ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

A Survey on Attribute Based Secure Information Retrieval in DTN

S.Kalpana[1], M.Jayalaxmi[2], M.Udhayavani[3]

PG Student [AE], Dept. of ECE, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India

PG Student [VLSI], Dept. of ECE, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India

Assistant professor, Dept. of ECE, Vivekanandha College of Engg for Women, Tiruchengode, Tamilnadu, India

ABSTRACT*:* Intermittent network connectivity and node partitions are frequently occur in military environments like battlefields and some hostile regions. Disruption-tolerant network (DTN) technologies are allows wireless devices to communicate with each other and access the confidential information in military applications by exploiting external storage nodes. The secure data retrieval scheme using Revocable Multi authority CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure text and video retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues The Multi authority CP-ABE and AES algorithm it provides secure retrieval of text and video respectively. The proposed system provides secure retrieval of text and video, using modified CP-ABE and AES algorithm for decentralized DTNs respectively. Also, demonstrating how to apply the proposed mechanism to securely and efficiently manage the confidential information distributed in the disruption-tolerant military network. It implemented using Network Simulator-2.

KEYWORDS*:* DTN, Revocable CPABE, secure text and video encryption, and Access control.

I.INTRODUCTION

In many military network scenarios, wireless devices connection carried by soldiers can be disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. 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.

The different features of DTNs are Fault-tolerant methods and technologies, Electronic attack recovery, Degradation quality from heavy traffic loads and Minimal latency due to unreliable routers.

Fig. 1 shows the architecture of the DTN. The architecture consists of the following system entities.

DOI:10.15662/IJAREEIE.2015.0411005

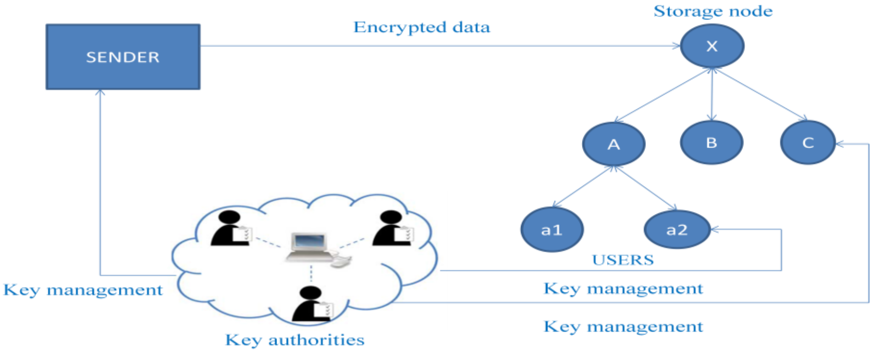

Fig. 1. Architecture of Disruption-tolerant network.

II. ATTRIBUTE BASED ENCRYPTION SCHEMES

An attribute based encryption scheme introduced by Sahai and Waters in 2005 and the goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryptions that allows users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). The ABE systems can be viewed as a generalization of Identity Based Encryption (IBE) systems. In IBE systems, only one attribute is used which is the identity of the receiver, whereas ABE systems enable the use of multiple attributes simultaneously. We have two alternatives in enforcing the access policy. The access policy can be embedded in the private key of a user, which results in a cryptosystem called Access control.

Key Policy Attribute- Based Encryption (KP-ABE). Alternatively, the access policy can be embedded in the cipher text, which results in the Cipher text Policy Attribute Based Encryption (CP-ABE) system. Both KP-ABE and CP-ABE systems ensure that a group of users cannot access any unauthorized data by colluding with each other.

A.KEY POLICY - ATTRIBUTE BASED ENCRYPTION

KP-ABE schemes are suitable for structured organizations with rules about who may read A KP-ABE scheme is parameterized by a universe of possible attributes U and consists of the following four algorithms.

Setup: this algorithm is run by the trusted attribute authority, which takes as input the security parameter λ and the attribute universe U. It outputs some public parameters *params* and the master secret key *msk.* The trusted attribute authority publishes *params* and keeps *msk* secret.

KeyGen: This algorithm run by the trusted attribute authority, which takes as input the public parameters *params*, master secret key *msk*, and an access structure A which is assigned by the trusted attribute authority to the user. It outputs a decryption key SK_A.

Encrypt: This algorithm run by the sender, which takes as input the public parameters *params*, a set of descriptive attributes W, and a message *m* € { 0,1 }*. It outputs the ciphertext *c*.

Decrypt: This algorithm run by the recipient, which takes as input the public parameters *params*, the ciphertext *c* that was encrypted under the set of attributes W , and the decryption key SK_A for access structure A . It outputs the message *m* if W € A.

B. CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION

In a ciphertext-policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the ciphertext, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority.

CP-ABE scheme consists of following four algorithms:

Setup: This algorithm takes input as security parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encryption: This algorithm takes input as public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.

Key Generation: This algorithm takes input as set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Decryption: This algorithm takes input as ciphertext CT and a secret key SK for an attributes set. It returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

Drawbacks of the most existing CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CPABE has limitations in terms of specifying policies and managing user attributes.

C. MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION

V Bozovic, D Socek, R Steinwandt, and Vil-lanyi, introduce Multi-authority attribute-based encryption. In this scheme it uses multiple parties to distribute attributes for users. A Multi Authority ABE system is composed of K attribute authorities and one central authority. Each attribute authority is also assigned a value dk.

The system uses the following algorithms:

Setup: A randomized algorithm runs by some trusted party (e.g. central authority). Takes input as security parameter. Outputs as public key, secret key pair for each of the attribute authorities, and outputs as system public key and master secret key which will be used by the central authority.

Attribute Key Generation: A randomized algorithm runs by an attribute authority. Takes input as authority’s secret key, the authority’s value dk, a user’s GID, and a set of attributes in the authority’s domain AKC. (We will assume that the user’s claim of these attributes has been verified before this algorithm is run). Output as secret key for the user.

Central Key Generation: A randomized algorithm runs by a central authority. Takes input as master secret key and a user’s GID and output as secret key for the user.

Encryption: A randomized algorithm runs by a sender. Takes as input a set of attributes for each authority, a message, and the system public key. Output as ciphertext.

Decryption: A deterministic algorithm runs by a user. Takes input as cipher-text, which was encrypted under attribute set AC and decryption keys for an attribute set Au. Output as message m.

It allows any polynomial number of independent authorities to monitor attributes and distribute private keys and tolerate any number of corrupted authorities.

D. DISTRIBUTED ATTRIBUTE-BASED ENCRYPTION

The system is built up of a Central Authority (CA) and multiple Attribute Authorities (AAs).These attribute authorities separately maintain attributes. The major components of the scheme are master, users and attribute authorities. The duty of the master is to distribute private user keys. Attribute Authority certifies the user and distributes private attribute key to the user that can be used for decrypting ciphertext. User produces ciphertext by the method of encryption. Whenever needed user decrypts the ciphertext and retrieves the original message.

The following algorithms are defined in a DABE scheme.

Setup: This algorithm generates the public key PK and the master key MK.

CreateUser: The outputs of this algorithm are a public user key PK_u and a secret user key SK_u.

Create_Authority: This algorithm generates a private authority key SK_a.

Request_Attribute PK: This algorithm generates the public attribute key of attribute A.

Request_Attribute SK: This algorithm generates a secret attribute key $SK_{A,u}$ for user u.

Encrypt: The inputs of this algorithm are public key, message, an access policy and the public keys associated with the attributes in the access policy. The output of this algorithm is the ciphertext.

Decrypt: The inputs of the algorithm are the ciphertext produced by the Encrypt algorithm, an access policy and a key ring. Decryption is performed based on certain conditions and if the conditions are satisfied, the algorithm will output the plaintext.

E. CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION WITH REVOCATION.

Another modified form of CPABE called CPABE-R introduced by Xiaohui Liang and Rongxing Lu. In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user’s private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user’s private key satisfies the access policy associated with the ciphertext. In a CPABE-R scheme, malicious users can be efficiently revoked.

CPABE-R scheme consists of following five algorithms:

Setup: This algorithm takes input as security parameter and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encryption: This algorithm takes input as public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.

Key Generation: This algorithm takes input as set of attributes associated with the user, unique identifier and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Key Update: This algorithm takes input as revocation list, a time stamp t, and master key MK. Output as Update Information UI.

Encryption: This algorithm takes input as public parameter PK, a message M, access structure T and a time stamp t. It outputs the ciphertext CT.

Decryption: This algorithm takes input as ciphertext CT, a secret key SK for an attributes set and update information UI. It returns the message M if and only if satisfies two conditions. First, attribute set related with secret key satisfies access structure and second, unique identifier associated with secret key has not been revoked in update information.

TABLE I: COMPARISON OF ABE SCHEMES

Techniques/Parameter	ABE	KP-ABE	CP-ABE	MA-ABE	RMA-ABE
Fine grained Access Control	Low	Low, High re-encryption technique	Average Realization of Complex Access Control	Better Access Control	Good Access control
Efficiency	Average	Average, High for broadcast type system	Average, Not efficient for modern environments	Scalable	Flexible
Computational Overhead	High	Most of Computational overheads	Average Computational overheads	Average	Some overhead
Collusion resistant	Average	Good	Good	High collusion resistant	Good

III.PROPOSED WORK

Issues such as scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. For improving the limitations of the above technique. We propose a new scheme called Revocable Multiauthority ciphertext policy attribute based encryption. Revocable Multiauthority ciphertext policy attribute based encryption scheme and AES scheme describes text and video retrieval with efficient revocation. This mechanism to securely and efficiently manage the confidential information distributed in the disruption-tolerant military network.

IV.CONCLUSION

In this paper, we analyze different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, MA-ABE, CPABE with efficient revocation. The main access polices are KP-ABE and CP-ABE, further schemes are obtained based on these policies. Based on their type of access structure the schemes are categorized as either monotonic or non-monotonic. Revocable Multiauthority CPABE is an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance the sensitive data, and moreover towards the anonymity of the data owner. Our scheme also enables dynamic modification of access policies to supports efficient on-demand user/attribute revocation access under emergency scenarios.

REFERNECES

1. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks IEEE transactions on networking vol:22 no:1 year 2014

2. Changji Wang and Jianfa Luo,‖ An Efficient Key-Policy Attribute- Based Encryption Scheme with Constant Ciphertext Length‖, Received 21 January 2013; Accepted 16 March 2013.

3. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2011.

4. Lewko, A., Waters, B.: ―Decentralizing Attribute-Based Encryption‖, In: CRYPTOLOGY ePrint Archive, Report 2010/351,2010.

5. M. Chase and S. S. M. Chow, "Improving privacy and security inmultiauthority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

6. S. S.M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.

7. J. Bethencourt and others. Ciphertext-policy attributebased encryption. In Proceedings of IEEE SP, Oakland, 2007.

8. Dr. M.Newlin Rajkumar, Ancy George, Brighty Batley C, An Overview of Multi-Authority Attribute Based Encryption Techniques‖2007.

9. M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534.