Effective Solution for Secure data Retrieval In decentralized DTNs.

P. A. Patil[1], A. A. Rajguru[2], V. V. Pottigar[3]

[1,2,3] ME Computer (Engineering), Dept. of Computer Science & Engineering, Solapur University,
SKN Sinhgad College of Engineering, Korti, Pandharpur, MS, India
[1]patilpraju25@gmail.com, [2]abhijitcse08@gmail.com, [3]vinayak.pottigar@gmail.com

Abstract* - The Disruption-tolerant network (DTN) is the famous technology which used in the military network in which Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions so it is having the storage network if the connection is not establish it will store in the storage node after the connection is establish then it transfer to the receiver to make it secure. CP-ABE is used in which the transfer data is encrypted and the key is required to decrypt as it is a decentralized network multiple key authorities are used means the Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues for decentralized DTNs where multiple key authorities manage their attributes independently.

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

I. INTRODUCTION

Network security describes the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing and altering secure information. In military system environment, associations of remote gadgets conveyed by officers may be briefly detached by sticking, ecological variables, and versatility, particularly when they work in hostile environments. Interruption tolerant system (DTN) technologies are becoming favourably result that authorize nodes to communicate with each other in these immensely networking environments [1].

Disruption Tolerant Networks (DTN) is a type of network that is designed to provide communications in the most unstable and intermittent connections, where the network would normally be subject to frequent and long lasting disruptions that could severely degrade normal communications. Also Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. 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[12][10].

Cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decrypted needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. Also 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 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 [6].

Therefore, the best solution for the above problem is that sender encrypts message with distinct public-keys, but the user uses private key for decryption so that key should be sent via a secure channel and kept secret.

Network provides a sharing of data among different user with the help of wireless devices. For this, a network must provide a secure communication among the network for data transfer to the entire user in the network. With the wireless network, transfer of data where done with the help of the intermediate node, here data may be lose because of unauthorized user in the network may hack the data. Disruption-tolerant network (DTN) is a technology which allows the node to communicate with each other in secure manner [15].

It is one of the successful solutions for transferring the data in network. Most of the military users use this technology for secure transfer of the data. In the large number of outgrowing commercial environment such as military each and everything based on the another sources to broadcast the data strongly and maintain the data as well in the regular medium. Usually, when there is no end-to-end communication among a source and a destination pair, the data from the source node may want to stay in the intermediate nodes for an extensive amount of time until the connection would be ultimately established. After the connection is ultimately established, the data is delivered to the destination node.

DTNs maintain interoperability of networks by cooperating a long disruptions and delays among those networks, and by communicating among the communications protocols of those networks. DTNs can accommodate many kinds of wireless technologies, including radio frequency (RF), ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies[11]. Transportable nodes in military environments, for example, in an antagonistic area are horizontal to practice in endure of asymmetrical system network and numerous partitions. Disruption-tolerant network (DTN) modernisms are receiving to be productive results that authorize remote device conveyed by officers to speak with one another and admit the private data or secret data or beckon unvaryingly by neglecting outside capacity nodes or storage nodes. A DTN node can forward package between two or more other nodes in one of two situations they were Routing and Equivalent Forwarding. In DTNs, data where stored or pretend such that only authorized mobile nodes can entrée the required information rapidly and efficiently.

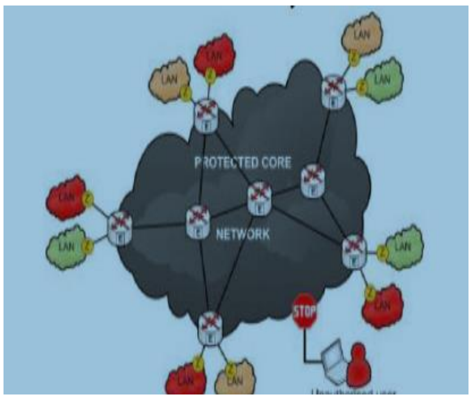

Fig: 1 Military Network

II. LITERATURE SURVEY

As more sensitive data is shared and stored by third-party sites on Internet, there will be need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at coarse-grained level (i.e., giving another party your private key). So this paper presents a new cryptosystem for fine-grained sharing of encrypted data that is Key-Policy Attribute-Based Encryption (KP-ABE) [2]

It is a type of public-key encryption in which secret key of user and cipher text is dependent upon attributes. In which decryption of cipher text is possible iff set of attributes of user key matches the attributes of cipher text. A crucial security aspect of Attribute-Based Encryption is collusion-resistance. This paper introduces attribute-based encryption (ABE) which is used for encryption. In which it finds match of each attribute from each group for encryption. [3].

Many network applications (e.g. information services) are based upon group communication model. So for providing authenticity of messages delivered between group members, will become critical issue. Now this paper gives solution to the scalability problem of group/multicast key management. Which defines secure group as triple (U, K, R) where U- a set of users, K-set of keys held by users, and R-user-key relation. [4].

The Attribute-Based Encryption system supports the non-monotone expression in key policies. This is achieved through a application of revocation methods into existing ABE schemes but performance of our scheme is less-expressive "Ciphertext-Policy" Attribute-Based Encryption is used in which attributes are used to describe the feature of key holder, and encryptor will associate access policy with ciphertext[5].

Developed a secure data retrieval scheme for data sharing in military network using Ciphertext-Policy Attribute-Based Encryption scheme. Implemented a cryptosystem where multiple key authorities manage their attributes independently. [1].

III. PROPOSED SYSTEM

A. General view of our proposal

Here we describe the main idea of data sharing in military network using following module, illustrated in Figure,

1. Key Authorities
2. Key management
3. Storage node
4. Sender
5. Soldier (User)

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. They grant differential access rights to individual users based on the users' attributes.

2. Key management:
It is the management of cryptographic keys which includes the generation, exchange, storage, use, and replacement of the keys.

3. Storage node:
This is an entity that stores the data from senders and provides the corresponding access to the users.

4. Sender:
This is an entity who owns confidential data (e.g. commander) and wishes to store them into external data storage node for ease of sharing A sender is responsible for defining access policy (attribute based) and own data by encrypting it under the policy before storing it to storage node.

5. Soldier:
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 attributes, then he will be able to decrypt the ciphertext and obtain data.

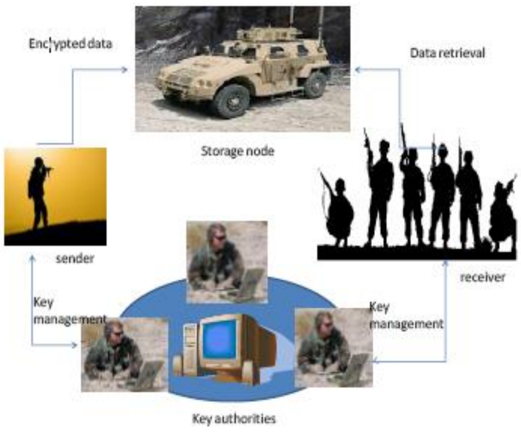

Fig.2 Architecture of secure data retrieval in a disruption-tolerant military network.

IV. RESULT AND EVALUATION

1. *Mathematical Model*

A CP-ABE scheme consists of following four steps as follows.

1. **SETUP** ($; U) the setup algorithm takes security parameter and attribute as input & outputs public parameters PK and master key MK.

2. **ENCRYPT** (PK; M; A) the encryption algorithm takes input as public parameters PK, message M, and access structure A. The algorithm will encrypt M and produce ciphertext CT such that only a user that possesses set of attributes that satisfies the access structure will be able to decrypt the message.

3. **KEY GEN** (MK; S) the key generation algorithm takes input as master key MK and set of attributes S that describe the key & outputs a private key SK.

4.**DECRYPT**(PK;CT;SK) the decryption algorithm takes input as public parameters PK, ciphertext CT, which contains access policy A, and private key SK, which is private key for a set S of attributes. If set S of attributes satisfies access structure A then algorithm will decrypt ciphertext and return message M

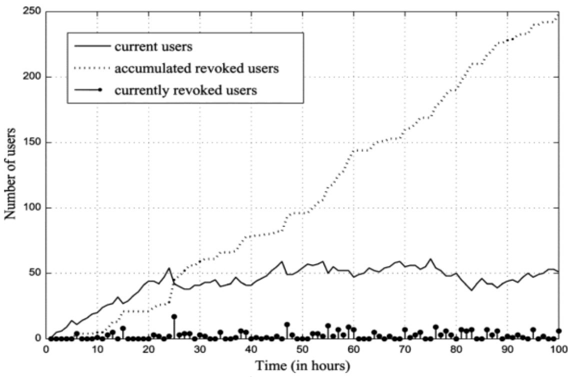

Fig 3. Number of users in an attribute group

Fig 3 represents the number of current users and revoked users in an attribute group during 100 h.

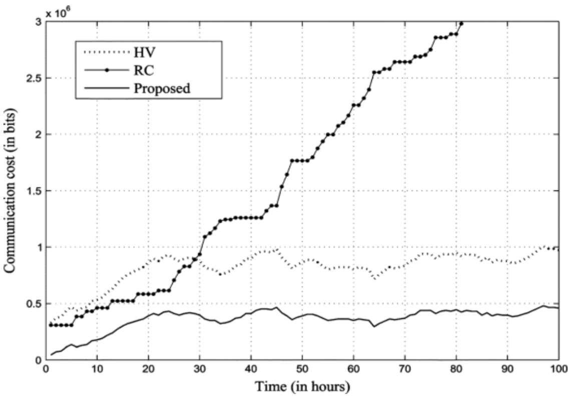

Fig 4. Communication cost in the multiauthority CP-ABE system.

Fig 4. Shows the total communication cost that the sender or the storage node needs to send on a membership change in each multiauthority CP-ABE scheme. It includes the ciphertext and rekeying messages for non revoked users.

V. CONCLUSION

DTN technologies are becoming successful solutions in military applications that 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 secures data retrieval issues. In this project, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks” IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.

[2] 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.

[3] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute based systems,” in Proc. ACMConf. Comput. Commun. Security, 2006, pp. 99–112.

[4] C. K.Wong,M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” in Proc. ACM SIGCOMM, 1998, pp. 68–79.

[5] 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

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

[7] 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.

[8] K. C. Almeroth and M. H. Ammar, “Multicast group behavior in the Internet’s multicast backbone (MBone),” IEEE Commun. Mag., vol. 35, no. 6, pp. 124–129, Jun. 1997.

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

[10] M. M. B. Tariq, M. Ammar, and E. Zequra, “Mesage ferry route design for sparse ad hoc networks with mobile nodes,” in *Proc. ACM*

[11] Mooi-Choo Chuah and Peng Yang, “Performance Evaluation of Node Density-Based Adaptive Routing Scheme for Disruption

[12] Tolerant Networks1J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle-based disruption tolerant networks,” in *Proc.*

[13] *IEEE INFOCOM*, 2006, pp. 1–11.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.

[14] “The Pairing-Based Cryptography Library,” Accessed Aug. 2010 [Online]. Available: http://crypto.stanford.edu/pbc/

[15] Ioannis Psaras, Lloyd Woodb, Rahim Tafazolli, “Delay-/Disruption-Tolerant Networking State of the Art and Future Challenges.