IJRRECS/June 2015/Volume-3/Issue-6/4235-4239 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPROVISATION OF PRIVACY CONCERNS IN ATTRIBUTE BASIS SYSTEMS

Mustabad Kalyani[1], K.Shirisha[2], Dr.K.Srujan Raju[3]

[1]M.Tech Student, Dept of CSE, CMR Technical Campus, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, CMR Technical Campus, Hyderabad, T.S, India

[3]Professor & HOD, Dept of CSE, CMR Technical Campus, Hyderabad, T.S, India

ABSTRACT:

Ciphertext-policy attribute-based encryption is more appropriate to disruption- tolerant network since it enables encryptors to select an access policy above attributes and in the direction of encrypting private data in access structure by means of encrypting with equivalent attributes. In ciphertext-policy ABE, the cipher text is encrypted by an access policy preferred by an encryptor, however a key is merely created regarding an attributes set. In our work, we recommend a secure scheme of attribute-based data retrieval system by means of ciphertext-policy attribute-based encryption for decentralized disruption- tolerant network where numerous key authorities handle their attributes autonomously**.** In the introduced scheme immediate attribute revocation improves backward/forward confidentiality of private data by dropping windows of vulnerability. The data confidentiality as well as confidentiality can be cryptographically implemented against any curious key authorities in the projected system. Problem of Key escrow is worked out by escrow-free key issuing practice that utilizes characteristic of decentralized disruption- tolerant network construction.

Keywords: Attribute-based encryption, Disruption- tolerant network, Key escrow, Attribute revocation, Key authority.

1. INTRODUCTION:

Attribute-based encryption is considered as a promising approach that provides secure data retrieval in Disruption- tolerant network which are the efficient solutions allows nodes to communicate with each other in intense environments of networking. Problem of applying attribute-based encryption to disruption- tolerant network introduces quite a lot of security challenges [1]. Attribute-based encryption (ABE) features a strategy that facilitates an access control above encrypted data by means of access policies between private keys as well as cipher-texts. For the most part of existing attribute-based encryption schemes are constructed on design where a distinct trusted authority contain the power to make complete private keys of users by its master secret information consequently, key escrow difficulty is intrinsic such that key authority can decrypt each ciphertext tackled to users within system by producing secret keys. In our work, we recommend a secure scheme of attribute-based data retrieval system by means of ciphertext-policy attribute-based encryption for decentralized disruption-tolerant network. In the introduced scheme immediate attribute revocation improves backward/forward confidentiality of private data by dropping windows of vulnerability [2][3]. The data confidentiality as well as confidentiality can be cryptographically implemented against any curious key authorities in the projected system. Ciphertext-policy ABE makes available an efficient means of encrypting data in order that encryptor defines attribute set that decryptor desires to possess to decrypt ciphertext consequently, several users are approved to decrypt several pieces of data for each security policy.

2. METHODOLOGY OF PROPOSED SCHEME:

Attribute-based encryption exists in two various types such as key-policy ABE as well as ciphertext-policy ABE. In ciphertext-policy ABE, the cipher text is encrypted by an access policy preferred by an encryptor, however a key is merely created regarding an attributes set. Ciphertext-policy ABE is more suitable to disruption- tolerant network since it enables encryptors to select an access policy above attributes and in the direction of encrypting private data in access structure by means of encrypting with equivalent attributes. In our work, we recommend a secure scheme of attribute-based data retrieval system by

means of ciphertext-policy attribute-based encryption for decentralized disruption-tolerant network where numerous key authorities handle their attributes autonomously. Every local authority provides partial components of personalized as well as attribute key towards a user by means of performing efficient protocol of two-party computation with the central authority. Every attribute key concerning a user can be modernized independently and instantaneously and hence the scalability as well as security can be improved in the projected scheme. The scheme which was projected gain the achievements such as: immediate attribute revocation improves backward/forward confidentiality of private data by dropping windows of vulnerability. Encryptors can describe a fine-grained access policy by means of any monotone access construction in attributes which are issued from any selected set of authorities. Problem of Key escrow is resolved is worked out by escrow-free key issuing practice that utilizes characteristic of decentralized disruption- tolerant network construction. Since ciphertext-policy attribute-based encryption system proposed by Bethencourt, later numerous designs of ciphertext-policy ABE schemes were projected. However the later developed schemes of ciphertext-policy ABE schemes are mainly motivated by more thorough security proof in standard representation. For the most part of schemes are unsuccessful to attain the lucidity of Bethencourt et al.'s system, which explained a resourceful system that was meaningful in that it approved an encryptor to convey an access predicate regarding any monotonic formula above attributes. The protocol of key issuing makes and issues keys of user secret by carrying out an efficient protocol of two-party computation between key authorities by their personal master secrets [4]. The efficient protocol of two-party computation deters key authorities from acquiring any master secret information of each other so that none of them could produce complete set of user keys alone. Consequently, users are not necessary to completely trust authorities to defend their shared information. The confidentiality of data can be cryptographically implemented against any curious key authorities in the projected system.

3. SECURE RETRIVAL OF DATA IN DISRUPTION- TOLERANT NETWORK:

Disruption- tolerant network structure was shown in fig1 which consists of several entities such as: Key Authorities which are considered as the centers of key generation that produce parameters of public or secret for ciphertext-policy ABE. The key authorities comprises of a central authority as well as numerous local authorities. They provide differential access rights towards individual users on the basis of users' attributes. The key authorities are supposed to be honest-but-curious. Storage node is an entity that accumulates data from sender and offer equivalent access to users and might be mobile or else static. Sender is an entity who possesses confidential data and stores them into storage node of external data for easiness of sharing to users in intense networking environments. A sender is accountable for defining access policy as well as implementing it on its personal data by encrypting data under policy earlier than storing it to storage node. User is a mobile node who desires to access data accumulated at storage node. While the key authorities are semi-trusted, they have to be deterred from accessing plaintext of data in storage node; in the meantime, they have to be still capable to issue secret keys towards users [5]. To understand this to some extent contradictory requirement, central authority as well as local authorities engage in arithmetic an efficient protocol of two-party computation with their own master secret keys and provide autonomous key components towards users at some stage in key issuing phase. The efficient protocol of two-party computation prevents them from recognizing each other's master secrets in order that none of them can make the complete set of secret keys of users independently [6].

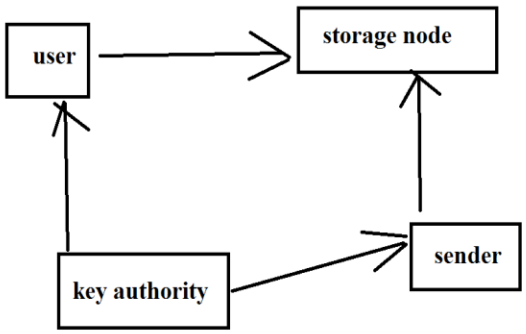

Fig1: structure of Disruption- tolerant network.

4. CONCLUSION:

Attribute-based encryption is considered as a promising approach that provides secure data retrieval in Disruption- tolerant network which are the efficient solutions allows

nodes to communicate with each other in intense environments of networking. For the most part of existing attribute-based encryption schemes are constructed on design where a distinct trusted authority contain the power to make complete private keys of users by its master secret information. In our work, we recommend a secure scheme of attribute-based data retrieval system by means of ciphertext-policy attribute-based encryption for decentralized disruption- tolerant network. Ciphertext-policy ABE is more suitable to disruption- tolerant network since it enables encryptors to select an access policy above attributes and in the direction of encrypting private data in access structure by means of encrypting with equivalent attributes. Ciphertext-policy ABE makes available an efficient means of encrypting data in order that encryptor defines attribute set that decryptor desires to possess to decrypt ciphertext consequently, several users are approved to decrypt several pieces of data for each security policy. In the introduced scheme immediate attribute revocation improves backward/forward confidentiality of private data by dropping windows of vulnerability. The efficient protocol of two-party computation deters key authorities from acquiring any master secret information of each other so that none of them could produce complete set of user keys alone.

REFERENCES

[1] 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.

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

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

[4] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in Proc. TCC, 2008, LNCS 4948, pp. 356–374.

[5] M.Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss,A.Hysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in Proc. Crypto, LNCS 5677, pp. 108–125.

[6] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Proc. CRYPTO, 2001, LNCS 2139, pp. 41–62.