ISSN:0975-9646

Efficient & Secure data Retrieval technique using CP-ABE for decentralized DTNs.

Prof. A.A.Rajguru[#1], Prof. V.V.Pottigar[#2], P.A.Patil[#3]

[#]ME Computer (Engineering), Dept. of Computer Science & Engineering, Solapur University,

SKN Sinhgad College of Engineering, Korti, Pandharpur, Maharashtra, India

Abstract -This survey paper is for secure data retrieval in which the Disruption-tolerant network (DTN) is the famous technology which used in the military network in which Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions so it is having the storage network if the connection is not establish it will store in the storage node after the connection is establish then it transfer to the receiver to make it secure. CP-ABE is used in which the transferred data is encrypted and the key is required to decrypt as it is a decentralized network multiple key authorities are used means the Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues for decentralized DTNs where multiple key authorities manage their attributes independently.

Keywords — Disruption-tolerant network (DTN), Ciphertext-policy attribute-based encryption (CP-ABE), secure data retrieval, Multiauthority.

I. INTRODUCTION

Network security describes the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. This means that a well-implemented network security blocks viruses, hackers, etc. from accessing and altering secure information. In military system environment, associations of remote gadgets conveyed by officers may be briefly detached by sticking, ecological variables, and versatility, particularly when they work in hostile environments. Interruption tolerant system (DTN) technologies are becoming favourably result that authorize nodes to communicate with each other in these immensely networking environments.

Disruption Tolerant Networks (DTN) is a type of network that is designed to provide communications in the most unstable and intermittent connections, where the network would normally be subject to frequent and long lasting disruptions that could severely degrade normal communications. Also 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.

Cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decrypter 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. Also in 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 encryptor 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

Therefore, the best solution for the above problem is that sender encrypts message with distinct public-keys, but the user uses private key for decryption so that key should be sent via a secure channel and kept secret.

II. LITERATURE SURVEY

The Attribute-Based Encryption system supports non-monotone expression in key policies. Which is achieved through a application of revocation method into existing ABE scheme but performance of our scheme is less-expressive so “Ciphertext-Policy” Attribute-Based Encryption is used in which attributes are used to describe the feature of key holder, and encryptor will associate the access policy. [2]

Many network applications are based upon group communication model. So providing authenticity of messages delivered between group members, will become critical issue. Now this paper gives solution to the scalability problem of group or multicast key management which defines secure group as triple (U, K, R) where U- a set of users, K-set of keys held by users, and R-user-key relation **[**3].

It is a type of public-key encryption in which secret key of user and ciphertext are dependent upon attributes. In which decryption of ciphertext is possible if and only if the set of attributes of user key matches the attributes of ciphertext. A crucial security aspect of Attribute-Based Encryption is collusion-resistance. This paper introduces attribute-based encryption (ABE) which is used for encryption. In which it finds match of each attribute from each group for encryption [4].

As more sensitive data is shared and stored by third-party sites on Internet, there will be need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared at coarse-grained level (i.e., giving another party your private key). So this paper presents new cryptosystem for fine-grained sharing of encrypted data is Key-Policy Attribute-Based Encryption [5].

Developed the secure data retrieval scheme for data sharing in military network using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme. Implemented a cryptosystem where multiple key authorities manage their attributes independently [1].

Referred Paper	Purpose	Conclusion
Attribute-Based Encryption with Non-Monotonic Access Structures	Data and access policies assigned to users for maintaining security of host.	In Attribute-Based Encryption an encryptor will associate data with attribute.
Secure Group Communications Using Key Graphs	Solution to problem of how to distribute secret to a group of users has been given in secure key graph.	The key graph is used for secure group communication in which user-key relationship given.
Secure Attribute Based Systems	Identity-based encryption in which public-key of user can be set as an identity.	Separate secret keys have to be generated for the identities.
Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data	Encryption of data can be selectively shared at the fine-grained level.	Fine-grained access control systems gives granting differential access rights to a set of users.

Table1. Summary of Literature Review

III.Scope

1. Multiple key authorities are allowed to decrypt different pieces of data per security policy
2. Disruption-Tolerant Network used for attribute key updating in Decentralized Military Networks.
3. This technique is useful for securely, efficiently, and flexibly share data with others in Military Networks
4. The scope of Disruption-Tolerant Networking (DTN) is in giving an alternative Solution for Future Satellite Networking Applications
5. In Protecting the Personal Health Record System the CP-ABE scheme is used in the DTN

IV.Proposed System

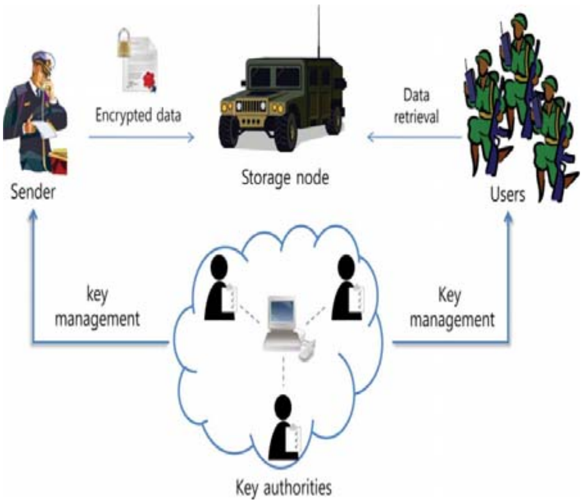

Fig 1: System Architecture

Here we describe the main idea of data sharing in military network using following module, illustrated in Figure,

1. Key Authorities
2. Key management
3. Storage node
4. Sender
5. Soldier (User)

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. They grant differential access rights to individual users based on users' attributes.

2. Key management:
It is the management of cryptographic keys which includes the generation, exchange, storage, use, and replacement of the keys.

3. Storage node:
This is an entity that stores the data from senders and provides the corresponding access to the users.

4. Sender:
This is an entity who owns confidential data (e.g. commander) and wishes to store them into external data storage node for ease of sharing A sender is responsible for defining access policy (attribute based) and own data by encrypting it under the policy before storing it to storage node.

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

V. 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 secures data retrieval issues. In this project, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

References

[1] Junbeom Hur 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] 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.

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

[4] C. K.Wong,M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in Proc. ACM SIGCOMM, 1998, pp. 68–79.

[5] 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

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[7] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444–458, May 2003.

[8] K. C. Almeroth and M. H. Ammar, "Multicast group behavior in the Internet's multicast backbone (MBone)," IEEE Commun. Mag., vol. 35, no. 6, pp. 124–129, Jun. 1997.

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

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. Conf. File Storage Technol., 2003, pp. 29–42.