IJRRECS/June 2015/Volume-3/Issue-6/4081-4085 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MANAGING OF ACCESS CONTROL IN ATTRIBUTE SYSTEMS FOR EFFECTIVE RECOVERY OF DATA

SK.Nagma[1], M.Venkat Rao[2]

[1]M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India

ABSTRACT:

The conception of attribute-based encryption is regarded as an effective means for assuring the requirements for secure retrieval of data in disruption tolerant networks. Cipher text-policy attribute-based encryption is a scalable solution to disruption tolerant networks when compared to others since it facilitates to decide an access policy on attributes. In our work we recommend an exceptional and protected data retrieval proposal by means of Cipher text-policy attribute-based encryption for decentralized disruption tolerant networks in which numerous key authorities administer their attributes autonomously. The setback of key escrow is worked out by means of an escrow-free key issuing procedure that exploits attribute of decentralized disruption tolerant networks construction. Key issuing method produces user secret keys by means of performing a protected two-party computation procedure between the key authorities by their own master secrets.

Keywords: Cipher text-policy attribute-based encryption, Key issuing, Disruption tolerant networks, Data retrieval, Key authorities, Decentralized.

1. INTRODUCTION:

Storage nodes in disruption-tolerant network were introduced by Roy and Chuah in which the data is stored or else replicated such that only the mobile nodes containing authorization can access necessary information promptly [1]. The efforts concerning disruption tolerant networks are becoming effective solutions that permit nodes to communicate in tremendous networking environments. The problem of

application of attribute-based encryption to disruption tolerant networks introduces quite a lot of security as well as privacy challenges. The technique of attribute-based encryption appears in two different forms such as key-policy attribute-based encryption and cipher text-policy attribute-based encryption. In the system of key-policy attribute-based encryption, encryptor has get to a label a cipher-text by means of a set of attributes. The key authority selects a policy in support of each user that concludes which cipher texts has to be decrypted and provide key to every user by means of embedding policy into user's key. In cipher text-policy attribute-based encryption, the cipher-text is encrypted by means of an access policy that was selected by means of an encryptor, however a key is just created regarding an attributes set [2][3]. Cipher text-policy attribute-based encryption is considered to be an effective solution to disruption tolerant networks when compared to others since it enables encryptors to decide an access policy on attributes and towards encryption of private data under access structure by means of encryption with analogous public keys. In our work we advise an outstanding and secure data retrieval proposal by means of Cipher text-policy attribute-based encryption for decentralized disruption tolerant networks in which numerous key authorities administer their attributes autonomously. The data confidentiality as well as privacy can be cryptographically enforced against any key authorities or else data storage nodes in proposed scheme.

2. AN OVERVIEW OF CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION:

Attribute-based encryption features a method that facilitates an access control above encrypted data by means of access policies and ascribed attributes between private keys as well as cipher texts. Cipher-ext-policy attribute-based encryption provides an effective means of encrypting data so that the attribute set was defined which is essential for the purpose of decrypting cipher-text. Consequently, various users are approved to decrypt various pieces of information for each security policy. In Cipher-ext-policy attribute-based encryption key authority produces private keys of users by means of applicator of authority's master secret keys towards user connected set of attributes. As a result, the key authority can decrypt each

cipher-text that is dealt to particular users by means of generating their attribute keys. The key escrow is a natural setback even in multiple-authority systems as long as each of the key authority contains complete privilege to produce their own attribute keys by means of their own master secrets. While such a key generation method on the basis of single master secret is fundamental method for most of the methods of asymmetric encryption for instance attribute-based or identity-based encryption protocols, removal of escrow in particular or else multiple-authority cipher text-policy attribute-based encryption is a essential open problem. Cipher text-policy attribute-based encryption is considered as an effective key in the direction of access control issues on the other hand, application of cipher text-policy attribute-based encryption in decentralized disruption tolerant networks introduces quite a lot of security as well as privacy challenges with reference to attribute revocation, key escrow [4], as well as coordination of attributes that are issued from several authorities.

3. MODELLING OF PROPOSED SYSTEM:

Our work provides a secure data retrieval proposal by means of cipher text-policy attribute-based encryption for decentralized disruption tolerant networks in which numerous key authorities administer their attributes autonomously. The proposed system achieves several benefits. The data confidentiality as well as privacy can be cryptographically enforced against any key authorities or else data storage nodes in proposed scheme. In the structure of disruption tolerant networks as shown in fig1 there are several entities. Key Authorities are the centres for key generation that usually produce public or secret parameters for cipher text-policy attribute-based encryption. The key authorities comprise in general a central authority as well as numerous local authorities and they grant differential access rights towards individual users on the basis of user attributes. Storage node is an entity that accumulates data from senders and grants parallel access towards users. It might be mobile or else static. Sender is accountable for defining of access policy and imposing it on own data by means of encrypting data in policy earlier than

accumulating it to storage node. User can be a mobile node who needs to access the data that is stored at storage node. The key escrow is a normal setback still in multiple-authority systems as long as each of the key authority contains complete privilege to produce their own attribute keys by means of their own master secrets. The problem of key escrow is solved by means of an escrow-free key issuing procedure that exploits attribute of decentralized disruption tolerant networks construction. Instantaneous attribute revocation increases privacy of confidential data by means of reducing windows of vulnerability. Encryptors can characterize a fine-grained access policy by means of any monotone access arrangement under attributes that are issued from any selected set of authorities. While the key authorities are considered as semi-trusted, they must be deterred from access towards plaintext of data within storage node; for the time being, they have to be still able to provide secret keys to users. To realize this to some extent an opposing necessity, the central authority as well as local authorities take on in arithmetic two-party computation protocol by master secret keys of their own and provide autonomous key components towards users throughout the key issuing phase. Key issuing procedure produces and provides user secret keys by means of performing a protected two-party computation procedure between the key authorities by their own master secrets [5]. Two-party computation procedure deters key authorities from attaining any master secret information of each other so that no one of them might produce complete set of user keys without help. The two-party computation protocol prevents them from recognizing each other's master secrets with the intention that no one of them can produce the complete set of secret keys of users independently. We consider an assumption that central authority does not collude with local authorities. Users are not essential to completely trust authorities in order to defend their data to be shared [6].

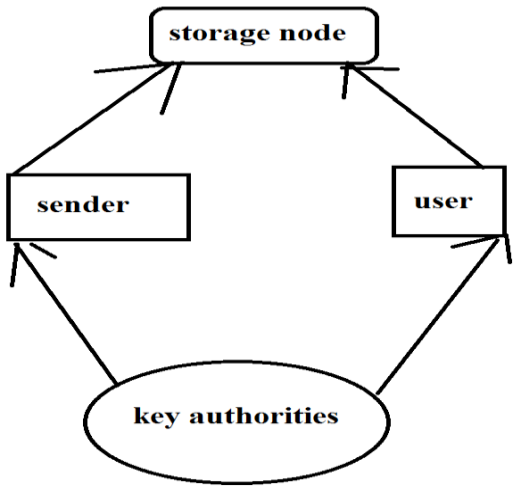

Fig1: Structure of disruption tolerant networks.

4. CONCLUSION:

The trouble concerning application of attribute-based encryption towards disruption tolerant networks introduces quite a lot of security as well as privacy challenges. Attribute-based encryption features a technique that makes possible an access control above encrypted data by means of access policies and ascribed attributes between private keys as well as cipher texts. Attribute-based encryption concerning cipher-ext-policy provides an effective means of encrypting data so that the attribute set was defined which is essential for the purpose of decrypting cipher-text. We consider an opinion of implementing an outstanding and secure data retrieval proposal by means of Cipher text-policy attribute-based encryption for decentralized disruption tolerant networks in which numerous key authorities administer their attributes autonomously. The key escrow is a standard setback still in multiple-authority systems as long as each of the key authority contains complete privilege to produce their own attribute keys by means of their own master secrets. Two-party computation practice put off key authorities from attaining any master secret information of each other so that no one of them might produce complete set of user keys without help. Key escrow is totally solved by means of an escrow-free key issuing procedure that exploits attribute of decentralized disruption tolerant networks construction.

REFERENCES

[1] S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.

[2] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp. Identity Trust Internet, 2008, pp. 26–35.

[3] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

[4] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[5] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[6] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009