Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

[1] **Shanmugasundaram. S,** [2] **Chitra. S,** [3] **Lokesh. V**

[1, 3] M. Tech. Student, Department of Computer Science and Engineering
Manakula Vinayagar Institute of Technology,
Pondicherry University, Pondicherry.

[2]Assistant Professor, Department of Information Technology
Manakula Vinayagar Institute of Technology
Pondicherry University, Pondicherry.

Abstract - Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant networks (DTN) technologies are emerging to become most successful solutions which allows the wireless devices to be carried by the soldier in-order to make communication with each other and access the information that are confidential or commands are made reliable by exploiting the external storage nodes. There are some of the most challenging issues present in this scenario, they are enforcement of authorization policy and policies that are updated for processing the data retrieval in a secure manner. Cipher text policy attribute-based encryption (CP-ABE) is a significant solution for cryptography in-order to access the control issues. The problem of implementing the CP-ABE is a de-centralized DTNs origins many security and privacy challenges regarding to attribute revocation key escrow, and co-ordinates of attributes given from different authorities. In this paper, we propose a secure scheme for retrieval of data using CP-ABE for de-centralized DTNs where the authorities of multiple key look after their attribute independently. We illustrate how to apply the proposed system to manage the confidential data with security and efficiency, distributed in the Disruption-tolerant military networks.

Keywords - *DTN, CP-ABE, Cipher Text, Attributes.*

1. Introduction

In several military networks scenario, the soldiers may temporarily disconnected from the connection of wireless devices due to jamming, mobility and environmental factor, mainly when they access in hostile environments [1, 2]. Disruption-tolerant network (DTN) techniques are emerging successful solution that permits the communication of for nodes within them, which occurs in the extreme networking environment. When the end-to-end connection does not exist between a source and a destination pair, the message from source to destination does not wait in the intermediate nodes for a substantial amount of time until the connection is established. DTN architecture is defined as where multiple authorities offer and look after their own independent attribute keys as de-centralized DTN. ABE is a significant approach that satisfies their requirements for data retrieval securely in DTNs. ABE features a mechanism that origins and access control over the encrypted data using success policy and ascribed attributes on private and cipher keys.

2. Disadvantages

The problem of applying ABE to DTNs origins many security and privacy challenges. Since, the associated attribute may be changed by some users, at some user, at some point, or some private keys may be compromised, the key revocation for each attribute must be necessary in-order to make the system secure. This issue remains even more difficult mainly in AES system. Hence, every attribute is conceivably shared by many users.

3. Problem Definition

The problem definition defines that revocation of any attribute (or) single user in an attribute may offer the other user in the group.

For example, if a user is included or separated from the attribute group, the key attribute must be converted and re-distributed to the other members who are present in that same group for forward (or) backward secrecy [3, 4] It results in bottle-neck during rekeying procedure or degradation of security due to vulnerability in windows, if the previous attribute key is not updated suddenly.

4. Challenges

One of the most significant challenges is the key-escrow problem. In CP-ABE the private key of user is generated by key authority. This process takes place by applying the master secret key of authority to user's associated set of attributes. Thus every cipher text can be decrypted by the key authority. A potential threat to the data confidentiality or privacy for highly sensible data may happen, when the key authority is compromised by adversaries when deployed in the hostile environment. Even in the multiple-authority systems the key escrow is an inherent problem has the entire privileges in order to empower their own attribute keys with their own master secrets. Since such a mechanism of key generation depends on single master secret is the general method for many for many of the asymmetric encryption systems, such as the identity-based or the attribute based encryption protocols, deleting the escrow in a single (or) multiple-authority, CP-ABE is an pivotal open problem.[5,6,7,8].

The last challenge is the coordination of attributes provided from different authorities. When the multiple authorities maintain and provide attribute keys to the users independently with their own master secrets, it is very difficult to determine fine-grain access policies over the attributes issued from different authorities. For example, if authority A manages the attributes "role 1" and "region 1" and authority B manages the attributes "role 2" and "region 2". Then, it is not possible to produce an access policy (("role 1" OR "region 1") AND ("role 2" OR "region 2") in the before schemes because the OR logic between attributes given from various different authorities cannot be implemented. This occurs due to the fact that the different authorities produce their own attribute keys using their own independent and individual master secret keys. Hence, access policy such as "out-of" logic, cannot be expressed in before schemes.

5. Existing System

5.1 Key-Policy attribute-Based Encryption (Kp-ABE)

In Kp-ABE, the encryption can only get to label a cipher text with set of attributes. The key authority selects a policy for every user that decides which cipher text he can decrypt and provide the key to every user by presenting the policy into the key of user [9,10,11].

5.2 Attribute Revocation

The solution is proposed in-order to append each attribute an expiration date or time and provide a new set of keys to the users who are considered to be valid after expiration.

5.3 Key Escrow

Many existing ABE schemes are built on the architecture where a single trusted authority has the power to provide the whole private keys of user with its master secret information. Hence, the key escrow problem is inherent in such a way that the key authority can be decrypted and every cipher text can be addressed to the users in the system by providing their secret keys at any time [12,13,14].

A distributed KP-ABE scheme proposed will solve the key escrow problem in a multi authority system. In this approach, all authorities of attributes are taking part in the key generation protocol in a distributed manner in such a way that, they cannot pool their data and link multiple attribute sets belonging to the same user.

5.4 De-Centralized Abe

A combined access policy over the attributes given from various authorities by simply encrypting the data multiple times. The main drawback of that technique is the efficiency and expressiveness of the access policy.

5.5 Disadvantages

The periodic attribute for ABE schemes has two main problems.

(i) The first and the foremost one is the degradation of security in terms of forward and backward secrecy.

(ii) The next is the scalability problem. The key authority regularly conveys a key update material by unicast at every time-slot, so that all the users who are not revoked can also update these keys. The single attribute up-dation of distributes entire non-revoked users who may share the attribute,

(iii) However, this solution will lack in efficiency performance.

(iv) Key Escrow system needs high communication overhead on the system set-up and also the components of rekeying phase besides the attribute keys, where there is number of authorities in the system.

(v) Under the de-centralized ABE, the access logic should only be AND, and they need operations of iterative encryption, where there is number of authorities of attributes. Here they are anyhow restricted in terms of access policy expressiveness and need computation and storage cost.

6. Proposed System

(i) To propose an attribute based secure data for the transaction of data retrieval using digital signature.
(ii) (CP-ABE) is used for encryption and decryption.
(iii) Key-Issue Protocol generates and issues the secret key for user.
(iv) Key authorization is used for sharing the keys between the sender and the receiver.
(v) Digital Signature is used for Key Authorization.
(vi) In, the two PC protocol the key authority act as master secret for sharing information.

6.1 Advantages

There are three main advantages of proposed work. They are,
(i) The first and foremost one is the immediate revocation of attribute that improves the forward/backward secrecy of confidential data by lowering the windows of vulnerability.
(ii) The second one is, encrypted can describe a fine-grained access policy by monotone access structure below attributes given from any chosen attribute sets.
(iii) The third one is, the key Escrow problem which is determined by an escrow-free key providing protocol that destructs the characteristics of decentralized DTN architecture.

7. Related Work

ABE is comprised two flavors called key-policy
ABE (KP-ABE) and
Cipher text-policy ABE (CP-ABE)

7.1 Kp-Abe

In Kp-ABE, the encryption only obtains to label a cipher text along with set of attributes. The key authority selects a policy for each and every user that decides which cipher text that user can decrypt and provides the key to each user by enhancing the policy into user's key.

7.2 Cipher Text Policy Abe (Cp-Abe)

The encryption of cipher-text is done along with an access policy selected by an encyptor, but the key is normally shaped with respect to an attribute set. The appropriation of CP-ABE is more in DTNs than KP-ABE because it allows encyptors such as commanders to select an access policy on the attributes and also encrypts confidential data.

7.3 Attribute Revocation

Results that proposed to order to append each attribute an expiration date and issue a new set of key to the appropriate valid users after the period of expiration.
The attribute of periodic revocable ABE process arises of two main problems. The first problem is degradation of security in terms of forward and backward secrecy.
The next is the scalability problem. The key authority frequently informs a key update material by unicast at each time-slot and hence all non-revoked users can also update their keys. This effects in the "I-affects-"problem, which defines that the single attribute updation will disturb the entire non-revoked users who shared the attribute.

This may result in blockage for both key-authority and all the non-revoked users. The sudden key revocation can by implemented by revoking users using ABE that supports negative clauses. In order to do it, one just includes conjunctively the ADD of negation of revoked user identifiers. Though, this result still fails in efficiency performance. This process will pretense slide group elements fanatic to the size of the private key over original CP-ABE process of Bethen law court et al.; where there is highest size of revoked attribute set. Golle et al. also proposed a KP-ABE scheme which is user revocable, but this process will work only when the number of attributes which is associated with cipher text is exactly half the size of the universe.

7.4 Key Escrow

Almost many of the existing schemes are built on the architecture where a single trusted authority has the access in order to kick-start the whole private keys of users along with its confidential information. Hence, the key escrow problem is inherent in such a way that, by kick-starting their secret key at any time, the key authority decrypts every cipher text addressed to the users present in the system.

Chase et al, proposed a distributed KP-ABE scheme that reveals the key escrow problem in a multi authority system. In this scheme, each attribute authority are taking-part in the key generation protocol in a distributed manner in such a way that they cannot group data and link multiple attribute sets which belongs to the same user. The main disadvantage of this approach is the performance degradation. Since, the centralized authority is not present in the master secret degradation, every attribute authority should deal with authorities present the system in order to produce a users's secret key. This tends to communication overhead on system setup and rekeying phases components moreover the attribute keys, where the system's number of authorities are present.

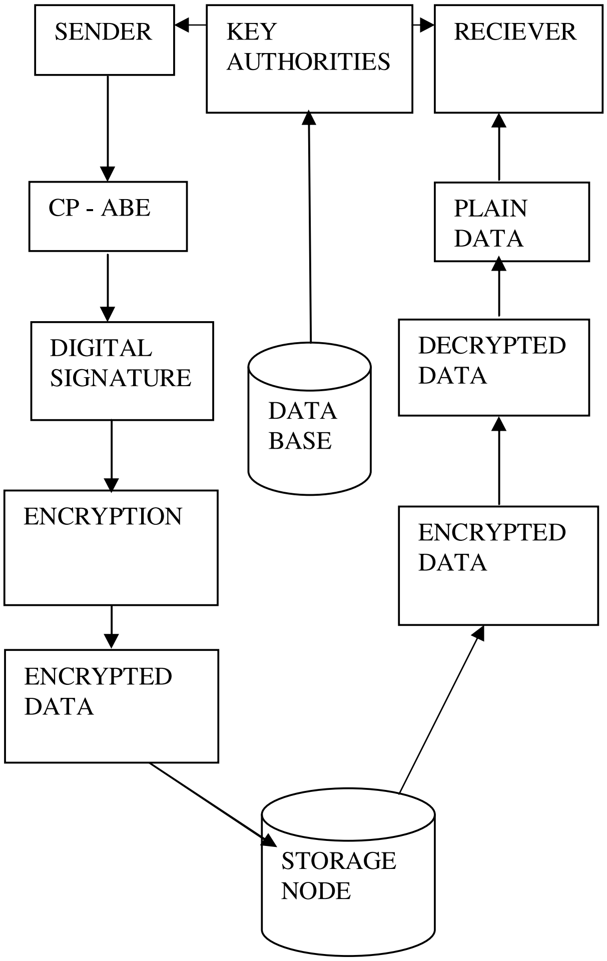

Fig 1. Architecture Diagram

7.5 Decentralized Abe

Huang et al. and Roy et al. determined a decentralized CP-ABE scheme in multi authority network environment. They obtained a joined access policy over the attributes given from various authority by encrypting the data many number of times. The main drawback of this scheme is the efficiency and expressiveness of access policy. For example, when a confidential mission is encrypted by a commander to soldier under the policy, it cannot by conveyed, when each attribute region is maintained by various authority, since the multiple encrypting approach cannot be expressed by any general. “Out-of-“logics. For example, let be the key authorities, and be the attributes stets they autonomously accomplish, respectively. Then the access policy which is expressed with is, can be determined by encrypting the message with by, and then encrypting the subsequent cipher text and then encrypting the subsequent cipher text with by and so on, this process goes on till multi encryption produces the final cipher text. Thus, the access logic must only be AND, and they need iterative encryption operations where the number of authorities are present. So, slightly they are restricted in terms of expressiveness of the access policy and need the cost of storage and computation. Even though, Chase and Leweko et al. proposed a multi authority KP-ABE and CP-ABE scheme, they will undergo the key escrow problem.

8. Conclusion

The DTN techniques are emerging to be the most effective solution in military applications that let the wireless devices to interact with each other and access the confidentially secure information consistently by exploiting the external storage nodes. CP-ABE is an ascendable cryptographic solution to the access control and retrieval of secure data issues. In this paper, we proposed an well-organized and secure data retrieval method using CP-ABE for decentralized DTNs where the attributes are autonomously managed by multiple key authorities. The characteristic key escrow problem is determined, such that the security of the stored data is guaranteed even in the hostile environment where the key authorities may be compromised or untrusted. The revocation for fine-grained key can also be done for each attribute group in addition. We elucidate how to apply the proposed system in order to manage the confidential data distributed in disruption-tolerance military network in a secured and efficient manner.

References

[1] JunbeomHur and Kyungtae Kang, Member, IEEE, ACM “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks”-IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.

[2] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle-based disruption tolerant networks,” in Proc. IEEE INFOCOM, 2006, pp. 1–11.

[3] M. Chuah and P.Yang,“Node density-based adaptive routing scheme for disruption tolerant networks,” in Proc. IEEE MILCOM, 2006, pp. 1–6.

[4] M. M. B. Tariq, M. Ammar, and E. Zequra, “Message ferry route de- sign for sparse ad hoc networks with mobile nodes,” in Proc. ACM MobiHoc, 2006, pp. 37–48.

[5] S.Royand,Chuah,“Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

[6] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2007, pp. 1–7.

[7] A.LewkoandB.Waters,“Decentralizing attribute-based encryption,” Cryptology ePrint Archive: Rep. 2010/351, 2010.

[8] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Eurocrypt, 2005, pp. 457–473.

[9] 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.

[10] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute- based encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[11] 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.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing withattributerevocation,”in Proc.ASIACCS,2010,pp.261–270.

[13] A.Boldyreva,V.Goyal,andV.Kumar,“Identity-based encryption with efficient revocation,”in Proc.ACM Conf.Comput.Commun. Security, 2008, pp. 417–426.

[14] RafaeliandD.Hutchison,“A survey of key management for secure group communication,” Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003