EPH - International Journal of Science And Engineering
ISSN (Online): 2454 2016
Volume 07 Issue 03 September 2021

DOI:https://doi.org/10.53555/ephijse.v7i3.191

SECURED DATA RETRIEVAL IN MILITARY APPLICATIONS USING CP-ABE

Persi Pamela I[1]*, Ms. Moneeca. R[2], Ms. Gladys Persia Christiana.S[3] ,
*[*1]M.Tech, Assistant Professor, Department of Information Technology, Kingston engineering College, Vellore, Tamil Nadu, India,*
[2]Final year B.Tech (IT) student, Kingston engineering College, Vellore, Tamil Nadu, India,
Email: moneecashantha@gmail.com , Ph:9677690983
[3]Final year B.Tech (IT) student, Kingston engineering College, Vellore, Tamil Nadu, India,
Email: - gladystorm@gmail.com , Ph:7708734530

Corresponding Author:
Email: persipamela@yahoo.com , Ph: 9952528217

Abstract:-

Disruption-tolerant network (DTN) technologies are only solutions for military environment because of their mobile nodes irregular network connectivity and frequent partitions. But due to its nature of having external storage node during the transmission there is chance of getting exploited. Cipher text-policy attribute-based encryption(CP-ABE), is a good solution however, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.Some users (receivers) may change their associated attributes at some point (for example moving their region) here there is a need of attribute updation and also provides forward and backward secrecy for the attribute revocation problem. So we proposed a system that provides a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs a variation of the CP-ABE algorithm that overcomes the attribute revocation problem.

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

1.INTRODUCTION

In military network there is a problem prevails with connections of wireless devices carried by soldiers that may be temporarily disconnect environmental factors. Disruptiontolerant network (DTN) technologies remain a successful solutions . The messages from source node may need to wait in the intermediate nodes for certain time until the connection is established. Roy [9] and Chuah [13] introduced storage nodes in DTNs where only authorized mobile nodes can access the necessary information quickly.

For example, in a disruption-tolerant military network, a commander may store a confidential information at a storage node, which should be accessed bymembers of "Battalion 1" who are participating in"Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons,which could be frequently changed (e.g., the attribute repre-senting current location of moving soldiers) [14]. We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN [3].

Cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext [11]. Thus, different users are allowed to decrypt different pieces of data per the security policy.

The keys for encrypting and decrypting the data are provided by the encryptor where it remains two kinds of retrieval one for the data or content retrieval from the source node through intermediator and other key retrieval as the retrieved data will only be in encrypted form to decrypt it the decryptor is in need to access the key from source those who sat

However, the problem of applying the ABE to DTNs introduces several security and privacy challenges in existing system (refer figure 1).

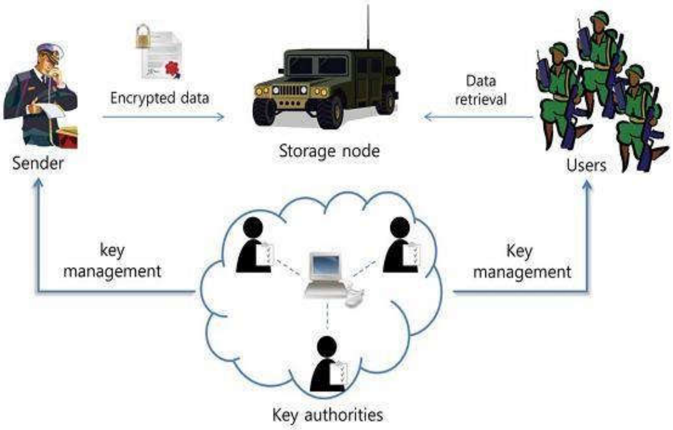

Figure 1: Existing System Architecture

Firstly, key revocation [15]-[16] (or update) which is the change in attributes at some point (for example, moving their region) for each attribute is necessary to ensure security.For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy.

Secondly, key escrow[24],[14],[13] problem. Inexisting model of CP-ABE,the key authority generates private keys of users by applying the authority's master secret keys to users associated set of attributes. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive that is shown in the existing working model (refer figure 3).

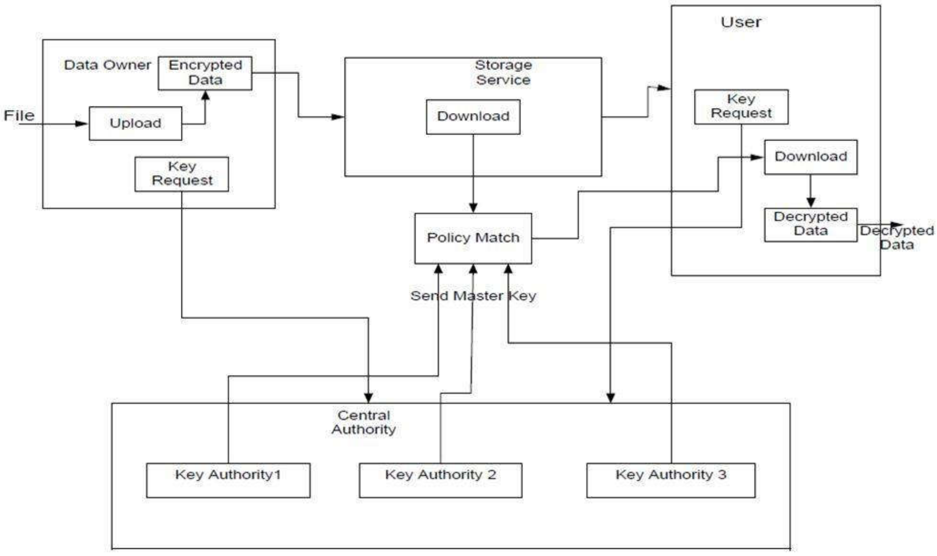

Figure 2: Working Model of Existing System

To overcome it in the proposed model the key generation are provided by the source where during key retrieval those who (decryptor) satisfies the access policies are only allowed to receive the key.

Third, coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently it is hard to define finegrained access policies over attributes issued from different authorities[9]. For ex-ample, suppose that attributes “role 1” and “region 1” are managed by the authority A, and “role 2” and “region 2” are man-aged by the authority B. Then, it is impossible to generate an access policy ((“role 1” OR “role 2”) AND (“region 1” or “re-gion 2”)) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented.Therefore, general access policies, such as “n-out-of-m” logic, cannot be expressed in the previous schemes, which is a very practical and commonly re-quired access policy logic.

2. Literature survey

D. Huang&M. Verma [1] they introduced a pathway between source and destination node using attribute based encryption.M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya [2] provided online data sharing systems such as Microsoft health vault, Google+, Facebook etc., renders security through promising cryptographic solutions *via CPABE.*A. Lewko and B. Waters [3], provided a purpose to act any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters.

Ostrovsky, A. Sahai, and B. Waters [4], they described about the secured access of data using storage nodes.M. Chase[5], “Multi-authority attribute based encryption,” There are control of policies needed for correct authentication of user & therefore the policies to retrieve the information.X. Liang, Z. Cao, H. Lin, and D. Xing [6], “Provably secure& efficient bounded ciphertext policy attribute based encryption, DTN technologies are designed to specific situations wherever it will tolerate noise, attacks etc which means that nodes will get confidential information with none loss.
R.
Yu, C. Wang, K. Ren,&W. Lou [7], “Attribute based data sharing with attribute revocation,” It explores about central-control revocation in CPABE environment, where the proposed key generation, encryption and decryption algorithms closely comply with CPABE model and key update algorithm is developed. S. Roy&M. Chuah [8], demonstrate how to apply the cp-abe in decentralized DTN to securely manages confidential data distributed in DTN. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker [9], “Mediated ciphertextpolicy attribute-based encryption and it application,” demonstrate how to apply mCP-ABE to securely manage Personal Health Records.
S.
J. Bethencourt, A. Sahai, and B. Waters [10], “Ciphertext-policy attributebased encryption,” This paper introduces the concept of attribute-based certificatless encryption system (ABCE), which is a new approach to mitigate the key escrow problem in attribute based Encryption scheme.M. Chase and S. S. M. Chow [11],It propose a solution which removes the trusted central authority &protects the users’ privacy by preventing the authorities. M. Chuah and P. Yang [12],explored about how a content based information retrieval system can be designed for DTN

N. Chen, M. Gerla, D. Huang, and X. Hong [13], provided a cryptographic based access control framework for vehicles to securely exchange messages in controlled fashion.
V. Goyal, O. Pandey, A. Sahai, and B. Waters [14], “Attribute-based encryption for finegrained access control of encrypted data,” Demonstrates the applicability of our construction to sharing of auto-log information and broadcast

encryption. A. Boldyreva, V. Goyal, and V. Kumar [15], An IBE scheme is proposed that significantly improves key update efficiency on the side of trusted party, while staying efficient for users.

3. Proposed system

In this section, the proposed model has two kinds of retrieval that are of content retrieval from source only if the decryptor satisfies the access policies he is allowed to access it also it will be in a decrypted form secondly it is of the key retrieval where again the decryptor request for key to the source satisfying the access policies. We also provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol [2] with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme.

3.1. System Architecture

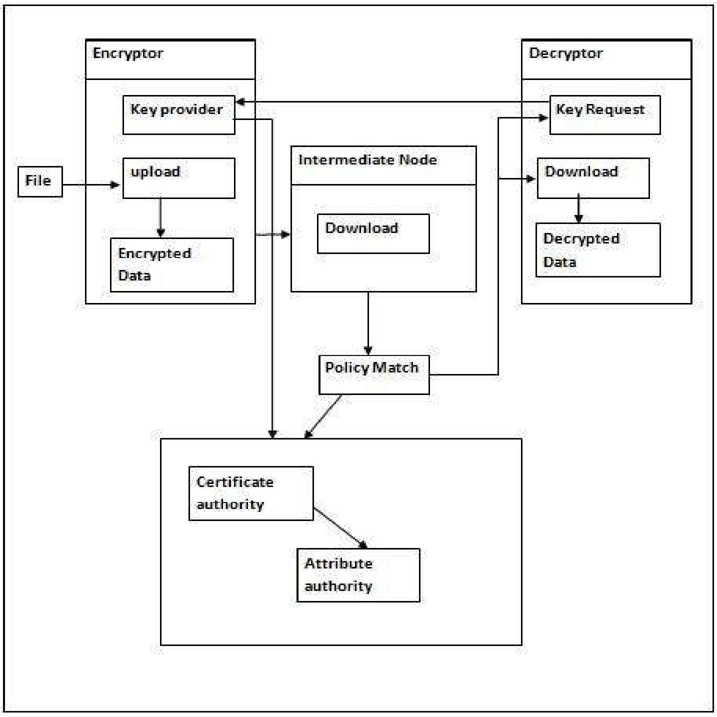

Figure 3: Proposed System Architecture

3.2 Module Description

Encryptor: An entity who owns confidential messages or data (e.g., a commander) to store them into the external data storage node.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. And the encryptor will provide the key for decryptor to encrypt.

Decryptor: A mobile node who wants to access the data stored at the storage node (e.g., a soldier) and the key from source. 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.

Central Authority: It handles two types of functions in it that are of certificate authority and attribute authority
Certificate authority: It allows to add any new users in to the military newtwork with their details and also to remove a personnel details who are not with in that military network.

Attribute authority: It provides the details of all the certified authority registered in the certificate authority with their details when connected.

Intermediary node: An entity that stores data from senders and provide corresponding access to users.It may be mobile or static. The storage node to be semi-trusted that is honest but-curious.

Revocation: Revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs.

One promising way to immediately revoke an attribute of specific users is to re-encrypt the cipher text with each attribute group key and selectively distribute the attribute group key to authorized (non-revoked) users who are qualified with the attribute.

3.3 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.

3.4 Algorithm Description:

Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encrypt (PK, M, A): The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

Key Generation (MK, S): The key generation algorithm takes as input from the source and a set of attributes S that describe the key. It outputs a private key SK.

Decrypt (PK, CT, SK): The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.
Delegate (SK, ~S): The delegate algorithm takes as input a secret key SK for some set of attributes S and a set ~S⊆S. It output a secret key~SK for the set of attributes ~S.

4. Conclusion and future enhancements

DTN technologies in military applications allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues.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.In addition, the fine-grained key revocation can be done for each attribute group. It demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.
The future enhancement focus on scope of proposed system can be extended to block unauthorized users and it can also be extended to encrypt and decrypt videos and other forms of data.

5. References

[1].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.

[2].M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in Proc. TCC, 2008, LNCS 4948, pp. 356–374.

[3].A. Lewko and B. Waters, "Decentralizing attribute-based encryption"Cryptology ePrint Archive: Rep. 2010/351, 2010.

[4].R. Ostrovsky, A. Sahai, and B. Waters, " SECURE ATC SURVEILLANCE FOR MILITARY APPLICATIONS," in Proc. ACM Conf. Comput.Commun. Security, 2007, pp. 195–203.

[5].L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

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

[7].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.

[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].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.

[10]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertextpolicy attribute-based encryption and its application,"in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

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

[12]. 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.

[13]. M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2007, pp. 1–7.

[14]. 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.

[15]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for finegrained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[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.