ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure data recovery method for decentralized DTNs where multiple key authorities manage their attributes Using CP-ABE

Peddapaka Anusha
MTech Student
Department of Computer Science Engineering
Chilukur Balaji Institute Of Technology

P. Dharshan
Associate Professor & HOD,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

Abstract*—Mobile nodes in military or defence environments such as a battlefield or a hostile area are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions by allowing wireless devices carried by soldiers to interact with each other and access the confidential data or command reliably by exploiting external storage nodes. A few most challenging issues in this mechanism are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a cryptographic key solution to prevent unauthorized access to confidential information. However, the problem of applying CP-ABE in decentralized DTNs introduces different security and privacy challenges related to the key escrow, attribute revocation, and coordination of attributes issued from different authorities. In this paper, we propose a high secure data retrieval mechanism using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords*—Secure Data Retieval, Access Control, Multi Authority, Cipertext Policy-Attribute Based Encryption (CP-ABE), Disruption Tolerant Network.

I. INTRODUCTION

Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

In Military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Roy and Chuah introduced storage nodes in DTNs where data is stored or replicated such that only authorized mo-bile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store a confidential information at a storage node, which should be accessed by members of “Battalion 1” who are participating in “Region 2.” In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers). It refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for se-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

cure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to de-crypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for ex-ample, moving their region), 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 even more difficult, especially in ABE systems, since each at-tribute is conceivably shared by multiple users (henceforth, it refer to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For ex-ample, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of at-tributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the at-tribute-based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem. The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities.

For ex-ample, suppose that attributes "role 1" and "region 1" are man-aged by the authority A, and "role 2" and "region 2" are man-aged by the authority B. Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as "-out-of-" logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

II. NETWORK ARCHETECTURE

In this section, we describe the DTN architecture and define the security model.

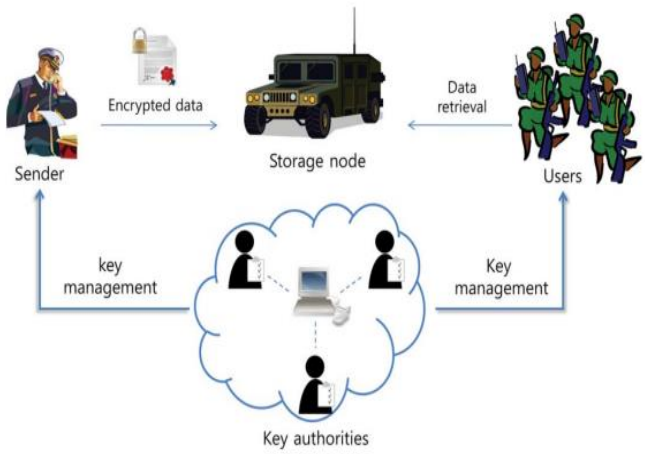

Fig: 1. Architecture of secure data retrieval in a disruption-tolerant militarynetwork.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A. System Description and Assumptions

Fig. 1 shows the architecture of the DTN. As shown in Fig 1,the architecture consists of the following system entities.

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious.

3) Sender: This is an entity who 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.

4) User: This is a mobile node who wants to access the data 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 sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

Since the key authorities are semi-trusted, they should be de-terred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users. In order to realize this somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

.

B. Threat Model and Security Requirements

1) Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

2) Collusion-resistance: If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone [11]–[13]. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.

3) Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be pre-vented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

III. Preliminaries And Difinition

A. Cryptographic Background

We first provide a formal definition for access structure recapitulating the definitions in [12] and [13]. Then, we will briefly review the necessary facts about the bilinear map and its security assumption.

1) *Access Structure:* Let $\{P_1,P_2,\ldots P_n\}$ be a set of parties. A collection $\mathbf{A} \subseteq 2^{\{P_1,P_2,\ldots,P_n\}}$ is monotone if $\forall B,C$: If $\mathbf{B} \in \mathbf{A}$ and $B \subseteq C$, then $C \in \mathbf{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbf{A}$ of nonempty subsets of $\{p_1, p_2, p_3, \ldots p_n\}$, i.e., $\mathbf{A}$ is subset of $2^{\{P1,P2,..Pn\}}\backslash\{\emptyset\}$. The sets in $\mathbf{A}$ are called the authorized sets, and the sets not in $\mathbf{A}$ are called the unauthorized sets.

In the proposed scheme, the role of the parties is taken by the attributes. Thus, the access structure $\mathbf{A}$ will contain the authorized sets of attributes. From now on, by an access structure, we mean a monotone access structure.

2) *Bilinear Pairings:* Let $\mathbf{G_0}$ and $\mathbf{G_1}$ be a ultiplicative cyclic group of prime order p. Let g be a generator of $\mathbf{G_0}$. A map $e : \mathbf{G_0} \times \mathbf{G_0} \rightarrow \mathbf{G_1}$ is said to be *bilinear* if $e(P^a, Q^b) = e(P,Q)^{ab}$ for all $\mathbf{P,Q}$ belongs to $\mathbf{G_0}$ and all $\mathbf{a,b}$ belogs to Z^*_p, and and *non degenerate* $e(g,g) \neq 1$ if for the generator g of $\mathbf{G_0}$.

We say that $\mathbf{G_0}$ is a bilinear group if the group operation in $\mathbf{G_0}$ can be computed efficiently and there exists $\mathbf{G_1}$ for which the bilinear map $e : \mathbf{G_0} \times \mathbf{G_0} \rightarrow \mathbf{G_1}$ is efficiently computable.

IV. PROPOSED SYSTEM

In this section, we provide a multiauthority CP-ABE scheme for secure data access 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. Every attribute key of a user can be updated individually and immediately to enhance the security for the proposed system

Because the first CP-ABE system proposed by Bethencourt *et al.* [13], dozens of CP-ABE schemes have been proposed [7]. The subsequent CP-ABE systems are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to reach the expressiveness of the Bethencourt *et al.*'s scheme, which describes an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt *et al.*'s construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch.

A. Access Tree

1) Description: Let be a tree representing an access structure.

Each nonleaf node of the tree represents a threshold gate. If num_x is the number of children of a node x and k_x is its threshold value, then $0 \leq k_x \leq \text{num}_x$. Each leaf node of the tree is described by an attribute and a threshold value $k_x = 1$. λ_x denotes the attribute associated with the leaf node in the tree. $p(x)$ represents the parent of the node in the tree. The children of every node are numbered from 1 to num. The function index(x) returns such a number associated with the node . The index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

B. *Revocation*

We observed that it is impossible to revoke specific attribute keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs.

For example, suppose that a user u_t is qualified with l different attributes. Then, all l attribute keys of the user u_t are generated with the same random number r_t in the ABE key architecture. When an attribute of the user is required to be revoked ($l - 1$ other attribute keys of the user are still valid), the other valid $l - 1$ keys should be updated with another new r'_t that is different from r_t and delivered to the user. Unless the other keys $l - 1$ are updated, the attribute key that is to be revoked could be used as a valid key until their updates since it is still bound with the same r_t. Therefore, in order to revoke a single attribute key of a user, $O(l)$ keys of the user need to be updated. If n users are sharing the attribute, then total $O(nl)$ keys need to be updated in order to revoke just a single attribute in the system.

V. ANALYSIS

In this section, we first analyze and compare the efficiency ofthe proposed scheme to the previous multi authority CP-ABE schemes in theoretical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation in terms of the communication cost. We also discuss its efficiency when implemented with specific parameters and compare these results to those obtained by the other schemes.

Table I
EXPRESSIVENESS, KEY ESCROW, AND REVOCATION ANALYSIS

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW [13]	single	-	yes	periodic attribute revocation
HV [9]	multiple	AND	yes	periodic attribute revocation
RC [4]	multiple	AND	yes	immediate system-level user revocation
Proposed	multiple	any monotone access structure	no	immediate attribute-level user revocation

A. *Efficiency*

Table I shows the authority architecture, logic expressiveness of access structure that can be defined under different disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme. In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [13] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be setto the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

Table II
EFFICIENCY ANALYSIS

System	Ciphertext size	Rekeying message	Private key size	Public key size
BSW [13]	$(2t+1)C_0 + C_1 + C_{\mathcal{T}}$	$l(2k+1)C_0$	$(2k+1)C_0$	$C_0 + C_1$
HV [9]	$(2t+m)C_0 + mC_1 + C_{\mathcal{T}}$	$l(2k+1)C_0$	$(2k+m)C_0$	$mC_0 + mC_1$
RC [4]	$(2t+3r+m)C_0 + mC_1 + C_{\mathcal{T}}$	0	$(3k+2m)C_0$	$m(t+4)C_0 + mC_1$
Proposed	$(2t+1)C_0 + C_1 + C_{\mathcal{T}}$	$(n-l)\log\frac{n}{n-l}C_p$	$(2k+1)C_0 + \log n C_k$	$C_0 + mC_1$

C_0: bit size of an element in $\mathbb{G}_0$, C_1: bit size of an element in $\mathbb{G}_1$, C_p: bit size of an element in $\mathbb{Z}_p^*$,
C_k: bit size of a KEK, $C_{\mathcal{T}}$: bit size of an access tree $\mathcal{T}$ in the ciphertext, r: the number of revoked users,
l: the number of users in an attribute group, n: the number of all users in the system,
m: the number of authorities in the system, k: the number of attributes associated with private key of a user,
u: the number of attributes in the system, t: the number of attributes appeared in $\mathcal{T}$.

Table II summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 ***m*** different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table II, the proposed scheme needs rekeying message **(Hdr)** size of at most $\mathbf{(n\text{-}l)\log^{n/(n-1)}}$ 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 ciphertext size is linear to the number of revoked users in the system since the user revocation message is included in the ciphertext. The proposed scheme requires a user to store **log(n)** more KEKs 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 ciphertext size while realizing more secure immediate rekeying in multi authority systems.

B. *Simulation*

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar [32] demonstrated the group behavior in the Internet's multicast backbone network (MBone). They showed that the number of users joining a group follows a Poisson distribution with rate **~λ**, and the membership duration time follows an exponential distribution with a mean duration **1/μ**. Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behavior distribution.

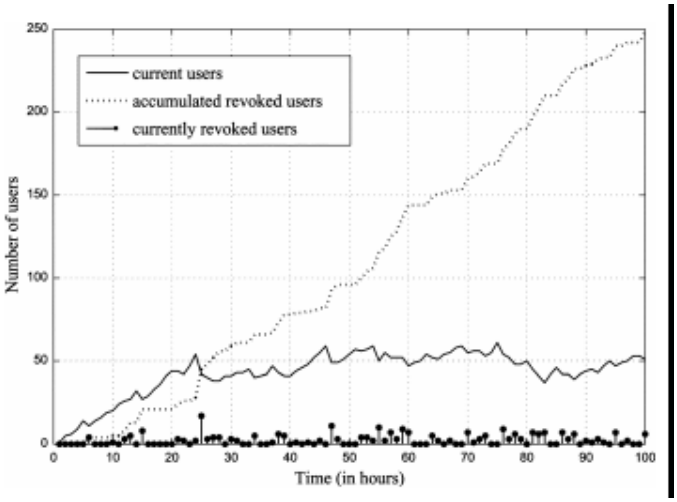

Fig2: Number of users in attribute group

We suppose that user join and leave events are independently and identically distributed in each attribute group following Poisson distribution. The membership duration time for an attribute is assumed to follow an exponential distribution. We set the interarrival time between users as 20 min **(~λ = 3)** and the average membership duration time as 20 h **(1/μ = 20)**.

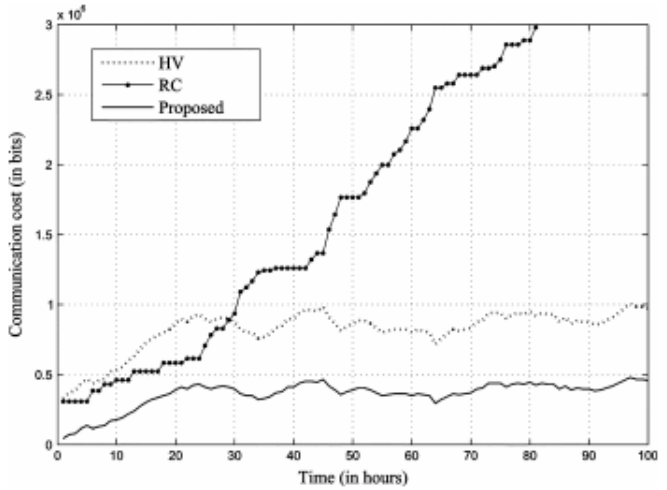

fig3: communication cost in the multi authority CP-ABP system

Fig. 2 represents the number of current users and revoked users in an attribute group during 100 h. Fig. 3 shows the total communication cost that the sender or the storage node needs to send on a membership change in each multiauthority CP-ABE scheme. It includes the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

ciphertext and rekeying messages for nonrevoked users. It is measured in bits. In this simulation, the total number of users in the network is 10 000, and the number of attributes in the system is 30. The number of the key authorities is 10, and the average number of attributes associated with a user's key is 10. For a fair comparison with regard to the security perspective, we set the rekeying periods in HV as **1/(~λ)** min. To achieve an 80-bit security level, we set $\mathbf{C_0 = 512, C_p = 160.}$ **CT** is not added to the simulation result because it is common in all multiauthority CP-ABE schemes. As shown in Fig. 3, the communication cost in HV is less than RC in the beginning of the simulation time (until about 30 h). However, as the time elapses, it increases conspicuously because the number of revoked users increases accumulatively. The proposed scheme requires the least communication cost in the network system since the rekeying message in is **Hdr** comparatively less than the other multiauthority schemes.

C. Implementation

Here we analyze and measure the computation cost for encrypting (by a sender) and decrypting (by a user) a data. We used a Type-A curve (in the pairing-based cryptography PBC) library) providing groups in which a bilinear map $\boldsymbol{e : G_0 \times G_0 \rightarrow G_1}$ is defined

Table III
COMPARISON OF COMPUTATION COST

		Pairing	Exp. in $\mathbb{G}_0$	Exp. in $\mathbb{G}_1$	Computation (ms)
Time (ms)		2.9	1.0	0.2	
BSW [13]	S		$2t+1$	1	$2t+1.2$
	U	$2k+1$		$\log t$	$5.8k+0.2\log t$ $+2.9$
HV [9]	S		$2t+1$	1	$2t+1.2$
	U	$2k+m$		$m\log(t/m)$	$5.8k+2.9m$ $+0.2m\log(t/m)$
RC [4]	S		$3t+1$	1	$3t+1.2$
	U	$3k+m$		$m\log(t/m)$	$8.7k+2.9m$ $+0.2m\log(t/m)$
Proposed	S		$2t+1$	1	$2t+1.2$
	U	$2k+1$	k	$\log t$	$6.8k+0.2\log t$ $+2.9$

S: sender, U: user

Table III shows shows the computational time results. For each operation, we include a benchmark timing. Each cryptographic operation was implemented using the PBC library anad the computational time results. For each operation, we include a benchmark timing. The public key parameters were selected to provide 80-bit security level. The implementation uses a 160-bit elliptic curve group based on the supersingular curve $\mathbf{y2 = x^2 + x}$ over a 512-bit finite field. The omputational cost is analyzed in terms of the pairing, exponentiation operations in $\mathbf{G_0}$ and $\mathbf{G_1}$. The comparatively negligible hash, symmetric key, and multiplication operations in the group are ignored in the time result. In this analysis, we assume that the access tree in the ciphertext is a complete binary tree.

VI. SECURITY

In this section, we prove the security of our scheme with regard to the security requirements discussed in Section II.

A. Collusion Resistance

In CP-ABE, the secret sharing must be embedded into the ciphertext instead to the private keys of users. Like the previous ABE schemes [11], [13], the private keys **(SK)** of users are randomized with personalized random values selected by the **CA** such that they cannot be combined in the proposed scheme. In order to decrypt a ciphertext, the colluding attacker should recover $\boldsymbol{e(g,g)^{(a1+a2+\ldots am)s}}$. To recover this, the attacker must pair $\mathbf{C_y}$ from the ciphertext and $\mathbf{D_y}$ from the other colluding users' private keys for an attribute λ_y(we suppose that the attacker does not hold the attribute λ_y). However, this results in the value $\boldsymbol{e(g,g)^{(a1+a2+\ldots am)s}}$ blinded by some random value, which is uniquely assigned to each user, even if the attribute group keys for the attributes that the user holds are still valid. This value can be blinded out if and only if the user has the enough key components to satisfy the secret sharing scheme embedded in the ciphertext. Another collusion attack scenario is the collusion between revoked users in order to obtain the valid attribute group keys for some attributes that they are not authorized to have (e.g., due to revocation). The attribute group key distribution protocol, which is complete subtree method in the proposed scheme, is secure in terms of the key indistinguishability [29]. Thus, the colluding revoked users can by no means obtain any valid attribute group keys for attributes that they are not authorized to hold. Therefore, the desired value

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$e(g,g)^{(a1+a2+...am)s}$ cannot be recovered by collusion attack since the blinding value is randomized from a particular user's private key.

B. *Backward and Forward Secrecy*

When a user comes to hold a set of attributes that satisfy the access policy in the ciphertext at some time instance, the corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key s in the ciphertext are reencrypted by the storage node with a random s^r, and the ciphertext components corresponding to the attributes are also reencrypted with the updated attribute group keys. Even if the user has stored the previous ciphertext exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the pervious ciphertext. This is because, even if he can succeed in computing $e(g,g)^{r(s+sr)}$ from the current ciphertext, it will not help to recover the desired value $e(g,g)^{(a1+a2+...am)s}$ for the previous ciphertext since it is blinded by a random s^r. Therefore, the backward secrecy of the stored data is guaranteed in the proposed scheme.

On the other hand, when a user comes to drop a set of attributes that satisfy the access policy at some time instance, the corresponding attribute group keys are also updated and delivered to the valid attribute group members securely (excluding the user). Then, all of the components encrypted with a secret key s in the ciphertext are reencrypted by the storage node with a random s^r, and the ciphertext components corresponding to the attributes are also reencrypted with the updated attribute group keys. Then, the user cannot decrypt any nodes corresponding to the attributes after revocation due to the blindness resulted from newly updated attribute group keys. In addition, even if the user has recovered $e(g,g)^{(a1+...am)s}$ before he was revoked from the attribute groups and stored it, it will not help to decrypt the subsequent ciphertext $e(g,g)^{(a1+...+am)(s+sr)}$ re-encrypted with a new random s^r. Therefore, the forward secrecy of the stored data is guaranteed in the proposed scheme.

VII. CONCLUSION

DTN technologies are becoming suitable solutions in military applications that allow wireless equipments to communicate with each other and access the confidential data witrh high reliable by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure information accessing 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 system to manage the confidential data distributed in the disruption-tolerant military network.

VIII. REFERENCES

[1] Junbeom Hur & Kyungtae Kang, Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks, The IEEE/ACM Transactions on Networking, (Volume:22, Issue:1)

[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 and ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.