# Ciphertext Policy Attribute Based Encryption for Secure Military Communication in Decentralized DTN

Poonguzhali. E
Dept. of CSE
AMCEC Bangalore

Ramya. M
Dept. of CSE
AMCEC Bangalore

***Abstract* - Disruption-Tolerant Network (DTN) is a successful solution for communication between nodes in extreme environments and access the confidential information provided by major authorities. Then the system provides efficient scenario for authorization policies and then the policies updated we secure data retrieval in most challenging cases. The cryptographic solution is introduced by Ciphertext Policy Attribute Based Encryption (CP-ABE) for control and access data. In this paper, we are known how to secure and access the data using decentralized DTN.**

***Key Words: - Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.***

## 1. INTRODUCTION

Now a day, The Internet service models are depending on some assumptions. That is (a) the existence of an end to-end path between a destination node and source node pair: if an end to end path between a destination node and source node, then message easily sent between source and destination node, else find the intermediate node to store the message, if end-to-end path exits then message sent between source node and destination node and (b) round-trip latency: the time taken to deliver a message from source to destination node. The round-trip latency between any node pair is less.

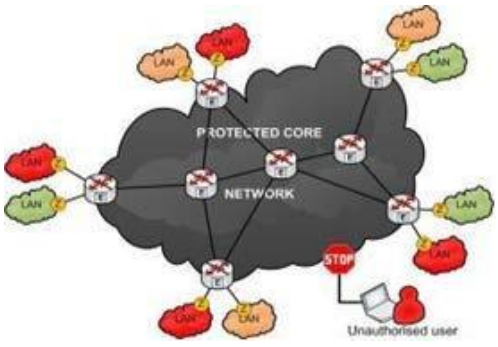


Fig.1. Military Networks

The drawback of these assumptions are:(i) battlefield Ad-hoc networks and (ii) Vehicular Ad-hoc networks where buses are equipped with wireless modems. Disruption-Tolerant network technologies allow the nodes to communicate with each other and DTN is used to overcome from these drawbacks.

## 2. LITERATURE SURVEY

The first step in software development process is Literature survey. Before developing the software, we need some tool. The tools are the time factor, economy and company strength. We are satisfied from these tools, then go to next step. The next step is to choose an operating system and language. When a programmer starts to write a program he need an external support. The external supports are senior programmers, book or websites. The ABE are two types in literature survey. They are ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In KP-ABE, the encrypto get a message that is a cipher text with a set of attributes. In CP-ABE, the cipher text is encrypted by an encryptor with an access policy. KP-ABE is less suitable to DTNs than CP-ABE because it enables encryptors to choose an access policy and confidential data.

## 3. EXISTING SYSTEM

The existing system is used for secure information recovery with satisfies the prerequisites in DTNs by using Attribute based encryption (ABE). The characteristics of ABE a control and access the information. The quality of ABE is providing private keys and ciphertexts. The ABE is used for secure and protect the data in challenging cases.

*Limitation of the existing system*

i) The data is secure and protect in challenging cases by applying the ABE to DTNs
ii) In CP-ABE, by applying the power's expert mystery keys to set of properties. These keys are given to clients for secure the data. The private keys of clients are created by key power.

## 4. PROPOSED SYSTEM

In proposed system, Ciphertext Policy Attribute Based Encryption (CP-ABE) for decentralized DTNs are used for secure data retrieval. The achievements of the proposed system are: (i) The revocation enhances immediate attribute of confidential data are secure by using either forward secrecy or backward secrecy. (ii) The access policies are defined by encryptor. The encryptor is access the structure using any monotone under set of authorities issued by attributes. (iii) The protocols issued escrow-free key. Using these keys we solve the key escrow problem.

*Advantages:*
i) Confidentiality data.
ii) Resistance collusion.
iii) Forward and Backward Secrecy.

## 5. SYSTEM ARCHITECTURE

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

i) Authorities key: It is a key generation center. It generates key parameters for CP-ABE. The authority key contain the multiple local authority.

ii) Storage Nodes: It is stores the message obtained from the senders and the users. It is act as an entity.
Example: mobile.

iii) Senders: It is act as an entity, who gets the confidential data from the storage node and sending these confidential data to user.
Example: a commander.


Fig.2: System Architecture.

iv) Users: The user is receive the data from sender and the stores data in storage node. It is act as the mobile node.
Example: a soldier.

## 6. FUNCTIONING OF SYSTEM

Key Powers: The CP-ABE with key era is creates the open or mystery parameters. The key powers contain the numerous focal power and numerous neighbourhood powers.
Storage Nodes: As the name suggest that it stores the message or information obtained from the senders and user. It is provides data for access.

Senders: The sender sent the private message or data obtained from the storage node to user.
Example: commandants.
Clients: The clients get the information from the sender and perform their function.
Example: a fighter.
CP-ABE Policy: In CP-ABE the encryptors can alter the decoded message. The decoded message is sent alongside the ciphertext.

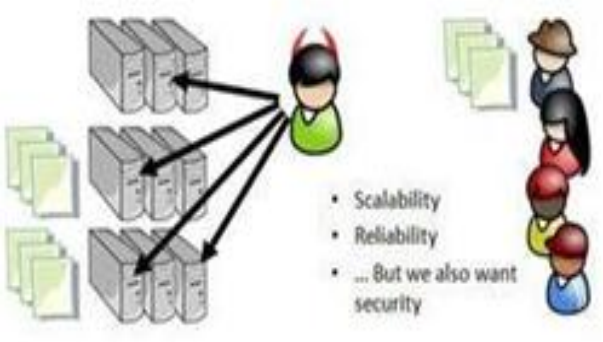


Fig.3 Storage the file using remote sensor

We need a tendency factor for store our files on remote servers. Access the data in our file we need a tendency factor. In this case tendency factor duplicate our files totally different information centers.

## 7. IMPLEMENTATION

The last step of every project/paper is an implementation. The implementation means the theoretical concept are done in pratically. The implementation stage involves planning, investment, methods for designing a project. The implementation is achieved by evaluation of changeover methods and changeover.
Modules:

i) Authority key
ii) Nodes for storage
iii) Sender
iv) Receiver

Modules Descriptions:
i) Authority key: The authority key contain the multiple local authority. It is a key generation center. It generates key parameters for CP-ABE.
ii) Nodes for storage: It is stores the message or information obtained from senders and user. It is act as an entity.
Example: mobile.
iii) Sender: It is get a data or information from the sender and sent these information to user for access these information.
Example: a commander.
iv) Receiver: It is receive the message from sender and storage these message in storage node.
Example: a soldier.

## 8. CONCLUSION

Disruption Tolerant network is a successful solution in military applications. In military networks, the user access the confidential information which is exploits in the external storage node. Here we are known how to access the data and secure the data using Ciphertext Policy Attribute Based Encryption (CP-ABE) and decentralised Disruption-Tolerant Network (DTN).

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, 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. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, 1526–1535, 2009.
[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"CryptologyePrint 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, "Attributebased encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006,
[13] J.Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased 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, pp. 195–203.
[15] S. Yu, C.Wang, K.Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270