IJARES/August 2015/Volume-3/Issue-8/2068-2072 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

A PIONEERING SOLUTION FOR MANAGING ISSUES OF ACCESS CONTROL

D.Anitha[1], D.Sudheer Reddy[2]

[1]M.Tech Student, Dept of CSE, Arjun College of Technology & Sciences, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Arjun College of Technology & Sciences, Hyderabad, T.S, India

ABSTRACT:

Disruption-tolerant network technology is a scalable solution in several applications. Attribute-based encryption fulfils the requirements for protected data retrieval in disruption-tolerant network. CTP ABE is a helpful cryptographic solution to access control and to the issues of secure data retrieval. The complexity of applying attribute-based encryption towards disruption-tolerant network set up quite a lot of security as well as privacy challenges. We recommend an attribute-based secure data retrieval structure by means of CTPABE for decentralized disruption-tolerant network where numerous key authorities supervise their attributes independently. Cipher text-policy ABE make available a well-organized means of encrypting data with the intention that attribute set was described that needs to possess with the purpose of decrypting cipher-text. The key escrow intricacy is resolved by means of an escrow-free key issuing procedure that exploits feature of decentralized disruption-tolerant network construction.

Keywords: Disruption-tolerant network, Key escrow, Cipher-text, Attribute-based encryption, Data retrieval, Key authority.

1. INTRODUCTION:

Numerous military applications have need of improved protection of confidential information including access control techniques that are cryptographically imposed. Attribute-based encryption (ABE) is an approach which is capable to fulfil the needs for protected data retrieval in

disruption-tolerant network [1]. Methods of disruption-tolerant network are gaining popularity which permits nodes to communicate with each other in intense networking environments. Attribute-based encryptions are of two types such as key-policy ABE and CTPABE. In CTPABE cipher-text is encrypted by means of an access policy that is selected by an encryptor, but a key is just created regarding an attributes set. In KP-ABE, encryptor only labels a cipher-text by a set of attributes. The key authority prefer a policy in support of each user that determines decryption of cipher text and offer key to each user by means of embedding policy into user's key. Roles of cipher texts and keys are inverted in cipher text-ABE. CTPABE is more suitable to disruption-tolerant network when compared to key-policy ABE since it facilitate encryptors to prefer an access policy and towards encrypting private information under access structure by means of encrypting with equivalent public keys or attributes [2][3]. In our work we offer attribute basis secure system of data retrieval by means of CTPABE for decentralized disruption-tolerant network. The projected system contains several achievements. First, instant attribute revocation improve backward/forward privacy of confidential data by means of reducing windows of vulnerability. Secondly, encryptors can identify a fine-grained access policy by means of monotone access construction under attributes that are issued from any selected set of authorities. Third, the key escrow difficulty is resolved by means of an escrow-free key issuing procedure that exploits feature of decentralized disruption-tolerant network architecture.

2. CHALLENGES FOR APPLYING ATTRIBUTE-BASED ENCRYPTION:

Attribute-based encryption features a method that facilitates an access control above encrypted data by means of access policies and recognized attributes between private keys and ciphertexts. Cipher text-policy ABE provides an efficient means of encrypting data with the intention that attribute set was described that decryptor needs to possess with the purpose of decrypting cipher-text. Different users are authorized to decrypt dissimilar pieces of data for each security policy. The difficulty of applying attribute-based encryption to disruption-tolerant network set up quite a lot of security as well as privacy challenges.

While a number of users may possibly modify their connected attributes at some point or several private keys may be compromised, key revocation for every attribute is essential to make systems safe. But this issue is even harder, particularly in Attribute-based encryption systems, as each attribute is possibly shared by various users. A different challenge is key escrow difficulty. In CTPABE key authority produce private keys of users by means of applying authority's master secret keys to user linked set of attributes consequently, key authority can decrypt each ciphertext that is addressed to specific users by means of producing their attribute keys. We offer an attribute-based secure data retrieval system by means of CTPABE for decentralized disruption-tolerant network. In the proposed system encryptors can make out a fine-grained access policy by monotone access construction under attributes that are issued from any particular set of authorities. The key escrow is an intrinsic trouble still in numerous authority systems so long as each key authority contains complete privilege to produce their individual attribute keys by means of their personal master secrets [4]. While such a key generation method on the basis of single master secret is fundamental method for most of asymmetric encryption systems for instance attribute-based or identity-based encryption procedures, removal of escrow in single or else multiple-authority CTPABE is a fundamental open problem.

3. AN OVERVIEW OF SECURE TWO-PARTY COMPUTATION:

Disruption-tolerant network technology is becoming effective solution in several applications that allows wireless devices to connect with each other and access confidential data consistently by means of using external storage nodes. CTPABE is an effective cryptographic explanation to access control and to the issues of secure data retrieval. An attribute basis system of secure data retrieval was introduced by means of CTPABE for decentralized disruption-tolerant network where numerous key authorities supervise their attributes autonomously. The inherent key escrow trouble is worked out such that privacy of stored data is assured even in hostile setting where key authorities may be compromised or not completely trustworthy. Procedure of key issuing generates and provides user secret keys by performing effective secure two-party computation protocol between key

authorities by their own master secrets. The two-party computation protocol prevents key authorities from gaining any master secret information of each other with the intention that none of them might produce total set of user keys consequently, users are not essential to completely trust authorities in order to defend their data to be shared. The data privacy can be cryptographically imposed against any interested key authorities or else data storage nodes in projected system. While key authorities are semi-trusted, they have to be deterred from accessing plaintext of data in storage node; for the time being, they have to be able to provide secret keys to users [5]. To recognize this somewhat contradictory prerequisite central authority as well as local authorities takes on in aritmetic two-party computation procedure by means of master secret keys of their own and provide independent key components towards users throughout key issuing phase. Two-party computation protocol prevents them from knowing each other's master secrets with the intention that none of them can produce complete set of secret keys of users independently. Consequently, we take a supposition that central authority does not plot with local authorities. Attribute-based encryption provides a method that facilitates an access control above encrypted data by means of access policies and recognized attributes between private keys and ciphertexts and such a multi authority CTPABE system is useful for effective data retrieval in decentralized disruption-tolerant networks. Every local authority provides partial personalized as well as attribute key components towards a user by means of performing effective two-party computation protocol with central authority. Every attribute key of a user is updated independently and instantaneously consequently; scalability in addition to security can be improved in the proposed system [6].

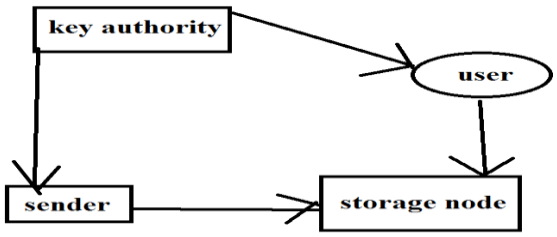

Fig1: Disruption-tolerant network structure.

4. CONCLUSION:

Techniques of disruption-tolerant network are attaining recognition which permits nodes to communicate with each other in intense networking environments. We suggest an attribute-based secure data

retrieval structure by means of CTPABE for decentralized disruption-tolerant network where numerous key authorities supervise their attributes. When compared to key-policy ABE, CTPABE is more suitable to disruption-tolerant network since it facilitates encryptors to prefer access policy and towards encryption of private information under access structure by means of encrypting with equivalent public keys or attributes. The key escrow is an fundamental problem still in numerous authority systems so long as each key authority contains complete privilege to produce their individual attribute keys by means of their personal master secrets nd it was worked out such that privacy of stored data is assured even in hostile setting where key authorities may be compromised or not completely truthful.

REFERENCES

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

[2] 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.

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

[4] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.

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

[6] 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.