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

Secure and Efficient Data Sharing for Decentralized DTN

Gauri N. Salodkar[1], **Komal B. Bijwe**[2]

[1]M.E. Istyear (CSE), P. R. Pote COE&M, Amravati, India

[2]Assistant Professor, P. R. Pote COE&M, Amravati, India

Abstract: ***Nowadays, there have been increasing demands and concerns for distributed data security, One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. Cipher text -policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance control issues. 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. 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 like commander or other superiors. 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. Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful 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. 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 securely and efficiently manage the confidential data distributed in the disruption-tolerant military network also we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.***

Keyword: Military Networks, Encryption, Decryption, DTN, CP-ABE.

1. Introduction

Now recent development of the network and computing technology each and everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. People can share their lives with friends by uploading their private photos or messages into the online social networks such as Facebook and MySpace; or upload highly sensitive personal health records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. Military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments [1]–[3].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. Actually, 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. Amount of time until the connection would be eventually established. After the connection is eventually established, the message is delivered to the destination node.

In this paper, we introduce a CP-ABE based encryption technique that provides fine-grained data access control. In a CP-ABE, each user is associated with a set of attributes based on which the user’s private key is created. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt. Our mechanism can provide fine-grained access control to each node and 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 [14]. In any case, the issue of applying CP-ABE in decentralized DTNs presents a few securities and protection challenges as to the key escrow, and coordination of characteristics issued from distinctive powers. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem [1].

2. Literature Review

This step is most important in any of the process of software development. Before we develop any software we have to consider time factor, economy and strength also decide which operating system and language can be used. After that program development get start by taking external support. This support includes web sites, books or history etc. for developing proposed system. ABE comes in two flavors called (a) key-policy ABE (KP-ABE) and (b) ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes [13]. 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 user’s 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 [3]–[4].

The existing system of Attribute based encryption (ABE) is a guaranteeing approach that satisfies the prerequisites for secure information recovery in DTNs. The issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related qualities sooner or later (for instance, moving their district), or some private keys may be traded off, key repudiation (or redesign) for each one characteristic is fundamental keeping in mind the end goal to make frameworks secure. This infers that renouncement of any property or any single client in a characteristic gathering would influence alternate clients in the gathering. Here, if a client joins or leaves a group, the related characteristic key ought to be changed and redistributed to the various parts in the same group it may bring about bottleneck amid rekeying method or security corruption because of the windows of powerlessness if the past characteristic key is not overhauled fast[2]–[3].

3. Related Work

In this paper, we propose efficient and secure data sharing for decentralized DTN using CP-ABE. The proposed system is having the specialty and following achievements. First, encryptions can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Second, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability [4]–[7]. Third, the key escrow problem is resolved by entering an escrow-free key issuing protocol that enhances the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-phase 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. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme. Thus, users are not required to fully trust the authorities in order to protect their data to be shared [4]–[5].

3.1 Advantages

(a)Firstly, 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, this gives collusion-resistance system [5].

(b)Secondly, 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, this is most useful application [5].

(c)Thirdly, 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, this provide data confidentiality to the existing system [6].

3.2 Challenges

The attribute revocation, key escrow, and coordination of attributes issued from different authorities these are some security and privacy challenges in decentralized disruption tolerant networks applying CP-ABE [7].

3. System Architecture

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

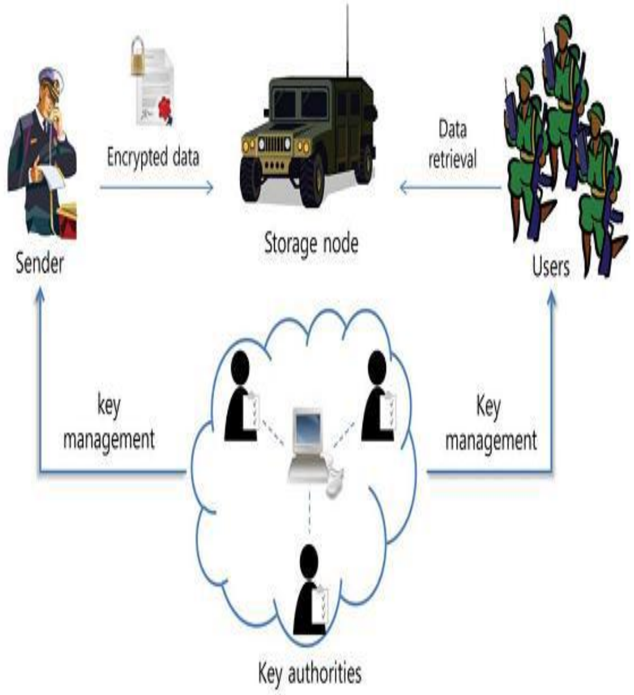

Figure 1: System Architecture [8]

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

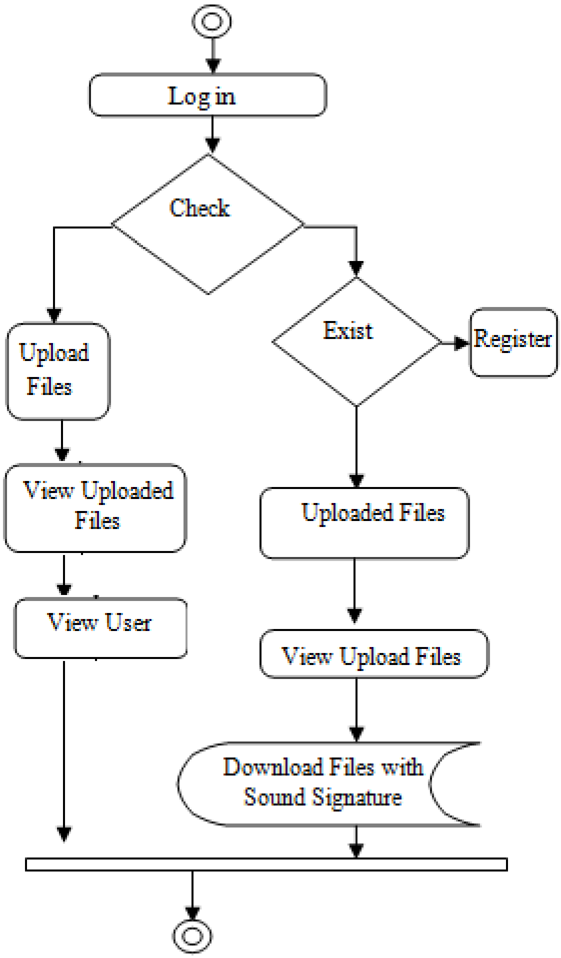

Figure 2: Flow Diagram of DTN [15]

4.1 User module

Sender: 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 [8]–[9]. User: 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 [8]–[9].

4.2 Vector module

1. Create User profile Vector (master): While registration of user information, the user id, sound frequency or time and tolerance are getting for creating master vector. Master vector: (User ID, Sound Signature frequency, Tolerance) [8].

2. Create Detailed Vector: To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created. Detailed Vector - (Image, Click Points) [8]

3. Compare User Profile/login Vector: Enters User ID and select one sound frequency or time which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points [10].

4. Upload/Download Module: Admin, defense, navy and air force are going to upload secret file between them. They can share the uploaded files. User (defense, air force and navy) uses sound signature for download files. System showed very good Performance in terms of speed, accuracy, and ease of use. In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice the profile vector is created [10].

4.3 Administrator module

1. Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users [12]. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible [10].

2. Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted that is honest-but-curious [11].

4. Conclusion

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 proposed scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials. The proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the ciphertext policy attribute-based encryption. As stated before 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. We demonstrate how the data can be efficiently and securely share for Decentralized DTN in 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, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

[4] 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.

[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007.

[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.

[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.

[8] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in *Proc. ACMConf. Compute Commun. Security*, 2006.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Newt.*, 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.

[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. Computes Commun. Security*, 2006.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput Commun. Security*, 2007.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010.

Author Profile

Gauri N. Salodkar. received her B.E (Computers) from in P. R. Pote College of Engineering and Manegement Amravati University,Amravati Maharashtra, India in 2013. Currently she is pursuing M.E. in Computer Science and Engineering from P. R. Pote College of Engineering And Technology Amravati, Maharashtra, India.

Komal B. Bijwe. Completed her M.E. Currently she is working as assistant professor in P. R. Pote College of Engineering and Manegment Amravati, Maharashtra, India.