Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.531 – 537

RESEARCH ARTICLE

Ciphertext-Policy Attribute-Based Encryption for Secure Data Retrieval in Decentralized Military Networks

Dr. Shubhangi.D.C, Archana Kadaganchi
Computer Science and Engineering, India
Computer Science and Engineering, India
shubhangidc@yahoo.co.in; archanakadaganchi@gmail.com

Abstract— Interruption-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 to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. The challenging issues are the enforcement of authorization policies and the policies update for secure data retrieval. This review, propose a new scheme called Cipher-text policy attribute-based encryption (CP-ABE), which is one of the most promising cryptographic solution to the access control issues. In CP-ABE a user's private key is associated with a set of attributes and a cipher-text specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher-text if and only if his attributes satisfies the policy of the respective cipher-text. Cipher-text policy attribute-based encryption scheme play an important role in decentralized ITNs for securing the data where multiple key authorities manage their attributes independently.

Keywords— Attribute-based encryption, ciphertext-policy attribute based encryption, interruption-tolerant network(ITN), multi-authority, key revocation, key escrow.

I. INTRODUCTION

Interruption tolerant system (ITN) is designed to provode communication in the most unstable and stressed environments. For examle, in military system situations, associations of remote gadgets conveyed by officers may be briefly detached by sticking, ecological variables, and versatility. particularly when they work in hostile environments. The storage nodes are introduced in ITNs in order to store the data. This is because when there is no end-to-end connection between a source and a destination the messages from source node to destination node may need to wait in the intermediate nodes. When a sender or commander wants to send the data to the particular user he first stores the data in storage nodes such that the only authorised users can access the necessary information efficiently. Increased protection of the confidentiality data is require in most of the military applications.

Sometimes, it is desirable to provide data access policies are defined over user attributes or roles,which are managed by the key authorities. For example,in a disruption-tolerant network,the commander stores the data at storage node which should be accessed by the members of 'Battalion1' who are participating in 'Region2'. So it is

reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions which could be frequently changed. We refer to this ITN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized ITN.

The attribute-based encryption is a promising approach that fulfills the requirements for secure data retreivalin ITNs. Attribute based encryption scheme enables an access control over encrypted data using access policies and attributes described among private keys and ciphertexts. Ciphertext-policy ABE provides a way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order decrypt the ciphertext.

However, the security and privacy challenges may be introduced due to the problem of applying ABE to ITNs. The key revocation is necessary,since some users may change their associated attributes or some private key might be compromised. However this issue becomes more difficult especially in ABE systems since each attribute is shared by.This implies that the revocation of any single user or attribute in an attribute group would effect the other users in the group.

If user joins or leaves an attribute group,the associated attribute key should be changed and redistributed to all other users in the group otherwise it results in rekeying procedure,or security degradation due to the windows of vulnerability if the previous key is not updated.

Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus the key authority can decrypt every ciphertext addressed to specific users by generating their attributes keys.If the key authority is compromised by adversaries when deployed in the hostile environments, this could be potential threat to the data confidentiality or privacy especially when the data is highly secure.removing escrow in single or multiple-authority CP-ABE is a pivotal open problem,since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems.

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained success policies over attributes issued from different authorities. For example, if attributes "role1" and "region1" are managed by authority A, and 'role2' and 'region2' are managed by the authority B. Then, it is impossible to generate an access policy (("role1" OR "role2") AND ("region1" or "region2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attributes keys using their own independent and individual master secret keys.

An attribute-based secure data retrieval scheme using CP-ABE for decentralized ITNs has been proposed. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized ITN architecture. 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. 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.

II. RELATED WORK

Traditional Ad-hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. M. Chuah and P. Yang [1] both together proposed the 'Node-density based adaptive routing scheme that allows the regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued connection. The main disadvantage of this scheme is, it fails to give any guarantee that mobile node in military environment to access the confidential data more efficiently and securely. V. Goyal et al developed new system for fine-grained sharing of encrypted data called Key-Policy Attribute-Based encryption (KP-ABE). In KP-ABE, cipher-texts are labeled with set of attributes and private keys are associated with access structures that control which cipher-text a user is able to decrypt. This scheme supported the delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) but fails the hide the set of attributes under which the data is encrypted [2].

Huang et al. [4] and Roy et al. [5] proposed decentralized CP-ABE schemes in the multi-authority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy.

The ciphertext-policy attribute-based encryption mechanism was proposed that enables an access control over encrypted data using access policies and attributes among private keys and cipher-texts. The main disadvantage of this mechanism is security degradation due to windows of vulnerability if the previous attribute key is not updated immediately and bottleneck during rekeying procedure [5].

A. Boldyreva et al [6] suggested key revocation mechanisms in both CP-ABE and KP-ABE respectively. The solution is to append to each attribute an expiration date and distribute a new set of keys to valid users after the expiration. Security degradation in terms of backward and forward secrecy and scalability were the major problems.

The content-based information retrieval scheme has been developed for ITNs. There are 3 important design issues such as cashing, query dissemination, message routing. The security design for such a system is very important but it is not addressed [7].

S. S. M Chow [8] presented a distributed KP-ABE scheme that solves the escrow problem in multi-authority system. All attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attributes sets belonging to the same user.

III. METHODOLOGIES

A) System Architecture:

As shown in the figure this architecture consists of following components.

1. Key Authorities: The key authorities are responsible for generating both public and private keys for cipher-text-policy attribute-based encryption. The key authorities consist of both central authority and multiple local authorities. Here we assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key set up and generation phase. Local authority manages different attributes and issues attribute keys to the user. Based on the user's attribute they grant the differential access rights to individual users. The key authorities are assumed to be honest-but-curious means they will honestly execute the assigned tasks in the system, however they would like to learn the information of encrypted content as much as possible.

2. Storage Node: The senders store their data in the storage node. The storage node provides the corresponding access to the users. It may be mobile or static. Similarly to the key Authorities the storage node is also semi-trusted, that is honest-but-curious.

3. Sender: The sender or the commander who owns confidential messages or data and wishes to store them into the external data storage node for ease of sharing for reliable delivery to users in the hostile environments.

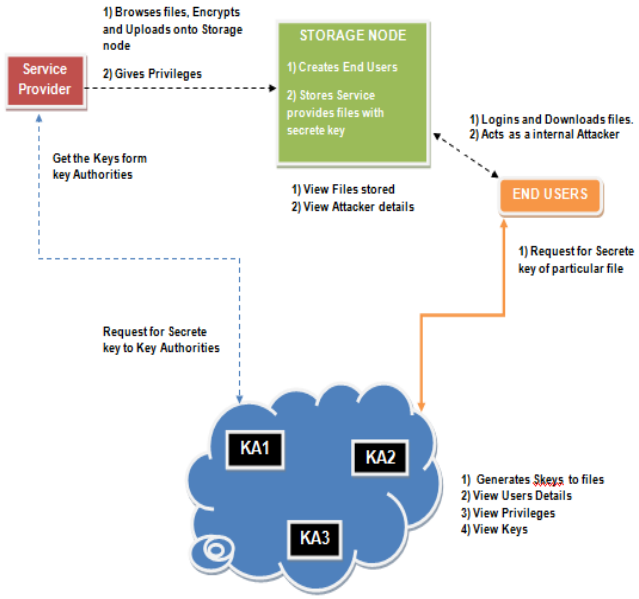

Fig. 1. Architecture of secure data retrieval in a interruption-tolerant military network.

A sender is responsible for defining access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4. User: This is a mobile node who wants to access the data stored at the storage node. If a user possess 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 ciphertext and obtain the data. The users issue key from the key authorities to encrypt the data.

The key authorities are semi-trusted; they should be deterred from accessing plaintext of the data in the storage node. But they should be still able to access secret keys to users. The central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol prevents them from knowing each other's master secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities.

B) Security Requirements:

1. *Data confidentiality:*

Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

2. Collusion-resistance:

If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.

3. Backward and forward Secrecy:

In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

C) Proposed scheme:

Let G_0 be a bilinear group of prime order p, and let g be a generator of G_0 . Let e : $G_0 \times G_0 \rightarrow G_1$ denote the bilinear map. A security parameter,k, will determine the size of the groups. We will also make use of Lagrange coefficients $\Delta_{i,\Delta}$ for any $i \in Z_p^*$ and a set,A of elements in Z_p^* : define $\Delta_{i,A}(x) = \prod_{j\in A, j\neq i} \frac{x-j}{i-j.}$. We will additionally employ a hash function H: $\{0,1\}^* \rightarrow G_0$ to associate each attribute with a random group elements in G_0, which we will model as a random oracle.

1. System Setup:

At the initial system setup phase, the trusted initializer chooses a bilinear group G_0 of prime order p with generator g according to the security parameter. It also chooses hash function $H : \{0,1\}^* \rightarrow G_0$ from a family of universal one-way hash functions.

Central key authority: CA chooses a random exponent $\beta \, \epsilon_R Z_p^*$. it sets$h = g^{\beta}$. The master public/private key pair is given by $(PK_{CA} = h, MK_{CA} = \beta)$.

Local Key Authorities: Each A_i chooses a random exponent $\alpha_i \in_R Z_{p.}^*$ The master public/private pair is given by $(PK_{A_i} = e(g,g)^{\alpha i}, MK_{A_i} = \alpha i)$.

2. *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 proposed key generation protocols composed of the personal key generation followed by the attribute key generation protocols.

Personal key generation: The central and each local authority are involved in the following protocol.

When CA authenticates a user u_t, it selects a random exponent $\gamma_{1,\ldots\ldots}\gamma_m \in_R Z_p^*$ for every local authority$A_{1,\ldots\ldots},A_m \in A$; and sets $r_t = \sum_{i=1}^{m} \gamma_i$. This r_t value is a personalized and unique secret to the user, which should be consistent for any further attribute additions to the users. Then, CA and each A_i engage in a secure 2PC protocol, where CA's private input is (γ_i, β), and A_i's private input is α_i. The secure 2PC protocol returns a private output $x = (\alpha_i+\gamma_i)\beta$ to A_i. This can be done via a general secure 2PC protocol for a simple arithmetic computation.

A_i Randomly picks $\tau \in_R Z_{p.}^*$ then, it computes $T = g^{\frac{x}{\tau}} = g^{\frac{(\alpha_i-\gamma_i)\beta}{\tau}}$ and sends it to CA.

CA then computes $B = T^{\frac{1}{\beta^2}} = g^{\frac{(\alpha_i-\gamma_i)}{\tau\beta}}$ and sends it to A_i.

A_i Outputs a personalized key component $D_i = B^{\gamma} = g^{\frac{(\alpha_i-\gamma_i)}{\beta}}$ and sends it to the user u_t securely.

Then, the user u_t, compute its personal key component $D = \prod_{i=1}^{m} D_i = g^{\frac{(\alpha_1+,\ldots\ldots,+\alpha_m)+r_t}{\beta}}$.

Attribute key generation: Each A_i generates attribute keys for a user u_t with a public parameter received from CA as follows.

CA first selects a random r' and sends $g^{r_t-r'}$ and $g^{r'}$ to A_i and $u_{t,}$ respectively.

A_i takes a set of attributes $A_i \subseteq A_i\ (L)$ as a input outputs a set of attribute keys for the user that identifies with that set A_i. Then, it gives the following secret key to the user u_t :

$\forall \lambda_j \in A_i : D_j = g^{r_t-r'}.H(\lambda_j)^{r_j}, D_j' = g^{r_j}.$

Then, the user computes $g^{r'}$. D_j For all its attributes key components and finally obtains its whole secret key set as

`SK_{u_t} = ($D = \frac{(\alpha_1+\cdots+\alpha_m)+r_t}{\beta}$. $\forall \lambda_j \in S :\ D_j = g^{r_t}$. $H(\lambda_j)^{r_j}$. $D_j' = g^{r_j}$) where $S \cup_{i=1}^{m} A_{i.}$

3. *Data Encryption:* To encrypt a message $M \in G_1$ under the tree access structure T , it constructs a cipher-text using the public keys of each authority as

CT = $(T, C = Me(g,g)^{(\alpha_1+\cdots+\alpha_m)^s}, C = h^s$. $\forall_y \in Y :\ C_y = g^{g_{y(0)}}$. $C_y' = H(\lambda_y)^{q_{y(0)}})$ where C can be computed as $C = M.(PK_{A_1} \times \ldots \times PK_{A_m})^s = Me(g.g)^{(\alpha_1+\cdots+\alpha_m)s.}$

IV. RESULT AND DISCUSSION

ITN applications using the Internet protected by the attribute-based encryption has been proposed. Almeroth and Anmar demonstrated the group behavior in the Internet's multicast backbone network, they showed that the number of users joining a group follows a Poisson distribution with rate λ , and the membership duration time follows an exponential distribution with a mean duration $1/\mu$.

The user joins and leaves events are independently and identically distributed in each attribute group following Poisson distribution. The membership duration time for an attribute is assumed to follow an exponential distribution. The inter-arrival time between users set as 20 min ($\lambda = 3$) and the average membership duration time as 20 h ($1/\mu = 20$).

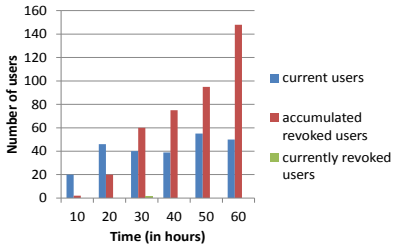

Fig.2. Number of users in the attribute group

Fig. 3 shows the total communication cost that the sender or 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 non-revoked users. It is measured in bits. As shown in the figure the total number of users in the network is 10,000, and the number of attributes is 30.

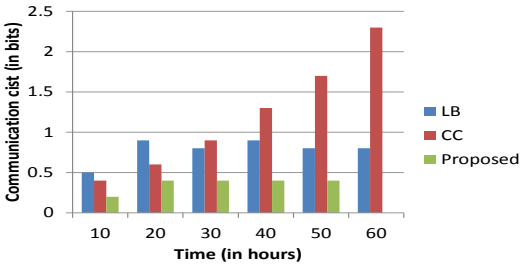

Fig.3. Communication cost in the multi-authority in CP-ABE systems.

The number of the key authorities is 10, and the average number of attributes associated with a user's key is 10. For a fair comparison with regard to the security perspective, set the rekeying periods in HV as $1/\lambda$ min. to achieve an 80-bit security level .Set $C_0 = 512$, $C_P = 160$. C_τ Is not added to the result because it is common in all multi-authority CP-ABE schemes. As shown in the figure 3, the communication cost in HV is less than RC in the beginning. However, as the time elapses, it increases conspicuously because the number of revoked users increases accumulatively.

V. CONCLUSION

An effective and secure information recovery technique called Cipher-content approach trait based encryption has been proposed for decentralized intrusion tolerant systems (ITNs). In CP-ABE different key powers are in charge of dealing with their own particular characteristics independently. Intrusion Tolerant systems administration is intended to give interchanges in the shakiest and focused on situations, where the system would ordinarily be liable to regular and dependable interruptions and high bit blunder rates that could extremely debase typical correspondences. The entrance control and secure information recovery issues can be determined by CP-ABE. The key renouncement or redesign of every property gathering should be possible to make the framework secure. The inalienable key escrow issue is made plans to guarantee the classifiedness of the put away information under the unfriendly environment where key powers may be bargained or not completely trusted. The secrecy of the information is guaranteed. Likewise, the forward and in reverse mystery can be ensured.

REFERENCES

[1] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp 1-6.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[3] 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.
[4] 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.
[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321-334.

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426.
[7] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.
[8] A. Lewko and B. Waters, "Decentralizing attribute- based encryption system," Cryptology ePrint Archive: Rep. 2010/351, 2010.

