Enhanced Approach for Secure Communication over Decentralize Opportunistic Network

[1]Ajay B. Kapase, [2]Mr. Pankaj Chandre
[1]P.G. Student, [2]Assistant Professor
[1]Department of Computer Networks,
[1]Flora Institute of Technology, Pune, India

Abstract **- Soldiers communicate with one other using wireless sensor devices which are carried by them. The soldiers need these wireless sensor devices to access the sensitive/confidential information. In this case decentralizes disruption tolerant network techniques are becoming the effective way to command consistently by abusing remote storage nodes. Ciphertext-Policy Attribute-Based Encryption is a competent solution such as cryptographic for the initial control issues. Still, the difficulty of relating CP-ABE in decentralized Disruption-tolerant Networks (DTNs) presents some security and protection challenges respecting the quality denial, key escrow, and in addition attribute coordination issued from changed powers. This paper proposes a protected data recovery approach utilizing Ciphertext-Policy Attribute-Based Encryption used for DTNs where numerous key authorities deal by means of their attributes freely. The framework turns out to be more secure by applying ABE and various characteristic encryption confirmations**

IndexTerms **- disruption-tolerant network; identity-base encryption; attribute-based encryption; Ciphertext-policy attribute-based encryption.**

I. INTRODUCTION

In numerous military network situations, contacts of wireless devices carried by soldiers are also briefly disconnected by jamming, environmental reasons, and mobility, particularly when the soldiers work in threatening situations. Disruption-tolerant network (DTN) technologies are getting successful solutions that enable nodes to communicate with one another in these dangerous networking environments. Ordinarily, once there is no limit to end association between a source and a destination pair, the messages from the source hub might need to go to inside of the middle of the intermediate hubs for an impressive amount of time until the association would be eventually built up.

In some application scenarios, there are some 'storage nodes' (which is also mobile or static) within the network wherever helpful knowledge is held on or replicated so other regular mobile nodes (such as users) will access the necessary data quickly and efficiently. . A demand in some security-critical applications is to design an access system to protect the confidential knowledge stored within the storage nodes or the secret messages text moved from end to end the network.

Modern distributed data systems need flexible models of access control that go past optional, compulsory and role-based access control. Recently projected attribute-based models, define access control strategies supported environment, the completely different requester attributes, or the information object. Another one is the current trend of service-based data systems and storage outsourcing need increased protection of knowledge together with that cryptographically enforced access management strategies. The thought of Attribute-Based encryption (ABE) fulfills the same needs. It provides an elegant approach of encrypting knowledge specified the encryptor already defines the set of attribute that needs to pass by the decryptor so as to decrypt that particular encrypted cipher-text. Since Sahai and Waters [1] projected the fundamental ABE theme, many additional advanced schemes are developed, like most notably Ciphertext-Policy ABE schemes (CP-ABE). In these schemes, a generated ciphertext is related to an access policy and also the secret key of user is related to a collection of attributes. Only the holder of secret key (i.e. owner) will decrypt the given ciphertext only if the attributes that are related to his secret key completely satisfy the access policy related to the ciphertext.

CP-ABE could be a public-key cryptography primitive that was projected to resolve the precise issue of fine-grained access control on shared information in one-to-many communications. In CP-ABE, every user gets assigned a collection of attributes that are embedded in the authorized user's private key. A public key component is already defined for every authorized user. When the message or file is encrypted, the encryptor encrypts the private message on set of attributes by selecting an access structure via encrypting with the equivalent user's public key components. When the users set of attributes satisfy the ciphertext access control then and then only users are able to decrypt that ciphertext of message. The ciphertext sizes and public key in CP-ABE are simply linear to the quantity of attributes and also the quality of the access arrangement. This arrangement is not depend on the set of users in system. Moreover, CP-ABE is unaffected by collusion attacks from unauthorized users of these good properties create CP-ABE very appropriate for fine-grained knowledge access control on untrusted storage.

The problem of using the ABE to DTNs still produces many privacy and security challenges. As a result, of most of the users might modify their associated attributes at some point (for example, moving their area), or many personal keys can be negotiated, key revocation (or modification) for each attribute is important for secure and protected systems development. Though, this drawback becomes harder, particularly in ABE [12], [13] systems, therefore of each attribute is possibly shared by various users.

This signifies that revocation of whichever attribute or whichever specific user in an attribute group would influence the opposite users to present within the group. For example, if a user tries or leaves an attribute group, the connected attribute key should be altered and once more redistributed to each alternative member within the identical group for forward or backward secrecy. It may importance in bottleneck through the rekeying technique or safety degradation due to the windows of vulnerability if the preceding attribute key is not changed immediately.

The next sections of paper are organized as follows: Section II gives the essential literature survey. Section III addresses existing techniques. Section IV introduces the proposed architecture overview. Section V proposed system setup and section VI describes results and analysis. Section VII accomplishes the paper.

II. Related Work

In the literature review, the topical methods over secure data retrieval are going to discuss.

S. Roy and M. Chuah [2] presented a scheme of access control that maintained the Ciphertext-Policy Attributed-Based Encryption (CP-ABE) method. This method is used to address the scenario where attributes are present for both static and dynamic conditions. Disadvantage of this method is that it requires assuming that every user can revoke any user using the negative attribute consistent to that user's identifier.

M. Chuah [3] defines K-copy random caching data system and K-copy intelligent caching data system. After that for query distribution, L-hop Neighborhood Spraying (LNS) system is defined. For message routing, Highest Encounter First Routing (HEFR) system is used. K-copy random or intelligent caching and L-hop neighborhood query spraying is used to increase the average query success rate. HEFR system is used to achieve smaller query reply time and therefore achieve higher query success rate. This scheme does not support mobility model.

L. Ibraimi, M. Petkovic et al. [4] presented CP-ABE with immediate attribute revocation. The system allows the encryptor to encrypt a message allowing to an access policy above a set of attributes, and simply users who satisfy the access policy and whose attributes are not revoked can decrypt the ciphertext. However, the system cannot provide security proof under standard complexity assumption.

N. Chen et al. [5] presented the function of fading, which renders attributes "dynamic". This also allows updating every one attribute from rendered independently. Dynamic ABE provides an effective mechanism for attribute revocation that does not need the reissuing of the entire key. But sender cannot control lifetime of attributes.

A. Lewko and B. Waters [6] projected Multi-Authority Attribute-Based Encryption (ABE) method. The core advantage of this system is that central authority is not needed. However, the system is suffered from the key escrow issue like the prior decentralized schemes.

J. Bethencourt et al. [7] presented CP-ABE system that allows for a novel type of encrypted access mechanism where private keys of users are definite by a set of attributes and authorized party encrypting information can identify anexact policy above these set of attributes stipulating which users are able to data decryption. This scheme allows expressing policies as any monotonic tree access control structure and is resistant to many collusion attacks from where attacker might obtain multiple set of private keys.

S. Yu et al. [10] proposed Identity-based encryption (IBE) at third party side. It increases the efficiency of system on user private key update. It uses binary tree generation technique but Binary tree generation takes more time if key updated more at a time by multiple users.

P. Golle et al. [11] presented a system that can work in conjunction with natural language processing (NLP) algorithms or user-generated tags, to protect identifying attributes in text. Mainly system proposed a user revocable KP-ABE scheme. The system encrypts not only sensitive special information, but also groups of private attributes which may indirectly allow for the inference of a person's identity, even though none of the attributes is directly sensitive. Limitation of this Scheme is that it only works if the set of attributes that associated with a ciphertext is exactly half of the original universe size.

M. Chase and Chow [15] presented KP-ABE system to resolves the difficult of key escrow in a multi-authority system. In this KP-ABE approach, all (individual) data attribute authorities are contributing in the protocol of key generation in a distributed approach. Performance degradation is limitation of this system because of no centralized authority with master secret information.

A. Lewko and B. Waters [16] projected Multi-Authority Attribute-Based Encryption (ABE) system is proposed which allows multiple authority to attribute monitoring and secret key distribution. The core advantage of this system is that central authority is not needed. However, the system is suffered from the key escrow issue.

S. S.M. Chow [17] presented modified Identity-based encryption (IBE) which used against anonymous ciphertext indistinguishability- key generation center (ACI-KGC) attacks. Privacy for user is weak for this application.

III. Existing Approach

Existing System Overview

Attribute-based encryption (ABE) [8] could be an approach that fulfills secure information retrieval (IR) necessities in decentralizes DTNs. ABE features a mechanism that permits an access control over encrypted information using access policies and recognized attributes among private keys and ciphertexts. Especially, CP-ABE [9] [14] provides an encrypting information scalable technique such that the encryptor defines the set of attributes that the decoder must require possess for ciphertext decryption. Thus, different users are allowed or permit to decode different section of knowledge per the security policy.

Solution on this problem can be an attribute-based secure information retrieval (IR) scheme using technique called as CP-ABE for decentralized DTNs. This proposed scheme features into the subsequent achievements for data security.

1) Attribute Revocation: Immediate attribute revocation improves backward/forward confidentiality of sensitive information by minimizing the vulnerability windows.

*2) Fine-grained Access Policy:*Encryptors will define a policy of fine-grained access using any access structure that is monotone. This policy is defined under attributes obtained from any chosen authorities sets.

3) Key Issuing Protocol: The key escrow difficulty is resolved by an escrow-free key issuing protocol that exploits the characteristic of the Decentralize Tolerant Network architecture. The key obtaining protocol generates as well as sends secret keys of user by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC [18] protocol prevents the key authorities from obtaining any master secret data of every alternative such that none of them might generate the entire set of user keys alone.

Thus, users are not needed to totally trust the authorities in order to protect their information to be shared. The information confidentiality and privacy may be cryptographically executed against some curious key authorities or data storage nodes within the proposed scheme.

Drawbacks of Existing Approach

Disadvantages of existing system are illustrated as:

- The issue of applying the ABE to DTNs presents several security as well as privacy challenges. If some users change their related set of attributes at several facts (such that, moving their region), or approximately private keys might be compromised, key update (or revocation) for every attribute in set is necessary in order to make secure systems or protected systems.
- Though, this issue is even much more difficult, particularly in ABE systems, since every attribute is conceivably shared by multiple users (henceforth, in this paper, such users set referred as an attribute group).
- Additional challenge for study is the key escrow issue. The key authority in this CP-ABE system produces private keys of every user by applying the master secret keys of authority to the related attributes of users.
- Another important challenge is the coordination of attributes delivered from different remote key authorities. When multiple key authorities manage and individually send attributes keys to users with their own master secrets, it is very tough to describe fine-grained access policies above attributes that are delivered from different remote key authorities.

IV. Proposed Architecture

This proposed system provides a multiple authority CP-ABE system for secure information retrieval in DTNs. Each public authority problems incomplete modified and attribute key elements to a user by operating secure 2PC protocol with the center authority. Each attribute key of a user will be modified severally and instantly. Hence, the safety and scalability will be improved within the planned system. To improve security, attributes are the first convert into the hash and combine with the private key of the user to make key more secure.

Architecture Overview

As in figure 1, the entities can explain as follows.

1) ***Key Authorities:*** Key Authorities are key generation middle that generates parameters like a public/private key for CP-ABE. The key authorities contain subsisting authority and various native authorities. For this key authority, section assumes that there are secure and reliable communication channels between a central authority and every local authority throughout the initial key setup and generation section. Every local authority manages completely different attributes and problems corresponding attribute keys to users. The proposed system grant differential fine-grained access rights to individual users based on the attributes of users. The key authorities presented in architecture are assumed to be very honest-but-curious. That is, they will honestly execute the assigned tasks within the system; but they might prefer to learn data of encrypted contents as much as possible.

2) ***Storage Node:*** Storage is a server or database entity that used to stores data obtains from senders and again forward equivalent access to users. The storage node could also be mobile or static [5], [6] depend upon the application during which it is used.

3) ***Sender:*** This is an entity that self-confidential messages or data (e.g., a commander just in case of military) and needs to store these messages into the external data storage node for simplicity of knowledge sharing or for consistent delivery to users within the intense networking environments. A sender is dependable for essential (attribute based) access policy and accomplishing it on its own knowledge by encrypting the knowledge under the policy previous to storing it to the storage node.

4) User: This can be a node who requests to access the knowledge keep at the storage node (e.g., a soldier just in case of military). If a user possesses a group of attributes fulfilling the access policy of the encrypted knowledge distinct by the sender, what is more is not revoked in any attributes, in order that then the user can decrypt the ciphertext and obtain the original information.

Proposed Architecture Diagram

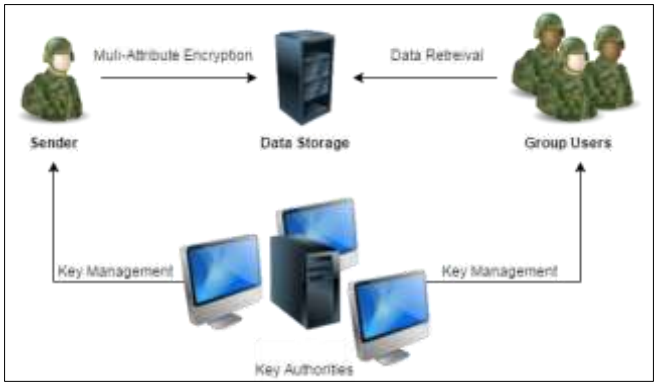

Fig. 1. *Proposed Architecture.*

V. PROPOSED SYSTEM SETUP

System Setup Phase

Step 1: *Generate Public and secret keys for central as well as Local Key Authorities.*

Let, a bilinear group is G_0 of prime order p with generator q according to the security parameter.It also selects hash functions as $H:\{0,1\}^* \rightarrow G_0$ from a family of common one-way file hash functions.

Step 2: Central Authority (CA) selects a random exponent $\beta \in_R Z_p^*$ and sets $h = g^{\beta}$, where p is some prime number. The master key, private key pair is given by following equation

$$PK_{CA} = h, MK_{CA} = \beta \qquad (1)$$

Step 3: Local Key Authorities selects a random exponent $\alpha_i \in R$. The master public as well as private key pair is given by

$$PK_{A_i} = e(g,g)^{u_i}, MK_{A_i} = \alpha_i \qquad (2)$$

Step 4: Central key Authority or local key authority authenticates a user u_t by selecting random exponents $\gamma_1,....,\gamma_m \in_R Z_p^*$ for every local authority $A_1,....,A_m \in A_i$ and set

$$r_t = \sum_{i=1}^{m} \gamma_i \qquad (3)$$

and this r_t value is a personalized and unique secret to the user, which should be consistent for any further attribute additions to the user.

Step 5: Then User u_t computes its personal key component as in algorithm 1) and 2) as follows:

Personal Key Generation

1. Local Authority A_i randomly picks $\tau \in_R Z_p^*$. Then it Computes

$$T = g^{\frac{x}{t}} = g^{\frac{(\alpha_i+\gamma_i)}{\tau\beta}} \qquad (4)$$

and send it to CA.

2. CA then computes

$$B = T^{\frac{1}{\beta^2}} = g^{\frac{(\alpha_i+\gamma_i)}{\tau\beta}} \qquad (5)$$

3. and sends it to A_i
4. A_i outputs a personalized key component

$$D_i = B^{\tau} = g^{\frac{(\alpha_i+\gamma_i)\beta}{\tau}} \qquad (6)$$

5. and sends it to the user u_t securely.
6. Then User u_t computes its personal key component

$$D = \prod_{i=1}^{m} D_i = g^{\frac{(\alpha_1 + \ldots + \alpha_m) + r_t}{\beta}} \quad (7)$$

Attribute Key Generation

After setting up the personalized key component, every A_i attribute generates attribute keys for a user with a public parameter received from CA as follows.

1. CA first selects a random r' and sends $g^{rt-r'}$ and $g^{r'}$ to A_i and u_t, respectively.
2. Attribute A_i takes a set of attributes $\Lambda_i \subseteq A_i(L)$ as inputs and outputs a set of attribute keys for the user that identifies with that set Λ_i. It chooses random $r_j \in Z_p^*$ for every attribute $\lambda_i \in \Lambda_i$. Then, it gives the following secret value to the user

$$u_t \; \forall \lambda_i \in \Lambda_i : D_j = g^{rt-r'}.H(\lambda_i)^{r_j}, D_j^{'} = g^{r_j} \quad (8)$$

3. Then, the user computes $g^{r'}.D_j$ for all its attributes key components and lastly a complete secret key set is obtained as

$$SK_{ut} = (D = g^{\frac{(\alpha_1 + \ldots + \alpha_m) + rt}{\beta}}, \quad \forall \lambda_i \in S : D_j = g^{rt}.H(\lambda_i)^{r_j}, D_j^{'} = g^{r_j} \quad (9)$$

Where,

$$S = \bigcup_{i=1}^{m} \Lambda_i \quad (10)$$

Step 6: Data Encryption: When a sender wants to deliver its confidential data M expresses the tree access structure T over the attributes set L, encrypts the data under T to enforce attribute-based access control mechanism on the data, and stores that data into the node called as storage node. Next the construction of ciphertext CT, the sender stores it to the storage node securely.

Step 7: Data Decryption: When a user receives the previously generated ciphertext CT from the storage node, the user decrypts that ciphertext by using its own secret key.

Revocation

To immediately revoke an attribute of specific users is to re-encrypt the ciphertext with each attribute group key and selectively distribute the attribute group key to authorized (non-revoked) users who are qualified with the attribute. Before distributing the ciphertext CT, the storage node accepts a set of membership information for every attribute group that performs in the access tree of from the corresponding authorities and re-encrypts. For revocation CT is re-encrypted to CT'. Then, the user can decrypt the ciphertext with its secret key following the decryption technique.

Key Updation

When a user comes to hold or drop an attribute, the corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively.

The key update procedure is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute groups, it notifies the storage node of the event.

It is very significant to note that though a user is revoked from particular attribute groups, he may still be capable to access the information with the other attributes that he holds on the assumption that they satisfy the policy since they would still be effective in the scheme.

VI. Analysis And Results

Data Confidentiality

In our trust model, the multiple key authorities are no longer fully trusted as well as the storage node even if they are honest. Therefore, the plain data to be stored should be kept secret from them as well as from unauthorized users. Data confidentiality on the stored data against unauthorized users can be trivially guaranteed. If the set of attributes of a user cannot satisfy the access tree in the ciphertext, he cannot recover the desired value.

Results

For the experiment, file is selected as per the size of the file. When the file is uploaded then the file is encrypted using multi-attribute encryption. The time requires encrypting file will get an increase when a size of the file increases. Similarly file is decrypted using decryption algorithm and its time gets increase if file size increases. The expected results for file encryption are as shown in figure 2.

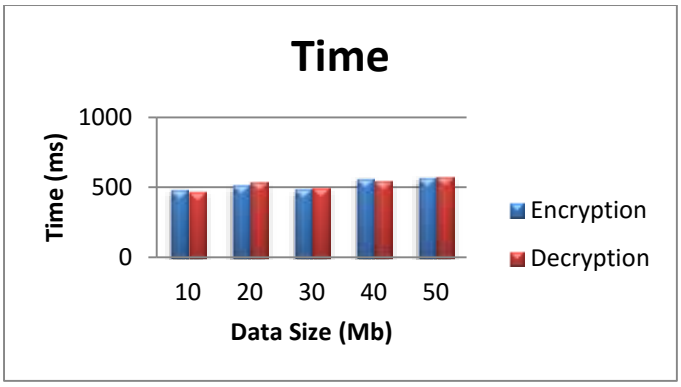

Fig. 2. *Time require for file encryption and decryption graph.*

VII. CONCLUSION

This paper proposed a CP-ABE system that is able to use in Disruption Tolerant Networks (DTNs). CP-ABE is an extensible cryptographic solution to the access control and prevents data retrieval problems. This paper projects a secure as well as efficient information retrieval technique via CP-ABE for decentralized DTNs where several key authorities handle their attributes individually. The issue of inherent key escrow is resolve in such way that the security of the stored data is assured even under the antagonistic environment where key authorities might be negotiated or not totally trusted. Additionally, the gentle key revocation can be complete for each attribute group.

VIII. ACKNOWLEDGMENT

The author would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the Prof. Pankaj Chandre for his valuable guidance and constant guidelines also thank full the computer department staff of Flora Institute of Technology, Pune, and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

REFERENCES

[1] J. Hur, K. Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE Trans. On Networking, vol 22, no. 1, Feb 2014.
[2] 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.
[3] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," IEEE MILCOM, 2007, pp. 1–7.
[4] M. Petkovic, L. Ibraimi, S. Nikova, and P. Hartel, W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," WISA, 2009, LNCS 5932, pp. 309–323.
[5] N. Chen, M. Gerla, X. Hong, and D. Huang, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," Ad Hoc Netw. Workshop, 2010, pp. 1–8.
[6] A. Lewko and Waters, "Decentralizing attribute-based encryption," Cryptology e-Print Archive: Rep. 2010/351, 2010.
[7] J. Bethencourt, B. Waters, and A. Sahai, "Ciphertext-policy attributebased encryption," IEEE Symp. Security Privacy, 2007, pp. 321–334.
[8] R. Ostrovsky, Waters, and A. Sahai, "Attribute-based encryption with non-monotonic access structures," ACM Conf. Comp. Communication Security, 2007, pp. 195–203.
[9] S. Yu, K. Ren, C. Wang, and W. Lou, "Attribute based data sharing with attribute revocation," ASIACCS, 2010, pp. 261–270.
[10] A. Boldyreva, V. Kumar, and V. Goyal, "Identity-based encryption with efficient revocation," ACM Conf. Comp. Communication Security, 2008, pp. 417–426.
[11] P. Golle, Gagne, J. Staddon, and P. Rasmussen, "A content-driven access control system," Symp. Identity Trust Internet, 2008, pp. 26–35.
[12] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
[13] V.Goyal, A. Sahai, O. Pandey, and A. Jain, "Bounded ciphertext policy attribute-based encryption," ICALP, 2008, pp. 579–591.
[14] X. Liang, D. Xing, Z. Cao, and H. Lin, "Provably secure and efficient bounded ciphertext policy attribute based encryption," ASIACCS, 2009, pp. 343–352.
[15] M. Chase and Chow, "Improving privacy and security inmulti-authority attribute-based encryption," ACM Conf. Comp. Communication Security, 2009, pp. 121–130.
[16] M. Chase, "Multi-authority attribute based encryption," TCC, 2007, LNCS 4329, pp. 515–534.
[17] S. S.M. Chow, "Removing escrow from identity-based encryption," PKC, 2009, LNCS 5443, pp. 256–276.
[18] M. Belenkiy, A. Lysyanskaya, M. Kohlweiss, and M. Chase, "P-signatures and non-interactive anonymous credentials," TCC, 2008, LNCS 4948, pp. 356–374.