced KP-ABE is provably secure under the Decisional Bilinear Diffie -Hellman (DBDH) assumption. (A formal security proof is available in our thesis). This turns out that the adversary is not able to decrypt the master key unless he owns the intended access structure. Therefore, our proposed scheme is able to control the disclosure of sensor data so that only authorized soldiers are able to access.

B. Data Confidentiality

In our trust model, the multiple key authorities are no longer fully trusted as well as the storage node even if they are honest. Therefore, the plain data to be stored should be kept secret from them as well as from unauthorized soldiers. Data confidentiality on the stored data against unauthorized soldiers can be trivially guaranteed. If the set of attributes of a soldier cannot satisfy the access tree in the ciphertext, he cannot recover the desired valuee(g,g)^{rs}during the decryption process, where is a random value uniquely assigned to him.On the other hand,when a soldier is revoked from some attribute groups that satisfy the access policy, he cannot decrypt the ciphertext either unlessthe rest of the attributes of him satisfy the access policy.

Even if the storage node manages the attribute group keys,it cannot decrypt any of the nodes in the access tree in the ciphertext. This is because it is only authorized to Reencrypt the ciphertext with each attribute group key, but is not allowed to decrypt it (that is, any of the key components of soldiers are not given to the node). Therefore, data confidentiality against the curious key authorities and storage node is also ensured.

C.Collusion-"safe"One drawback of all previous schemes is that by colluding, soldier and the proxy can recover commander secret key: for Dodis-Ivan, $s = s1 + s2$; for BBS, $a = (a/b) * b$. We will mitigate this problem allowing recovery of a "weak" secret key only. In a bilinear map setting, suppose Commander public key is $e(g,g)^a$and her secret key is a; then we might allow Soldier and the proxy to recover the value g^a, but not a itself.

The property of collusion "safeness" is extremely useful in our context since we allow the sender to generate first-level encryptions, that can be opened only by the intended recipient (Commander), or second-level ones that can be opened by any of the recipient's delegatees (e.g., Soldier). Indeed, this property implies that even if Soldier and the proxy collude, they will not be able to open any of Commander first level-encryptions!

In general, collusion "safeness" allows Commander to delegate decryption rights, while keeping signing rights for the same public key. In practice, a soldier can always use two public keys for encryption and signatures, but it is theoretically interesting that she doesn't *need* to do so. Prior work on "signcryption" explored this area (e.g., [41, 5, 3]); here we present, what can be viewed as, the first "signcryption" scheme (although we will not be formally concerning ourselves with the security of the signatures in this work).

ISSN 2348 – 7968

V.CONCLUSION

Disruption Tolerant Network technology are becoming successful solution that allow wireless devices are carried by soldier to access the confidential data or command reliably by exploiting external storage node .CP-ABE with proxy Re-encryption method given the full security. The primary challenge in this work is to find a new systems with elegant forms of expression that produce more than an arbitrary combination of techniques. Thus improve the efficiency of CP-ABEscheme, reducing the amount of issued updateinformation. The Re-encryption schema has taken low cost to implement and the confidentiality in storage node resolve the key escrow problem.

REFERENCES:

1) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp.321–334.
2) S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.
3) Dayananda RB ,Prof. Dr. G.Manoj Someswar,"Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment," in *IJETST.ISSN* 2348-9480.
4) Giuseppe Ateniese , Kevin Fu, Matthew Green, Susan Hohenberger , "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage",www.signcryption.org/publications/pdffiles/acm-tissec06-p1-ateniese.pdf.
5) Junbeom Hur and Kyungtae Kang, *Member, IEEE, ACM* "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE TRANSACTIONS ON NETWORKING VOL:22 NO:1 YEAR 2014.
6) S.Revathi, A.P.V.Raghavendra "Advanced Data Access Scheme in Disruption- Tolerant Network", IJIRCCE oct 2014.
7) S. S.M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.