ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 23 – 26 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp05.pdf

ENHANCING SECURITY FOR DATA RETRIEVAL USING CP-ABE IN DECENTRALIZED DISRUPTION-TOLERANT MILITARY NETWORKS

N.R.Sandhya[1], Y.Vijay kumar[2]
[1]M.Tech CS Student, S.V .College of Engineering, Tirupati, AP, India
sandhya1241@gmail.com
[2]Assistant Professor, Dept. of CSE, S.V.College Of Engineering, Tirupati, AP, India,
vijaykumar.y@svcolleges.edu.in

ABSTRACT

Generally, security plays a crucial role in a network communication. It should be highly enhanced while dealing with confidential information especially with armed forces. Movable nodes in a network are predicted to occur at regular or irregular intervals and fractionnements One of the best and successful technique is Disruption-tolerant networks provides reliable communication between an armed forces consistently. The most proficient elucidation that changes the data into an unreadable format is an technique called Ciphertext-policy attribute based encryption. Decentralized DTNs having CP-ABE convey in several security and isolation challenges with regard to the attribute revocation, a fair cryptosystem, and the combination of attributes issued form different authorities. Multiple key authorities manage their attributes individually in an proposed system.

Key words : Disruption-tolerant network (DTN), intermittent network connectivity, multiple key authorities, network disruptions.

1.INTRODUCTION

During loads of armed network scenarios, links of wireless plans approved by armed forces may be for the moment isolated by overcrowding, natural calamities, mobility, most probably when they run in aggressive surroundings. Disruption-tolerant network (DTN) techniques are fetching winning solution that let nodes to converse with each other in these tremendous networking. Typically, if there exists no direct connection between source node and destination node messages send by source node has to wait at the middle of the nodes in a network until link is finally recognized. Many armed abstractions have need of enlarged security of secret data together with control access methods which are stored in an unreadable format. In many situations, it is enviable to supply differentiated access services such that access policies of an information are clear over attributes users, which are supervised by the key authorities. For example, in a disruption-tolerant network, a chief officer may store up top secret information at a storage node, which should be accessed by members of “troop 1” who are involving in “Area .In this case, it is sensible hypothesis that several key authorities are liable to deal with their own lively attributes for military in their deployed sections, which could be regularly altered (e.g., the attribute representing present position of moving soldiers). We refer to this DTN structural design where numerous authorities issue and deal with their own attribute keys separately as decentralized DTN.The useful approach of an attribute-based encryption (ABE) is the data can be decrypted only if the user satisfy attribute credentials. Encryptor defines the attribute set and decryptor must posses in order to decrypt the cipher text. Hence multiple users satisfy user credentials can decrypt the text securely using CP-ABE.

Applying ABE to an DTN’s introduces several security issues. First confront in Attribute revocation is if the user leave an attribute set and change his location, the key of the previous set is known to the revoked user hence whenever the user changes his location the key has to be changed. If the key is not updated of altered instantly if may result in the blockage during rekeying procedure and security is highly compromised heavily if the key updation is not done instantly.

Next introduces scalability problem when the users often changes an attribute set authorities has to find the set and update key for an particular set instantly. On frequent updating the key may affect the non-revoked users.
The next confront is fair cryptosystem problem where the encrypted and decrypted data can be accessed by some third party with some conditions controlled. Private key generated by CP-ABE key authority uses his own master key. This may lead to data degradation when the key authority is compromised. Hence it is essential to remove third party access where data retrieved using escrow in CP-ABE single or multiple-authority.

The last confront is attributes organizing which are provided from various authorities. Numerous authorities when dealing with issueing attributes keys with their master keys to users, it is very rigid to classify policies with fine-grained access issued by authorities over attributes. For example, suppose the attributes “role 3” and “region 6” are managed by the Authority X, and “role 4” and “region 8” are managed by the authority Y. Then, it is impossible to generate an access policy ((“role 1” OR “role 2”) AND (“region 1” or “region 2”)) because the OR logic cannot be implemented issued by different authorities between attributes. This is due to the reality that the different authorities

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 23 – 26 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp05.pdf

generate their own attribute keys using their own individual master secret keys.

Therefore, the logic"-out-of-", cannot be expressed in the previous schemes, requires policy access logic which is realistic.

Propose technique we implement here is an using CP-ABE for decentralized DTN's attribute-based protected data recovery scheme. Immediate attribute officially changing decreases windows liability and enhance backward/forward secrecy of secret data. And encryptions using monotone access structure can be described as a fine-grained access policy under attributes issued from any chosen set of authorities. The fair cryptosystem problem exploits the feature of DTN in decentralized structural design determined by an escrow-free key issuing protocol. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The key issuing generates an secure protocol known as 2PC protocol which deters the key authorities from obtaining any master covert data of each other such that none of them could produce the complete set of user keys unaided.

2. RELATED WORK

In the present growing networking technologies privacy and security plays a major role it has to be highly enhanced while dealing with an confidential information likely in an armed forces or military communication. ABE (attribute based encryption, it is public key encryption technique where decryption of a ciphertext can be done by an user only when key match the attributes of the ciphertext when compared.

Disruption-tolerant networks are network intended so that temporary or intermittent problems has as less adverse impact on using DTN's. Movable nodes in a network are predicted to occur at regular or irregular intervals and fractionnements One of the best and successful technique is Disruption-tolerant networks provides reliable communication between an armed forces consistently. The most proficient technique used here is CP-ABE that changes the data into an unreadable format. CP-ABE introduces several isolation challenges on applying for decentralized DTNs with regard to the attribute changing officially, faircryptosystem, and the coordination of attributes issued form different authorities.

First confrot in Attribute revocation is if the user leave an attribute set and change his location, the key of the previous set is known to the revoked user hence whenever the user changes his location the key has to be changed. If the key is not updated of altered instantly if may result in the blockage during rekeying procedure and security is highly compromised heavily if the key updation is not done instantly.

Next introduces scalability problem when the users often changes an attribute set authorities has to find the set and update key for an particular set instantly. On frequent updating the key may affect the non-revoked users.

The last confront is faircryptosystem where the encrypted and decrypted data are placed in escrow where the third party can access the encrypted or decrypted data under some controlled conditions. Using ones own master key CP-ABE generates private key. Which may lead to data degradation when the key authority is compromised.When compared to existing system in proposed system it enables authority to revoke user attributes with minimal cost. by using of proxy re-encryption with CP-ABE and improves efficiency.

3. PRESENT TECHNOLOGY

ABE (attribute based encryption) is public key encryption technique where decryption of a ciphertext can be done by an user only when key match the attributes of the ciphertext when compared. The most proficient elucidation that changes the data into an unreadable format is an technique called Ciphertext-policy attribute based encryption. Decentralized DTNs having CP-ABE convey in several security and isolation challenges with regard to the attribute revocation, a fair cryptosystem, and the combination of attributes issued form different authorities. Multiple key authorities manage their attributes individually in an proposed system.

3.1 Drawbacks

First drawback in Attribute revocation is if the user leave an attribute set and change his location, the key of the previous set is known to the revoked user hence whenever the user changes his location the key has to be changed. If the key is not updated of altered instantly if may result in the blockage during rekeying procedure and security is highly compromised heavily if the key updation is not done instantly.Next introduces scalability problem when the users often changes an attribute set authorities has to find the set and update key for an particular set instantly. On frequent updating the key may affect the non-revoked users.

The last confront is faircryptosystem where the encrypted and decrypted data are placed in escrow where the third party can access the encrypted or decrypted data under some controlled conditions.Using ones own master key CP-ABE generates private key. Which may lead to data degradation when the key authority is compromised.

4. 2 PC Protocol

The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The key issuing generates an secure protocol known as 2PC protocol which deters the key authorities from obtaining any master covert data of each other such that none of them could produce the complete set of user keys unaided.

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 23 – 26 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp05.pdf

5. IMPLEMENTING AN TRUSTWORTHY SYSTEM

In traditional distributed system user can able to access the data if he satisfy certain attribute policies. But at present the only way to implement such policies is to use of trust worthy server to store the data and reconcile access control. The main problem here is if the security of the server is compromised then the data confidentiality is also compromised. The most proficient elucidation that changes the data into an unreadable format is an technique called Ciphertext-policy attribute based encryption. CP-ABE for decentralized DTN's are not completely provide trustworthy server. To address these challenges a novel public-key cryptography ABE is enhanced. There comes three enhancement schemes for ABE. First is to focus on how to remove users officially in an untrusted servers in this work we can enable data owner to delegate most task performing user removal without sending data to them. Second is addressing key attacks where untrusted users share their decryption keys with unauthorized users. Third is studying the enhancement schemes on issuing the privacy storage in ABE.

6. NETWORK ARCHITECTURE

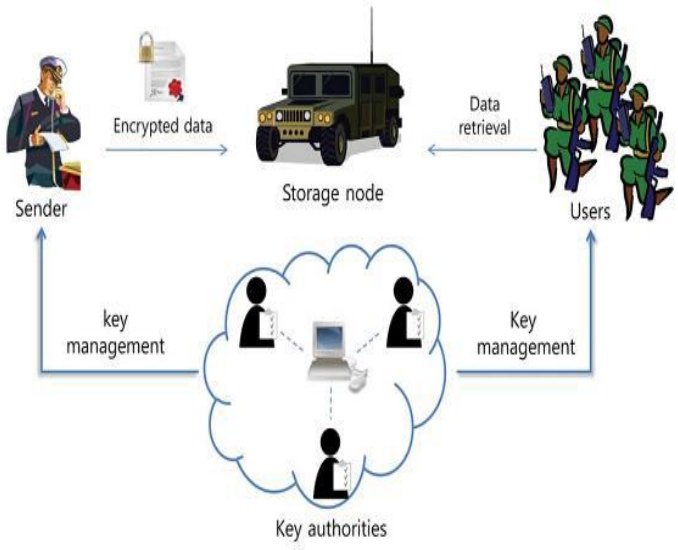

Figure 1:Secure data retrieval in a disruption-tolerant military network.

1) Key Authorities: They generate keys to the users. They have a central authority. They issue key based on the attributes.
2) Storage node: They stores data from sender node. User who satisfies the sender attributes can retrieve the data from storage node.
3) Sender: They are the one who sends data to users.
4) User: User who wants to access the information store at the storage node (e.g., a soldier). But must satisfy user credentials.

7.RESULTS

The effectiveness of an proposed system is improved when compared to an existing system. Authority can revoke user attributes with minimal cost by using proxy re-encryption with CP-ABE reduces communication costs and improve performance cost. And also by using some enhancement techniques like. First is to focus on how to remove users officially in an untrusted servers in this work we can enable data owner to delegate most task performing user removal without sending data to them. Second is addressing key attacks where untrusted users share their decryption keys with unauthorized users. Third is studying the enhancement schemes on issuing the privacy storage in ABE. Thus performance also get increased.

8.ENHANCEMENT OF PROPOSED SCHEME

1. Information privacy: Users who do not satisfy the access rules are to be removed from using the basic information in the storage node.
2. Collusion-resistance: Numerous users obtaining same attributes can decrypt the cipher text by combining their attributes.
3. Backward and forward Secrecy : Forward secrecy means the user should be banned from attaining the plain text of the data on or before holding on attribute, on the other hand backward secrecy means when an user missed an attribute should be banned from regaining the plain text.

9. CONCLUSION

DTN technique now fetching winning solutions in armed application that allow communications reliably and maintaining secrecy. CP-ABE for DTN's provides reliable cryptographic approach where numerous key system manage their key attributes separately. A fair cryptosystem problem is determined where the confidentiality of data is definite under aggressive environment. Also providing a key removal in a fine grained for an element set when created.

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] 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.
[3] M. Chuah and P. Yang, **"Node density-based adaptive routing scheme for disruption tolerant networks,"** in Proc. IEEE MILCOM, 2006, pp. 1–6.
[4] M. M. B. Tariq, M. Ammar, and E. Zequra, **"Mesage ferry route design for sparse ad hoc networks with mobile nodes,"** in Proc. ACM Mobi Hoc, 2006, pp. 37–48.

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 23 – 26 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp05.pdf

[5] 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.

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

[7] 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.

[8] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, **"Mediated cipher text-policy attribute-basedencryption and its application,"** in Proc. WISA, 2009, LNCS 5932, pp. 309–323.