ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization *Vol.3, Special Issue 4, April 2015*

National Conference On Emerging Trends in Information, Digital & Embedded Systems (NC'e-TIDES -15)

Organized by

Dept. of ECE, Annamacharya Institute Of Technology & Sciences, Rajampet, Andhra Pradesh-516126, India held on 28th February 2015

Secure Knowledge Retrieval for Localized Military Networks

D. Ganesh, C.V. Lakshmi Narayana

II M.Tech, Department of CSE, AITS, Rajampet, India

Assistant Professor, AITS, Rajampet, India

ABSTRACT: The sharing of information between soldiers in battlefield must be confidential, and there is need of separate network for their communication, Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and to access the confidential information or command reliably by exploiting external storage nodes with the help of Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach, those it has some security problems like soldiers remembering their private keys every time there are moving from one location to another location in the battlefield, to over this problem in this paper we are proposing a central trusted authorities to have all the soldiers keys and acting as medium between soliders in this communication, and we are also improving communication speed and efficiency.

KEYWORDS: Attribute Based Encryption (ABE), Efficiency, Disruption Tolerant Network, Security.

I. INTRODUCTION

In many 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. 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.

DTN architecture may be referred as where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

II. EXISTING SYSTEM

Storage nodes in DTNs were used, where data is stored or replicated such that only authorized mobile 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.

Attribute-based encryption (ABE):

ABE is a promising approach that fulfills the requirements for secure 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. ABE comes in two flavors called

- key-policy ABE (KP-ABE) and
- Ciphertext-policy ABE (CP-ABE).

KP-ABE

In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user's key.

Ciphertext-policy ABE (CP-ABE)

The ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

Attribute Revocation:

Solutions proposed to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration.

The periodic attribute revocable ABE schemes have two main problems.

The first problem is the security degradation in terms of the backward and forward secrecy.

The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the nonrevoked users can update their keys. This results in the "1-affects- " problem, which means that the update of a single attribute affects the whole non-revoked users who share the attribute.

This could be a bottleneck for both the key authority and all nonrevoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. This scheme will pose overhead group elements1 additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt et al., where is the maximum size of revoked attributes set . Golle et al. also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the universe size.

Key Escrow

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

Chase et al. presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. This results in communication overhead on the system setup and the rekeying phases components besides the attributes keys, where is the number of authorities in the system.

Decentralized ABE

Huang et al. and Roy et al. proposed decentralized CP-ABE schemes in the multiauthority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multiencrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively. Then, the only access policy expressed with is, which can be achieved by encrypting a message with by , and then encrypting the resulting ciphertext with by (where is the ciphertext encrypted under), and then encrypting resulting ciphertext with by , and so on, until this multiencryption generates the final ciphertext . Thus, the access logic should be only AND, and they require iterative encryption operations where is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require computation and storage costs.

Chase and Lewko et al. proposed multiauthority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

2.1 Disadvantages

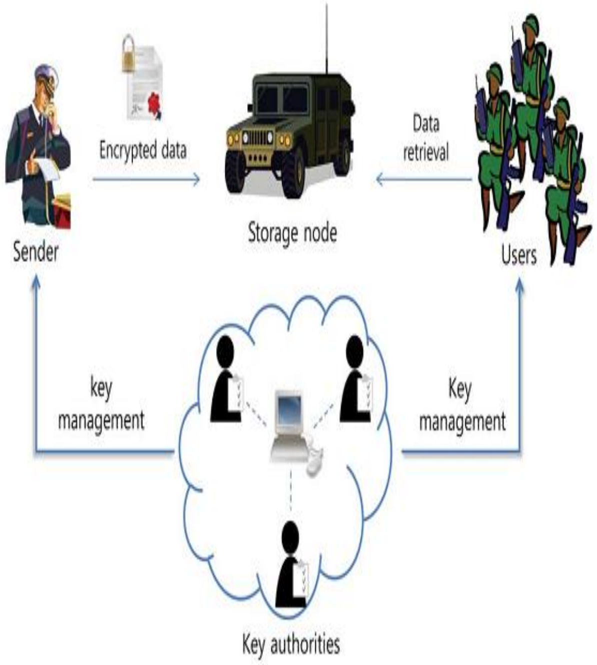
However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users.

III. PROPOSED SYSTEM

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 decrypt the ciphertext. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets.

The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone.

3.2 SYSTEM ARCHITECTURE:



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.

Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static

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.

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.

3.3 Advantages

The proposed scheme features the following achievements.
First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.
Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities.
Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture.
Thus, users are not required to fully trust the authorities in order to protect their data to be shared.
The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

IV. CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues.

REFERENCES

1. J. Bethencourt and others. Ciphertext-policy attributebased encryption. In *Proceedings of IEEE SP, Oakland*, 2007.
2. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *SIAM Journal of Computing*, 2003.
3. J. Burgess and others. Maxprop: Routing for vehiclebased disruption tolerant networks. In *Proceedings of IEEE Infocom*, 2006.
4. M. K. et al. Plutus: scalable secure file sharing on untrusted storage. In *Proceedings of ACM Usenix*, 2002.
5. V. Goyal and others. Attribute-based encryption for finegrained access control of encrypted data. In *Proceedings of ACM CCS*, 2006.
6. A. Harrinton and C. Jensen. Cryptographic access control in a distributed file system. In *Proceedings of ACM SACMAT*, 2003