International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Mechanism for Secure Fault Tolerant Data Access in Disruption-Tolerant Networks

**Subhashini P[1], Ashwin Kumar M[2]**

[1]Department of Computer Science & Engineering, Mangalore Institute of Technology and Engineering Mangalore, Karnataka, India

[2]Sr. Assistant Professor, Department of Computer Science & Engineering, Mangalore Institute of Technology and Engineering Mangalore, Karnataka, India

**Abstract:** ***This paper presents the secure fault tolerant data access in Disruption-Tolerant networks using the mechanism multiauthority Ciphertext-Policy Attribute Based Encryption (CP-ABE) where each key authority manages the attributes independently. In military environments such as battlefield, there will be no proper network connectivity. Hence, Disruption-Tolerant Networks (DTN) is designed to provide communication in most unstable environment. To overcome the security issues such as enforcement of authorization policies and policies update, CP-ABE mechanism is used. The earlier single authority and multiple authorities CP-ABE mechanism had few disadvantages such as Attribute revocation, Key escrow problem and coordination of attribute keys issued from different authorities. These drawbacks are overcome in this paper. And also, when an authority fails or shutdowns, we demonstrate how securely and efficiently the data can be still accessed using Shamir's Secret Sharing mechanism.***

**Keywords:** Disruption-Tolerant Network, multiauthority, access policy, ciphertext, key authorities

## 1. Introduction

In military environments such as battle field, there will be no proper network connectivity. The connections of wireless devices carried by the soldiers may undergo temporary disconnectivity due to jamming and some environmental factors. So, here comes DTN technology [1] which allows the devices to communicate with each other and access confidential information. DTN is designed to provide communication in most unstable environment. Storage nodes in DTN is necessary to store or replicate the data such that only authorized users can access the data.

In military scenario, the data which is transmitted require high protection with cryptographically enforced access control methods. Cryptography is nothing but transmitting the data in particular format such that only the authorized user can access the data. The security issues in DTN are enforcement of authorization policies and policies update i.e. who can access the data and latest updates respectively. These security issues can be overcome by using Ciphertext-Policy Attribute Based Encryption (CP-ABE).

In CP-ABE, the encryptor who encrypts the data, will also define an access policy such that the same access policy has to be possessed by the decryptor to decrypt the data. The data owner (may be commander) who possess the data which has to be encrypted will first define an access policy and obtain an attribute key from the key authority to encrypt the data. After encryption, the ciphertext will be stored in the storage node. Only the users (may be soldiers) who possess the same specified access policy can decrypt the ciphertext using the attribute key. The disadvantages of applying CP-ABE mechanism in DTN are Attribute revocation, Key escrow problem and coordination of attribute keys issued from different authorities.

In attribute revocation, the users who are moving from one region to another region may have to change their attributes or changing the attributes of a single user in an attribute group would affect the other users in the group i.e in some cases, the user might join or leave the attribute group where the associated attribute key have to be changed and redistributed to the other members in the same group in order to provide backward and forward secrecy. Backward secrecy is not allowing the user who satisfies the access policy to access the data which is been exchanged previously. Forward secrecy is not allowing the user who drops the access policy to access the subsequent data that is been exchanged. But redistributing or rekeying the attribute key will result in bottleneck or security degradation problem.

The second challenge is the key escrow problem. When the user requests for the attribute key, the key authority generates the private key using its master secret key on associated attributes of user. There are chances for the key authority itself to get compromised and decrypt the ciphertext. Hence, key escrow is a security risk because third party is involved during encryption and decryption.

The last challenge is the coordination of attribute keys issued from different authorities. In case of multiple authorities, each authority generates its attribute key using its own master secret key and issues independently to the user. Hence, defining an access policy is very difficult since different authorities issues its own attribute keys.

These challenges are overcome using multiauthority CP-ABE mechanism where each key authority manages the attributes independently. And also when a key authority fails or shutdowns, Shamir's Secret Sharing mechanism is used to securely and efficiently access the data. Using Shamir's secret sharing mechanism, the keys will be split to total of M shares and out of it minimum N shares is needed to recompute the key.

## 2. Literature Survey

Data encryption is very much required to prevent sensitive and confidential messages from unauthorized access. In identity-based encryption systems [2] and [3], the encrypted data can be decrypted only by a known single user. But this system lacks when it is needed for more advanced data sharing. To solve this issue, Attribute-based encryption system [4] was proposed in which an access policy can be specified into the ciphertext or decryption key. Attribute-based encryption is an extension of identity-based encryption where the user identity contains a set of attributes instead of a single string. ABE achieves one-to-many encryption instead of one-to-one encryption. It also addresses the problem of sharing the data securely and providing necessary access control.

There are two classes of ABE called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE [5], the ciphertexts are labeled by the data owner with a set of attributes. Here, it's the responsibility of the key authority to select an access policy for every user and determine which type of ciphertexts the user can decrypt and also issues the key to every user where the key includes the access policy. But in CP-ABE [6], it's the responsibility of the data owner to specify the access policy and a key is generated by the key authority with respect to the access policy with which the data is encrypted. CP-ABE is a better approach in DTN than KP-ABE because it enables the data owner to choose an access policy and encrypt the data using public key generated based on the access policy.

**A. Attribute Revocation:** Attribute revocation methods was first proposed in CP-ABE and KP-ABE by Bethencourt [6] and Boldyreva [7] respectively. Revoking one attribute of a user instead of the whole attributes without the other users private key being affected is important and the user must still be able to use the same private key to decrypt the ciphertext as long as the unrevoked attributes of the user satisfies the access policy. In military environments, the soldiers may have to change their location often. i.e. the attribute location may change frequently. Then, the user who satisfies the access policy can access the previously encrypted data until the data is reencrypted using new attribute keys during rekeying procedure. Preventing this kind of access is called Backward secrecy. And also the user who is been revoked and does not satisfy the policy any more can still access the encrypted data till the key updation time. Preventing this kind of access is called Forward secrecy. Hence if the key is not updated immediately, it leads to security degradation. The update of a single attribute of the user may affect the attributes of other unrevoked users who share the attributes, will lead to 1-affect-n problem. This causes scalability problem.

**B. Key escrow:** Usually, the key will not be known except the data owner and the user. Without proper authentication, the key will not be released to anyone. But when a third party which is authorized gains access to the keys, it leads to security risk. When there is a single authorized authority which can generate the whole private key using its master secret key, then the authority itself can decrypt the ciphertext easily. So, this authority acts as a third party between the data owner and the user which decrypts the ciphertext. This is known as key escrow problem. A distributed KP-ABE mechanism was proposed in multiauthority which solves key escrow problem [8]. In this mechanism, there was no central authority which contains master secret key. So, all the authorities has to communicate with each other for the generation of the secret key. Hence, the drawback in this mechanism was performance degradation. If N were the total number of authorities present, then it required $O(N^2)$ communication overhead and $O(N^2)$ additional keys to be stored by each user. A CP-ABE mechanism was proposed in multiauthority system which also suffered from key escrow problem [9].

**C. Decentralized ABE:** A Decentralized CP-ABE system [10] was proposed in multiauthority environment. In this system, the data was encrypted multiple times to achieve combined access policy over the attributes which was issued from different authorities. But the drawback in this system was specifying a well defined access policy which is efficient and expressive. For example, in military environment, if authority A is responsible for the attributes "battalion 1" and "region 1" and authority B is responsible for the attributes "battalion 2"and "region 2" then we cannot generate an access policy ((battalion 1 OR battalion 2) AND (region 1 OR region 2)). The OR logic cannot be applied over the attributes issued from different authorities. This is because each authority generates its own attribute keys using its own master secret key and issues independently to the user. Therefore, n-out-of-m logic (e.g. OR, i.e. 1-out-of-m) cannot be applied in previous mechanisms which is a necessary access policy logic.

Hur and Kang [11] have proposed the solution for these disadvantages. The attribute revocation problem is solved by immediately revocating the attributes which enhances backward and forward secrecy. The key escrow problem is solved by each key authority generating and issuing its own master secret key independently to the user. Each authority performs a secure two-party computation (2PC) protocol such that it prevents them knowing each other's master secret key so that none of the authority can generate the whole set of key individually. Finally, the data owner can specify a well defined access policy using any monotone access structure over the attributes issued from chosen set of authorities. In this paper, when an authority fails or shutdowns, Shamir's secret sharing mechanism [12] is used to efficiently and securely access the data.

## 3. Methodology

The proposed system consists of the following entities.

1) **Data owner:** This is an entity who owns confidential messages which has to be encrypted and stored in the storage node for the users to access it whenever needed. The data owner is also responsible to specify the access policy so that only the users who satisfy the policy can access the encrypted data stored in storage node.
2) **Key Authorities:** This is a key generation center which generates keys when requested. It consists of a central authority and multiple local authorities. Each local authority will manage different attributes and will issue its own master secret key independently to the user. They are semitrusted because they will be curious to get the information of the encrypted content as much as possible.

3) **Storage node:** This entity stores the encrypted data from the data owner and provides associated access to the corresponding users. This can be mobile or static.
4) **User:** This is an entity who wanted to access the encrypted data from the storage node. Only if the user satisfies the access policy specified by the data owner, he can decrypt the encrypted data in storage node.

Each authority will have its own master secret key and when the key is requested, each authority will issue its own master secret key independently to the user. The central authority and the local authorities will be provided with a secure two-party computation (2PC) protocol. This is because 2PC protocol prevents them from knowing each other's master secret key so that none of them can generate the complete key of user individually. Initially the data owner who contains the data which has to be encrypted, has to define the access policy. After specifying the access policy, the data owner requests for the key from the key authority. Once the key is been requested, the central authority issues public key to encrypt the data. Using the public key, the data will be encrypted and stored in the storage node. When the user who comes with the satisfied access policy requests for the key from the key authority, each local authority which manages the corresponding attributes will issue its own master secret key independently to the user. Concatenating all the master secret keys, the user will form another key called private key to decrypt the ciphertext stored in the storage node.

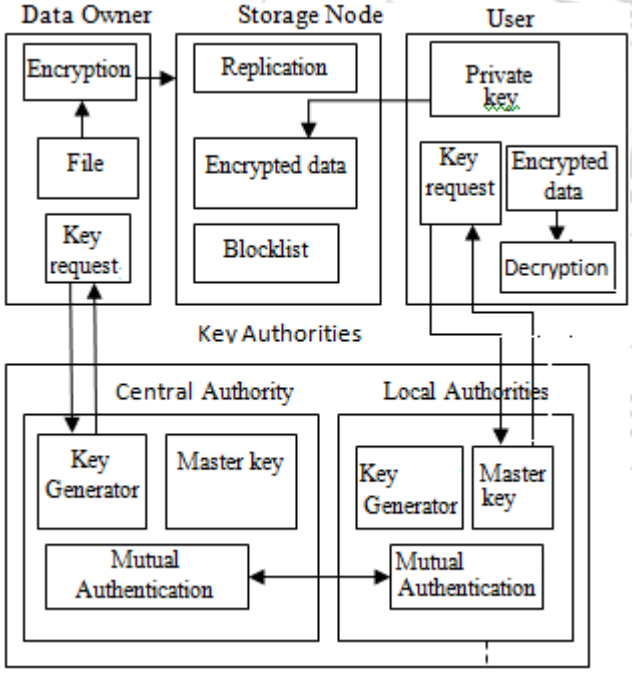


**Figure1:** Block diagram of the proposed system

By deploying this proposed mechanism, the disadvantages of earlier single authority and multiple authorities such as Attribute revocation, Key escrow problem and coordination of attribute keys issued from different authorities will be solved. When the attributes are changed after the data is been encrypted using the attribute key say $K_s$ and stored in the storage node, the data owner will generate a random key say $K_m$ and using $K_m$ he will reencrypt the encrypted data stored in the storage node. When the user who satisfies the access policy requests the key authority to issue the key for decryption, then the key authority will issue the randomly generated key by data owner i.e. $K_m$ to the users who are in the same attribute group. Using $K_m$, he will decrypt the reencrypted data and obtain $K_s$. Using $K_s$, the user will decrypt the earlier encrypted data and can access the data.

Since there are multiple authorities which perform a secure 2PC protocol, it prevents them from knowing each other's master secret key so that they cannot guess the private key by sharing their master secret keys. And also, no individual authority can generate the whole set of key used to decrypt the data. Even if an authority gets compromised, the key cannot be generated. Hence, key escrow problem can be solved.

This approach also solves the problem of coordination of attribute keys issued from different authorities. The data owner can define a fine grained access policy over the attributes issued from chosen set of authorities.

### 3.1 Shamir's Secret Sharing Mechanism

Secret sharing is also known as secret splitting. In secret sharing, the secret will be split into n number of shares. Two or more people will contain the shares of the secret. Suppose, if you and your friend discover a map which will lead to an island full of treasure. Both of you are excited about the map and happily go home. But both of you don't trust each other and are scared that if the map is with one person, he/she might go alone and take everything. So, there should be some scheme to share the map so that no one would go alone leaving the other. The solution for this problem is to split the map into two pieces and give one piece to each. Now you and your friend need not to be scared because both the pieces are required to form the original map and no one will be left out for the trip.

A well known example of secret sharing scheme is shamir's secret sharing scheme. In cryptography, Shamir's Secret Sharing mechanism is used to distribute the secret among the group of participants where each participant will be allocated with a share of the secret. Only when all the shares or some of the shares are combined together, the original secret can be reconstructed. The individual shares are of no use. The secret will be divided into parts and each participant will be given a unique part such that some or all of the parts are needed to reconstruct the secret. Secret sharing is an ideal approach to store the information which is highly confidential and sensitive. For example, Encryption keys, numbered bank accounts, missile launch codes etc. Each of these shares should be kept confidentially and these shares should not be exposed and lost as well.

In this paper, Shamir's (m,n) secret sharing scheme is applied on the centralized authority's master secret key. The centralized authority's master secret key will be split into n shares and distribute to all the local key authorities. Among n shares, only minimum of m shares will be needed to reconstruct the original master secret key. For example, if shamir's (3,10) secret sharing scheme is applied, then the master secret key will be split into 10 shares and distributed among all the authorities. But for the reconstruction of the key, only a minimum of 3 shares will be needed. So, even when one of the local authority which posses certain shares fails, a minimum of 3 shares can be obtained from other

local authorities to reconstruct the original key. And the user can easily decrypt the ciphertext stored in the storage node using the centralized authority's public key and the reconstructed master secret key. The properties of shamir's secret sharing scheme are secure, minimal, extensible, dynamic and flexible.

## 4. Expected Outcome

The data owner will specify the access policy such that only the user who comes to access the ciphertext satisfies the specified access policy can decrypt the ciphertext stored in the storage node. The data owner will request for the public key from the centralized authority to encrypt the data. Once the public key is issued, the data owner will encrypt the data using the key and store it in the storage node. When the user comes with the satisfied access policy to access the ciphertext stored in the storage node, each local key authoritiy will issue its own master secret keys independently to the user. Combining these master secret keys, another key will be formed to decrypt the ciphertext. If the user's access policy doesn't satisfy the specified access policy by the data owner, then the user cannot decrypt the ciphertext. When one of the authority fails or shutdowns, the Shamir's secret sharing scheme will be applied on centralized authority's master secret key where the master key will be split into n shares and distributed among all the local authorities and a minimum of m shares will be needed to recomputed the original master key which will be used to decrypt the ciphertext.

## 5. Conclusion

DTN technology is a solution for efficient communication among the wireless devices carried by soldiers in military environment. The security issues in DTN technology will be solved using CP-ABE mechanism. But applying CP-ABE mechanism in DTN has certain drawbacks such as Attribute revocation, Key escrow problem and coordination of attribute keys issued from different authorities. These drawbacks are overcome in this paper using multiauthority CP-ABE where each key authority manages the attributes independently. And also, when one key authority fails or shutdowns, Shamir's secret sharing mechanism will be used to securely and efficiently access the data.

## 6. Future Scope

The future work includes using a cloud server for storing the encrypted data for the user to access it reliably and efficiently. The earlier used storage node has the possibility of getting attacked or destroyed. If attacked or destroyed, the data stored in the storage node will be completely lost. This becomes the disadvantage in the proposed system. Hence by storing the data in the cloud server, the data will not be lost and can be accessed efficiently.

## References

[1] Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges, Maurice J. Khabbaz, Chadi M. Assi, and Wissam F. Fawaz. IEEE communications surveys & tutorials, accepted for publication.
[2] Identity-Based Encryption from the Weil Pairing, Dan Boneh, Matthew Frankliny.
[3] Fuzzy Identity-Based Encryption, Amit Sahai, Brent Waters.
[4] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, Vipul Goyal, Omkant Pandey*y*, Amit Sahaiz ,Brent Waters.
[5] An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. Changji Wang and Jianfa Luo.
[6] Ciphertext-Policy Attribute-Based Encryption, John Bethencourt, Amit Sahai ,Brent Waters.
[7] Identity-based encryption with efficient revocation, A. Boldyreva, V. Goyal, and V. Kumar, in Proc. ACM Conf. Comput. Commun. Security, 2008, pp. 417–426. [8]. Certain Investigations on Motion Blur Detection and Estimation Shamik Tiwari1, V. P. Shukla 2, Ajay Kr. Singh.
[8] Improving privacy and security in multiauthority attribute-based encryption, M. Chase and S. S. M. Chow, in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.
[9] Multi-authority attribute based encryption, M. Chase, in Proc. TCC, 2007, LNCS 4329, pp. 515–534.
[10] Decentralizing Attribute-Based Encryption, Allison ,Lewko.
[11] Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014
[12] Implementation of Shamir's Secret Sharing on Proactive Network, Saria Islam, A. S. M Mahmudul Hasan.
[13] International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 6 – No.2, September 2013 – www.ijais.org

## Authors Profile

**Subhashini.P** completed the bachelor's degree in Computer Science & Engineering from visvesvaraya technological University (VTU). Currently pursuing Masters in Engineering in Computer Network Engineering at Mangalore Institute of Technology, Mangalore

**Ashwin Kumar.M** completed bachelors degree in Electronics Communication & Engineering and masters degree in Computer Science and Engineering. Currently working as Senior Assistant Professor in Mangalore Institute of Technology, Mangalore.