International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

Key Management Using CP-ABE For Secure Group Communication

[1]C.Vishal,[2]V.Sujananth,[3]T.TamilSelvan,[4]K.Rejini
[1][2][3] B.E, IV year students, Department of Computer Science and Engineering
[4]Assistant Professor of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.

Abstract — **Theconfidentiality is prominent in military environment and large scale network. Ciphertext-policy attribute-based encryption (CP-ABE) is a solution to the access control issues. Disruption-tolerant network (DTN) technologies are solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. But, introducing CP-ABE in DTN may cause some security issues. Most challenging issues are 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 whereimmediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. This mechanism helps to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network**

Index Terms — **Attribute based Encryption, Access Control, Cipher text Policy, Revocation,multiauthority.**

I. INTRODUCTION

people to easily share their data with others, using online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks; or sharing data in military environments. As we use the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to the data. It is important to make the sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-Based Encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. It provides a way of defining access policies based on different attributes of the requester, environment and the data object. Especially, Cipher text-Policy Attribute-Based Encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data as per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach such as the reference monitor Nevertheless, applying CP-ABE in the data sharing system has several challenges. In CP-ABE, the Key Generation Centre (KGC) generates private keys of users by applying

the KGC's master secret keys to users' associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storing public key certificates under traditional Public Key Infrastructure (PKI). However, the advantage of the CP-ABE comes with a major drawback which is known as a key escrow problem. The KGC can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems. Another challenge is the key revocation. Since some users may change their associate attributes at some time, or some private keys might be compromised, key revocation or update for each attribute is necessary in order to make systems secure. This issue is even more difficult especially in ABE, since each attribute is conceivably shared by multiple users.This implies that revocation of any attribute or any single user in an attribute group would affect all users in the group. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability.The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. This is due to the fact that the different

All Rights Reserved © 2015 IJERCSE

authoritiesgenerate their own attribute keys using their own independent and individual master secret keys.

A.RELATED WORK

Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access policy over attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. In several distributed systems a user should only be able to access data if a user possesa certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control . In a paper, they created public key revocation encryption systems with small cryptographic private and public keys. Their systems have two important features relating respectively to public and private key size. First, public keys in our two systems are short and enable a user to create a cipher text that revokes an unbounded number of users. This is in contrast to other systems where the public parameters bound the number of users in the system and must be updated to allow more users. Second, the cryptographic key material that must be stored securely on the receiving devices is small. Keeping the size of private key storage as low as possible is important as cryptographic keys will often be stored in tamper-resistant memory, which is more costly. This can be especially critical in small devices such as sensor nodes, where maintaining low device cost is particularly crucial . Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, the identities (e.g. emails or IP addresses) of the latter are sufficient to encrypt. Any setting, PKI- or identity-based, must provide a means to revoke users from the system. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority . Cipher text-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure. Beside this basic property, practical applications usually have other requirements . In cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. This provides fine-grained access control on shared data in many practical settings, e.g., secure database and IP multicast. The communication model is one-to-one, in the sense that any message encrypted using a particular public key can be decrypted only with the corresponding secret key. The same holds for identity-based encryption (IBE), where user public keys can be arbitrary bit strings such as email addresses.

I. EXISTING SYSTEMS AND PROPOSED SOLUTIONS

The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data storing center, fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system. Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information Thus, the key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users.

In this paper, we propose a novel CP-ABE scheme for a secure data sharing system. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme.

All Rights Reserved © 2015 IJERCSE

II. PROPOSED SOLUTION

In this paper, we propose a CP-ABE scheme for a secure data sharing system. The key issuing protocolgenerates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme. Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.Attribute Revocation as suggested by Bethencourt and Boldyreva.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 distributea new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy. 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. 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 reencrypted with the newlyupdated attribute keys by periodic rekeying (backward secrecy).For example, assume that at time, a ciphertext is encryptedwith a policy that can be decrypted with a set of attributes (embedded in the users keys) for users with . After time, say, a user newly holds the attribute set. Even if the new user should be disallowed to decrypt the ciphertext for the time instance, he can still decrypt the previous ciphertext until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypteddata even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute at time, he can stilldecrypt the ciphertext of the previous time instance unless the key of the user is expired and the ciphertext is reencryptedwith the newly updated key that the user cannot obtain. 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 theirkeys. This results in the "1-affects" problem, which meansthat the update of a single attribute affects thewhole nonrevokedusers who share the attribute. This could be a bottleneck for both the key authority and all nonrevoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses . To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance.This scheme will pose overhead group elements, additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme of Bethencour*tet al.* , where is the maximum size of revoked attributes set. Golle also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the universe size.

III. NETWORK ARCHITECTURE

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

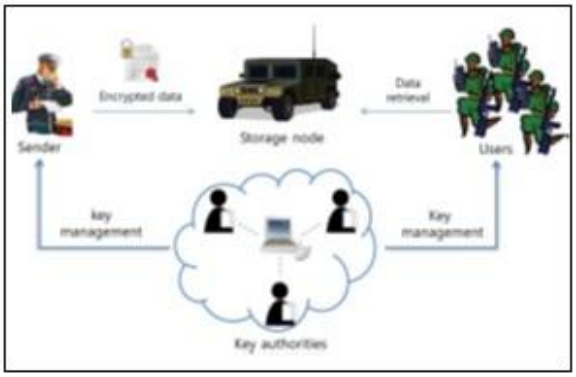

Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network.

A. System Description and Assumptions

Fig. 1 shows the architecture of the DTN. As shown in Fig. 1, the architecture consists of the following system entities.

1) Key Authorities:It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Key generation is the process of generating keys for

All Rights Reserved © 2015 IJERCSE

cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

2) Storage node: It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. Data storing centre store the data. Data Storage Centres provides offsite record and tape storage, retrieval, delivery and destruction services.

.

3) Sender: It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

4) User: This is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data.

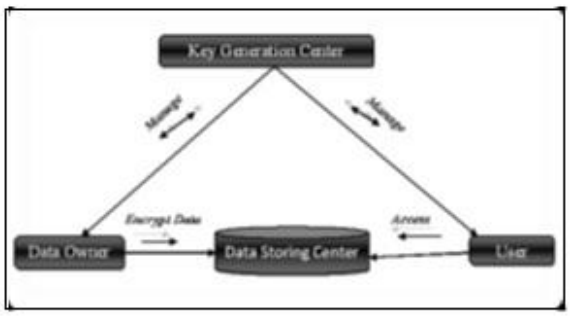

Fig. 2. Node Structure of a Data Sharing System

The node structure of the Attribute based data sharing system is shown in Fig. 2. The nodes involved are admin and clients which stands as UI for the system. The nodes are Key Generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storing center is an entity that provides a data sharing service. The data storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce afine-grained user access control. It is a client who owns data, and wishes to upload it into the external data storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. User is an entity who wants to access the data.

A. Functional Requirements

The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme.

B. Non Functional Requirements

Efficiency Attribute Based Data Sharing System encrypting the content, hence solving the performance degradation problem of distributed approach.

IV. PROPOSED SCHEME

we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements

1.Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.**2.**Encryptors can define a fine grained access policy using a monotone access structure under attributes issued from any chosen set of authorities.**3.**The key escrow problem is resolved by an escrow free key issuing protocol that exploits the characteristic of the decentralized DTN architec

CONCLUSION

To achieves more secure and fine-grained data access control in the data sharing system. We demonstrated that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system. Data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials.

All Rights Reserved © 2015 IJERCSE

FUTURE ENHANCEMENT

In the future, it would be interesting to consider attribute-based encryption systems by applying advanced cryptosystem for data sharing. In future, we encrypt multimedia content, Solve the performance degradation of fully distributed approach, Neglected key expired time, we can use multi Data Storing Centre, Proxy servers to update user secret key without disclosing user attribute information.

REFERENCES

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

[2] JunbeomHur and Dong Kun Noh, ―Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems‖, IEEE Transactions on Parallel and Distributed Systems, pp 1214-1221, 2011.

[3] Lewko, Allison; Sahai, Amit; Waters, Brent, ―Revocation Systems with Very Small Private Keys‖, Security and Privacy (SP), IEEE Symposium, May 2010, 978-1-4244-6895-9, pp 273 – 285, 2010.

[4] Alexandra Boldyreva, VipulGoyal, Virendra Kumar, ―Identity-based encryption with efficient revocation‖, Proceedings of the 15th ACM conference on Computer and communications security, ISBN: 978-1-59593-810-7, pp 417-426, 2008

[5]Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, ―Attribute based data sharing with attribute revocation‖, Proceedings of the 5th ACM Symposium on Information, ISBN: 978-1-60558-936-7, pp 261-270, 2010.

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

[7] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policyattribute-based encryption (CP-ABE) system for the DTNs," LehighCSE Tech. Rep., 2009

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

[9] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures andnoninteractive anonymous credentials," in *Proc. TCC*, 2008, LNCS 4948, pp. 356–3747

All Rights Reserved © 2015 IJERCSE