International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 5 No. 6, June, 2015

Data Retrieval in Wireless Military Networks Using Advanced Encryption Technique

[1]V. Anbarasu, [2]A.Sundar Rajan and [3]S.Sudhakar
[1]Assosiate Professor, Jeppiaar Engineering College, Chennai.
[23]B.Tech (Information Technology), Jeppiaar Engineering College, Chennai.

ABSTRACT

In the transformation of data sources in military systems, the security constraints have serious issues. In order to retrieve the data secured and efficiently we use the CP-ABE. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The problems of key Escrow, Revocation and co-ordination are discussed and we demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. The overall monitoring of the system is and uses of analysis are discussed.

Key Words: *Attribute Based Encryption, Cipher Text Policy-Attribute Based Encryption, Key Policy- Attribute Based Encryption And Disruption Tolerant Network.*

1. INTRODUCTION

Military networks normally have several wireless interconnected communication devices to carry forward secure information. The major scenario is the effective and secured communication on both the ends. The connection problem caused by Jammers, Towers, and many other natural calamities are met by recently developed Disruption Tolerant Network (DTN) technologies, When one message is sent to another node, due to disruption, it stores the in intermediate storage nodes. Hence, information can be assessed quickly through these nodes when connection is found out.

The secured data retrieval among the sources is met by Attribute Based Encryption (ABE) [2] [4].It is encryption algorithm to encrypt the confidential data's. Since the attributes are encrypted, if one user suddenly changes the location (or) position, it results in key revocation problem [8], where immediate update of the attribute becomes difficult and there is a possibility of secret key leakage.

Key escrow is also an major issue, where the un-authorized non-trusted user accesses the network on the login when the key is leaked. Since all the members of the crew are having a public secret key, the whole military's confidential data's get exploited [7]. In order to resolve these issues, The cipher text policy-Attribute based encryption(CP-ABE), provides a multiple authority schemes, where each user is given a own private key generated by the Master's secret key based on their Attributes[5][6]. This gives the advantage of maximum confidentiality in hostile environments. ex: If a non-trusted user tends to leak his secret key, Then the data's of only his functionality get exposed there by keeping others information secured. Since it has multi authority to single-user, it updates the attributes individually and immediately, solving the revocation and co-ordination problem.

2. RELATED WORKS

Military Networks with many wireless communicating devices suffers an end to end node communication problem in DTN, which came out with the proposal gave on Message Ferry Route Design for Sparse Ad hoc Networks with Mobile Node that generates a ferry route which assures good performance without any online link between the nodes and the ferry[3]. This Design has an intermediate node communication. In these DTNs The Attribute based Encryption (ABE) is the suggested algorithm for Secure Attribute Based System presenting cryptographic optimizations that vastly improve enforcement efficiency of complex policies, proposed by Matthew Pirretti and Patrick Traynor [4].This Method led to Key Revocation Problem, when handled in the Disruption tolerant Networks (DTN) .Then with the Fuzzy Identity Based Encryption (F-IBE) from Lattices proposed on Learning With Errors (LWE) [2]. This was possible by observing properties that secret sharing schemes need to satisfy, becomes complicated. Resolving this, The Identity-based Encryption (IBE) with Efficient Revocation proposed a scheme that improves key-update efficiency of the trusted party, based on the ideas of the Fuzzy IBE primitive and binary tree data structure[2][9]. This module has a constraint in data sharing, since it has the user's identity encrypted. So, by using the method of proxy re-encryption with CP-ABE, the Attribute Based Data Sharing with Attribute Revocation is achieved, which enables the authority to revoke user attributes efficiently, but the Authorization Problem With the single public key is a major challenge in confidentiality [8].

In hostile environments on military sources, if a soldier tends to leak the public key, the whole system gets distorted and results in the Key Escrow problem. It is the scenario that a un authorized person gets in to the networks. Therefore, Sherman S.M. Chow proposed on Removing Escrow, which is new system architecture with a private key generation protocol issuing a private key to an authenticated user not

considering their identities [7].This individual multiple keys to individual users improves the networks security. The management of this key remains complicated process [1] and has a separate group key management.

3. PROPOSED SCHEME

We propose a decentralized CP-ABE scheme in multi authority network environment to secure the encrypt and decrypt data using key authority generating the key. Secure data retrieval of military tolerant network in decentralized DTNs. Thus, the scalability and security can be enhanced in the proposed scheme. The role of the parties is taken by the attributes. Thus, the access structure will contain the authorized sets of attributes.

Cipher text policy attribute based encryption (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the descriptor needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. Further monitoring of the whole function and analysis is also done for the network to determine the most-trusted user by the Admin. The cross-system User Data Discovery is used for this purpose. The number of times the user logged in, the time, date and various factors are monitored using the (CS-UDD).Therefore the most trusted user ,ex:-(battalion, soldier) can be selected based on these Analysis.

4. SYSTEM COMPONENTS

The data transmission in these networks is carried out between the admin and the end users. In the midst of this functioning, database holds the user's login details and the storage node has control of encrypted keys. The requests on both the ends is managed by the storage node

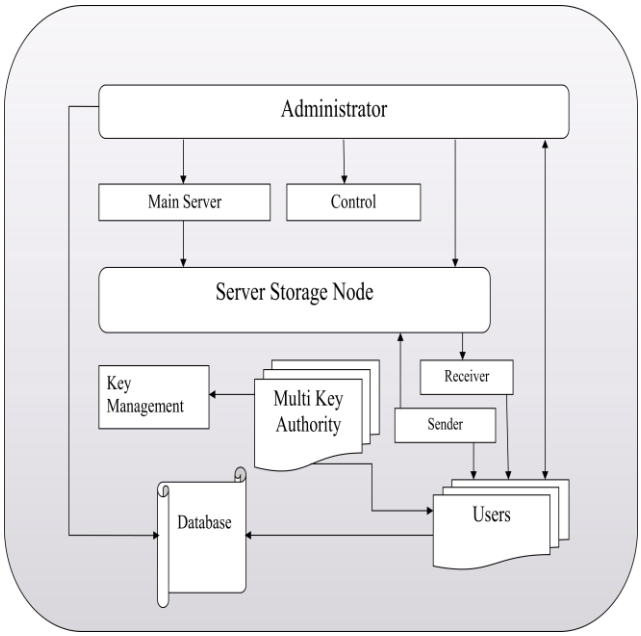

Figure 1. Architecture of the secured data retrieval system.

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. The Administrator is the higher authority controlling the subsequent data retrieval to the end users. 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.

4.1 Key Generation

This is the first phase, where the user gets checked in to the network. This component is created for the security purpose with the user interface design. In this we have a login page to enter user name and password. It validates the given data by referring the database. If found matched, then enters the user page, else re-transmits to the initial page. So we are preventing unauthorized user entering the network. It will provide a good Initial security for highly confidential datas.

4.2 Storage Node

The user will upload some data's in the User Page. The system will calculate size of the file and sends through Storage node. Therefore storage node can get the data without traffic and also transmit the data in less time. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme. This is an entity that stores data from senders and provide corresponding access to users. We also assume the storage node to be semi trusted, that is honest-but-curious.

4.3 Store-carry and forward

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. 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 cipher text and obtain the data.

4.4 Decentralized user

We provide a multi-authority CP-ABE scheme for secure data retrieval 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. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Communicate with every user in network.

5. RESULTS

The home page for various authorities to login is illustrated in Figure 2.

Figure 2. Control page for multiple users to login to their domains.

Figure 3.implies the authentication of the user is with respect to their ID and Passwords.

Figure 3. Login page for user's validating check.

The command transformation among the network of users and the status of the message is shown in the Figure 4.

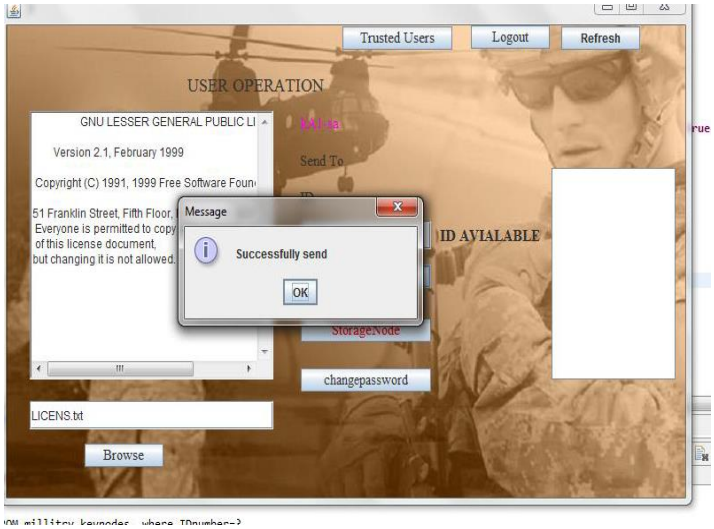

Figure 4. Data transfer between end to end users.

The Admin's monitoring page, where the user activities, data sending are managed is shown in the Figure.5.

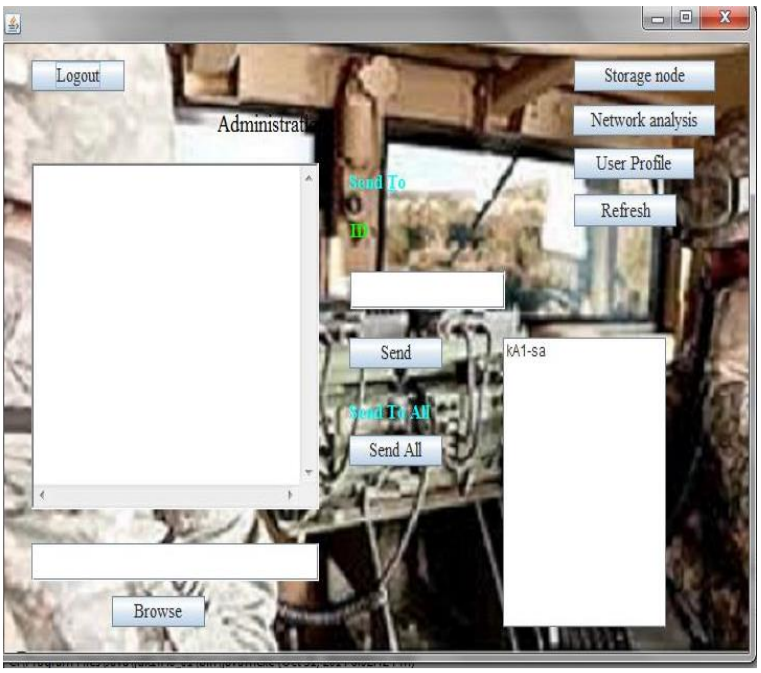

Figure 5. Administrator's control page for monitoring user's activity.

Finally the analysis of the overall system, to select the trusted party is shown in the Figure .6.

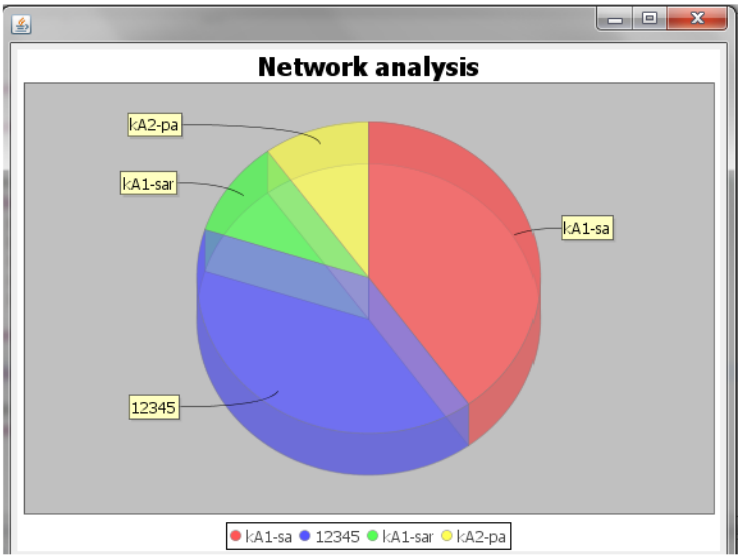

Figure 6. Analysis on user for selecting trusted authority.

6. CONCLUSION

We proposed an efficient and secure data retrieval 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 mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. The overall monitoring system also enhances the security and betterment of the system

REFERENCES

[1] Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 2000, pp. 277–288.

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

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in Proc. ACMConf. Compute. Commun. Security, 2006, pp. 99–112.

[10]

[5] M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534.

[6] .M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM Conf. Comput. Comm. Security, 2009, pp. 121–130.

[7] S. S.M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.

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

[9] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption withefficient revocation," in Proc. ACM Conf.Comput.Comm.Security, 2008, pp.417–426.