ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

An Approach for Secure Data Retrieval for Decentralized Disruption Tolerant Network

Sujata Patil [1], Prof. S L Deshpande [2]

P.G. Student, Department of Computer Network Engineering, Centre for PG studies, VTU Belagavi, Karnataka, India[1]

Professor, Department of Computer Network Engineering, Centre for PG studies, VTU Belagavi, Karnataka, India[2]

ABSTRACT: Sometimes sharing of information becomes difficult in any network because of environmental changes. Delay tolerant network provides continuous packet transmission between source nodes to destination node. The end user should have access permission to access any information from trusted third party node. The cipher-text policy attribute based encryption provides solutions to overcome from access control issues. The data needs to be encrypted by advanced encryption standard algorithm to provide more security to the data. The security challenges arise such as multi key authority coordination due to applying of attribute based encryption over delay tolerant networks. The proposed method involves single key authority system which provides more efficiency and less communication cost, file modification mechanism by storing an immutable file to trusted third party node. By storing an immutable type of file level of security will be increased within a network and there is no any modification or leakage of information from trusted node.

KEYWORDS: Delay tolerant network (DTN), Cipher-text policy attributes based encryption (CP-ABE)

I. INTRODUCTION

The connectivity of devices may be down because of environmental factors in any network. In such situations Delay tolerant network is best possible solution that provides a continuous packet transmission in order to avoid such problems. It allows nodes to communicate with other without any interruption. The data will be stored in trusted third party node so that an end user can access the information securely. The security issue is major challenge in this scenario. It is important to characterize a few information get to strategies over user qualities that are overseen by key specialists. Because of the security purpose the data has to be encrypted before storing it in node. The encryption which is based on characteristics provides requirement for protected information retrieval within delay tolerant networks. The converted text strategy characteristic based encryption has capability to encrypt the data such that user should possess attribute set to decrypt the data. The various issues arises due to using attribute based encryption over disruption tolerant network are key custody, key update and multi authority coordination. Another security issue in DTN is file modification in storage node. The key custody issue can be solved by an attribute based encryption technique. The file which is stored at trusted party node can be modified before it will reach to destination by any third party member. So an immutable type of file will be stored at that node which can be modified or deleted.

II. RELATED WORK

Characteristic based encryption [1] mechanism provides facility to access the data securely in DTNs. By defining its strategies and features over personal and parent keys the ABE enables access control mechanism on encrypted data. Cipher-text policy attribute based encryption (CP-ABE) resolves scalability issue by converting original text and providing converted test. The user should have characteristic set to get encoded information. CP-ABE possess capability to encode the information such that user should possess attribute set to decode the information.

The encrypted text strategy character based encryption is one of the best techniques which have logic expression on both characteristics. To get selected cipher-text secure extension by one time signature they have applied Canetti-

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Halevi-Katz technique [2] and for the necessity to maintain selected plain text they introduce hierarchical attributes for reducing both size of encoded text and encryption/decryption time.

Any system can become any rights within multi-authority characteristic based encryption system [3]. Any party can pretend as an Attribute based encryption authority by generating public keys and providing personal keys to all users. By using any Boolean formula a user can encode the information over features provided by authorities. The system becomes secure by using dual system encryption methodology which involves converting the original text and personal keys to a partly purposeful form and providing protection. Some variations have been occurred in this technique and they proved system protection in casual vision model.

Identity-based encryption helps to revoke users from system. By connecting with trusted management, the sender needs to use time periods for encoding the information and receiver can updates personal keys. The key updates in the system suffer from bottleneck issue. The key update effectiveness on trusted party could improve by identity based encoding [4].

The problem of applying attribute based encryption over delay tolerant networks will leads to various security issues. In the network some users may move from one region to another region, at this point there attributes can be changed and private keys may be compromised. There are multiple key authorities they can be compromised within the system. By observing node association the key revocation issue can be solved and they propose quick randomized calculation [5] Quality based encryption technique helps to solve key escrow problem.

The personal key of users is associated with set of characteristic and an access policy will specified by an encrypted cipher text over attributes. The user attributes should specify the cipher-text attribute based encryption stratergies then only a customer can decode the data. Based on number of assumptions they represents CP-ABE scheme [6] first, and they had develop the access structure that are represented by size access tree with entry gates as its nodes.

III. SYSTEM DESIGN

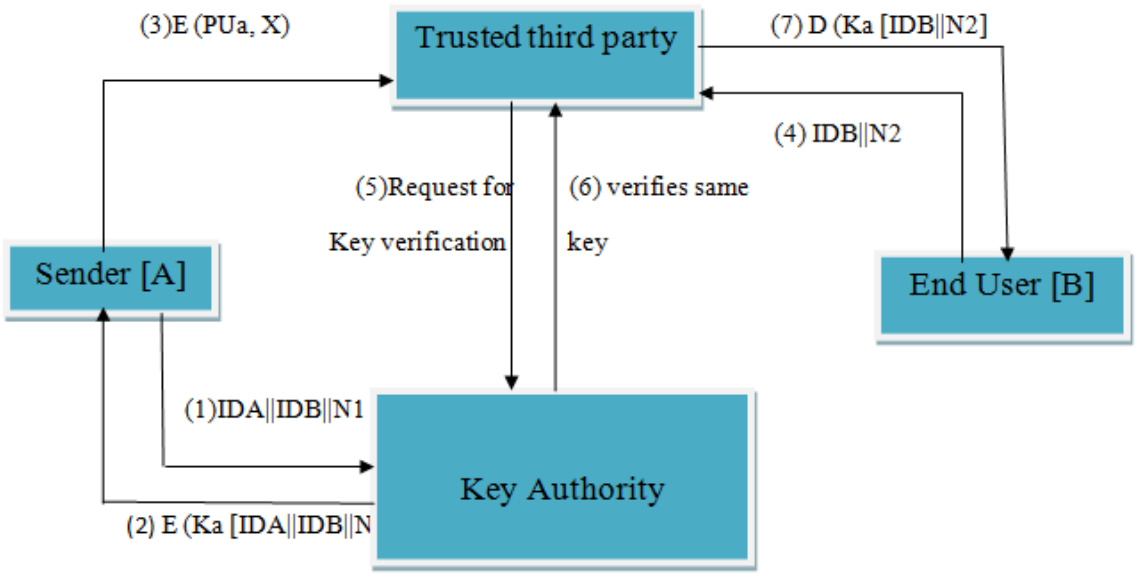

Fig1Block diagram of proposed system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

The above diagram depicts block diagram of proposed system. The description of each module is shown below. The steps involved in above diagram are as follows.

1. The authorized sender issues request for secret key to key authority it involves identification of A, identification of B followed by nonce N1.
   Nonce is a random number which is known to only key authority and sender to maintain security.
   (1)IDA||IDB||N1
2. The key authority verifies that sender is authorized or not then it will accept the request and sends secret key (ka) which is encrypted to sender.
   (2) E (Ka [IDA||IDB||N1])
3. The sender will receive secret key then it will encrypt the plain text (X)by using his/her public key (PUa) and stored it in trusted third party node.
   (3) E (PUa, X)
4. The end user issues request to trusted third party node for secret key to decrypt the data which involves identification of B followed by nonce N2.
   (4) IDB||N2
5. The third party node will receives request and sends request to key authority for verifying secret key.
6. If same secret key is found the key authority conforms and sends response to the third party node.
7. The third party node sends secret key to end user along with identification of B followed by nonce. The end user receives secret key and decrypt the data by using his/her public key.
   (7) D (PUb, M)

IV. EXPERIMENTAL RESULTS

1. The proposed system involves single authority where the communication cost will be reduced compared to multi authority system. The fig2 shows comparison graph for communication cost between multi authority and single authority system.

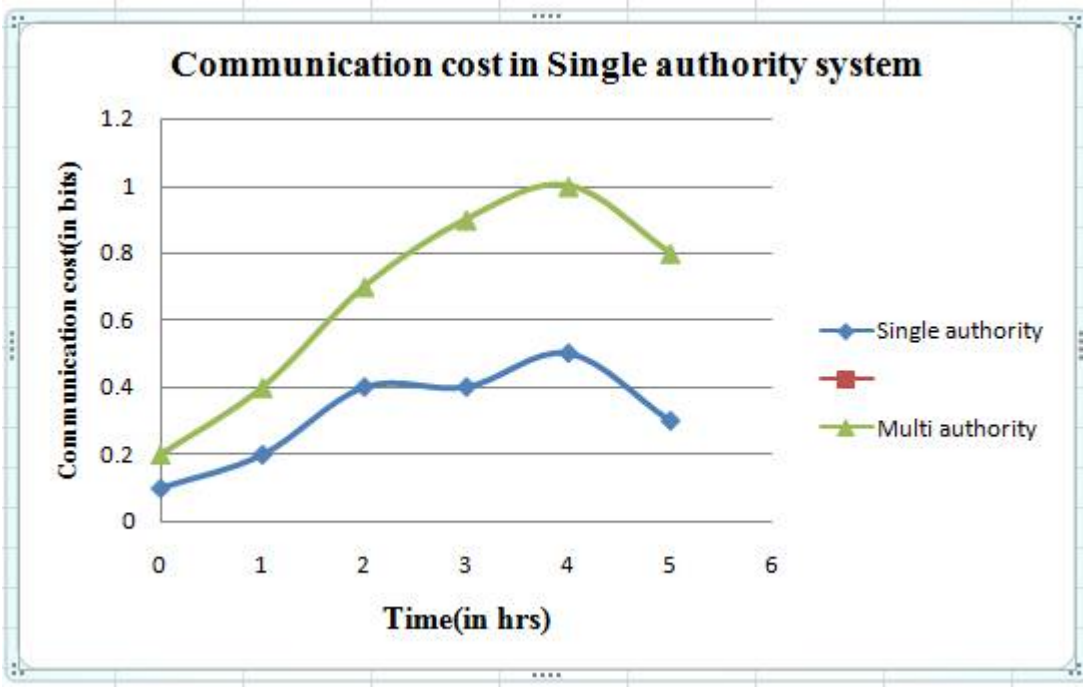

Fig2-Communication cost in single authority system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

1. The fig3 shows how much the power will be utilized within the entire process. From graph it is concluded that power utilization is less in single authority compared to the multi authority system.

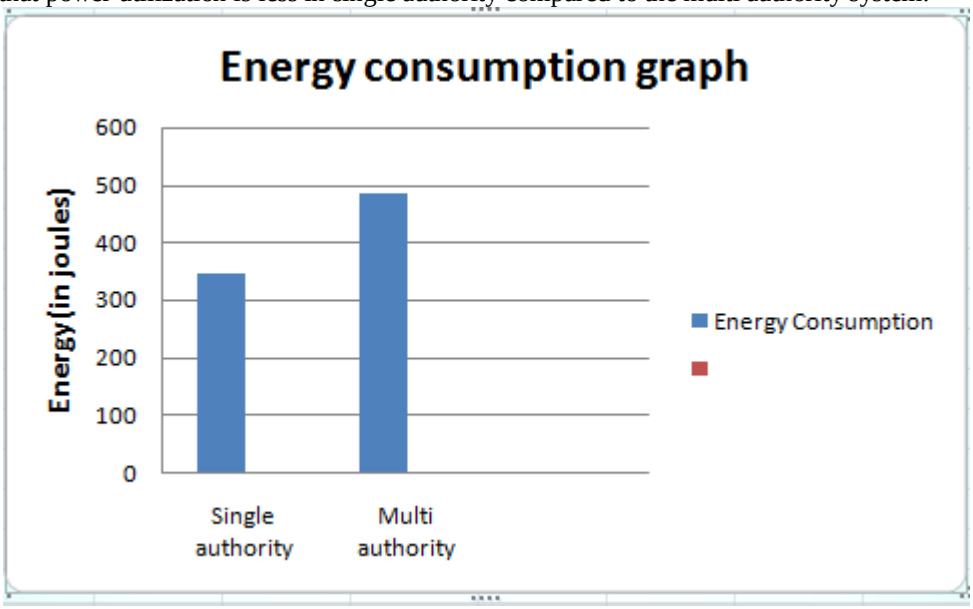

Fig3-Power utilization in single authority system

2. The fig4 presents how much time is required to transfer the packets within single authority system. From graph it is concluded that time requirement is less compared to multi authority system as shown below.

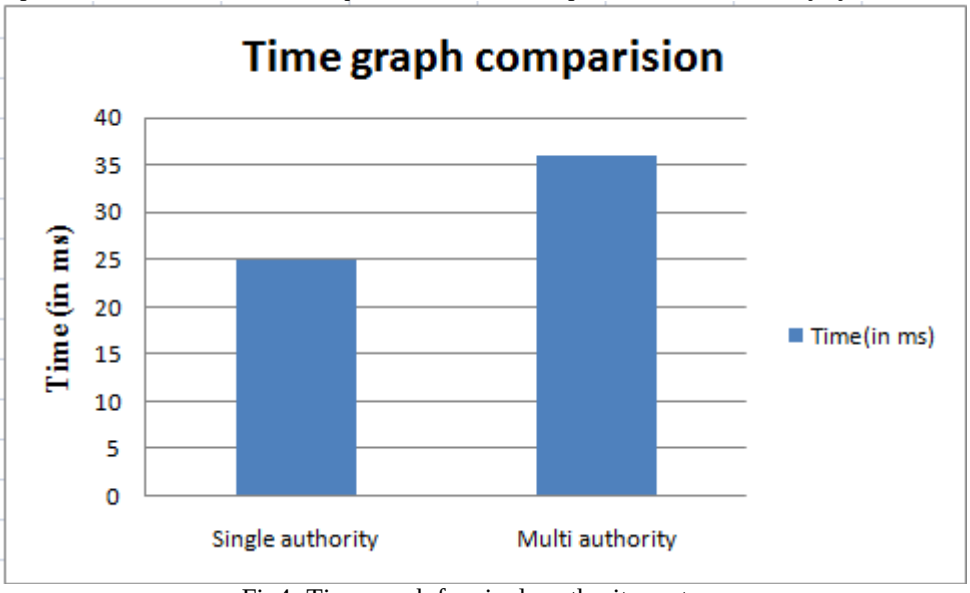

Fig4- Time graph for single authority system

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

V. CONCLUSION

The delay tolerant network provides continuous packet transmission between source nodes to destination node. The encoded text strategy attribute based encryption defines an access control policies on user attributes. The end should posses an attribute set to access any confidential information stored in trusted third party node. The immutable type of file avoids modification of data by providing more security to the data. The use of single authority system in network provides less communication cost, less power utilization and less time compared to the multi authority system. The total time required for single authority system for an entire process is 25ms as multi authority requires total 35ms for entire process in the system. Total power utilization for single authority system will be 345J which is less as compared with the multi authority system

REFERENCES

[1]L. Ibrahim, M. Petkovic, S. Nikova, P.Hartel, and W. Jonker, "Mediated ciphertextpolicy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS5932, pp. 309–323.
[2] L. Cheung and C. Newport, "Provablysecure ciphertext policy ABE," in Proc. ACMConf. Comput. Commun. Security, 2007, pp. 456–465.
[3] Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[4] Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun Security, 2008, pp. 417–426.
[5] Hur And Kang," Secure Data Retrieval For Decentralized Disruption-tolerant Military Networks" ICM IEEE Transc, Feb 2014.
[6] V.Goyal, A. Jain,O. Pandey, and A. Sahai, "Bounded cipher text policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.