ISSN 2347 - 3983

**International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 124- 126 (2015)**
*Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati*
***http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp25.pdf***

# AN ATTRIBUTE BASED SECURED DATA RETRIEVAL MECHANISM FOR DECENTRALIZED MILITARY NETWORKS

**K.Jayanthi[1], T S Sandeep[2]**
[1]M.Tech CSE Student, S.V Engineering College for Women, Tirupati, AP, India
jayjeeva516@gmail.com
[2]Assistant Professor, Dept. of CSE, S.V Engineering College for Women, Tirupati, AP, India,
sandeep.t@svcollege.edu.in

## ABSTRACT

There are partitions in military environments such as a battleground or a hostile region. They are likely to suffer from intermittent network connectivity. They are having frequent partitions. Disruption-tolerant network DTN technologies are is a true and easy solutions. It allows devices which are wireless and carried by peoples in a military to interact with each other. These devices access the confidential information or command reliably by abusing external storage nodes. In these networking environments DTN is very successful technology. When there is no wired connection between a sender and a user device, the information from the sender may need to wait in the intermediate nodes for a large amount of time until the connection would be correctly recognized. One of the challenging approaches is an ABE. That is attribute-based encryption which fulfills the requirements for secure data retrieval in DTNs. The concept is Cipher text Policy ABE (CP-ABE), it gives an appropriate way of encryption of data. The encryption includes the attribute set that the decryption needs to possess in order to decrypt the cipher text. Hence, many users can be allowed to decrypt different parts of data according to the security policy.

**Key Words:-** Disruption-tolerant network (DTN), Attribute-based encryption (ABE), Cipher-policy Attribute-Based encryption (CP-ABE).

## 1. INTRODUCTION

The concept of attribute-based encryption (ABE) is a favorable approach that fulfills the requirements for secure data retrieval in Disruption Tolerant Networks(DTN). DTNs provide a successful solutions for network communications. By using access policies and attributes of users that enables an access control over encrypted data. By using the key generation authorities each user performs the certain task. Sender want to send the encrypted data to the storage node, with the help of key authorities users are decrypt the information. Thus we allowed access nodes for decryption when at least *n* attributes enclosed between a cipher text and a secret key. While this original was shown to be useful for error-tolerant encryption with network communications, the lack of expressibility seems to limit its applicability to larger systems.

In CP-ABE, the cipher text is used to encrypt the plain text as well as plain text is used to decrypt the cipher text by using key manage and generation algorithm. while the secret key is associated with a set of attributes. These will be shown by following architecture.

## 2. RELATED WORK

In this work is focused on ABE, ABE dividing with KP-ABE and CP-ABE. Key Policy Attribute Based Encryption (KP-ABE), sender only get to the label of cipher text . And Cipher Policy Attribute Based Encryption (CP-ABE) the sender chooses an access policy on user attributes. In this work shows the key revocation means that key updation, key escrow means that only one trusted master authority manage their whole set of keys, suppose master authority compromise these work it will goes wrong way and coordination problems means that mutual problems of local key authorities.

## 3. NETWORK ARCHITECTURE

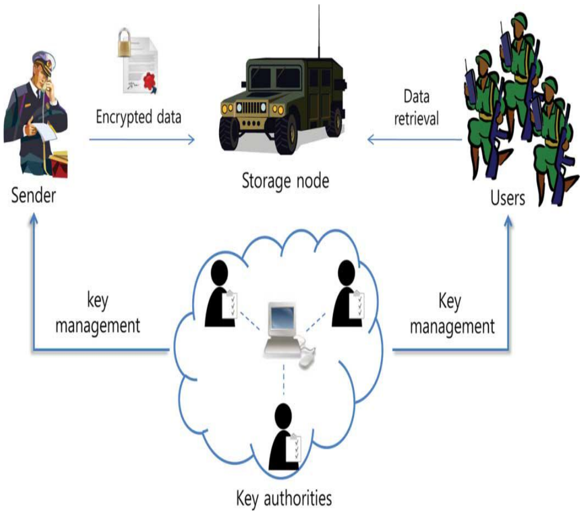

**Figure 1:** Secure data retrieval for DTN's military network

I. Sender: This is an entity who has most confidential data

II. Storage Node: This is an entity that stores data from senders and user

III. Key Authorities: Key authorizes are generates public/secrete for cipher policy-ABE. It contains central as well as local authorities. Local authority contains multiple attributes and provides corresponding attribute keys to the users. By using this key authorities, users are updated immediately.

IV. User: This is mobile node who needs to access the data stored at the storage node.

Sender want to sends the confidential data the users by using storage nodes, at that time CP_ABE, key authority generates private keys of users by applying the authorities trusted master keys. Suppose key authority is negotiated by oppositions 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. This is called key escrow. Each attribute contain limited period of time and provide the new keys to the legal users after completion time.

When many key authorities generate attribute keys to users separately with their own master secrets. It is critical to define fine-grained access policies over attribute generated from many key authorities.

The chief objective of our framework is to provide secure data retrieval access and capable key management at the same time. Whenever attributes are changing at certain period of time, by using this attributes the user should not be capable to access future data so, it is going to for forward/backward secrecy.

## 4. MULTI ATTRIBUTE BASED TECHNIQUE IN KEY GENERATION SYSTEM

In this encryption scheme, many attribute authorities operate separately. A Multi-Authority ABE system is comprised of multiple attribute authorities and one central authority. Each attribute authority is also allotted a value, dk. The system uses the following algorithms:

**I) Set up:** A random algorithm that is run by the central authority or some further trusted authority. It takes as input the security parameter and outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

**II) Attribute Key Generation:** A random algorithm run by an attribute authority. It takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.

**III) Central Key Generation:** A randomized algorithm that is run by the central authority. It takes as input the master secret key and a user's GID and outputs secret key for the user.

**IV) Encryption:** A randomized algorithm runs by a sender. It takes as input a set of attributes for each authority, a message, and the system public key and outputs the cipher text.

**V) Decryption:** A deterministic algorithm runs by a user. It takes input a cipher-text, which was encrypted under attribute set and decryption keys for that attribute set. This algorithm outputs a message m.

## 5. MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION

In a multi-authority ABE systems contains multiple attribute authorities and multiple users. Central authority contains multiple local authorities. every local authority provides the attribute set that used to update immediately. Any key generation authority depends on user attributes, and request the equivalent decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user.by using this attribute keys users are updated his data. Every user works under the k number of battalions of military environment and every battalion controls the n number of regions. Each region under controls the different local key authorities. Suppose region A controls one local key authority, region B controls another local key authority.so different region users contains different attributes. At that time coordination problems are raised. Every local authority should generates the appropriate keys to users. Any party can also choose to encrypt a message. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

By using these algorithm keys should be generated properly, and key revocation, key escrow, coordination problems are resolved.

A secure two-party computation (2PC) protocol contains the key authorities with their own master secrets. By using master secret information no one can generate the entire set user keys alone. The authorities are not fully trusted to share the users data. The data confidentiality and privacy can be cryptographically required against any curious key authorities or data storage nodes in the proposed scheme. So key escrow problem is resolved.

## 6. FINE GRAINED ACCESS CONTROL

Fine-grained access control systems enable approving differential access rights to a set of users and allow flexibility in specifying the access rights of individual users

One of the technique is that the storage nodes are storing the date in an encrypted form while different users are still acceptable to decrypt different data per the security policy. This effectively eliminates the need to depend on the storage nodes for preventing unauthorized data access.

## 7. ATTRIBUTE REVOCATION

Users are going to one area to another area so key must be updated properly. The system should be highly scalable, in terms of complexity in key management, communication, computation and storage.

Before distributing the cipher text, the storage node receives a set of association information for each attribute group G that seems in the access tree of cipher text from the equivalent authorities and re encrypts it as follows.

1. For all attribute group G, chooses a random keys then, re encrypt and generates

2. Generates a header message Hdr

On receiving any data request probe from a user, the storage node responds with header message and re encrypted cipher text to the user. When the user receives them, first obtains the attribute group keys for all attributes in S that holds from Hdr. So backward/forward secrecy problems can be resolved.

## 8.SECURITY

In this attribute based secured data retrieval mechanism for decentralized networks provides the security to military environment. As this purpose collusion resistant occurs at local authorities so colluding local authorities are not properly generates entire keys. Provide the data confidentiality of stored data and finally backward/forward secrecy. It means that users are adopt the any attribute set that satisfies the access policies. In this security mechanism provide the security for all authorized sender and users.

## 9.RESULT

An attribute-based secure data retrieval mechanism for decentralized networks scheme features the following achievements.

- Using any monotone access structure under attributes allotted from any chosen set of authorities encryptions can define a fine-grained access policy.
- The key escrow problem is determined by an escrow-free key issuing protocol
- Reducing the windows of vulnerability.

## 10.CONCLUSION

In this an attribute based secure data retrieval mechanism for decentralized networks are allow wireless devices to communicate each other and access the confidential data reliably by abusing the storage nodes. Where multiple key authorities generate the keys to users based on attributes. The key escrow problem is solved, reduce the windows vulnerability and fine-grained key revocation can be done.

## REFERENCES

[1].S. Roy and M. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

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

[3]. 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.

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

[5].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].V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded cipher text policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated

[7]."cipher text-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[8].S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309–329,2003.

[9] 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.

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

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.

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

[19] 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.

[20] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

[21] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[22] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 99–112.