IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ADVANCED APPROACH FOR SECURE RETRIEVAL OF DATA IN DISRUPTION TOLERANT MILITARY NETWORKS

Divina T.K Premdas*, Dr.D.Loganathan
*Final year M. Tech-CSE, MET'S School of Engineering, Mala, Thrissur, Kerala, India
Professor and Head, Department of CSE, MET'S School of Engineering, Mala, Thrissur, Kerala, India

DOI: 10.5281/zenodo.58603

ABSTRACT

Communication nodes in military environments such as a battleground regions are likely to suffer from connectivity issues in various locations in a battle field. Disruption-tolerant network (DTN) technologies are becoming promising solutions that allow wireless devices which the soldiers carry to communicate with each other and access the confidential information Some of the most facing issues in this area is the enforcement of Authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a powerful cryptographic solution to the access control issues in a secure environment. However, the problem of applying CP-ABE in decentralized in this paper we solve the issue of security and privacy challenges such as key escrow, attribute revocation and coordination of attributes issued by different authorities. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data by providing unique security measure using certificates by protecting the systems used and authorizing the system network.

KEYWORDS: Access control, Attribute Based Encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval, MAC, I.P, Certificate.

INTRODUCTION

Generally, security plays an important role in a network communication. It should be highly secured while dealing with security information especially with armed forces. Movable nodes in a military network are predicted to occur at regular or irregular intervals at various point of time based on the situations. One of the emerging and successful technique is Disruption-tolerant networks [2], [3] which provides a reliable communication between an armed force consistently. The most proficient elucidation that changes the data into an unreadable format is a cryptographic technique called Cipher text-policy attribute based encryption [7], [8]. Decentralized DTN are constantly facing security issues as mobile nodes tend to change their positions. In this paper we have introduced a feature which will generate a certificate for each system, the certificate generated cannot be manipulated and misused as it is an image file with data hidden in that image. In this paper we are securing systems by acquiring the MAC address through I.P address hashing the MAC address. MAC address being a permanent address it cannot be changed so we can make the system secure and with authorization technique we make the network safe. Here, we use CP-ABE to generate keys, with an access policy embedded in it in order to increase the security measure.

RELATED WORK

ABE comes in two flavours called key-policy ABE (KPABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, encrypt or only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user from their attribute list that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the cipher text is encrypted with an access policy chosen by a sender, but a key is simply created with respect to an attributes set of the user. CPABE is more appropriate to DTNs [5] than KP-ABE because it enables encrypt or 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: In attribute revocation each attribute has an expiration date or time and a new set of keys is distributed to valid users after the expiration. Key Escrow: Most of the existing ABE schemes are constructed on the architecture where a trusted authority has the power to generate entire private keys of users with its master secret information only. Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. A distributed KP-ABE scheme proposed solves the key escrow problem in a multi authority 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.

Decentralized ABE: 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.

Drawbacks

First drawback in Attribute revocation is if the user leave an attribute set and change his location the key of the revoked user should be invalid. If the key is not updated immediately it may result in the blockage during rekeying procedure and will be insecure heavily if the key updating is not done instantly. Next introduces scalability problem which is caused when users constantly update their attributes, the keys have to be generated again.

PRESENT TECHNOLOGY

The Attribute-Based Encryption (ABE) concept is providing us to satisfy us to supplies for secure data retrieval in DTNs [1],[4]. ABE (Attribute Based Encryption) is public key encryption technique where decryption of a cipher text can be done by a user only when key match the attributes of the cipher text when compared. The most proficient technique that changes the data into an unreadable format is a technique called Cipher text-policy attribute based encryption. Decentralized DTNs having CP-ABE convey in several security and isolation challenges with regard to the attribute revocation, a fair cryptosystem, and the combination of attributes issued form different authorities. Multiple key authorities manage their attributes individually in a proposed system.

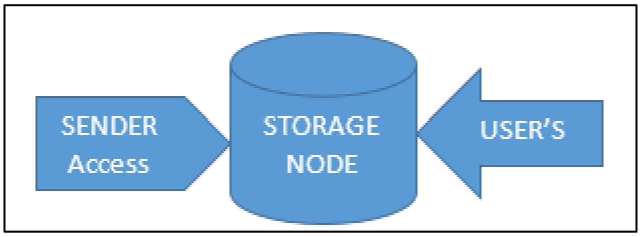

Figure 1. Data Flow from sender to user.

The key may affect the non-revoked users. The last confront is fair cryptosystem where the encrypted and decrypted data are placed in escrow where the third party can access the encrypted or decrypted data under some controlled conditions. Using one's own master key CP-ABE generates private key. Which may lead to data degradation when the key authority is compromised.

PC Protocol

The key issuing protocol generates and issues user with secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets and user attributes. The key issuing generates a secure protocol known as 2PC protocol which deters the key authorities from obtaining any master covert data of each other such that none of them could produce the complete set of user keys alone.

IMPLEMENTING AN SAFER SYSTEM.

In traditional distributed system user can able to access the data only if satisfies certain attribute policies. But at present the only way to instrument such policies is to use of trust worthy server to store the data and reconcile access control. The main problem here is if the security of the system is compromised then the data confidentiality is also compromised. The main problem here is if the security of the system is compromised then the data confidentiality is also compromised. Chances are there to misuse the system to pass false information. The main problem here is if the security of the system is compromised then the data confidentiality is also compromised.

There come three enhancement schemes for ABE. First is to focus on how to remove users officially in an untrusted network in this work we can enable data owner to delegate most task performing user removal without sending data to them. Second is authenticating the system with the help of certificates. Third is studying the enhancement schemes on issuing the privacy storage [6] in ABE.

NETWORK ARCHITECTURE

The DTN architecture (Figure 3) and the security model can be described as follow,

1) Key Authorities: They generate keys to the users. They have a central authority. They issue key based on the attributes. It is shown in the figure 2.

2) Storage node: They stores data from sender node (Figure 1). User who satisfies the sender attributes can retrieve the data from storage node.

3) Sender: They are the one who sends data to users.

4) User: User who wants to access the information store at the storage node (e.g., a soldier). But must satisfy user credentials.

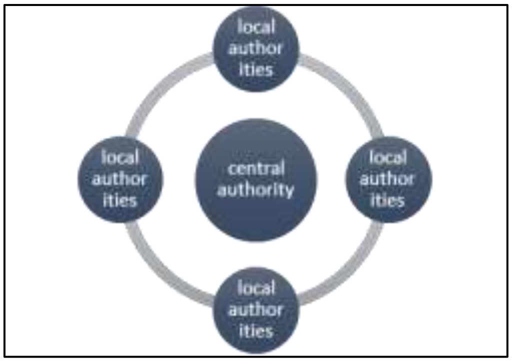

Figure 2 Authorities.

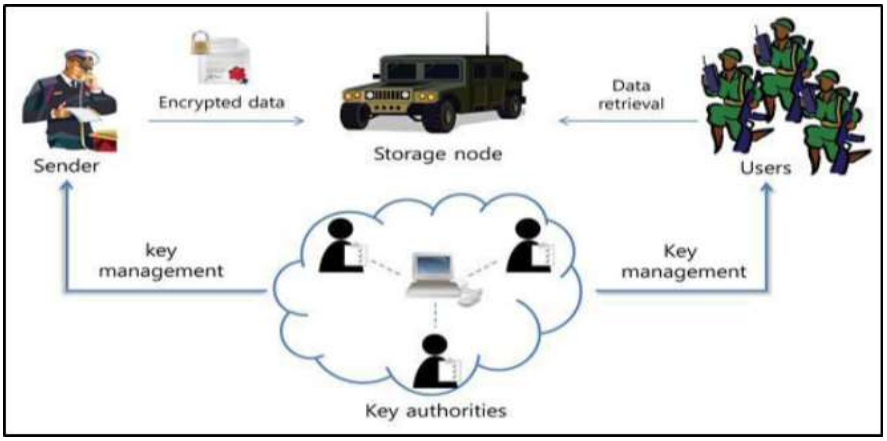

Figure 3: Secure data retrieval in a disruption-tolerant military network.

ENHANCEMENT OF PROPOSED SCHEME

Here we introduce the certification approach through by authentication MAC address to enhance the data security system, the following concepts have been incorporated,

1. Information privacy: Users who do not satisfy the access policy will not be able to access data from the storage node.
2. Collusion-resistance: Many users obtaining same attributes can decrypt the cipher text by combining their attributes.
3. Backward and forward Secrecy: Forward secrecy means the user should not be allowed to attain the plain text of the data on or before holding on attribute, on the other hand backward secrecy means when an user missed an attribute should not be allowed to regain the plain text.
4. Update Policy: - If a user changes his attributes a new key will be generated based on his new attributes for privacy issues.
5. Certification: - certificates is issued to authorized systems and these certificates should be uploaded for communications. Only authorized systems can receive certificates.

EXPERIMENTAL RESULTS

The effectiveness of a proposed system is improved when compared to an existing system. Authority can revoke user attributes with minimal cost by using proxy re-encryption with CP-ABE reduces communication costs and improve performance cost. And also by using some enhancement techniques like. First is to focus on how to make secure systems by checking the authorized MAC address. In this work we can enable data owner to perform user removal without sending data to them. Second is addressing key attacks where untrusted users share their decryption keys with unauthorized users, for this we are adding a random value along with ABE. Thus performance also get increased. Thus the system security is guaranteed.

CONCLUSION

DTN technique now fetching captivating solutions in armed presentation that allow communications consistently and sustaining secrecy. CP-ABE for DTN's provides reliable cryptographic approach where many key system manages their key attributes individually. A fair cryptosystem problem is strongminded where the confidentiality of data is definite under hostile environment. Also providing a key removal in a fine grained for an element set when created and updating the attributes there by, regenerating the keys. Here we used the certification approach to keep the systems safe, and by authentication MAC address access through unauthorised system is blocked. So, the proposed mechanism to strongly and competently manage the confidential data by providing unique security measure using certificates by protecting the systems used and authorizing the system network.

REFERENCES

[1] Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks Arram Sriram Asst.Prof, IT Depatment, Anurag Group of Institutions V: Venkatapur, M: Ghatkesar, D: Rangareddy, Telangana,

[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, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] S.Royand M.Chuah,"Secure data retrieval based on cipher text 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. Swaminath an, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. Conf. File Storage Technol., 2003, pp. 29–42.

[7] A.Lewkoand B.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.