International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secure Data Retrieval Using CP-ABE Approach For Decentralized Disruption-Tolerant Military Networks

Karpe Navanath R. Patil Kalyani S. Panchabuddhe Priyanka P.

Student at JSPM"s ICOER, Wagholi, Pune-412207, India

Student at JSPM"s ICOER, Wagholi, Pune - 412207, India

Student at JSPM"s ICOER, Wagholi, Pune - 412207, India

Abstract: ***To undergo from continual partitions and infrequent network connectivity, the military environments mobile nodes are likely. The wireless devices carried by soldiers Disruption-tolerant network (DTN) technologies and to allow that wireless drivers, which are now find successful solutions for communication to each other and access the confidential information or command dependently by applying external storage nodes for retrieval of data securely and the update the policies, in this scenario Some of the most challenging issues are the authorization policies enforcement. A Cipher text-policy which is attribute-based encryption (CP-ABE) is the bright solution for the accessing the control issue. However, there introduced the many privacy and security challenges by the problem of applying CP-ABE Approach in decentralized DTNs with attention to the revocation of attribute, escrow of key, and attributes coordination taken from different authorities. In this paper, using CP-ABE we are going to propose a scheme which retrieves the data securely for decentralized DTNs where their attributes are independently managed by the multiple key authorities. In the disruption-tolerant military network for managing the confidential distributed data securely and efficiently, we determine how to apply the mechanism of proposed system.***

Keywords: Access control, Attribute-based Encryption (ABE),Multi-authority, Disruption-Tolerant Network (DTN), Secure Data Retrieval.

1. Introduction

Due to the factors of environment, mobility and jamming, wireless devices connections carried by soldiers may be disconnected for limited time, particularly when they are operating in hostile environments of military network scenarios. Through the DTN technologies, Nodes for contact with each other are becoming successful solutions in these environments of extreme networking. Typically, for the time in considerable amount, when there is no end-to-end contact between a source and a destination pair, until the connection would be ultimately produced, there may wait the messages from the source node in the transitional nodes. In DTNs Roy and Chuah introduced storage nodes that data is stored or reflect such that the required information efficiently and quickly can access by only and only authorized mobile nodes. Including methods of access control which are cryptographically enforced. In many cases, policies of data access `are defined over attributes of user or roles, it is desirable for providing the comprehend service access, which are handled by the key authorities.

The need for retrieval of data securely in DTNs are fulfill by the concept of ABE approach. By ABE, a mechanism features that enables an control of access over encrypted data using policies of access and ascribed attributes between cipher texts and private keys. Especially, a scalable way of encrypting data provided by CP-ABE such that to possess in order to decrypt the cipher text, the encrypt or defines the attribute set that the decrypt or needs. Thus, as per the security policy, by different users there are different pieces of data are decrypted.

However, there specify the many privacy and security challenges due to the problem of applying the ABE to DTNs. Since, at some point, associated attributes may be alter by some users or for system security, there might be compromised some private keys, and for each attribute is required the revocation of keys. However, especially in ABE systems, this concern is even more difficult, as a group of attribute, we refer to such a collection of users) since by multiple users, each attribute is maybe shared. This specify that, the other users in the group would be afflicted by revocation of any attribute or any single user in an attribute group.

The problem of key escrow is other challenge. In CP-ABE, by applying the master secret keys authority"s to users connect to the set of attributes, there produce private keys of users by key authority. Thus, by generating their attribute keys the key authority can decrypt each and every cipher text addressed to particular users. To the data privacy this could be a potential threat especially when the data is very important if the key authority is agreed by adversaries when deployed in the environments of hostile. To generate their own attribute keys with their own master secrets, the key escrow is amanly basic problem even in the many authority systems as long as each key authority has the whole authority. Since, based on the secret of single master, the mechanism of a generation of key is the basic methods used in most of the asymmetric encryption systems such as the CP-ABE is a significant open problem.

The last challenge is the attributes allocation taken from different authorities. Over attributes taken from disparate

authorities it is very difficult to define access policies of fine-grained when multiple authorities independently manage and issue attribute keys to users with their own secrets of master.

2. Literature Survey

ABE is has two policies which are ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, with a set of attributes, the encryptor only gets to label a cipher text. The user that determines which cipher text he can decrypt and also issues the key for each user by embedding the policy into the users key the key authority chooses a policy for that user. However, in CP-ABE the roles of the cipher texts and keys are reversed. To choose an access policy on attributes, CP-ABE is more suitable to DTNs than KP-ABE because it enables encryptor such as a commander and to encrypt intimate or intimate data under the access structure via encrypting with the corresponding public keys or attributes.

2.1 Attribute Revocation

The key revocation mechanism is suggested first by Be then court et al. and Boldyreva et al. in CP-ABE and KP-ABE algorithm, respectively. Their solutions are to affix to each attribute an expiration date (or time) and after the expiration, distribute a new set of keys to valid users. The two main problems have to the periodic attribute revocable ABE schemes.

In terms of the backward secrecy and forward secrecy the first problem is the security degradation. User‟s such as soldiers may varies their attributes frequently. After time, say, a user newly holds the attribute set. User can still decrypt the previous cipher text until it is re-encrypted with the newly updated attribute keys. Even if the newly added user should be disallowed to decrypt the cipher text for the time instance, a revoked user would still be able to access the encrypted data. For example, user can still decrypt the cipher text of the previous time instance unless the key of the user is expired.When a user is disqualified with the attribute at time and the cipher text is re-encrypted with the newly updated key that the user cannot obtain.

Scalability problem is another problem. By unicast at each time-slot so that all of the no revoked users can update their keys the key authority regularly announces a key update material. The update of a single attribute affects the whole no revoked users who share the attribute this results in the “1-affects-m” problem. For both the key authority and all no revoked users this could be a bottleneck. By reverse users using ABE that supports negative clauses, the immediate key revocation can be done.

2.2 Key Escrow

To generate the whole private keys of users with its master secret information, most of the existing ABE approach is based on the architecture where a single trusted authority has the potential. In this way, users of this system are generating their secret keys at any time; the key escrow problem is intrinsic such that the key authority can decrypt every cipher text addressed. In a multi-authority system Chase et al. presented a distributed KP-ABE approach that solves the key escrow problem in this approach. The performance degradation is the one disadvantage of this fully distributed approach. All attribute authorities should be communicate with each other in this system to generate a secret key of the user‟s, since there is no centralized authority with master secret information. To store additional auxiliary key components other than the attributes keys, where is the number of authorities in the system this results in communication overhead on the system setup and the rekeying phases and requires each user.

2.3 Decentralized ABE

In the multi-authority network environment Huang et al. and Roy et al. proposed decentralized CP-ABE schemes. Over the attributes issued from various authorities by simply encrypting data multiple times, they achieved a combined access policy. Efficiency and expressiveness of access policy are the main disadvantages of this approach. For example, under the policy (“Battalion 1” AND (“Region 2” OR „Region 3”)), when a commander encrypts a secret mission to soldiers.

3. Proposed System

In this paper, using CP-ABE approach we are proposing a secure data retrieval based on attribute for decentralized DTNs. The following performances are features by the proposed mechanism. First, by decreasing the windows of susceptibility, revocation of immediate attribute appreciate backward/forward secrecy of confidential data. Second, using access structure of any monotone under attributes taken from any chosen authorities set, a fine-grained access policy can defined by encrypt or. Third, by an escrow-free key issuing protocol the problem of key escrow is resolved that accomplishments the decentralized DTN architecture‟s characteristic. By performing a secure computation of two-party (2PC) protocol between the key authorities with their own master secrets, user secret keys generates and issues by the key issuing protocol. Thus, for protecting their data to be shared, there is no required for users to fully trust the authorities. In the proposed scheme the data confidentiality and privacy can be enforced cryptographically against any inquisitive key authorities or nodes of data storage.

4. Network Architecture

We describe the DTN architecture and defined the security model, in this section.

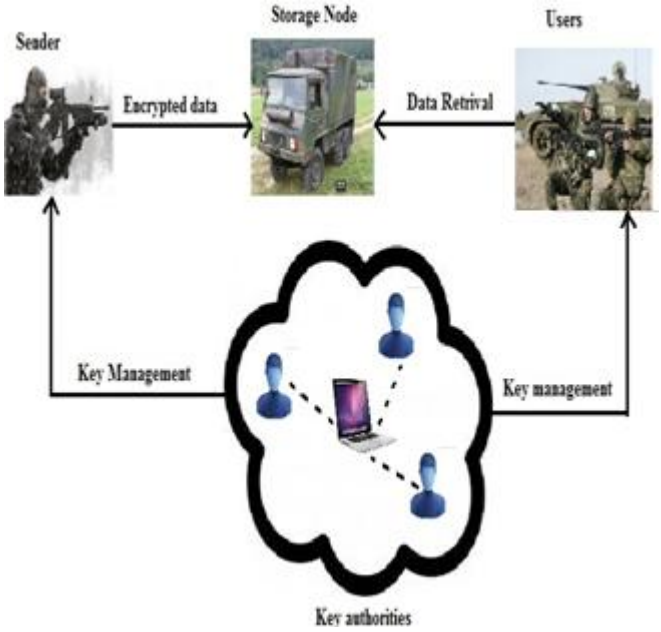

Figure 1: System Architecture

4.1 System Description and Assumptions

The architecture of the DTN is shows in figure 1. As shown in Figure 1, the architecture consists of the following system entities.

1) **Key Authorities:** for CP-ABE they are key generation centers that generate public/secret parameters. A Central authority as well as multiple local authorities are consist by the key authorities. During the initial setup of key and phase generation, we assume that between a central authority and each local authority, there are secure and reliable communication channels. Different attributes and issues corresponding attribute keys to users which are manages by each local authority. Differential access rights are grant by them to individual users based on the attributes of users‟. The key authorities are assumed to be honest-but-curious.
2) **Storage node:** This is an entity that data from senders are firstly stored and then it allow the user for corresponding access. It may be mobile or static. We also assume the semi-trusted storage node that is honest-but-curious which similar to the earlier schemes.
3) **Sender:** in the environments extreme networking for ease of sharing or for reliable delivery to users, this is an entity who owns confidential messages and that store them into the external data storage node. Before storing it to the storage node by encrypting the data under the policy, for defining access policy a sender is responsible and on its own data, enforcing it.
4) **User:** The users are the mobile nodes. The data stored at storage node are accessed by the user. For accessing the data of storage node, the user decrypt his cipher text if a user possesses a set of attributes satisfying the access policy of the encrypted data which is defined by the sender, and is not revoked in any of the attributes. In the storage node user‟s should be deterred from accessing plaintext of the data; Since the key authorities are semi-trusted, means that, to issue secret keys to users they should be still able. The central authority and the local authorities engross in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase in order to realize this somewhat contradictory requirement

4.2 Threat Model and Security Requirements

1) **Data Confidentiality:** For accessing the plain data from the storage node unauthorized users who do not have enough satisfying credentials the access policy should be deterred. In addition, from the storage node or key authorities, there should be also prevented unauthorized access.
2) **Collusion-Resistance:** If multiple users collude user may be able to decrypt a cipher textafterthe combination of their attributes even if each of the users cannot decrypt the cipher text alone. For the combination of their attributes we do not want these colluders to be able to decryption of the secret information. To derive users keys, collusion attack among curious local authorities also consider.
3) **Backward and Forward Secrecy:** Backward secrecy means that, any user should be obviated from acquiring the plaintext of the earlier data replaced before hisinfluence the attribute who comes to influence an attribute. On the other hand, forward secrecy means that, except the other valid attributes that he is holding satisfy the access policy, any user who drops an attribute should be obviated from acquiring the plaintext of the consecutive data replaced after he drops the attribute.

5. Conclusion

The successful solutions in military applications are DTN‟s technologies which allow wireless devices to communicate with each other and by employing external storage nodes reliably access the confidential information. For the concerns like control of access and retrieval of data securely, a scalable cryptographic solution is the CP-ABE Approach. In this paper, for decentralized DTNs where many key authorities manage individually their attributes, we would propose the efficient and secure data retrieval method using CP-ABE. In addition, for every attribute group the fine-grained revocation of key can be done. For managing the distributed data securely and efficiently, there distributed the confidential data in the disruption-tolerant military network, we determine how to apply the proposed mechanism.

6. Acknowledgment

We would like to thanks Junbeon Hur and Kyungtae Kang two referees for their very useful comments and suggestions on earlier versions of the manuscript. Their input has led to an improved version of the paper. The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who made it possible. We are grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasant endeavor to undertake this project. We have a great pleasure in working project Secure Data Retrieval Using CP-ABE Approach for Decentralized Disruption-Tolerant Military Networks under the guidance of Prof. Chitnis P. O. We are truly indebted and grateful to Head of Computer Department Prof. Todmal S. R. for their valuable guidance and also encouragement. We take an opportunity to thank all the staff members of our department. Finally we express our sincere thanks to Prof. Phursule R. N., Prof.

Kothawale S. L. and all those who helped us directly or indirectly in many ways in completion of this project work.

References

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," inProc. IEEE INFOCOM, 2006, pp. 1–11.
[2] M. Chuah and P. Yang, "Node density-based adaptive routing schemefor disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp. 1–6.
[3] 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.
[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-basedinformation 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.HuangandM.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," inProc. 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. 321–334.
[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryptionwith 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 sharingwith 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. Securit, 2008, pp. 417–426.
[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in Proc. ACM Conf. Comput. Commun. Security, 2006,pp. 99–112.
[18] Junbeon Hur and Kyungtae Kang, Member,IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" in Proc. IEEE VOL.22,2014.