International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 6: June 2015, pp 52-54. www.aetsjournal.com ISSN (Online) : 2394-6237

Secure Data Retrieval Based on Attribute-Based Encryption in Military Networks

M.Nagarajan ,R.Rajkumar

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 network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. 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. The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. 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 decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy.

Keywords — Proposed works, Network Setup, Disruption-tolerant network, attribute-based encryption.

I. INTRODUCTION

The Wireless device that are carried by soldiers in hostile environments are disconnected by using jamming and mobility in our Military Networks. There are many networks that are used by the soldiers but the most successful solution in Wireless is Disruption-tolerant network (DTN) technologies. In our Military it is very important to keep our accessing data more confidential. So in these cases the data access policies are defined over attributes or roles. They are managed by the key authorities. . For example, it is important for the commander to store the confidential information at a storage node to be accessed by the soldiers. For this purpose they are using the key authority for the whole group but 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. Due to this purpose, I am referring to this DTN where multiple authorities issue and manage their own attribute keys independently as decentralized. The data has to be wait until the connection is established, if there is no end-to-end connection between a source and destination.

There are many security problems when applying ABE to DTNs. Some of the soldiers under one group can change their associated attributes at some points and access the other group information's. Another important challenge is the key escrow problem. In ABE, through the master key and set of attributes the private key is generated. If the key authority is compromised by adversaries when deployed in the hostile environment, this could be a potential threat for the confidential data. The private key is generated in both ways they are Attribute-based encryption or Identity-based encryption protocols.

Attribute-Based encryption concept is a promising approach to fulfill the requirements for secure data retrieval in DTNs. The best policy is Ciphertext-policy ABE that provides a scalable way for encrypting data. Through this CP-ABE, different users are allowed to decrypt different pieces of data.

The last challenge is the coordination of attribute issued from different authorities. The commander will sent the data as well as the secret key in same file so the hacker can easily hack the file and get the secret key. Through the secret key they can decrypt the file and see the confidential data.

II. Related works

The concept of attribute-based encryption (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. 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. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the gro up. For example, 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.

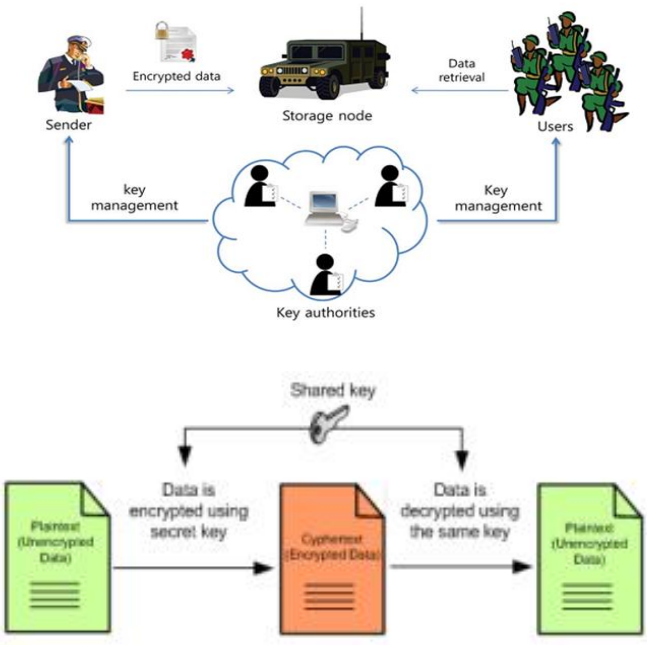
M.Nagarajan, Final year (B.Tech), Department of Information Technology, Kalasalingam Institute of Technology, Krishnan Koil

R.Rajkumar is Assistant Professor, Department of Information Technology, Kalasalingam Institute of Technology, Krishnan Koil

III. PROPOSED WORKS

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 decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. 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 attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

IV. BLOCK DIAGRAM



V. SYSTEM MODELLING

Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the users, what it will work efficient and effectively. It involves careful planning, investing of the current system, and its constraints on implementation, design of methods to achieve the changeover methods.

The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out in these plans; discussion has been made regarding the equipment, resources and how to test activities.

The coding step translates a detail design representation into a programming language realization. Programming languages are vehicles for communication between human and computers programming language characteristics and coding style can profoundly affect software quality and maintainability. The coding is done with the following characteristics in mind.

- Ease of design to code translation.
- Code efficiency.
- Memory efficiency.
- Maintainability.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

5.1 NETWORK SETUP

In this module, the soldier and commander are considered as nodes. Hence network of nodes is formed. These nodes are equipped wireless communication. This model is designed to deliver data with the use of DTNs. This system is also designed to produce high secure secret key.

5.1.1 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.

5.1.2 STORAGE NODE

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted. In our project we are using the storage as mail or local system.

5.1.3 COMMANDER (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.

5.1.4 SOLDIER (USER)

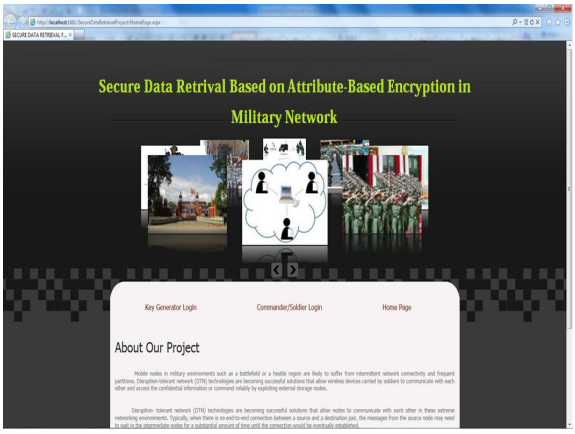
This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

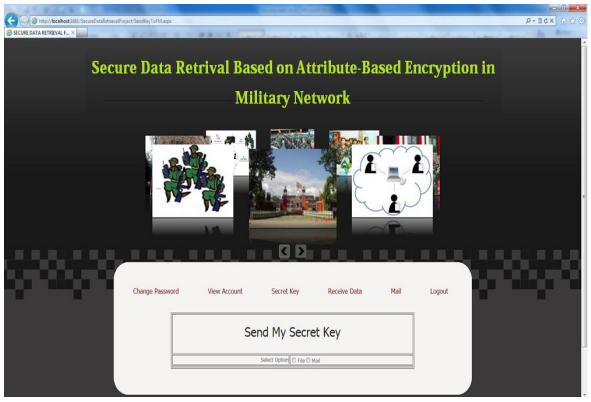
5.1.5 CP-ABE METHOD

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

VI. RESULT

The proposed CP-ABE handles each responsibility and delivery latency in DTNs. Key Authority build the secret key and send to the soldiers. Commander sends the data without secret key so the hackers cannot hack the data. And the secret key is send through mail or any other ways without any hacking.





VII. 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. In this paper, we proposed an efficient and secure data retrieval method usingCP-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, thefine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

REFERENCES

[1] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd edition, Morgan Kaufmann, 2011. p. 444.
[2] T.W. Liao, ”Clustering of Time Series Data: A Survey,” Pattern Recognition, vol. 38, no. 11, pp. 1857-1874, Nov. 2005.
[3] A.K. Jain, ”Data Clustering: 50 Years Beyond K-means,” Pattern Recognition Letters, vol. 31, no. 8, pp. 651-666, June 2009.
[4] S. Guha, A. Meyerson, N. Mishra, R. Motwani, and L. OCallaghan, ”Clustering Data Streams: Theory and Practice,” IEEE Trans. Knowledge and Data Eng., vol. 15, no. 3, pp. 515-528, May 2003.
[5] J. Beringer and E. Hullermeier, ”Online Clustering of Parallel Data Streams,” Data and Knowledge Engineering, vol. 58, no. 2, pp. 180-204, Aug. 2006.