International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 03, March-2016

Secured Information Sharing in Military Networks

Dr. V. D. Ambeth Kumar, D. Elangovan , K. Gunasekaran, Melvina
Department of Computer Science and Engineering,
Panimalar Engineering College,
Chennai, Tamil Nadu, India

***Abstract* - Several military operations require enlarged protection of confidential data including access control methods that are enforced crypto-graphically. In many cases, it is desirable to provide differentiated access services such that data access strategies are defined over user attributes or roles, which are managed by the key authorities. Mobile nodes in military environments such as battle fields may have intermittent network connectivity and frequent partitions. Disruption-tolerant network provides efficient way for soldiers to communicate using wireless devices and also gives access to the confidential information or commands. In this scenario, the most challenging issues are enforcement of authorization policies and policy updates for secure data retrieval. So we are using Cipher text-policy attribute-based encryption to solve access control issues. However, the problem of applying CP-ABE in fragmented DTN introduces several security and privacy challenges with various fields such as attribute revocation, key escrow, and categorizing of attributes issued from different authorities. We demonstrate how to apply the proposed workings to securely and smoothly manage the confidential data distributed in the disruption-tolerant military network**

Keywords— DTN, Information, Bi-linear Diffie-Hellman, Military.

1.INTRODUCTION:

In military networks, the wireless devices carried by the soldiers may be temporarily disconnected by various factors such as jamming, environmental factors and mobility. To overcome this situation, Disruption-Tolerant Network is used. The DTN enables communication between wireless devices even under extreme environments. lack of point to point communication is also supported here. The message from source node may need to wait in the intermediate node for some amount of time until the connection is established.

The storage node in DTN is introduced by Roy [8], where data can be stored or replicated and are accessed by authorized mobile nodes. The roles or data policies for user attributes which are managed by key authorities are defined. For example, in a DTN military network, a commander may store confidential information in storage node, which can be accessed by members of Battalion 1 who are participating in Region 2. So, it is assumed that multiple key authorities are likely to manage their own dynamic attributes for soldiers [8], [1]. We refer this DTN architecture where multiple authorities manage their own attribute keys independently [2].

The attribute - based encryption (ABE) [9] approaches in such a way that it provides secure data retrieval in DTN. It enforces access policies over encrypted data. And the cipher-text-policy ABE (CP-ABE) encrypts as well as decrypts the data with attribute set key using encryptor. Still, the problem of applying ABE to DTN introduces several security and privacy issues.

1)Attribute Revocation: Some users may change their attributes at some point and key revocation for each attribute is necessary since they are shared by multiple users. So, the new set of key is introduced to valid user with time limits [6]. The periodic attribute revocable ABE scheme [1], [6] has two main problems.

a) The first problem is security degradation of backward and forward secrecy. It happens when user access the cipher-text with his previous attribute key even after the key id dropped or changed. And the second problem is scalability. The key authority announces a periodic key update for each time-slot even for non-revoked users [8]. This could be a bottleneck for both key authorities and all non revoked users.

b) Key Escrow: The existing ABE schemes are based on the single trusted authority, which has the power to generate the private key for all users with their master secret information [9], [6], [7]. To solve this multiple authority system is used [2]. In this system all attribute authorities are made to participate in distributed way in the key generation protocol. In some cases, it may degrade the performance of user since there is no central authority with master secret information.

c) Coordination of attributes issued by multiple authorities: In decentralized CP-ABE schemes in the multiple authority networks. They achieved a combines access policy over the attribute issued from different authorities by encrypting data multiple times. The main disadvantage is efficiency and expressiveness.

2. EXISTING SYSTEM:

In the past, most existing systems has focused only on providing expressive and scalable way of retrieving the data, but little attention has been paid for the need of security. Existing approaches toward secure data retrieval mostly rely on the attribute based encryption (ABE). The ABE [7] features a policy that can provide access to the encrypted data using access mechanisms. But it fails to provide security and privacy to data. The first challenge is attribute revocation, some users may change their attribute at some point and key revocation for each attribute is necessary since they are shared by multiple users. So these key updates may cause security degradation. The challenge is key escrow; the existing ABE schemes are based on the single trusted authority, which has the power to generate the private key for all users with their master secret information. To solve this multiple authority system is used. Finally, different authorities cannot coordinate the attributes. When each authority manages and provides attribute keys to clients with their own master confidentialities, it is very hard to define fine-grained access policies over attributes issued from different authorities.

3. PROPOSED SYSTEM:

In this paper we provide a multi authority CP-ABE [2] scheme for secure data retrieval in decentralized DTN. Our approach achieves immediate attribute revocation and enhances backward and forward secrecy of confidential data. We allow encryptor to define the access policies using any monotone access structure under attributes that are issued from any chosen set of attribute. It also handles the key escrow problem by introducing a escrow-free key issuing propriety. The key issuing propriety generates and issues secret key by performing 2PC protocol. The main advantage of the proposed system is, it avoids collusion attack among local authorities and provides data confidentiality is maintained. It gives backward and forward secrecy to key attributes.

4. METHODOLOGY DESCRIPTION:

Cipher text Mechanism Attribute Based Encryption

While the ABE schemes are constructed on the architecture where the data is encrypted using access policies and set of attributes, the cipher text policy attribute based encryption uses the access policy to encrypt and provides a key with respect to an attribute set. It enchants the immediate attribute revocation that allows backward and forward secrecy. It helps encryptor to define fine-grained access policy using any monotone access structure under the attributes issued from any chosen set of attribute. It avoids the key escrow problem by introducing escrow free key issuing protocol .

The key issuing protocol performs 2PC using their master secrets among key authorities, generates and issues user secret keys. The 2PC protocol prohibits the key authorities to obtain any master secret information . This makes the users independent of the authorities for data protection. The Data confidentiality is cryptographically enforced against storage nodes or key authorities. The plain text data is prohibited from key authorities which are semi-trusted.

The central and local authorities have 2PCwith master keys of their own. The 2PC keeps master key safely from each individual. Thus it is assumed that the central authority will never collide with the local authorities.

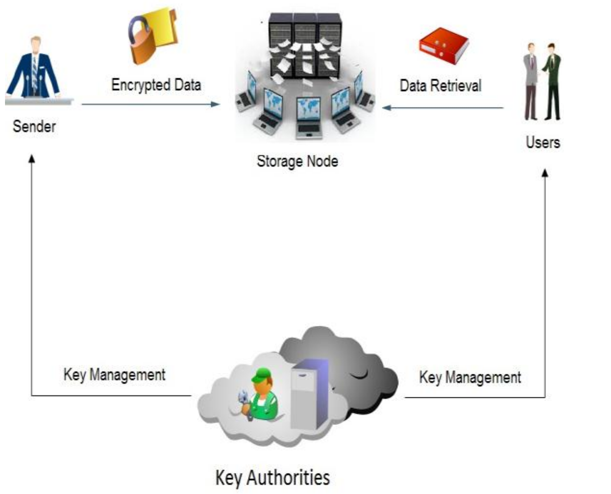

Figure1. Architecture of secure data retrieval in interference - tolerant military network.

System descriptions:

The architecture consists of the following system concepts.

1)Key Authorities: They are the center for key generations that generates public/secret parameter. It has a central authority and a local authority. The central authority can manage one or more local authorities at a time whereas each local authority manages different attribute. The local authorizes are responsible for key issuing.

2)Storage Node: It Stores the data from sender and enables the respective user to access them. It may be static or mobile.

3)Sender: It is an entity that owns confidential information and wishes to store in storage node.

4)User: It is a mobile node who wants to access the data stored at storage node.

5. BACKGROUND

We provide formal definition for security of cipher text policy based encryption (CP-ABE). Next, we give background information on bi-linear maps [4] and [6].

A. Access Structure: Let { $Q_1, Q_2, \ldots, Q_n$} be a set of parties. A collection $X \subseteq 2^{\{Q1,Q2,....Qn\}}$ is monotone if $\forall$ Y, Z : if $Y \in Q$ and $Y \subseteq Z$ then $Z \in X$. An access structure is a collection A of non empty subsets of $\{Q_1, Q_2, \ldots. Q_n\}$,i.e., $A \subseteq 2^{\{Q1,Q2,....Qn\}} \backslash \{\phi\}$. The set in X are called authorized sets, and the sets not in X are called unauthorized sets.

In our context, the role of the parties is taken by the attributes. It is also possible to realize general access structure using technique.

B. Bi linear Pairing: Let H_1 and H_2 be a multiplicative cyclic group of prime group *p*. Let *g* be a generator of H_1 and *e* is a bi-linear map, *e*: $H_1 \times H_2 \rightarrow H_1$.

The bi-linear map *e* has the following properties:

1.Bi-linearity: $\forall x, y \in H_1$ and $a, b \in Z_p$, we have $e (x^a, y^b) =e (x, y)^{ab}$.

2.Non-degeneracy: $e (g, g) \neq 1$.

We say that H_1 is a bi-linear group if the group operation in H_1 and bi-linear map e: $H1 \times H_2 \rightarrow H_1$ e is symmetric since $e (g^a, g^b) =e (g, g)^{ab}=e(g^b, g^a)$.

C. Bi linear Diffie-Hellman Assumption: The Bi-linear Diffie-Hellman (BDH) problem is used to compute $e (g,g)^{abc} \in H_1$ given a generator *g* of H_1 and elements g^a, g^b, $g^c$for a, b, c $\in Z_p^*$.An equivalent formulation of the BDH problem is to compute $e(A,B)^c$ given a generator *g* of H_1, and elements A, B and g^c in H_1.

6. PERFORMANCE EVALUATION:

In this section we analyze the efficiency of the proposed work to the previous multi authority CP-ABE patterns in theoretical aspects. It also describes the suggested work ‘s efficiency , and how we might handle the key revocation.

Efficiency:

The efficiency of key generation and encryption algorithm are fairly straight forward. The encryption algorithm will include two exponentiation for each leaf and the cipher text will have two group elements for each tree leaf in the cipher text’s access tree. The key generation requires two exponentiation for every attribute and the private key has two group elements for every attribute. However, there might be several ways to satisfy a policy, so more algorithm might be tried to optimize.

Table 1 Expresiveness,Key Escrow And Attribute Revocation Analysis

Scheme	Authority	Expressiveness	Key Escrow	Attribute Revocation
BSM[6]	Single	-	Yes	Periodic
RC[8]	Multiple	And	Yes	Immediate
Proposed	Multiple	Any monotone access structure	No	Immediate

Table 1 shows the authority architecture, logic expressiveness of access structure, key escrow, and repudiation of each CP-ABE scheme.In the proposed work, the logic can be very expressive because it has the single authority system like BSW[6] and accept any monotone access structure. Whereas in the HV[8] scheme AND gate and the set of attributes are allowed, which can be managed by multiple authorities.

The revocation in the proposed work can be done immediately when compared to the BSW. So the attributed of users can be revoked at any time before the expire of assigned time. Therefore it en-chances the security of data by reducing the windows of vulnerability. The Proposed system uses fine -grained user revocation for each attribute as opposed to RC. Even if the uses comes to hold or drop the attribute,he can still access the data if he satisfy the defined access policies. Finally the key escrow problem is also resolved.

7. SECURITY:

A. Conspiracy Resistance

In CP-ABE, the classified information must be attached to the cipher text instead to the users private keys . In proposed work the private keys of various users are randomized like other ABE schemes[6]. In order to decrypt a cipher text, the conspiring attacker should recover e(g, g)(1+ 2...+ m)s. To recover this, the attacker must pair Cy from the cipher text and Dy from the other colluding users private key. However, this results in the value e (g, g) (a1+a2+...+am)s , which is uniquely assigned to each users even if the group key for attributes exist.

Another Conspiracy attack scenario is the collusion between the revoked users in order to obtain the valid group key for some attributes that they have not access permission. Using the attribute group key protocol, the colliding users will no longer obtain any valid attribute group keys.

Finally the collusion among local authorities could be determined by personalizing key. However, each users attribute key components are blinded in the local authorities view. And those key are viewed only by the users and central authorities. Therefore, the colluding local authorities cannot derive the whole set of secret key of users.

A. Data confidentiality

The multiple key authority as well as storage node or cache is not fully trusted. So, In our model we are enabling the data confidentiality to all the data in cache. Even if the cache manages the attribute group keys, it cannot decrypt any of the nodes. This is because, it is only authorized to re encrypt but not decrypt the cipher text with each attribute group key. Even if a user is revoked from some attribute group, he cannot decrypt the cipher text unless he satisfy the access policy.

If the key authorities and storage node are partially trusted, then they are subjected to attack and leads to the loss of information confidentiality. The local authority issues and manages the set of attributes to each users, and allows them to combine with the secret key received from central authority. By this way the key authority can give protection to confidential data.

Even if the storage node has attribute group key, it cannot decrypt any of the nodes in access tree. Therefore, data confidentiality against the key authorities and storage node is also ensured.

B. Backward and Forward secrecy

When a user comes to hold a set of attributes that satisfies the access policy in the cipher text at some point, the corresponding updated attribute group keys are delivered to valid attribute group. Then all the components encrypted with a secret key is re-encrypted by the storage node. Even if the user has stored the previous cipher text, he cannot decrypt it.

On the other hand, when a user comes to drop a set of attribute that satisfies the access policy at some time, the corresponding attribute group key is updated and delivered to them. Then all the components encrypted with a secret key is re-encrypted by the storage node . And the user cannot decrypt any node, because he holds a new attribute.

8. CONCLUSION:

Generally mobile nodes in military environments such as battle fields may have sporadic network connectivity and frequent partitions. Delay-tolerant network provides efficient way for soldiers to communicate using wireless devices and also gives access to the confidential information or commands. Our schemes manage multiple key authorities and their attributes independently. It allows wireless devices to communicate with each other and also provides access to confidential data. The inherent key escrow problem can be resolved so that the data confidentiality is guaranteed. Along with these, we can provide a fine- grained key revocation for each attribute group.

9. REFERENCES

[1] Luan Ibraimi, Milan Petkovic, Svetla Nikova, P. Hartel, and W. Jonker, “Medi-atedciphertext-policy attribute-based encryption and its application,” in *Proc. Springer* LNCS 5932, *WISA*, 2009, pp. 309–323.

[2] Allison Lewko and Brent Waters, “Decentralizing attribute-based encryption,” Cryptology ePrint Archive: Rep. 2010/351, 2010.

[3] Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian. Wang, and K. Fu, “Plutus: Scalable secure file sharing on untrusted storage,” in *Proc.Conf. File Storage Technol.*, 2003, pp. 29–42.

[4] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, “Attribute-based en-cryption for fine-grained access control of encrypted data,” in *Proc.ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[5] Shucheng Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in *Proc. ASIACCS*, 2010, pp. 261–270.

[6] M. Chase and S. S. M. Chow, “Improving privacy and security in multiauthority Attribute-based encryption”, *ACM Conf. Comput.Commun. Security*, 2009, pp. 121–130.

[7] L.Cheung and C.Newport,”Provably secure ciphertext policy ABE”, in *proc ACM Conf, Computer and Communications Security, 2007,* pp.456-465.

[8] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” in *Proc. ACM Conf. Computer and Communications Security*, 2006, 99–112.

[9] Sherman S.M. Chow, “Removing escrow from identity-based encryption,” in *Springer* LNCS 5443, *Proc. PKC*, 2009, pp. 256–276.

[10] 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.

[11] Amit Sahai and Brent Waters, “Fuzzy identity-based encryption,” in *Proc. Eurocrypt*, pp. 457–473. 2005,

[12] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” *ACM Conf. Comput.Commun. Security*, 2007, pp. 195–203.

[13] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.