IJRRECS/November 2015/Volume-3/Issue-11/4758-4763 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

EFFECTIVE MANAGEMENT OF DATA PRIVACY IN DECENTRALIZED NETWORKS

Guntur Purna Tejeswi Kavya[1], K.Praveen Kumar [2]

[1]M.Tech Student, Dept of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur, A.P, India

[2]Assistant Professor, Dept of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur, A.P, India

ABSTRACT:

Attribute-based encryption approach will satisfy the recovery of secure data within disruption tolerant networks. Traditional attribute based encryption are put up on design in which particular trusted authority will produce complete private keys of users by its master information. We introduce an approach of an effective data retrieval based on the attribute for the disruption tolerant networks of decentralized type in which several key authorities will control their attributes separately. In the data retrieval system, instant attribute revocation will improve enhances data privacy by means of dropping the windows of susceptibility. Key escrow difficulty is solved by key issuing approach that makes use of feature of decentralized disruption tolerant networks design. Data privacy is cryptographically made compulsory against curious key authorities in projected system.

Keywords: Attribute-based encryption, Disruption tolerant networks, Key escrow, data retrieval, Data privacy, Key authorities, Decentralized.

1. INTRODUCTION:

Disruption tolerant networks are efficient solutions for communication of nodes with each in extreme situation. The nodes of storage were introduced by Roy and Chuah in disruption tolerant networks in which only approved mobile nodes will have permission to essential data. Attribute-based encryption will provide an approach that facilitates access control above encrypted

data by means of access policies between private keys as well as cipher texts [1]. Application of attribute-based encryption approach to the disruption tolerant networks will introduce many of the security demands. While some of the users will alter related attributes at some stage, key revocation for every attribute is needed to make the system protected but such an issue is extremely difficult, particularly in attribute-based encryption approach, as each of the attribute is shared by several users. Another challenge is attribute coordination that is provided from several authorities. When several authorities will manage attribute keys to users by means of their own master secrets, it is tough to describe access policies above attributes that are provided from several authorities. In cipher text basis encryption approach, key authority will produce private keys of users by means of application of master keys to user connected attributes. Consequently, key authority will decrypt cipher-text that is addressed to particular users by means of generation of their attribute keys. Application of cipher text basis system in decentralized networks will bring in several challenges regarding attribute revocation that is provided from various authorities [2][3]. Key authorities will comprise central authority along with multiple local authorities and provide access rights to users based on attributes. The problem of key escrow is intrinsic still in multiple systems as long as key authority contain complete opportunity to make own attribute keys by own master keys. For the most part of asymmetric encryption system, such method of key generation is the basic approach, removal of escrow in particular or else numerous authority systems is a fundamental trouble. In our work we present the approach of an effective data retrieval based on the attribute for the disruption tolerant networks of decentralized type.

2. METHODOLOGY:

Attribute-based encryption is of key-policy based and cipher text-policy based. In key policy based encryption type, encryptor obtains to label a cipher-text by set of attributes. In cipher text based encryption type, cipher-text is encrypted by access policy selected by encryptor, but key is created regarding an attributes set simply. Attribute-based encryption will make available an approach that facilitates access control above encrypted data by means of access policies between private keys as well

as cipher texts. Cipher text-based system will provide an effective way of data encryption so that encryptor identify attribute set that decryptor needs to have. Hence various users have permission to decrypt data per security policy. Established attribute based encryption are build on designs where particular trusted authority will produce complete private keys of users by its master information. Application of these methods to disruption tolerant networks will introduce many of the security demands. Key escrow is intrinsic still in multiple systems as long as key authority contain complete opportunity to make own attribute keys by own master keys. Huang et al. as well as Roy et al have introduced decentralized schemes of cipher-text based in multiple authority environments. They have made collective access policy on the attributes that are provided by encryption of data several times. However the disadvantage of this method is efficiency of access policy. We present the approach of an effective data retrieval based on the attribute for the disruption tolerant networks of decentralized type in which several key authorities will control their attributes separately. The system of effective data retrieval based on the attribute will provide several achievements such as: Firstly, instant attribute revocation will improve enhances data privacy by means of dropping the windows of susceptibility [4]. Key escrow difficulty is solved by means of key issuing approach that makes use of feature of decentralized disruption tolerant networks design. The key issuing approach will produce and issue secret keys of user by implementing a two-party computation procedure among key authorities. Confidentiality of data is cryptographically made compulsory against curious key authorities in projected system. Encryptors will describe access policy by means of any monotone access construction in attributes that are provided from selected authorities.

3. AN OVERVIEW OF EFFECTIVE PROVESS OF DATA RETRIEVAL:

Various applications of military services will need protection of data privacy including methods of access control that are implemented cryptographically. Cipher text based encryption process is capable cryptographic solution towards access control issues. In this encryption type, cipher-text is encrypted by access policy selected by encryptor, but key is created regarding an attributes set. Problem of

application of cipher text basis system in decentralized disruption tolerant networks will bring in several challenges regarding attribute revocation, and attribute coordination that is provided from various authorities. In cipher text basis approach, key authority will produce private keys of users by means of application of master keys to user connected attributes hence key authority will decrypt cipher-text that is addressed to particular users by means of generation of their attribute keys. We present approach of an effective data retrieval based on the attribute for the disruption tolerant networks of decentralized type. In the structural design of proposed system as shown in fig1 there are various entities such as: Key Authorities are the centers of key generation that make parameters for cipher text system. Key authorities will include central authority along with multiple local authorities and provide access rights to users based on attributes. User is mobile node who access data stored at storage node. Storage node is an entity that store up information and offer access to users. Sender is an entity who posses confidential data and store them to external data storage for sharing to users in extreme situations. While key authorities are semi -trustable, they have to be put off from accessing data plaintext in storage node [5]. Problem of key escrow is basic in multiple systems as long as key authority contain complete opportunity to make own attribute keys by own master keys. Removal of escrow in particular or else numerous authority systems is a fundamental trouble and it is solved by means of key issuing approach that makes use of feature of decentralized disruption tolerant networks design. The key issuing approach will produce and issue secret keys of user by implementing a two-party computation procedure among key authorities. Central authority as well as local authorities will engage in two-party computation by master secret keys of their personal and provide autonomous key components towards users throughout phase of key issuing [6]. Two-party computation will put off them from recognizing others master secrets in order that no one of them will produce complete set of secret keys independently.

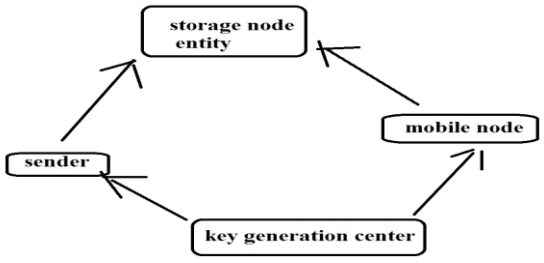

Fig1: an overview of effective data retrieval.

4. CONCLUSION:

Applying the technique of attribute-based encryption to disruption tolerant networks will introduce many of the security demands. Here we present the approach of an effective data retrieval based on the attribute for the disruption tolerant networks of decentralized type. The effective data retrieval based on the attribute will offer quite a lot of achievements. Instant attribute revocation will improve enhances data privacy by means of dropping the windows of susceptibility. Data privacy is cryptographically made compulsory against curious key authorities in projected system. Encryptors will describe access policy by means of any monotone access construction in attributes that are provided from selected authorities. Problem of key escrow is intrinsic still in multiple systems as long as key authority contain complete opportunity to make own attribute keys by own master keys. The problem is solved by means of key issuing approach that makes use of feature of decentralized disruption tolerant networks design. The key issuing mechanism will produce and issue secret keys of user by implementing a two-party computation procedure among key authorities.

REFERENCES

[1] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

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

[3] 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.

[4] 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.

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

[6] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.

Guntur Purna Tejeswi Kavya received the B.Tech degree Computer Science &Engineering in Malineni Lakshmaiah Women's engineering college, JNTUK,AP India in 2013.Currently doing M.Tech in Computer Science &Engineering in Malineni Lakshmaiah Women's engineering college, Guntur , India. Her research interests include Computer Networks, Network Security.

Mr.K.Praveen Kumar Assistant Professor, Department of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur, AP. He

received B.Tech degree in Information Technology from R.V.R&J.C College of Engineering, ANU, AP, India in 2007 and M.Tech in Computer Science &Engineering from R.V.R&J.C College of Engineering ANU, AP India in 2010. And now at present, he is pursuing PhD at JNTUK. His area of research is Network Security and Cryptography and having teaching experience of 5 years. His interested subjects are Network Security &cryptography, Artificial Intelligence, Neural Networks, Compiler Design. Data Structures and Algorithm Analysis, Formal Languages and Automata Theory.