IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 4, April 2015
ISSN: 2394 - 6598
www.ijetie.org

Secured Data Retrieval In Disruption Tolerant Military Networks Using Cp-Abe

J.Naskath[#1] S.Jenefa Jemima[#2], P.Anitha[#3]
Research student[#2,3 2], Professor[#1],
Computer Science and Engineering Department,
National Engineering College, India. [#1, 2, 3]
[3]naskath.nec@gmail.com

ABSTRACT

Mobile nodes in military environments such as battle field or hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption Tolerant Network(DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting externally storage nodes. Cipher text policy attribute based encryption(CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of CBE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation. The proposed paper considers an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Key escrow problem is resolved by an escrow-free key issuing protocol.The proposed mechanism demonstrates how to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. This system uses Java Eclipse as front end and MySQL as back end.

KeyWords: **Cipher–Text Policy Attribute Based Encryption, Key Authorities, Disruption Tolerant Military Networks, Key Generation, Storage Node, Key Generation Centre, Key Policy Attribute Based Encryption**

1.INTRODUCTION

Network security is a term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing and altering secure information.**D**isruption **T**olerant **N**etworks(DTN)is a type of network that is designed to provide communications in the most unstable and intermittent connections, where the network would normally be subject to frequent and long lasting disruptions that could severely degrade normal communications.Data retrieval means obtaining data from a database management system.In order to retrieve the desired data the user present a set of criteria by a query. Then software for managing databases, selects the demanded data from the database. The retrieved data may be stored in a file, printed, or viewed on the screen

2. RELATED WORKS

CP-ABE schemes are constructed on the architecture where multiple key authority has the power to generate the private keys with its secret information.The key escrow problem is resolved by escrow- free key issuing protocol in CP-ABE system[4][8][4].Cipher text Policy Attribute Based Encryption. Performance degradation is avoided in CP-ABE by resolving Key escrow problem. In Authentication and key generation phase The User Interface Design plays an important role for the user to move login the Application. This module has created for the security purpose. In this login page we have to enter user name and password, it will check username and password, if valid means directly go to home page, invalid username or password means show the error message and redirect to registration page. So we are preventing from unauthorized user entering into the login page to user page. In storage node phase data is stored from senders and corresponding access is provided to the valid users. Storage node may be mobile or static .This node stores the secret confidential information.store-carry and forward phase owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.If a user possesses a set of attributes satisfying the access

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 4, April 2015
ISSN: 2394 - 6598
www.ijetie.org

policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the cipher text and obtain the data. In Decentralized user phase We provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs[4]. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Communicate with every user in network. In Analysis phase module we are going to develop the user satisfied trust worthiness. This is analysed with the following information like i)how long user has touch with network , ii)what type of file sharing and when the user file sharing takes place with the specified time and date . iii) how many users are using in the network .

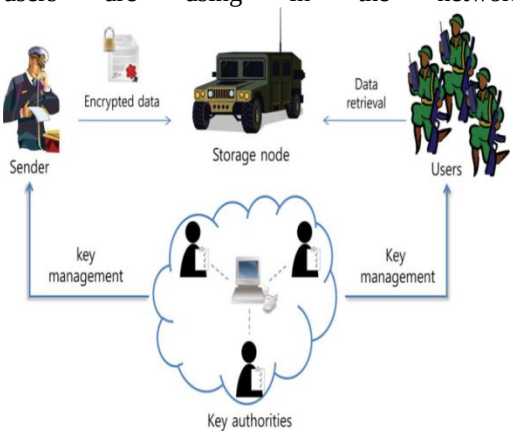


Figure 2.1 Architecture Design

The algorithm techniques that are used are*:* Ciphertext-policy attribute-based encryption[8] It is an identity-based encryption.In identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys. It allows policies specifying which private keys can decrypt which cipher-texts. The private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt. It is a Key generation algorithm that uses encryption and decryption modes to generate keys based on the attributes.2PC protocol-This protocol is used to communicate with the users.Escrow Free Key Issuing Protocol this protocol avoids the hacking by third party servers.The user validation for set of attribute in authentication of multi authority network environment is implemented in our work finally. We can hide the attribute in access control policy of a user. Different users are allowed to decrypt different pieces of data per the security policy. We going to achieve the data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes. The multi key authority is such no longer as well as the storage node in unauthorized user. In confidentially data of authority issues set of attribute keys for their managing attributes to an authenticated user. The trusted authority is analysis by values of distributed identically. To analysis the graphical network communication.Thus we Proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage stheir attributes independently[4][8][12]. 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.

3. PROPOSED WORK

The paradigm of Attribute Based Encryption (ABE) is generally divided into Cipher-text Policy Attribute Based Encryption (CPABE) and Key Policy Attribute Based Encryption(KPABE)[12][4].Intuitively, CPABE allows a secret key with an attribute set can decrypt a cipher text with an access structure while KPABE allows a secret key with an access structure can decrypt a cipher text with an attribute set. Recently, a dual policy attribute based encryption, conjunctively combining CPABE and KPABE schemes. Revocation as an indispensable function in public key encryption . As the development of ABE, a lot more revocation techniques are invented and applied into such new primitive. In Cipher text-Policy Attribute-Based Encryption (CP-ABE)[12][4][8], the cipher text is associated with an access policy over attributes and the user secret key is associated with a set of attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the access policy specified in the cipher text. Several CP-ABE schemes have been intended, however, some practical problems, such as revocation, still need to be addressed. In the prevailing system, a user's identity must be validated by the authority, in distributed system; it is a complex task to manage numerous user identities. Also, all users must trust the central authority, if the authority is malicious; he can impersonate any user without being detected. Hence we are facing a major issue

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 4, April 2015
ISSN: 2394 - 6598
www.ijetie.org

with Key-Escrow problem .The secret key is generated in a single space. In turn, the system can be easily attacked by attacking the single space. Keys were generated randomly and it is decided by the key generation center and the user doesn't have any control/preferences or specification of deciding the key based on user centric purpose. The key generation center (KGC) can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential risk to the data confidentiality or privacy in the data sharing systems. The revocation of any attribute or any single user in an attribute group would affect all users in the group.Most of the existing ABE (Attribute-based encryption) [8] schemes are constructed on the architecture where a single trusted authority or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time[4][8][12]. The major drawbacks of the prevailing system is that the data sharing is not much secure and any other user can easily access the data in data store. In addition to it, the system won't distribute the data based on the attributes of the user. Hence in the proposed system, the key issuing protocol generates and issues user secret keys by using the multiple attributes obtained from the user. The major advantage of the proposed system is that the data is shared between the data owner and the users based on the attributes.

4. MODULE DESCRIPTION

AUTHENTICATION & KEY GENERATION

In this module the User Interface Design plays an important role for the user to move login the Application. This module has created for the security purpose. In this login page we have to enter user name and password, it will check username and password, if valid means directly go to home page, invalid username or password means show the error message and redirect to registration page. So we are preventing from unauthorized user entering into the login page to user page.

STORAGE NODE

In *storage node* phase data is stored from senders and corresponding access is provided to the valid users. Storage node may be mobile or static .This node stores the secret confidential information.*store-carry and forward* phase owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then user will be able to decrypt the cipher text & obtain data .

STORE-CARRY AND FORWARD PHASE

store-carry and forward phase owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments.

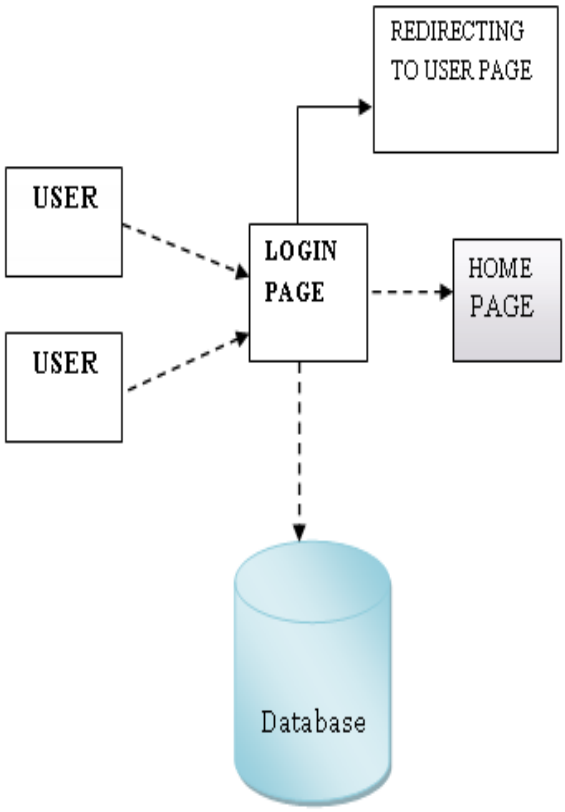


Figure 4.1 Authentication & Key Generation

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 4, April 2015
ISSN: 2394 - 6598
www.ijetie.org

.

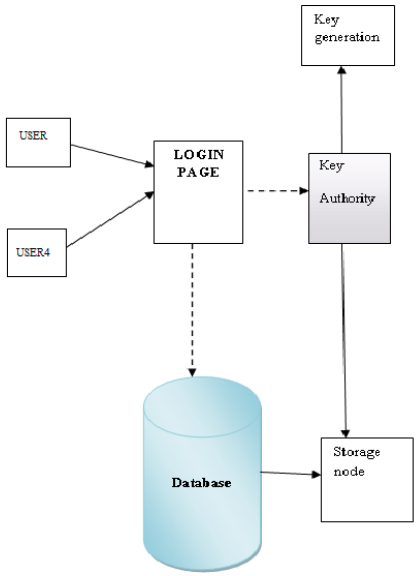


Figure 4.2 Storage Node

A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

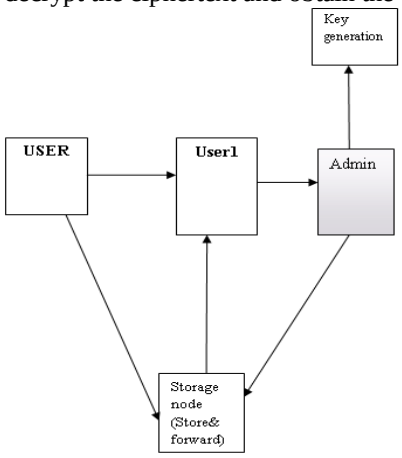


Figure 4.3 Store Carry and Forward

DECENTRALIZED USER PHASE

In Decentralized user phase**,**We provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Communicate with every user in network**.**

ANALYSIS

In *Analysis* phase module we are going to develop the user satisfied trust worthiness. This is analysed with the following information like i)how long user has touch with network , ii)what type of file sharing and when the user file sharing takes place with the specified time and date . iii) how many users are using in the network

System	Cipher Text Size	Rekeying Message	Private Key Size	Public Key Size
BSW	(t+)A0+A+ At	l(k+)A 0	(k+)A0	A0+A
DDTN	(t+m)A0+m A+At	l(k+)A 0	(k+m)A 0	mA0+ mA
Proposed	(t+)A0+A+ At	(n-l) log n/n-l A0	(k+)A0 +log n	A0+Ma

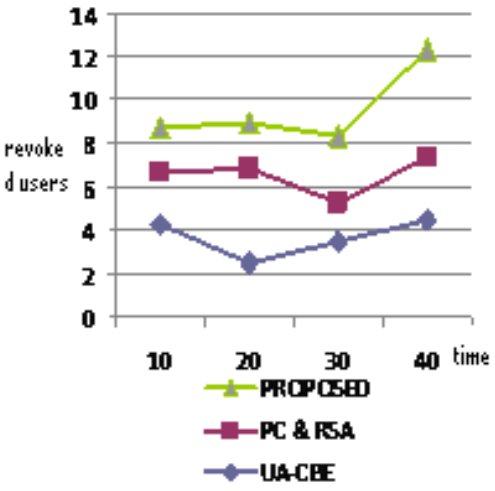
TABLE I- EFFICIENCY ANALYSIS

t- Number Of Attributes Appeared in T
A0- Bit Size Of An Element A-Bit Size O An Element T
Ct- Bit Size Of An Access Structure in T n-Number Of All Users In The System
k- Number Of Attributes Associated With Private Key Of User
m- Number Of Authorities In A System l-Number Of Users In Attribute Group

Table I summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update non revoked users' keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table I, the proposed scheme needs rekeying message size of at most to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 4, April 2015
ISSN: 2394 - 6598
www.ijetie.org

cipher text size is linear to the number of revoked users in the system since the user revocation message is included in the cipher text. The proposed scheme requires a user to store more KEYs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the cipher text size while realizing more secure immediate rekeying in multi authority systems.



4.5. Performance Analysis

5. CONCLUSION

Proposed an 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.

6.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. ACMMobiHoc, 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] Avi Kak and P. Yang, "Public-Key Cryptography and the RSA Algorithm ",March 24, 2015

[9] Brendan Burns University of Massachusetts – Amherst*," MV Routing and Capacity Building in DisruptionTolerant Networks ",2005*

[10] University of Florida Department ," Network Security: History, Importance, and Future challenges"2010

[11] Misael Mongiov`ı, Ambuj K. Singh, Xifeng Yan and Bo Zong "Efficient multicasting for delay tolerant networks using graph indexing",2008

[12] Li Qiu, Yong Li, Pan Hui, Depeng Jin, Li Su, Lieguang Zeng "Edge-Markovian Dynamic Graph Based Performance Evaluation for DelayTolerant Networks",2011

[13] Ioannis Psaras1, Lloyd Woodb, Rahim Tafazolli1a Center for Communication Systems Research (CCSR)," Delay-Disruption-Tolerant Networking State of the Art and Future Challenges",2012.

[14] S. Roy, M. Chuah Lehigh," Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs",2010.

[15] Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen,"Ciphertext policy attribute based encryption with efficient revocation",2011.

[16] Allison Lewko," Decentralizing Attribute-Based Encryption",2013

[17] Nishant Doshi and Devesh Jinwala ," Updating attribute in CP-ABE: A New Approach ",2010