Secure Data Retrieval in Wireless Networks Using Advanced Encryption System

[1]Ms.Shanthi.S, [2]Nagenthra Babu.J,
[1,]Assistant Professor,[2]B.E Stuent,
[1,2,]Department Of Computer Science and Engineering
[1,2,]Valliammai Engineering College, Chennai,India,Tamilnadu

---

***Abstract* - The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the descriptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy.In the large number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. Portable nodes in military environments, for example such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be successful results. Thus a new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. We demonstrate how to apply the proposed mechanism to safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network**

***Index Terms* - Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval**

I. Introduction

The design of the current Internet service models is based on a few assumptions such as (a) the existence of an end to-end path between a source and destination pair, and (b) low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Some examples are: (i) battlefield ad-hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped with wireless modems and have intermittent RF connectivity with one another.

In the above scenarios, an end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic ,predictably connectable, or periodically connected. To allow nodes to communicate with each other in these extreme networking environments, Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other. Typically ,when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. After the connection is eventually established, the message is delivered to the destination node.

Roy and Chuah introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. A requirement in some security-critical applications is to design an access control system to protect the confidential data stored in the storage nodes or contents of the confidential messages routed through the network. As an example, in a battlefield DTN, a storage node may have some confidential information which should be accessed only by a member of „Battalion 6" or a participant in „Mission 3". Several current

solutions follow the traditional cryptographic-based approach where the contents are encrypted before being stored in storage nodes, and the decryption keys are distributed only to authorized users. In such approaches, flexibility and granularity of content access control relies heavily on the

underlying cryptographic primitives being used. It is hard to balance between the complexity of key management and the granularity of access control using any solutions that are based on the conventional pair wise key or group key primitives. Thus, we still need to design a scalable solution that can provide fine-grain access control. That is a DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

In this paper, we describe a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the users private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt. Our scheme can provide not only fine-grained access control to each content object but also more sophisticated access control antics. Ciphertext-policy attribute-based encryption (CP-ABE) is a guaranteeing

cryptographic answer for the right to gain entrance control issues. In any case, the

issue of applying CP-ABE in decentralized DTNs presents a few securities and

protection challenges as to the property disavowal, key escrow, and coordination of characteristics issued from distinctive powers.

A. Contribution

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the users key. However, the roles of the ciphertexts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes

B. System Design

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. 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 underattributes 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 DTN 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. NETWORK ARCHITECTURE

In this section, we describe the DTN architecture and define the security model
Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network

A. System Entities

key generation: User Interface Design plays an important role for the user to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user name and password. It will check username and password is match or not (valid username and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user name and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. Here we validate the login user and sever authentication.

2)Storage Nodes: The user will upload some data's in the User Page. The system will calculate size of the file and sends through Storage node. Therefore storage node can get the data without traffic and also transmit the data in less time. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme. This is an entity that stores data from senders and provide corresponding access to users. We also assume the storage node to be semi trusted, that is honest-but-curious.

3) Story –carry and Forward: This is an entity 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 reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node. If a user possesses 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.

4) Users:

This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses 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.

5) Decentralized user: Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users. In order to realize this somewhat contradictory requirement, 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 others master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).
Analysis: we are going to develop the overall process in 2PC protocol file sharing concept and user satisfied trust worthiness. Then how long user touch with network and one more thing what type of file sharing and when it is user file sharing with time and date is calculated. After that we are calculated how many user using in some network based on to the trust implemented in user satisfactions.
B . Advantages

1) Securacy of Data : 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.

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. Challenges:
The problem of applying CP-ABE in decentralized disruption tolerant networks introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

III. PROPOSED SCHEME

Thus extending user validation for set of attribute in authentication of multiauthority network environment. We can hide the attribute in access control policy of a user. Different users are allowed to decrypt different pieces of data per the security policy. We going to achieve the data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes. The multi key authority is such no longer as well as the storage node in unauthorized user. In confidentially data of authority issues set of attribute keys for their managing attributes to an authenticated user. The trusted authority is analysis by values of distributed identically.

Fig 2 : Access Control via CP-ABE

Key Generation: 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.
It is easy to Retrieve user profile information of communication in networking system *Key Update*: When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively.The key update procedure is launched by sending a join or leave request for some attribute group from a user who wants

to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute groups, it notifies the storage node of the event. Without loss of generality, suppose there is any membership change in (e.g., a user comes to hold or drop an attribute at some time instance).

IV. CONCLUSION:

It is an endeavour attempt to have a precise scenario of what the terms "secure data retrieval for decentralized disruption tolerant network" is meant to be and its
implementation as well on which we are currently working. As stated before, our proposed system can enhance the security of military network by using CP-ABE mechanism. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. 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 uit is easy to retrieve user log information in the network. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.
[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Message ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM Mobi Hoc*, 2006, pp. 37–48.
[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] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
[6] 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.
[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.
[8] 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.
[9] 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.
[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.
[12] 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.
[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 334.
[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.
[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.
[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.
[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in *Proc. ACM Conf. Computer. Commun. Security*, 2006,
[18] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Computer. Surv.*, vol. 35, no. 3, pp. 309–329, 2003.
[19] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288.
[20] 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.
[21] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.
[22] V.Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.
[23] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. ASIACCS*, 2009, pp. 343–352.

[24] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attri[25] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.
[26] S. S.M. Chow, "Removing escrow from identity-based encryption," in *Proc. PKC*, 2009, LNCS 5443, pp. 256–276.
[27] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in *Proc. TCC*, 2008, LNCS 4948, pp. 356–374.
[28] M.Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss,A.Hysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in *Proc. Crypto*, LNCS 5677, pp. 108–125.
[29] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proc. CRYPTO*, 2001, LNCS 2139, pp. 41–62.
[30] C. K.Wong,M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proc. ACM SIGCOMM*, 1998, pp. 68–79.
[31] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol. 29, no. 5, pp. 444–458, May 2003.
[32] K. C. Almeroth and M. H. Ammar, "Multicast group behavior in the Internet's multicast backbone (MBone)," *IEEE Commun. Mag.*, vol. 35, no. 6, pp. 124–129, Jun. 1997.
[33] "The Pairing-Based Cryptography Library," Accessed Aug. 2010 [Online].
Available: http://crypto.stanford.edu/pbc/ bute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.