International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 5, Volume 2 (May 2015) www.ijirae.com

Secure Information Retrieval from DTN

Mr. Ajay Kapase*
Computer Networks
Flora Institute of technology, Pune

Mr. Pankaj Chandre.
Computer Networks
Flora Institute of technology, Pune

Abstract— In several distributed systems a user should only be able to access data if a user posses a certain set of attributes or credentials. For example, in military environments like as a battlefield or a hostile region are possible to go through intermittent network connectivity and frequent partitions. Disruption Tolerant Network (DTN) technologies are planned to allow mobile nodes in such environments to converse with each other. Some application scenarios necessitate a security design which provides fine grain access control to contents stored in storage nodes contained by a DTN or to contents of the messages routed throughout the network. Ciphertext-Policy Attribute Based Encryption (CP-ABE) is a capable cryptographic primitive for fine-grained access control of collective information. CP-ABE provides an encrypted access control technique for broadcasting messages. On the other hand, the issue of applying the ABE to DTNs defines some security and privacy challenges like key escrow, Attribute Revocation. This paper introduces a protected data retrieval system using CP-ABE for decentralized Tolerant Networks (DTNs) where many key authorities manage their attributes separately.

Keywords— Disruption-tolerant network (DTN), Ciphertext-policy attribute-based encryption (CP-ABE), attribute-based encryption, secure data retrieval.

I. INTRODUCTION

The structure of the existing Internet service models is anchored in a few assumptions for example (a) the existence of an end-to-end path among a source and destination pair, and (b) low round-trip latency among every node pair. Though, these assumptions do not hold in several emerging networks. Several instances [4] are: (i) battleground ad-hoc networks in which wireless devices approved by soldiers manage in hostile environments where overcrowding, environmental factors and mobility might cause momentary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped by means of wireless modems and contain intermittent RF connectivity with one and more.

In the above conditions, a sideways pathway between a source and a destination pair possibly will not forever exist where the links stuck between intermediate nodes may be predictably connectable, opportunistic, or periodically associated. Recently the research community has projected an innovative architecture known as the disruption tolerant network (DTN) to let nodes to communicate with one other in these tremendous networking environments. In numerous military network structures, connections of wireless devices approved by soldiers perhaps provisionally disconnected by congestion, mobility, environmental factors, particularly when they function in hostile environments. Disruption tolerant network (DTN) technologies are becoming doing well results that allocate nodes to broadcast with every other in these tremendous networking environments.

Numerous distributed file and data systems necessitate composite access-control structures, where access choice depend on attributes of the protected information and access policies allow to users. Conventionally, such access control systems have been obligatory by a server that acts as a confidential orientation monitor; the monitor will access a consumer to view information simply if his way in policy allows it. While the utilization of trustworthy servers allows for a comparatively straightforward answer, there is a great drawback to this move towards both the servers and their storage has to be trusted and stay uncompromised. By means of the rising number of virus attacks and previous forms of interruption, maintaining the safety of any exacting host is becoming more and more difficult. This issue is exacerbated in more systems where receptive data must be simulated across some servers for the reason of survivability and scalability things. A usual answer to this issue is to encrypt stored data so as to decrease data vulnerability in the incident that a storage server is compromised. Though, usual public-key encryption techniques require that information be encrypted to single particular user's local key (public key) and are inappropriate for expressing other complex access control policies. The idea of attribute-based encryption (ABE) is a capable approach that fulfils the desires for protected data recovery in DTNs. ABE describes a method that allows an access control above encrypted information using access policies and credited attributes between private keys and cipher texts.

Attribute Based Encryption (ABE) comes in two types called Ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In KP-ABE, the encryptor simply brings to tag a Ciphertext along with a set of attributes. The key authority determines a policy for every user that decides which Ciphertexts he/she is able to decrypt and issues the key to every user by enclosing the policy into the user's key. Though, the acts of the keys and Ciphertexts are altered in CP-ABE. In CP-ABE, the Ciphertext is encrypted through an access policy determine by an encryptor, however a key is only produced regarding set of attributes. CP-ABE is more suitable to DTNs as compare to KP-ABE because it facilitate encryptors for instance a commander to decide an access policy on attributes and also to encrypt private data below the access structure by means of encrypting with the equivalent public keys or attributes.

However, the issue of employing the ABE to DTNs produces several privacy and security challenges. Because most of users may modify their associated attributes at some point (for example, moving their area), or several private keys might be negotiated, key revocation (or modification) for every attribute is essential so as to make systems secure and protected. Though, this problem becomes more difficult, particularly in ABE systems, because every attribute is possibly shared by numerous users (hereafter, consign to such a group of users as an attribute collection). This signifies that revocation of whichever attribute or whichever particular user in an attribute group would influence the other users present in the group. For instance, if a user ties or leaves an attribute group, the connected attribute key should be altered and again redistributed to every other member in the identical group for forward or backward secrecy. It may consequence in bottleneck throughout rekeying process or safety degradation due to the windows of susceptibility if the preceding attribute key is not modified immediately.

The rest of paper is organized as follows: Section II gives the essential background. Section III addresses contribution. Section IV introduces the system architecture. Section V describes assumptions and security Requirements. In Section VI system flow is explained shortly. Section VII concludes the paper.

II. LITERATURE REVIEW

S. Roy [5] and P. Yang [6] introduces data storage nodes in DTNs where user information is replicated in this way that just authorized mobile nodes be able to access the essential information speedily and efficiently.

In Paper [5] authors S. Roy and M. Chuah introduced an access control mechanism which is depending on the Ciphertext Policy Attributed-Based Encryption (CP-ABE) paradigm. The system provides a supple fine-grained access control in such way that the encrypted data can be accessed by only authorized users. System provides two unique features: (i) the incorporation of dynamic attributes whose cost may vary over period, and (ii) the revocation characteristic.

In Paper [6] M. Chuah, P. Yang explored that how a Content based information retrieval scheme can be deliberate for DTNs. There are three significant design errors, specifically (a) how should information be replicated and how can it be stored at numerous nodes, (b) how should a query be distributed in lightly connected networks, (c) how should a query reply be routed back to the querying node.

In paper [8] Luan Ibraimi et al. propose a new system intended for attribute revocation in CP-ABE known as mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE). In this system the secret key is divided into two parts, first share for the mediator and the second for the user. To decrypt the information, the user is required to contact the mediator to accept a decryption token. The mediator conducts an attribute revocation list (ARL) and trashes to problems the decryption token for revoked attributes. Devoid of the token, the user cannot decrypt the ciphertext, thus the attribute is completely revoked.

In [9] author N. Chen et al. introduced fading function, which provides attributes ”dynamic” and allows us to modify every one of them independently to keep CPU bandwidth, resources and time. This indicates a user can modify or update partial attributes, more willingly than all of them, in one modification.

In [11] A. Lewko and B. Waters propose a Multi-Authority Attribute-Based Encryption (ABE) methodology. In this scheme, several parties can become ability and there is no obligation for any public coordination except the construction of a primary set of ordinary reference parameters. A party can basically act as an ABE authority by generating a public key and sending private keys to various users that replicate their attributes. A user can encrypt information in provisions of any Boolean formula over attributes send from every chosen set of authorities. At last, their system does not need any central authority.

J. Bethencourt et al. provide construction of a ciphertext-policy attribute-based encryption (CP-ABE). In this system, a user’s private key will be related with a random number of attributes uttered as strings. Conversely, when a party encrypts a message in stated scheme, they specify related access structure over attributes. In this, a user will be able to decrypt a ciphertext if and only if user’s attributes pass all the way through the ciphertext’s access formation [14].

III. PROPOSED SYSTEM

To solve ABE related problems, this paper addresses an attribute-based secure information retrieval mechanism using CP-ABE for decentralized DTNs. The proposed system features the subsequent achievements. (i) Instantaneous attribute revocation increases forward/backward secrecy of confidential information by decreasing the windows of vulnerability. (ii) Encryptors can explain a gentle access policy by means of any monotone access arrangement under attributes send from several chosen set of authorities. (iii) The key escrow issue is determined by an escrow-free key issuing protocol that accomplished the characteristic of the DTN architecture. The key publishing protocol creates and issues user secret keys by operating a secure two-party computation (2PC) protocol between the key authorities with their own master secrets. The 2PC protocol obstructs the key authorities from accessing any master secret data of each other like none of them could create the whole set of user keys without help. Therefore, users are not necessary to fully faith the authorities with the intention of protect their information to be shared. The information privacy and confidentiality can be cryptographically imposed against any inquisitive key authorities or data storage nodes in the proposed system. This paper provides a multiple authority CP-ABE system for secure information retrieval in DTNs.

Every public authority issues incomplete modified and attribute key components to a user by operating secure 2PC protocol with the middle authority. Every attribute key of a user can be modified independently and instantly. Hence, the security and scalability can be improved in the proposed system.

IV. PROPOSED ARCHITECTURE

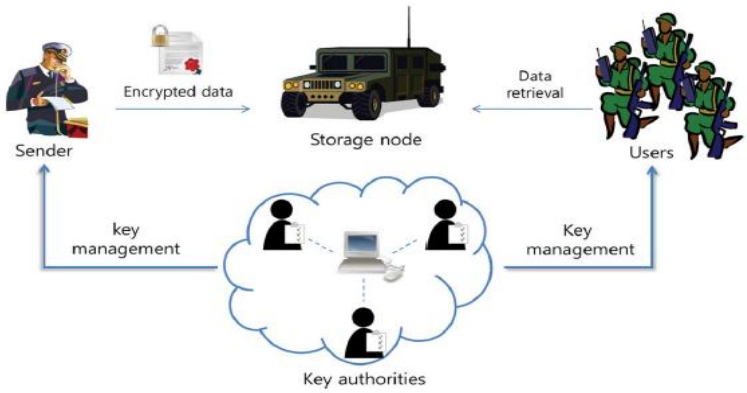

Fig. 1 Architecture of secure data retrieval in a military DTN

As in figure 1, the entities can explain as follows.

A. *Key Authorities*

Key Authorities are key generation middle that generates parameters like public/private key for CP-ABE. The key authorities consist of subsist authority and various local authorities.

B. *Storage node*

This is an entity that stores information obtains from senders and forward equivalent access to users. Storage node may be mobile or static [5], [6] depend on application in which it is used.

C. *Sender*

This is an entity that self confidential messages or information (e.g., a commander in case of military) and desires to store these messages into the external information storage node for simplicity of data sharing or for consistent delivery to users in the intense networking environments. A sender is dependable for essential (attribute based) access policy and accomplishing it on its own data by encrypting the information under the policy previous to storing it to the storage node.

D. *User*

This is a node who requests to access the information stored at the storage node (e.g., a soldier in case of military). If a user possesses a set of attributes fulfilling the access policy of the encrypted data distinct by the sender, moreover is not revoked in any attributes, so that then user will can decrypt the Cipher text and get the original data.

V. ASSUMPTIONS AND SECURITY REQUIREMENTS

A. *Assumption*

In case of Key Authorities and storage nodes suppose that there are secure and dependable communication channels among a central authority and each local authority throughout the initial key setup and creation stage. Every local authority handles different attributes and issues consequent attribute keys to users.

In this allowance discrepancy access rights to individual users depend on the users' attributes. The key authorities are supposed to be truthful but inquisitive. Specifically, authorities will sincerely execute the given responsibilities in the scheme; conversely they would resemble to learn data of encrypted contents to the extent that possible.

B. *Security Requirements*

1. Unauthorized users who do not enclose enough credentials fulfilling the access policy should be blocked from collecting the simple user information in the storage node. And also, illegal access from the key authorities or storage node should be in addition prevented.
2. If numerous users get together, they may be capable to decrypt a Cipher text by concatenating their attributes still if every one of the users cannot decrypt the Cipher text by himself. Furthermore believe collusion attack between interested public authorities to get users' keys.

In the circumstance of ABE, the backward secrecy wealth one user who that satisfies the access policy (i.e. who comes to hold an attribute) should be prohibited from bringing the plaintext of the preceding data exchanged before user holds the attribute. In contrast, forward secrecy wealth one user who drops an attribute should be prohibited from bringing the plaintext of the succeeding data altered subsequent to user drops the attribute, except the other convincing attributes that he is holding assure the access policy.

VI. SYSTEM CONSTRUCTION

A. The initial system setup phase

In this phase the trustworthy initialize decide a bilinear group G_0 of prime order p with generator g according to the security parameter. It also decides hash functions H: $\{0, 1\}^* \rightarrow G$.

B. Key Generation

Key authority and user generated public and private keys using this hash function. In this phase, the central authority first generates personal key and then generate attribute key.

C. Data Encryption

When a sender needs to bring its confidential information, he defines the tree access constitution above the creation of attributes encrypts the information under to implement attribute-based access control on the information, and stores it into the storage node.

D. Data Decryption

When a user receives the Cipher text from the storage node, the user decrypts the Cipher text with its secret key.

E. Revocation

One capable way to instantly revoke an attribute of detailed users is to re-encrypt the Cipher text with every attribute collection key and selectively share out the attribute collection key to authorized (non-revoked) users who are experienced with the attribute. On delivery every request query from a user, the storage node responds with message to the user.

F. Key Update

When a user gets to drop or hold an attribute, the equivalent key should be modified to avoid the user from accessing the preceding or succeeding encrypted information for forward or backward secrecy, respectively.

The key modification process is launched by distributing a leave or join request for a number of attribute collection from a user who requirements to hold or drop the attribute to the consequent authority. On receiving of the membership modify request for several attribute groups, it notifies the storage node of the result.

VII. CONCLUSIONS

This paper presented a CP-ABE system which is able to use in Disruption Tolerant Networks. To the access control and prevents data retrieval problems, CP-ABE is an extensible cryptographic solution. This paper projects a secure and efficient information retrieval technique via CP-ABE for decentralized DTNs where numerous key authorities handle their attributes separately. The problem of inherent key escrow is solved in such way that the privacy of the stored data is assured even under the antagonistic environment where main core authorities might be negotiated or not completely trusted. Additionally, the gentle key revocation can be complete for every attribute group.

ACKNOWLEDGMENT

This study has been supported by author Junbeom Hur and Kyungtae Kang member of IEEE, ACM.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang, “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks”, member IEEE, ACM, Feb 2014.
[2] 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.
[3] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
[4] M. M. B. Tariq, M. Ammar, and E. Zequra, “Mesage ferry route design for sparse ad hoc networks with mobile nodes,” in *Proc. ACM MobiHoc*, 2006, pp. 37–48.
[5] S. Roy andM. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.
[6] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” Cryptology ePrint Archive: Rep. 2010/351, 2010.

[12] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.
[13] 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.
[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.
[15] 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.
[16] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.
[17] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.
[18] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112..
[19] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Comput. Surv.*, vol. 35, no. 3, pp. 309–329, 2003.
[20] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288.
[21] 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.
[22] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.
[23] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.
[24] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. SIACCS*, 2009, pp. 343–352.
[25] M. Chase and S. S. M. Chow, "Improving privacy and security inmultiauthority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.
[26] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.
[27] S. S.M. Chow, "Removing escrow from identity-based encryption," in *Proc. PKC*, 2009, LNCS 5443, pp. 256–276.
[28] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in *Proc. TCC*, 2008, LNCS 4948, pp. 356–374.
[29] 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.
[30] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proc. CRYPTO*, 2001, LNCS 2139, pp. 41–62.
[31] C. K.Wong,M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proc. ACM SIGCOMM*, 1998, pp. 68–79.
[32] 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.

