Secure Data Recovery Encryption Scheme for Decentralized Disruption Tolerant Military Networks

M. Nanda Kishore.
MCA. MTech Dept. of Master of Computer Applications
Sri Venkateswara College of Engineering and Technology
Chittoor, Andhra Pradesh

T.Roopa Devi, T.Siva Kumar Reddy
Dept. of Master of Computer Applications
Sri Venkateswara College of Engineering andTechnology
Chittoor, Andhra Pradesh

***Abstract*—In the large number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the usual medium. Portable nodes in military environments such as a battlefield or a hostile region are likely to suffer from discontinuous network connectivity and frequent partitions. Disruption tolerant networks (DTNs) 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 abusing external storage nodes. The most challenging issues in this scenario are the enforcement of authorization policies and the policies update for Secure Data Recovery (SDR) in challenging cases. The requirements for Secure Data Recovery in DTNs fulfilled by the Attribute-Based Encryption (ABE). The most assured cryptographic solution is introduced to provide the access control issues called Cipher text Policy Attribute Based Encryption (CP-ABE). However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and Attributes coordination issued from multi authorities. In this paper, we recommend a secure data recovery encryption scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We show how to apply the proposed scheme to securely and proficiently deal with the classified data dispersed in the Disruption Tolerant Network (DTN).**

***Keywords*—Access Control, SDR, CP-ABE, DTNs, ABE, Multi Authorities**.

I. INTRODUCTION

The wireless devices used by the soldiers in Military environments might be gets disconnected due to jamming, ecological factors, and changes in location, mainly when they operate in remote environments. Disruption-tolerant network (DTN) architectures are best solutions that permit nodes to communicate with each other in farthest networking environments. DTN reduces intermittent communication issues by addressing technical problems in heterogeneous networks that lack continuous connectivity. When there is no end-to-end connection, the messages from the sender may need to wait in the intermediate nodes for a large amount of time until the connection would be correctly established. Roy and Chuah introduced storage nodes in DTNs where data is stored such that only authorized mobile devices can access the necessary data fastly and proficiently. In many scenarios, it is pleasing to provide differentiated data access policies are defined over user attributes. The data access policies are managed by the key authorities. For example, in DTNs, a sender may store secret data at a intermediate node, which must be retrieved by "Battalion 1" who are participating in "Region 2." It is a reasonable assumption that multiple key authorities are possible to manage their individual dynamic attributes for soldiers in their deployed regions, which could be repeatedly altered. We refer DTN architecture where multi authorities issue and deal with their own attribute keys independently as a decentralized DTN.

II. ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. Attribute Based Encryption (ABE) gives ordinary encryption and additional access control policy. ABE is more proficient, adaptable and suitable than other cryptographic strategies and may be a lightweight security arrangement. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). CP-ABE is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon

attributes (e.g. the region, or the kind of attribute he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text where the user keys are manages by the key authorities.

Analysis of existing system describes about the concept of Attribute-based encryption (ABE) approach that fulfills the requirements of retrieving the secure data in DTNs. ABE characterize a mechanism that empowers an access control over encrypted data utilizing access policies and attributed traits among private keys and cipher texts. Particularly, Cipher text-Policy ABE (CP-ABE) gives a versatile method for encrypting data, such that the encryptor characterizes the trait set that the decryptor needs to decrypt the cipher text. CP-ABE is more proper to DTNs than KP-ABE in light of the fact that it empowers encryptors consequently; different users are allowed to decrypt distinctive bits of data as per the security policy. Applying of ABE approach in DTNs leads to several security and privacy challenges. Since some of the users (clients) may exchange their associated attributes in some situations, some of the private keys might be used, revocation of keys for each attribute is essential to enhance the secure system. The major problem is the key escrow problem and the coordination of attributes that are issued by different authorities. Defining of fine-grained access policy becomes very hard, when multiple authorities issue different kind of attribute keys to all the users independently with their own master secret key.

1. Attribute Revocation: Since users may change their associated attributes at some point (for ex-ample, mobility), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is more challenging, mainly in ABE, since each attribute is conceivably shared by multiple users (we refer to such a collection of users as an attributes). This shows that attribute revocation or any single user in an attribute group would affect the other users in the group. For instance, if a member joins or leaves an attribute group, the corresponding attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may cause problem during rekeying procedure, or degrade the security due to the windows of vulnerability if the previous attribute key is not updated immediately.

2. Key Escrow: The key authority provides private keys by applying the authority's master secret keys to users associated set of attributes. Thus, the key authority can decrypt every cipher text to specific users by generating their attribute keys. If the key authority is compromised by hackers when deployed in the remote environments, this could be a main threat to the data secrecy or privacy especially when the data is highly sensitive. The key escrow is an main problem in the multi-authority systems as long as each key authority has the whole access to generate their own attribute keys with their own master secrets. Since the key generation mechanism based on the single master secret is the basic method for the asymmetric encryption systems such as the attribute-based or identity-based encryption rules, removal of key escrow in single or multiple-authority CP-ABE is a pivotal open problem

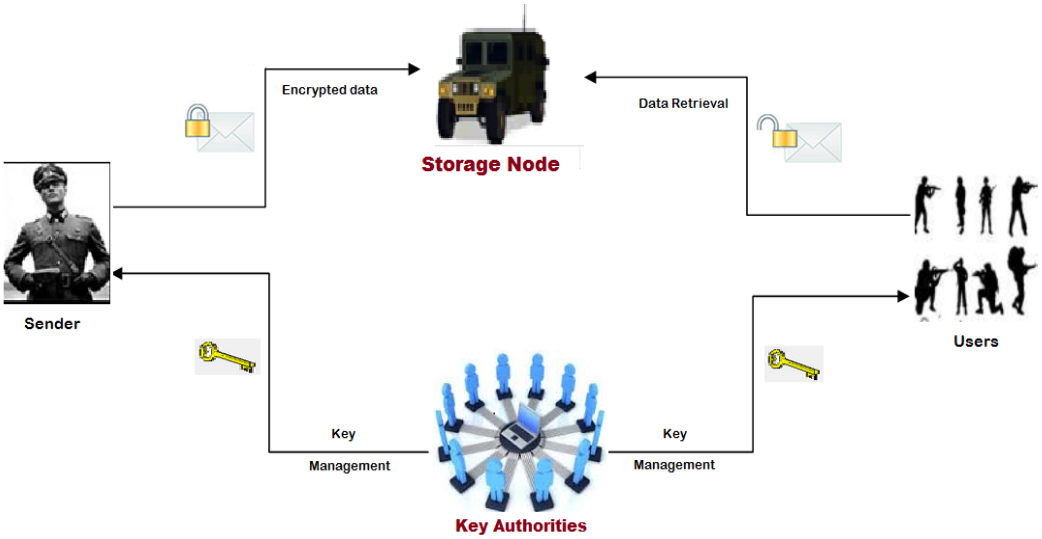
.

3. Attribute Coordination: When multiple key authorities manage and issue attributes keys to users with their own master secrets, which is very difficult to define fine-grained access policies over attributes issued from different key authorities. Because, the fact that the different authorities generate their own attribute keys using their own independent and separate master secret keys. Hence, general access policies cannot be expressed in the previous methods, which is very practical and commonly required access policy logic.

To overcome the problems in Existing analysis we recommend a novel CP-ABE scheme for a Secure Data Recovery (SDR).For Encoding and Decoding of data we can use the Advanced Encryption Standard (AES) algorithm. This is Symmetric key algorithm using the same private/public key for encrypting and decrypting the text. The key issuing centers use AES algorithm generates and issues user secret keys by performing a secure computation between the key-authorities and the data storing centre with their own master keys. The AES deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone The data secrecy and privacy can be cryptographically enforced against any curious data Storing centre in the proposed scheme.

1. The solving of key escrow problem done by escrow-free key using AES, which is constructed using the secure two-party computation between the key authority and the data storage centre.
2. Fine-grained user revocation for each attribute could be done which takes advantage of the selective attribute group key distribution on top of the ABE.

III. SYSTEM ARCHITECTURE



A. Sender: It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. Data Owner to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

B. Storage Centre: It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users for each attribute, which are used to enforce a fine-grained user access control. Data storing centre stores the data. Data Storage Centers provides offsite record and tape storage, retrieval, delivery and destruction services.

C. User: This is a mobile node who wants to right to use the facts stored at the storage node (e.g., a soldier).If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data.

D. Key Authorities: They are key generation centers that generate secret keys for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. We assume that there are protected and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. They grant differential access rights to individual users based on their attributes. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

E. Sensor Head: It is responsible for sensing the data stored in the storage node and it will provide the secure path to deliver the data for particular user by using their access policy.

IV. METHODOLOGY

An Advanced Encryption Standard (AES) is used for encrypting and decrypting the data and for generating the private keys for users, a symmetric block cipher that can process **data blocks** of **128 bits**, using cipher **keys** with lengths of **128**, **192**, and **256 bits**. Rijndael was designed to handle additional block sizes and key lengths; however they are not adopted in this standard. Throughout the remainder of this standard, the algorithm specified here in will be referred to as "the AES algorithm." The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256". Most of the existing ABE 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.A CP-ABE scheme consists of the following four algorithms:

1. Setup: This is a randomized algorithm that takes a security parameter as input, and yields the public parameters *PK* and a master key *MK*.*PK* is used for encryption and *MK* is used to generate user secret keys and is known only to the central authority.

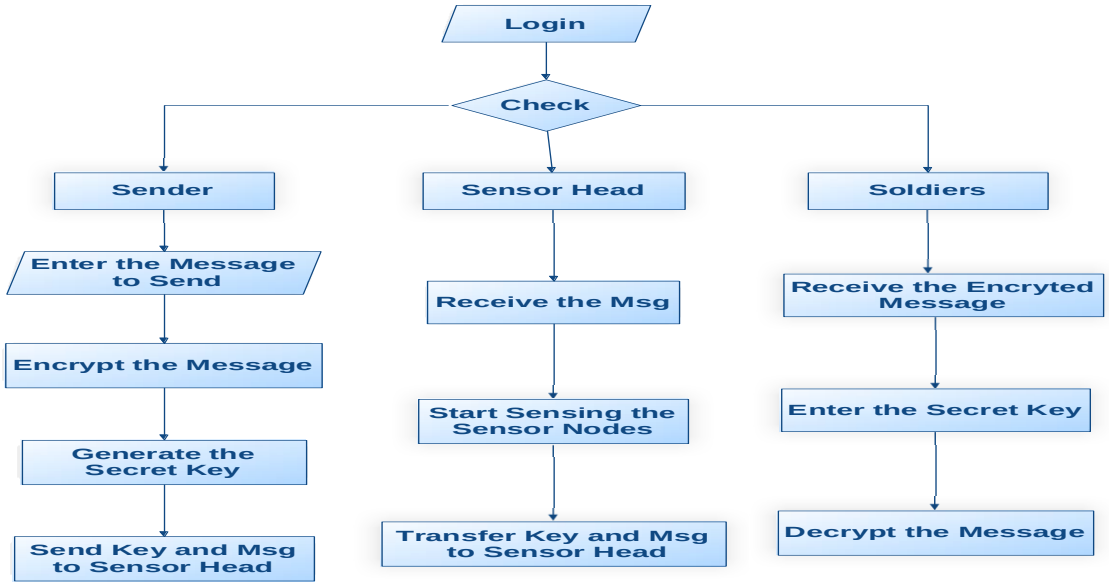
2. Encryption: This is a randomized algorithm takes as input a message *M*, an access structure, and the public parameters *PK*. It generates the cipher text *CT*.

*3. Key Generation***:** This is a randomized algorithm that takes as input the set of a user (say *X*)'s attributes *SX*, the master key *MK* and generates a secret key *SK* that identifies with *SX*.

4. Decryption: This algorithm takes as input the ciphertext *CT*, a secret key *SK* for an attribute set *SX*. If *SX* satisfies the access structure fixed in *CT*, it will provides the original message *M*.

V.DATA FLOW DIAGRAM (DFD)

1. DFD is also referred as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.



VI. RESULTS AND ANALYSIS

The implementations of Secure Data Recovery scheme have the following components.

Sender: Sender is the owner of the data that is encrypted (e.g., Commander) and that encrypted data send to the storage node and generates the secret key for that message. For this the sender need to register for authentication purpose. Sender has the components as Registration, Login, Encryption and Secret key generation.

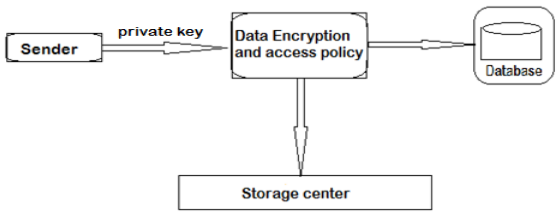


Fig: Sender (Encrypt data, Access policy)

Sender Login:

Data Encryption and Key generation:

Sensor Head: Sensor Head is server generates secure path and access policy to the user for retrieving the data from sender to storage node and storage center to Receiver (User). Sensor need to login and then make the sensing of transferring data.

User: User can decrypt the ciphertext that is encrypted plaintext by the sender using the generated secret key by the key authority for user attribute set. Here keys are managed by key authorities and retrieves the confidential data from sender in efficient way. Here the Receiver (User) has to register and login and then decrypt the data by applying the correct access that is matched to sender access policy.

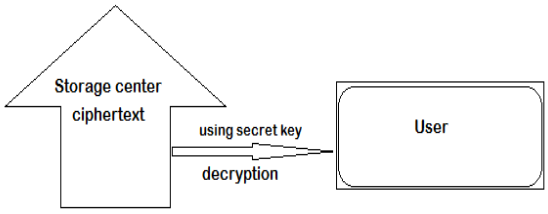
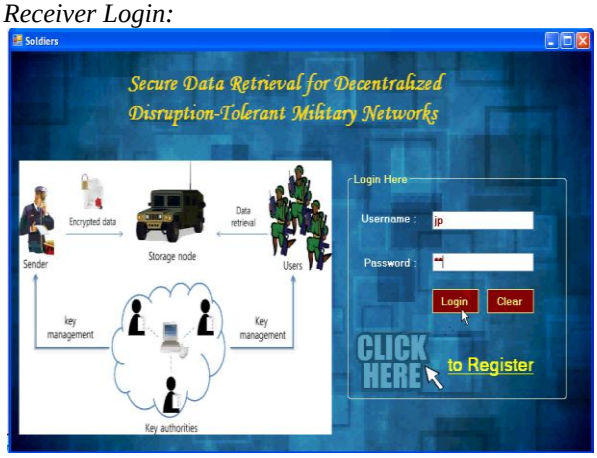
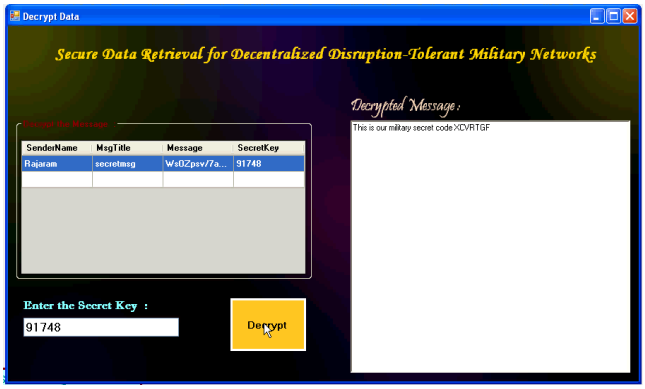


Fig: Data Retrieval

Receiver Login:



Data Retrieval:



VII. SECURITY ANALYSIS ANDFUTURE ENHANCEMENT

A. Security Analysis

1).Data confidentiality: Unauthorized users who do not have enough certifications fulfilling the access policy should be prevented from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities ought to be additionally forestalled.

2).Collusion-resistance: If multiple users collude, they may be able to decrypt a ciphertext by consolidating their attributes regardless of possibility that each of the users can't decrypt the ciphertext alone.

3).Backward and forward Secrecy: In the context of ABE, backward secrecy implies that any user who comes to hold an attribute (that fulfills the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. Then again, forward secrecy means that any user who drops an attribute ought to be prevented from accessing the plaintext of the consequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding fulfill the access policy.

B. Future Enhancement

In the future, it would be interesting to consider attribute-based encryption systems by applying advanced cryptosystem for data sharing. In future, we encrypt multimedia content, Solve the performance degradation of fully distributed approach, Neglected key expired time, we can use multi Data Storing Centre, Proxy servers to update user secret key without disclosing user attribute information.

VIII. CONCLUSION

DTNs technologies becoming more promising solutions to allow wireless devices to communicate in Military environments. CP-ABE is a scalable cryptographic solution to secure data and access control issues. Here the key authorities manage their attributes separately. We achieve more secure and efficient data access control in the data

recovery system. The fine-grained key revocation can be done and resolving of key-escrow guarantees that storage of secret data even under the hostile environment when the key authorities might not fully trust. We demonstrated that the proposed scheme is efficient and scalable to securely manage users data in the data retrieval system. Data can be shared with privacy and confidentiality.

IX. ACKNOWLEDGEMENT

First and foremost, we record our sincere thanks to Almighty GOD and we are grateful to our college & **Mr. Sendhil Kumar.MCA, M.Tech,** our Head of the Department of Master of Computer Applications and **Mr.NandaKishore, MCA. M.Tech,** our Assistant Professor for providing the necessary facilities during the execution of our project work. We also thank for their valuable suggestions, advice, guidance and constructive ideas in each and every step, which was indeed a great need towards the successful completion of the project.

REFERENCE

1. B.Bhuvaneshwaran and A. Vijay," Distribution of Secure Data Retrieval using Efficient Tolerant Military Network", Journal of Recent Research in Engineering and Technology (ISSN):2349-2252 Volume 2 Issue 2 Feb 2015.
2. JunbeomHur, KyungtaeKang,"Secure Data Retrieval for Decentralized Disruption Tolerant Military Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, Volume 22, NO.1, February 2014.
3. Fathima Nizer, G.S.Santhosh Kumar", a Survey on ABE Based Secure Data Retrieval Schemes for DTN Networks", International Journal of Engineering Trends and Technology (IJETT): Volume 20 Number 1-Feb 2015.
4. R.Dhivya,Ms.K.P.RamyaRani.M.E.,"Multi Secured Data Recovery from Disruption-Tolerant Military Networks",IJISET-International Journal of Innovative Science, Engineering and Technology, Volume 2 Issue 3,March 2015.
5. Karan Bhatia, "Performance Analysis: Symmetric key Cryptography vs. Ciphertext Policy Attribute Based Encryption on Cloud".
6. Federal Information Processing Standards Publication 197, November 2001.
7. S. Roy and M. Chuah, "Secure data retrieval based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) system for the DTNs", Lehigh CSE Tech. Rep., 2009.
8. S.Revathi and A.P.V.Raghavendra, "Advanced Data Access Scheme in Disruption- Tolerant Network", IJIRCCE Oct 2014.
9. B.SakthiSaravanan.M.Tech,R.Dheenadayalu.M.Sc, A.Vijayaraj (PhD), "Improving Efficiency and Security Based Data Sharing in Large Networks", International Journal of Engineering and Science and Innovative Technology (IJESIT), Volume 2,Issue 1,January 2013.

AUTHORS REFERENCE

1. **M.NandaKishore.MCA.,MTech**(Assistant Professor), Dept. of Master of Computer Applications, SriVenkateswaraCollegeof Engineering and Technology, Chittoor, Andhra Pradesh.
2. **T.Roopa Devi, MCA** (Scholar), Sri Venkateswara College of Engineering and Technology, Chittoor, Andhra Pradesh.
3. **T.Siva Kumar Reddy, MCA** (Scholar), Sri Venkateswara College of Engineering and Technology, Chittoor, Andhra Pradesh.