Military Secured Network Data Transmission

Shubham Jain[1], Umesh Dusane[2], Smita Lokhande [3], Vinod Kadam [4], Asst. Prof. Neha Jamdar[5]

[1]University of Pune, Sinhgad Institute of Technology and Science,
STES Campus, Lonavala-410401, India
jains7272@gmail.com

[2] University of Pune, Sinhgad Institute of Technology and Science,
STES Campus, Lonavala-410401, India
umeshdusane115@gmail.com

[3] University of Pune, Sinhgad Institute of Technology and Science,
STES Campus, Lonavala-410401, India
Lokhandesmita6@gmail.com

[4] University of Pune, Sinhgad Institute of Technology and Science,
STES Campus, Lonavala-410401, India
balu.98889@gmail.com

[5] Asst. Prof. At Sinhgad Institute of Technology and Science,
STES Campus, Lonavala-410401, India
nnj.sknsits@sinhghad.edu

Abstract - *Mobile nodes in military situations, for example, a war zone or an unfriendly region are probably going to experience the ill effects of discontinuous system availability and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that permit wireless devices carried by soldiers to communicate with each other and get to the private data or charge dependably by abusing outside storage nodes. Probably the hardest issues in this situation are the requirement of approval strategies and the arrangements upgrade for secure information recovery. Ciphertext-approach characteristic based encryption (CP-ABE) is a promising cryptographic solution to the access control problem. However, the problem of applying CP-ABE in decentralized DTNs presents a few security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and proficiently deal with the classified information conveyed in the disturbance tolerant military system.*

***Key Words*: Communication, Network Encryption Permission Transmission**

1. INTRODUCTION

Military environment is a unfriendly and a turbulent one in this way, applications running in this environment needs more security to ensure their data, get to control and their cryptographic strategies. For correspondence to occur a node must be made and a connection established between the node and the neighbor nodes in this hostile networking environment, yet in the event that there is no association between the source and the destination the message from the source node may have to hold up depending on when the connection will be

eventually established. We refer to this DTN architecture where various authorities issue and deal with their own property keys independently as a decentralized DTN. In this paper, we describe a CP-ABE based encryption scheme that gives fine-grained get to control. In a CP-ABE scheme, every client is connected with an arrangement of characteristics in view of which the client's private key is produced. Substance are encoded under a get to arrangement with the end goal that exclusive those clients whose properties coordinate the get to strategy can decode. The idea of attribute-based encryption (ABE) is a promising methodology that satisfies the requirements for secure data recovery in DTNs. ABE features a mechanism that enables to get control over encrypted data using access strategies and credited attributes among private keys and figure writings. Particularly, figure content approach ABE (CP-ABE) gives a versatile method for encoding information with the end goal that the encryptor characterizes the attribute set that the decryptor needs to have so as to decrypt the figure content. In CP-ABE, the key power creates private keys of clients by applying the power's master keys to clients' related arrangement of attributes. The key authorities are semi-believed, they should be discouraged from accessing plain text of the information in the storage node; then, they should be still ready to issue secret keys to clients. On the off chance that the key authority is compromised by enemies when deployed in the threatening situations, this could be a potential danger to the data confidentiality or security particularly when the data is highly sensitive. Keeping in mind the end goal to understand the objectives of CP-ABE the key power makes utilization of masters secret keys and private keys of which the users apply by asking for it from the key authority. At the point when a client entered in a few qualities that matches or compares with the one in the get to arrangement, it is updated to coordinate with the group attributes which gives security for group members.

2. Literature Survey

1. Secure Data Retrieval For Decentralized Disruption Tolerant Military Network, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248- 9622:

In this paper, Author propose a ensured data recovery arrange using CP-ABE for decentralized DTNs where various key powers manage their credits independently. We display how to apply the proposed framework to safely and proficiently deal with the assembled information scattered in the Interruption or disturbance tolerant system.

2. Attribute Based Secure Data Retrieval System for Decentralized Disruption Tolerant Military Networks", Sagar. International Journal on Recent and Innovation Trends in Computing and Communication 2014:

In these frameworks organization circumstances DTN is especially compelling development The thought is Cipher content Policy ABE (CP-ABE).it gives a fitting strategy for encryption of data. The encryption incorporates the property set that the decoding needs remembering the true objective to unscramble the figure content. Consequently, Many customers can be allowed to decode various parts of data as indicated by the security approach.

3. Secure Data Retrieval For Decentralized Disruption Tolerant Military Network, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248- 9622:

In this paper, Author propose a ensured data recovery arrange using CP-ABE for decentralized DTNs where various key powers manage their credits independently. We display how to apply the proposed framework to safely and proficiently deal with the assembled information scattered in the Interruption or disturbance tolerant system.

4. Advanced Data Access Scheme in Disruption Tolerant Network, International Journal of Innovative Research in Computer and Communication Engineering:

In this methodology, each center point separates other neighbor centers, which are arranged in the same subtask group. While each subtask cluster pioneer recognizes diverse SGLs and center points in its subtask total and took after with the distributed trust evaluation is discontinuously upgraded considering either organize observations or indirect perceptions. The trial comes about exhibit that, the

proposed ETMS system achieves high efficiency and security with less complexity.

5. CP-ABE in Decentralized Disruption-Tolerant Military Networks for Secure Retrieval of Data, Proceedings of the International Conference, "Computational Systems for Health Sustainability"17-18, April, 2015:

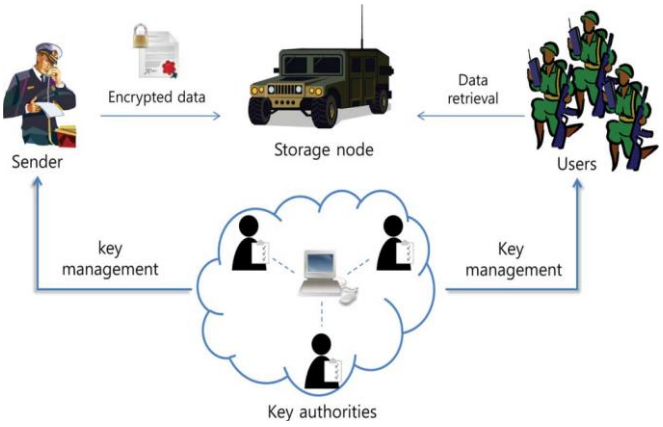
CPABE is one such cryptographic framework which gives the response for the passageway control issues. Nevertheless, there exists a couple issues regarding key escrow, trademark repudiation and coordination of attributes which are issued by various key powers while applying CP-ABE in decentralized DTNs. In this paper, more secured methodology for the recovery of ordered data using CP-ABE for decentralized DTNs is proposed where sets of attributes will be created and administered by various forces independently and addresses a couple existing issue.

.

1. PROPOSED SYSTEM

To propose a characteristic based secure information recovery scheme utilizing CP-ABE for decentralized DTNs. Ciphertext-arrangement ABE (CP-ABE) gives a versatile method for encoding information with the end goal that the encryptor characterizes the quality set that the decryptor needs to have keeping in mind the end goal to decrypt the ciphertext. The key issuing protocol creates and issues user secret keys by playing out a secure two-party computation(2PC) protocol among the key authorities with their own master secrets.The 2PC protocol stops the key authorities from obtaining any master secret data of each other with the end goal that none of them could generate the entire arrangement of client keys alone.

2. SYSTEM ARCHITECTURE



3. ALGORITHM

CP-ABE consists of four polynomial algorithms as follows.

1. Setup (**1** $\boldsymbol{k}$: It will take implicit security parameter k and output public parameter MPK and master key MSK.

2. KeyGen (MSK, S): The key generation algorithm run by Central Authority (CA), takes as input the master key of CA and the set of attributes S for user and then generates the secret key SK.

3. Encrypt (MPK, M, A): The encryption algorithm takes as input the message M, public parameter MPK and access structure A over the universe of attributes. Generate the output CT such that only those users who had valid set of attributes which satisfy the access policy can only able to decrypt. Assume that the CT implicitly contains access structure A.

4. Decrypt (MPK, CT, SK) : The decrypt algorithm run by user takes input the public parameter MPK, the ciphertext CT contains access structure A and the secret key SK containing attribute set S. If S satisfies the access tree then algorithm decrypt the CT and give M otherwise gives "ϕ".

5. MATHEMATICAL MODEL

a. Let 'S' be the | Military Security system as the final set

S = {……

b. Identify the inputs as D , Q,E,F

S = {D, R, L,P …

D = {D1, D2, D3, D4, ...| 'D' given database updates}
R = {R 1, R 2, R 3, R 4, ...| 'R' given User Register.}
L = {L 1, L 2, L 3,L 4, ...| 'L' given username and password for login .}
E = {E 1, E 2, E 3, E4, ...| 'E' given username and encrypted data To Process.}

c. Identify the outputs as O

S = {D, R, L,E ,M , …
M = {M 1, M 2, M 3, M 4, ...| 'M' given search result as decrypted data}

d. Identify the functions as 'F'

S = {D, R, L,M, F…
F = {F1(), F2(), F3(), F4(), F5(),F6() ,F7() }

F1(D) :: Update Database
F2 (R) :: Process Requestsas Register User
F3 (L) :: Process Requests as Login User
F4 (P) :: Process Requests on data to sending
F F5 (R) :: Respond to Register Success
F F6 (L) :: Respond to Login Success
F F7 (E) :: Respond as Decrypted data

6. RESULTS AND DISCUSSION

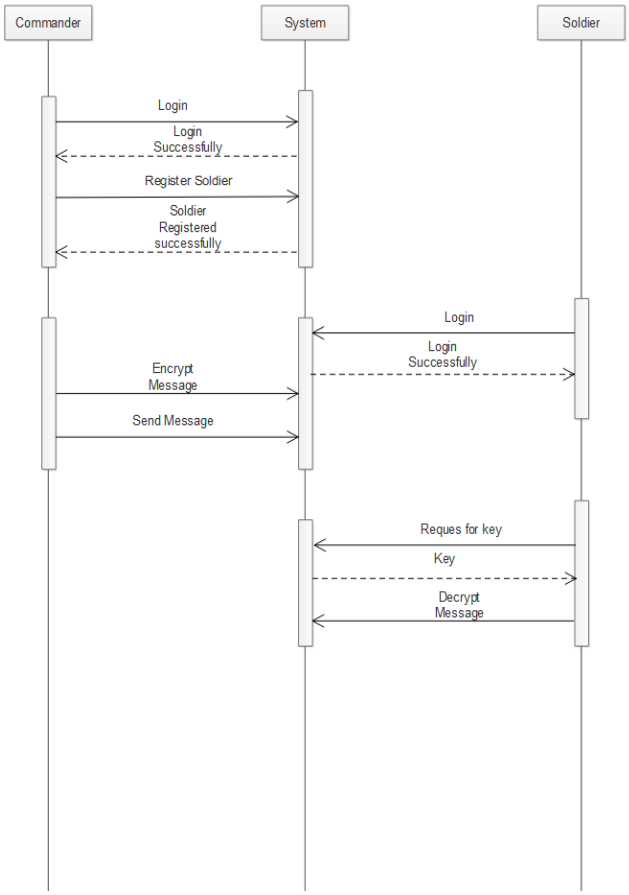


Fig 2. Sequence Diagram

7. 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 secure data retrieval issues. In this paper, efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow

problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption tolerant military network.

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,
pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint 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, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

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