International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Securing Data retrieval using CPABE scheme with Two Party Computation in DTN military network – A Survey

Shivkanya J. Jadhav[1], Prof. N. G. Bhojne [1]

[1] *Department of Computer Engineering, Sinhgad College of Engineering, Pune-41, Maharashtra, India*

Abstract - *Disruption tolerant network (DTN) is store and forward network where end- to-end connectivity is not assumed and where links between nodes are used to transfer data. DTN is applicable in rural area, military network, vehicular ad-hoc network (VANET). With DTN, arise many challenges such as routing of data in lack of end to end connectivity and also with the security. Current open issues in privacy of data are such as key management, key agreement, and key revocation in this network. Several routing scheme such as store and forward approach designed for DTN but not much work has been done on providing information access in such challenging network. To overcome these challenges many techniques are designed. But still use of these technique in decentralized DTN's gives rise to challenges related attribute revocation, key escrow and co-ordination of attributes issued from different authorities. To overcome the challenges related to security and privacy in decentralized DTNs, here introduce a secure data retrieval scheme using CP-ABE. In this scheme, multiple key authorities handle their attribute independently on DTN using 2pc protocol. This mechanism handles distributed confidential data securely and efficiently.*

Key Words: *Data retrieval, DTN network, Attribute revocation, Key escrow, Decentralized ABE, CPABE, Two Party Computation.*

1. INTRODUCTION

Many environment needs protection of secrete data with retrieval control mechanism using cryptography concept. Many scheme, defines access services in which attribute of users or roles are used to define access policies. Access policies are managed by the key authorities. For example, in military network is normally DTN, an encryptor (or commander) placed confidential information at a storage device, which is only be accessed by user (or soldiers) in "Battalion 1" who are participating in "Region 1." In this condition, it is to be considered that many key authorities are handled their self attributes for user (or soldiers) who are participating in their regions. But in this case a issue raised that soldiers or users could be continuously changed their place. Main motivation to this topic is in decentralized DTN, issue to use multiple authorities and these authorities handled their self attribute keys independently.

The attribute-based encryption (ABE) is technique which is effective approach which access information securely in DTNs. ABE has a technique in which encryption is carried out based on user attributes and policies are defined over encrypted data. In ciphertext-policy ABE (CP-ABE) scheme, in which encryptor encrypts some attribute sets that decryptor required to follows those to decrypt the ciphertext information. Hence, different users are permitted to decrypt data as they satisfy the policies which are provided by encryptor (or data owner).

However in DTNs, by applying the ABE arises many security and privacy challenges. First challenge is key revocation that is updation of key for each attribute is required to provide security. This case arise when users (or decryptor) could be change their attributes at some turn, or key authorities might be compromised some private keys, since each attribute is shared by multiple users. Attribute key must be changes immediately for backward and forward secrecy.

Next challenge is key escrow problem. In CP-ABE, the key authority has master secrete key. By applying this master secrete key to users associated attribute set, authority creates private keys of users. Thus, every ciphertext addressed to specific users could be decrypted by key authority that can create their attribute keys. Also adversaries can compromise key authority in the hostile environments. When the data is more sensitive then this could be a powerful threat to the data confidentiality or privacy.

Attributes are issued from different authorities and coordination of these attributes is become last challenge. Over attributes issued from different authorities, it is very hard to define fine-grained access policies when multiple authorities handled and attribute keys issued to users independently with their own master secrets key.

2. PROBLEM STATEMENT

The military applications are requires to increased protection of a confidential data including access control methods. In many cases, it is a desirable to provide a differentiated access services that a Data access policies are defined over a user attributes or a roles, which are managed by the key authorities.

3. LITERATURE SURVEY

Attribute Based encryption (ABE) is classify into two way, key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In key-policy ABE, the encryptor only has tags of ciphertext addition to an attributes set. The authority of key

selects an access policy for each user that notify which ciphertext information user can decrypt and generate the key to each user by taking use of the policy into the user's key. In CP-ABE, an access policy selected by an encryptor is used to encrypt the ciphertext, but a key is normally generated using a set of attributes.
Thus, CP-ABE is more suitable and efficient to DTNs as compared to KP-ABE.

3.1 Attribute Revocation

First key revocation method in CP-ABE and KP-ABE introduced by Bethencourt *et al.* and Boldyreva *et al.* respectively. In this method solutions are to update each attribute up to time (or expiration date) and distribute a new key set to authenticate users after the expiration of time. The periodic attribute revocable ABE schemes arise two main troubles.
The first one is degradation of the security in form of the backward and forward secrecy. In this scenario, users (or soldiers) may vary their attributes repeatedly, e.g., place or location change when assumed these as attributes. Then, a soldier (or user) who currently holds the attribute might be allow to retrieve the earlier data encrypted previous he get the attribute until the data is re-encrypted using the newly revoked attribute keys by periodic rekeying (backward secrecy).
The scalability is other trouble. After a periodic time, the key authority declares a key append material by unicast at each time-slot so that all of the users who are nonrevoked can append their keys. This outputs "1-affects-n" trouble, which means that the append of a single one attribute affects to all other nonrevoked users who have shares of the attribute. This results a bottleneck for both the key authority and all nonrevoked users.

3.2 Key Escrow

Many of the presented ABE methods are built on the infrastructure in which a single central authority generate the all private keys of users using its own master secret information. Thus, the key escrow problem is arising as in this situation the key authority can decrypt every ciphertext related to users in the system by creating users secret keys at any instance.
So, a distributed KP-ABE technique is introduced by Chase *et al.*. This scheme gives solution to the key escrow trouble in a multiauthority system. In this scheme, all (different) attribute authorities are get participated in the key creation protocol in a distributed manner such that they cannot group their data and connects multiple attribute sets belonging to the same user. One drawback of this fully distributed scheme is, has no central authority that has information of master secret. To create a user's secret key whole authority of attributes should contact with each other in the system.

3.3 Decentralized ABE

In the multiauthority network environment, Roy *et al.* introduced a decentralized CP-ABE technique. In this technique, a collective access policy is applied on the attributes issued from different authorities that are normally encrypting data multiple times. The main drawbacks of this technique are access policy expressiveness and efficiency. As example, when a commander (or major) such as encryptor encrypts a secret mission (confidential data) to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be articulated when each "Region" attribute is handled by different authorities, thus normal multi-encrypting techniques can by no means express any general "-out-of-" logics (e.g., OR, that is 1-out-of-n). For example, let $A_1,\ldots,A_N$ is authorities of key, and $a_1,\ldots,a_N$ is sets of attributes that authorities independently handled, respectively. Then, the only access policy is defined with $a_1,\ldots,a_N$ is (a_1 AND… AND a_N) , which can be evaluated by encrypting a plaintext message with a_1 by A_1 , and then resulting ciphertext C_1 is encrypting with a_2 by A_2 (where C_1 is the ciphertext encrypted using a_1), and then resulting ciphertext C_2 is encrypting with a_3 by A_3, and so on. This multi-encryption process continue until create the final ciphertext C_N. Hence, the access logic should be only AND, and needs N iterative encryption operations where N is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require more computation and storage costs. Multiauthority KP-ABE and CP-ABE technique are introduced by Chase and Lewko *et al.* respectively. However, these techniques also arises the key escrow problem as in decentralized technique.

4. EXISTING TECHNIQUE

CPABE: There are many existing technique, are used to secure data. These techniques are traditional public key encryption, attribute based encryption (ABE) and identity based encryption (IBE). These techniques allow party to encrypt data to particular user but unable to efficiently handle more expressive type of encrypted access control. Along this problem, these techniques have another problem such as lack of security against collusion attack and key revocation in which attacker might obtain multiple private keys. To address those problems, a technique is implemented by J. Bethencourt, A. Sahai, and B. Waters , called ciphertext policy-attribute based encryption (CP-ABE). This technique allow new type of encrypted access control where user's private key are specified a set of attribute and party encrypting data can specify a policy over these attribute specifying which user are able to decrypt. This technique resistant to collusion attack and address problem of key revocation.

CPABE with PRE: In ciphertext policy-attribute based encryption (CP-ABE), user holds set of attributes data is encrypted with access structure on attributes. A user is able

to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure. Now a day, computing technologies becomes a popular for more people to store their private data on third party server for sharing of data. While storing of data on third party, their concern about data security arise that people would like to share their private data only to authorized users. So there is also need of differential access services such as data access policies over attribute and role. So there are many traditional access control strategies implemented but are not effective for different trusted domain, and third party are not fully trustworthy. To overcome this issue of attribute revocation for attribute based system, a technique is implemented by S. Yu, C. Wang, K. Ren, and W. Lou. This technique combine ciphertext-policy attribute based encryption (CP-ABE) with proxy re-encryption (PRE). PRE enable third party to convert (proxies) a ciphertext encrypted by one party to another ciphertext that can decrypted by other party without reveal of plaintext. This method minimize load on authority upon attribute revocation task and provide security against chosen ciphertext attack. But this method require continuous online and honest proxy server.

IBE with AKI: In identity-Based Encryption (IBE) cipher-text are associated with identity of user to protect confidentiality of user data. But there is a trusted authority; called Key Generation Center (KGC) can simply generate user's private keys after user authentications using KGC's master secrete key to user identities. This system has main disadvantage is key escrow problem, that KGC could decrypt any message of user by generating user's private key. There are many IBE techniques implemented such as Boneh-Franklin's IBE (BF-IBE), Hierarchical ID-Based Encryption (HIBE), Sakai and Kasahara IBE (SK-IBE). These techniques improve security reduction but fail to address key escrow problem. So technique is implemented by S. S.M. Chow [15], uses Anonymous Key Issuing protocol (AKI) to protect confidentiality of user's identities. Technique employs non colluding two parties which separate the tasks of authentication and key issuing called Identity-Certifying Authority (ICA) and KGC. By employing two non colluding parties system removes key escrow problem addressed in Identity based encryption.

5. SECURE CPABE SCHEME WITH 2PC

DTN architecture involves system design and security model.

5.1 System Design

Following figure shows the architecture of the DTN. The architecture consists of the following system modules.

1) *Key Authorities:* Key authorities are key creation centers that create parameters of public/secret keys for CP-ABE. The key authorities involve central authority and many local authorities. Consider, during the initial key setup and creation phase: communication channels between a central authority and each local authority are secure and reliable. Each local authority handles different attributes and issues related keys of attributes to users. They allow different access rights to different users corresponding to attributes of users. The key authorities are considered as honest-but-curious. This means, key authority executes their tasks in the system honestly; however they can learn information ciphertext which is encrypted data as much as possible.

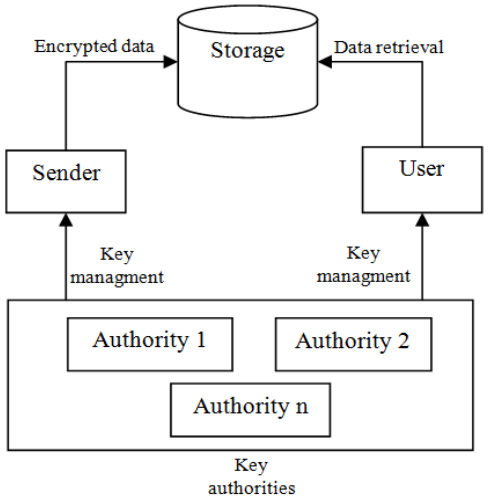

Fig. Architecture of secure data retrieval in a disruption-tolerant network.

2) *Storage node*: Storage node is other entity of DTN architecture that stores encrypted content received from senders and allow different user to access corresponding attributes. It can be movable or stationary. As key authorities can be semi trusted, also considered the storage nodes are to be semi-trusted, that means honest-but-curious.

3) *Sender*: Third entity is a sender, who has secrete content or data (e.g., major a commander) and wants to save this data in the external data storage node for purpose to sharing or for reliable delivery to users (or soldiers) in the challenging networking environments. A sender decides access policy for each user and before storing data in the storage node, sender applies this access policy on its own content by encrypting the data or content under the policy.

4) *User*: User (e.g., a soldier) is movable node who wishes to access or retrieve the content stored in the storage node by sender (or commander). If a user has an attributes set satisfying the access policy of the encrypted data decided by the sender, then he will be allow to decrypt the ciphertext and obtain the plaintext that is original data.

Thus the key authorities are semi-trusted, they should be debarred from accessing original data saved in the storage node; meanwhile, they also able to issues secret keys to users. To achieve this contradictory requirement, the central authority and the local authorities busy in the arithmetic 2PC protocol in addition with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol does not permit key authorities to know master secrets of each other's. Thus, no one of key authority can create the whole set of secret keys of

users alone. So, consider that the central authority does not collude or contact with the local authorities (If so, they can generate the secret keys of every user by sharing their master secrets).

5.2 Threat Model and Security Requirements

1) *Data Secrecy*: Users who are no authorized do not have sufficient credentials to access the policy should be debarred from accessing the plaintext that is original data in the storage node. Along this, access from storage node or key authorities who are such unauthorized should also be prohibited.

2) *Collusion-resistance*: If more than one user collude or group, by combining their attributes they may be able to decrypt an encrypted data even though each of the users cannot decrypt the ciphertext alone. We do not wish these user or colluders to become successful in decrypting the secret information by combining attributes they posses. Along this also assume collusion attack between curious local authorities to generate users' keys.

3) *Backward and forward Secrecy*: In the concept of ABE, backward secrecy defines that any user who holds an attribute and also satisfies the access policy should be prohibited from accessing the plain content of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy defines that any user who just drops an attribute should also be prohibited from accessing the plain content of the subsequently exchanged data after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

6. CONCLUSIONS

In many challenging environment, DTN techniques are becoming efficient solutions that permit wireless devices to communicate with each other and retrieve the secrete information stored at external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. Scheme introduced here is a method using CP-ABE provides secure data retrieval for decentralized DTNs where multiple key authorities manage their attributes independently. By enforcing secure Two Party Computation scheme between multiple parties involved in system, 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 and provide confidentiality of data.

REFERENCES

[1] 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.

[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] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *Proc. Conf. File Storage Technol.*, 2003, pp. 29–42.

[4] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[5] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep 2010.

[6] 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.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[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] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[10] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.

[11] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Comput. Surv.*, 2003.

[12] 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.

[13] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009.

[14] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.

[15] S. S.M. Chow, "Removing escrow from identity-based encryption," in *Proc. PKC*, 2009, LNCS 5443, pp. 256–276.

BIOGRAPHIES

Shivkanya Jadhav is pursuing her ME in Computer Networks from SCOE, Pune. She has done BE in Computer Science Engineering from MGM College Of Engineering, (SRTM University Nanded) in 2013.

Prof. N. G. Bhojane graduated in CSE from Dr. B.A.M. University Aurangabad in 2000 and completed M.E. in Computer Network from STES, Sinhgad College Of Engineering, Pune in 2012. He works with Sinhgad College of Engineering, Pune. His research interests are in the field of Soft Computing and image processing.