Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.407 – 413

Military Network Security for Data Retrieval with Touch of Smell Technology

Suchita Ghugal[1], Mrunali Vaidya[2]

[1]M-Tech Student, Department of CSE, Ballarpur Institute of Technology (BIT),
Gondwana University, Gadchiroli, Maharashtra, India
[2]Assistant Professor, Department of CSE, Ballarpur Institute of Technology (BIT),
Gondwana University, Gadchiroli, Maharashtra, India
[1] suchitaghugal@gmail.com; [2] mrunalidhawas@gmail.com

ABSTRACT: In military environment mobile nodes suffer from some communication challenges. In such environments DTN (Disruption tolerant network) technologies gave fruitful results. This allows soldiers in battlefield area to communicate with each other and can able to share secret information. As such there are several privacy challenges related to storing and sharing of secret information, the CP-ABE is the best approach to deal in these cases. By using this technique secret information can be able to keep confidential even if server is entrusted. In this paper we are going to retrieve secure information using this CP-ABE scheme. In addition for improving security we introduced face detection concept.

Keywords: - DTN, CP-ABE, tolerant network.

1. INTRODUCTION

In many military networks the end to end connection between two nodes may not always exists. So in such cases DTN technologies are becoming successful. When there is no end to end connection then by using intermediate nodes source an destination can able to communicate with each other without any communication delay [1]-[2]. The actual work of DTN is based on use of storage node, source node store all messages on storage node and may need to wait there until connection is established [3]. Eventually destination node can access that message. On storage node useful data is stored and replicated so that data should be always available to the users.

In this paper we describe data stored on the storage node should be stored in encrypted form so that here we are using CP-ABE scheme for increasing security of data. CP-ABE is much more flexible than plain identity-based encryption. In this scheme it allows complex rules specifying which private keys can decrypt which cipher text. Specifically, the private keys are associated with sets of attributes (for example, region and battalion) or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt the cipher text.

As we know in DTN attribute based encryption (ABE) is the promising approach for achieving security. ABE comes in two flavors first is KP-ABE and another is CP-ABE. In KP-ABE i.e. key policy attribute based encryption the encryptor only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher text he can decrypt and issues the key to each user by embedding the policy into the user's key. Whereas in CP-ABE the process is exactly reversed i.e. in CP-ABE, the cipher text 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 encryptor 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.

2. EXISTING SYSTEM

In DTN on applying ABE approach the network has to face several security and privacy challenges such as attribute revocation. Key escrow problem and last is coordination of attributes. Some users may change their associated attributes at some point or some private keys might be compromised, so in that case attribute revocation is necessary. But in ABE systems, since each attribute is conceivably shared by multiple users attribute revocation is very difficult [4]-[5].

Another is key escrow problem it is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. 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. It is very inherent problem.

The last is coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities [8]-[9]. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B. Then, it is impossible to generate an access policy.

3. PROPOSED SYSTEM

We provide a multiauthority scheme CP-ABE for secure data retrieval in decentralized DTN. Followings are the achievements of our proposed scheme. First, attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. And the third is encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities [1],[10].

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.

The security requirements suggested by our proposed scheme are as below [11]:

3.1 Data confidentiality:

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.

3.2 Collusion-resistance:

If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone. For example, suppose there exist a user with attributes {”Battalion 1”, “Region 1”} and another user with attributes {”Battalion 2”, “Region 2”}. They may succeed in decrypting a cipher text encrypted under the access policy of (“Battalion 1” AND “Region 2”), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive user’s keys.

3.3 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.

4. SYSTEM ARCHITECHTURE

In this paper we describe DTN architecture and its security model.

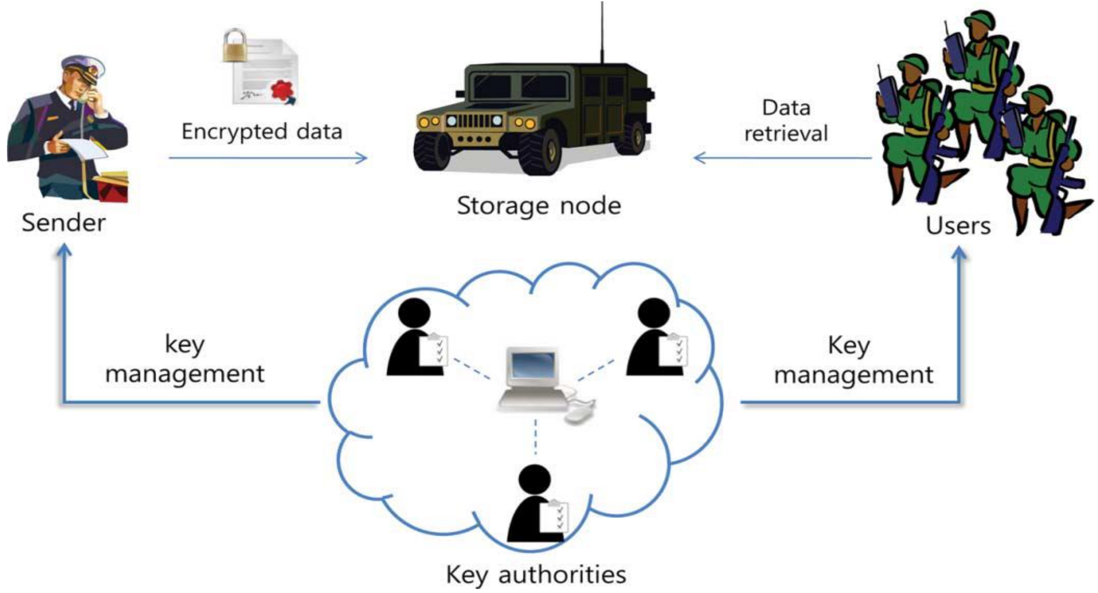

Fig 1. Architecture of DTN

DTN architecture shows following system entities:

4.1 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. 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.

4.2 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.

4.3 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.

4.4 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 cipher text and obtain the data.

In this paper we are going to implement one another module for increasing security of whole network i.e. face detection module.

4.5Face detection:

In this module we are going to detect human face by using skin tone segmentation i.e. by counting pixels in an image and by using region labeling we detect human faces and identify by their names [14]-[15]. The system model can be shown in fig.2.

In our face detection system we are going to achieve face detection in three steps:

1. First, we will capture an image and then convert that image into gray scale image.

2. Second, by using skin tone segmentation we are going to recognize that image.

3. And third, by using region labeling we named that image and detect human faces.

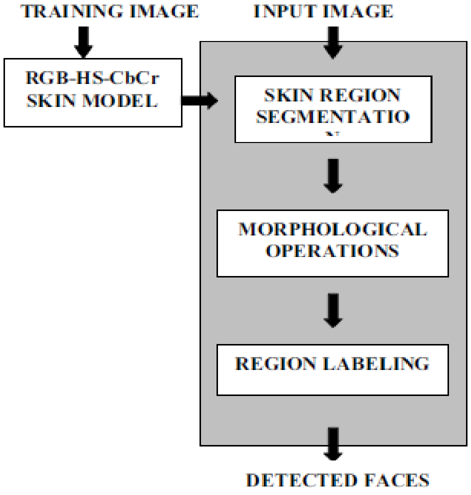

Fig.2. face detection system

5. FUNCTIONING OF CP-ABE

The cipher text policy attribute based encryption (CP-ABE) scheme can be viewed as generalization of identity based encryption. So as in identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys. However, CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which cipher text. Specifically, the private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt [6]-[7].

In our DTN system we store our files or data on storage node or we can say on remote server because we want to provide scalable access to other resources and we want more reliability in case of failures in this case we want to replicate our files to different data. But we want security i.e. who can access which files. The problem is when more we replicate our files, the more we introduce potential points of compromise and the more trust we require. In this case CP-ABE is useful.

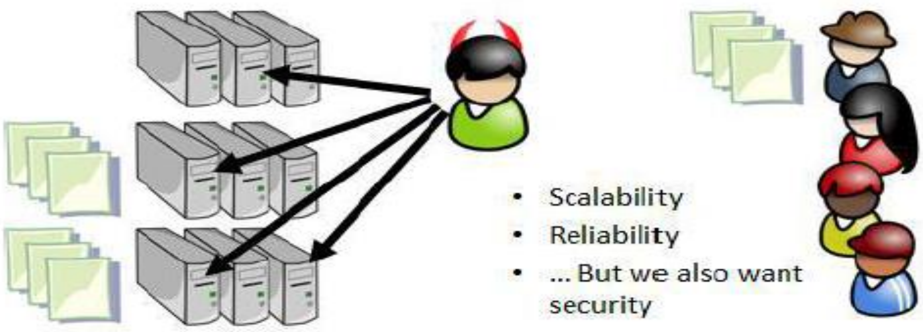

Fig. 3. Remote file storage

So in this case on applying CP-ABE, when we upload a file, we also provide a policy specifying who should be permitted to access the file [12]-[13]. Now when another user comes along and authenticates himself to the server somehow, the serve can evaluate the policy and check whether he is allowed to access that fie or not. To increased confidentiality of system we are storing encrypted file on remote servers. After file is encrypted, say we put it on the server now the policy checking happens that is, nobody explicitly evaluates the policies and makes an access decision. Instead, if the policy is satisfied, decryption will just work, otherwise it won't.

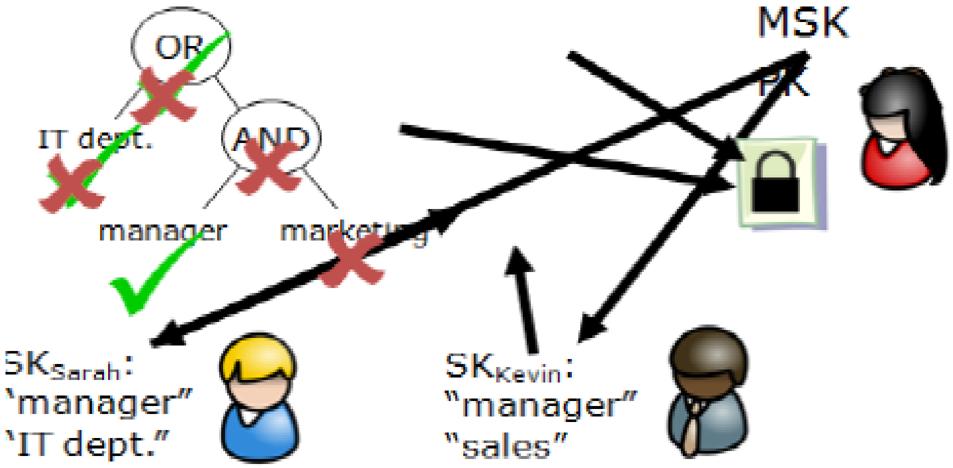

Fig. 4. Access control via CP-ABE.

6. CONCLUSION

In this paper we introduced to CP-ABE scheme for secure data retrieval using DTN technologies. As we see DTN is an appropriate solution for intermittent network connectivity and it make use of storage node for storing files on intermediate server so that connection reliability should be achieved. For accessing files from storage node we use CP-ABE scheme which is very beneficial as per as security is concern. In this paper we gave brief idea about one most new thing that is face detection mechanism for increasing confidentiality of data. In future such as for video conferencing we can use this mechanism and can extend this project

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] S M. Chuah and P. Yang, "Node density- based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.

[3] D 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] W. M. Chase and S. S. M. Chow, ―Improving privacy and security in multiauthority attribute-based encryption," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 121–130.

[6] J. Bethencourt, A. Sahai, and B. Waters "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

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

[8] 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

[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] 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.

[11] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, E. Travis and H. Weiss, "Interplanetary Internet (IPN): Architectural Definition," 2001.

[12] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Intel Research Berkley, 2003.

[13] M. Loubser, "Delay Tolerant Networking for Sensor Networks," SICS Technical Report, ISSN 1100-3154, January 2006

[14] A. S. Pentland, R. Fletcher and A. Hasson, "DakNet: Rethinking Connectivity in Developing Nations," IEEE Computer, January 2004.

[15] M. J. Khabbaz, W. F. Fawaz and C. M. Assi, ‖Probabilistic Bundle Relaying Schemes In Two-Hop Vehicular Delay-Tolerant Networks,‖ IEEE Communications Letters, to appear, 2011.

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

[17] 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.

[18] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext policy attribute-based encryption and its application," in Proc. WISA, 2009.

[19] Sribhashyam Sathvik and K.M.V Madan Kumar, ―A Strategic Review on Cipher Text Policy Attribute Based Encryption‖. 2650-2654, December 2014.

[20] M. Chase, ―Multi-authority attribute based encryption, in *Proc. TCC*, 2007, LNCS 4329, pp. 515–534.