ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Analysis on Attribute Based Encryption for Secure Data Retrieval in DTNS

Jothipriya. C [1], Rizvana. M[2] Prof Srinivasan. R[3]

M.Tech (IT) Student, Department of IT, PSV College of Engg & Tech, Krishnagiri, TN.India1

Assistant Professor, Department of IT, PSV College of Engg & Tech, Krishnagiri, TN,India2

Head of Department , Department of IT, PSV College of Engg & Tech, Krishnagiri, TN, India3

ABSTRACT: Secure data retrieval plays vital role in all communication environments. To communicate between nodes in the network data should transfer and any one can retrieve it securely. Disruption- tolerant network (DTN) technologies are considered to be the successful solutions, allow nodes to communicate with each other in the extreme networking environments. It implements store and forward scheme by using external storage nodes. Since the data is sensitive that one needs to consider the security policies of cryptographic solution like data encryption techniques. Here we talk over several encryption techniques for access control and secure data retrieval in DTNs environments.

KEYWORDS: Disruption Tolerant Networking (DTN), Node Location, Access Control, Attribute Based Encryption (ABE) Secure Data Retrieval, Encryption, Security.

I. INTRODUCTION

Now days many computing devices e.g. PDAs, smart-phones, sensors have wireless interfaces and hence can form ad hoc networks. Wireless ad-hoc networks allow nodes to communicate with one another without relying on any fixed infrastructure. These rapidly deployable networks are very useful in several scenarios e.g. Military network environments, connections of wireless devices carried by soldiers may be temporarily disconnected by environmental factors, jamming and mobility, especially when they operate in terrestrial environments. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme terrestrial 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. For storage and replicate the data storage node is introduced where authorized mobile nodes can access the necessary information quickly. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced. In many cases, it is desirable to provide differentiated access services.

In a network communication between two hosts should be encrypted to enhance security. There are different types of encryption algorithms used for transferring the data securely.

II. ENCRYPTION TECHNIQUES

Encryption is that the method of coding messages in a way that solely licensed parties will read it. Encoding denies the message content to the fighter. The original messages are considered as a plaintext. The plaintexts are encrypted to a cipher text. The encryption is done by encryption algorithm. The cipher text is decrypted to get the plaintext. The encryption algorithm generates key for encrypting the plaintext. The receiver who has the key is called authorized one, so they can able to decrypt the cipher text. Unauthorized person who does not have the key cannot able to decrypt the text. Encryption is used for data protecting while transferring.

2.1 Encryption Types

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

2.1.1 Symmetric Key Encryption

For both encryption and decryption same keys are used in symmetric key encryption. It is secure if both keys are the same. The message can be decrypted if the unauthorized person knows the key. The problem here is management of keys, transforming the keys securely not the messages. Keys are generated before the message because it is smaller than the messages. Private key encryption is shown in Fig 1.

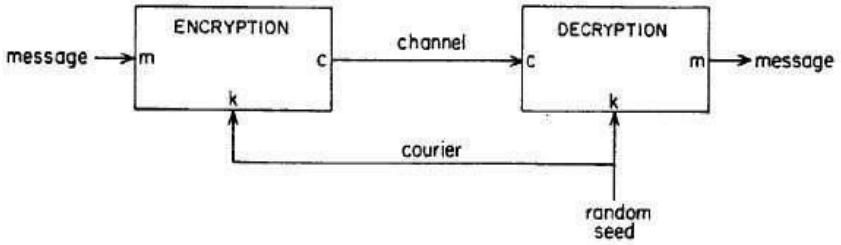

Figure 1 Symmetric Key Encryption

2.1.2 Asymmetric Key Encryption

For both encryption and decryption different keys are used. Hence the key management problem is overcome. Both the keys are sufficient for encrypting and decrypting the message. A pair of key is used; one key for encrypting and other is for decrypting the message. Private/Public key is used encrypting/decrypting message and shown in Fig. 2.

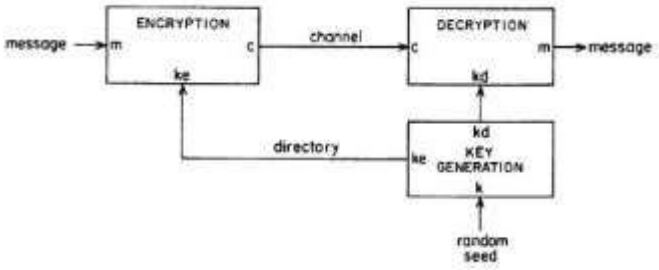

Figure 2 : Asymmetric Key Encryption

III. ASYMMETRIC KEY ENCRYPTION

It is also known as public key encryption algorithm. The use of public key cryptography is public key encryption. Based on the public key encryption there are many algorithms for transferring the message securely. The security in public key encryption is confidentiality, the sender encrypts the message using receiver public key and it is decrypted only by the receiver paired private key.

3.1 Identity Based Encryption Algorithm

Shamir [13] and Boneh et al. [11] introduces Identity-Based Encryption (IBE) with an efficient determinable bilinear map. Halevi et al. [12] put forward IBE in a random oracle representation. The efficiency is increased by the two schemes in outside random oracles that were proposed by Boyen et al. [10]. Sahai et al. [4] introduces different type of Identity-Based Encryption (IBE) called Fuzzy Identity-Based Encryption. A set of descriptive attributes is viewed as an identity in Fuzzy IBE. It is used for application like Biometric identities in IBE and attribute-based encryption. They proposed error tolerance between the identities of keys that are used for encryption. In Fuzzy-IBE there are few problems. If attributes come from multiple authorities, the Fuzzy- IBE is possible or not.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

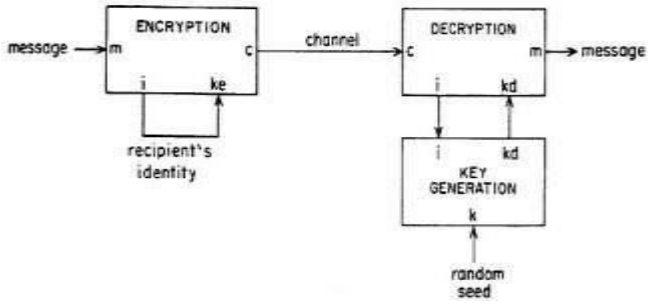

Figure 3 Identity Based Encryption

Identity-based encryption was to simplify certificate management in e-mail systems. When Alice sends mail to Bob at bob@company.com she simply encrypts her message using the public key string "bob@company.com". There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted mail he contacts a third party, which we call the Private Key Generator (PKG). Bob authenticates himself to the PKG in the same way he would authenticate himself to a CA and obtains his private key from the PKG. Bob can then read his e-mail. Note that unlike the existing secure e-mail infrastructure, Alice can send encrypted mail to Bob even if Bob has not yet setup his public key certificate. Also note that key escrow is inherent in identity-based e- mail systems: the PKG knows Bob's private key.

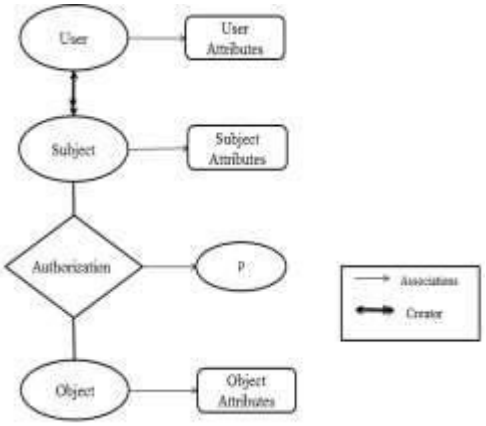

Figure 4 Overview of ABE based access control model

3.2Attribute-Based Encryption

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP- ABE) or policies defined over a set of attributes (cipherext-policy ABE - CP-ABE). The key issue is that someone should only be able to decrypt a ciphertext if the person holds.

proposed Attribute-Based Encryption (ABE) in Fuzzy IBE. The secret key is based on a set of attributes. While decryption the set of attributes must match cipher text attributes. ABE has two types: Key- Policy ABE (KP-ABE), Cipher text-Policy ABE (CP-ABE). In Key-Policy ABE [5], the cipher text is encrypted with the attribute set. For decrypting, the policy is chosen by the key authorities. **Fig -3**: represents the schematic representation of Attribute-Based Encryption [14]. Based on the attributes the signature of information takes place. 3.2.1 Mediated Cipher Text-Policy Attribute-Based Encryption Ibraimi et al. [2] proposed mediated Cipher

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

text-Policy Attribute-Based Encryption (mCP-ABE) based on mediated cryptography. It is an extension of CP-ABE with rapid attribute revocation. The cipher text is decrypted by the user only if the access policy is satisfied by the attribute set of schemes in outside random oracles that were proposed by Boyen et al. [10]. Sahai et al. [4] introduces different type of Identity-Based Encryption (IBE) called Fuzzy Identity-Based Encryption. A set of descriptive attributes is viewed as an identity in Fuzzy IBE. It is used for application like Biometric identities in IBE and attribute-based encryption. They proposed error tolerance between the identities of keys that are used for encryption. In Fuzzy-IBE there are few problems. If attributes come from multiple authorities, the Fuzzy-IBE is possible or not.

3.2.2 Multi Authority Attribute-Based Ecryption

Chase [9] proposed Multi authority Attribute-Based Encryption in a fine grained access control ABE. They proposed schemes that permit polynomial number of individual authorities and accepts the random number of dishonest authorities. Later Lewko et al. [3] present this algorithm in new version. The authority can be anyone and it doesn't require any coordination between authorities. It doesn't need a central authority. The algorithm is scalable by preventing the occurrence incurred by depending on central authority. In addition to scalable, efficiency and security is also enhanced.

3.2.3 Attribute-Based Encryption with Non-Monotonic Access Structures

Attribute-Based Encryption with Non-Monotonic Access Structures was introduced by Waters et al. [7]. In an attribute the private key of users can be articulated by any access rule. Earlier ABE algorithms uses only monotonic access structure, this limitation is overcome by this algorithm. While conserving collusion resistance structure they encounter challenges because of the negation method.

3.2.4 Bounded Cipher Text-Policy Attribute Based Encryption

Goyal et al. [8] proposed Bounded Cipher text-Policy Attribute Based Encryption, having a security proof based on a number theoretic assumption. It encourages the access policy signified by bounded size access construction along with the nodes having threshold gates. With certain variations it supports non-monotone access structure.

3.2.5 Cipher Text-Policy Attribute Based Encryption

Cipher text-Policy Attribute Based Encryption (CP-ABE) was introduced by Bethencourt et al. [6] .CP-ABE is encrypted data for complex access control in a system. The set of attributes provide the private key for users. The policies are specified by the party who is encrypting data over the attributes that specifies which user can able to decrypt. This algorithm keeps the encrypted data as confidential and secure opposed to collusion resistance. This algorithm allows any monotone access structure, single authority and periodic attribute revocation. Key escrow is not addressed. To overcome the limitations of previous CP-ABE are overcome and it is intended by Hur et al. [1].The attribute revocation, key escrow and attributes coordination that are issued by different authorities are solved using this algorithm. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed where key authorities may be compromised. For each attribute group the fine-grained key revocation should be done. The components of a partial personalized and attribute key to a user issued by the local authority, by performing secure 2PC protocol with the central authority. The user attribute key can be updated individually and immediately. Thus, the scalability and security can be enhanced.

3.2.6 Trust based Cipher Text-Policy Attribute Based Encryption

Secure data retrieval scheme is needed for using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. But the main drawback is that the updating of attributes is not so efficient and high complexity. In order to overcome the above cited problems here proposing a new technique Trust based CP-ABE [15], for reducing complexity and also to improve the security in DTN. Here data encryption and decryption implemented by elliptical curve digital signature algorithm and for key generation we used Diffie–Hellman key generation method. In addition to that the geographical routing is also used for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

finding the location of the nodes. In this method, each node analyzes other neighbour nodes, which are located in the same subtask group. The trust based CP-ABE is shown in Fig. 5.

Trust Calculation: Trust value calculated to make more secure and to improve performance. The flow control of trust value calculation is shown in Fig. 6.

Node location tracking: This location of node also traced to reduce overhead and increase performance. The position of the node can be tracked by using geographical routing protocols .according to previous activity and velocity. It will reduce complexity of communication.

$$A = \sum_{i=1} T_y(i)$$

Where:
$T_y(i)$ – trust value of the ith trust categor
n – number of trust categories.

$$B = \frac{\sum_{j=1}^{n} T_j(x)}{n}$$

Where:
$T_j(x)$ – trust value of node J on Node X.
n – number of the surrounding nodes.

$$D = \sum_{k=1}^{n} T_k(x)$$

Where:
$T_k(x)$ - the risk value of k^{th} trust categor
n – number of trust categories.

$$C = f_1(A,B)$$

$$E = f_2(C,D) = f_2(f_1(A,B),D)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

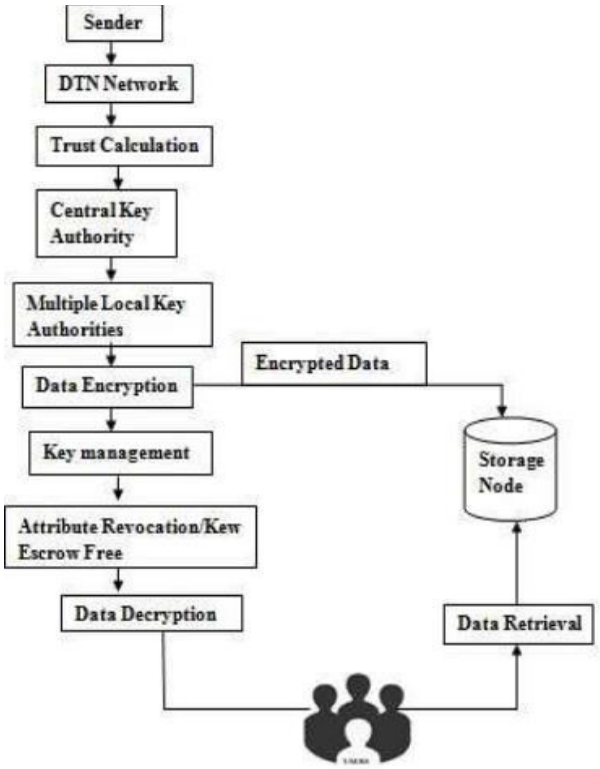

Figure 5 Trust based CP-ABE

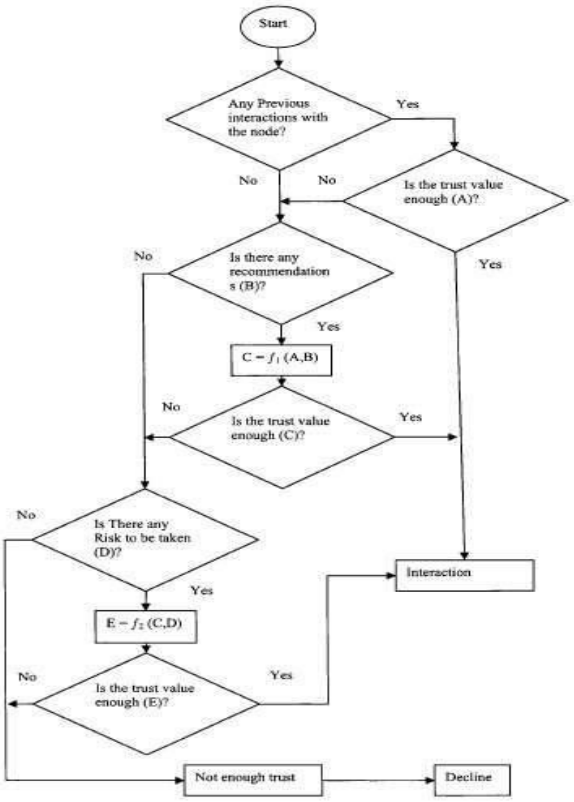

Figure 6 Algorithm for Trust calculation

IV. CONCLUSION

In this paper we survey about data encryption in network security and various encryption algorithms used in cryptography to improve the data secrecy. In attribute based encryption gives more challenging solution to cryptography .CP-ABE provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decrypt or needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy in public key encryption there is no necessary for sharing the keys. Diffie–Hellman key exchange method is used in many of these encryption algorithms. This key exchange makes it desirable to securely transfer the data more protectable over an unsafe network. Diffie - Hellman key exchange method is a way in which people may generate combined confidential information that cannot be estimated by snoopier. Finally in the trust based CP-ABE the trust value calculated to make more secure and reduce communication cost apart from this location of node also traced to reduce overhead and increase performance.

REFERENCES

1. J. Hur and K. Kang,"Secure data retrieval for decentralized disruption-tolerant military networks", in Proc.IEEE/ACM Transactions on Networking, 2014.
2. 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.
3. Lewko and B. Waters, "Decentralizing attribute-based encryption, "Cryptology ePrint Archive: Rep. 2010/351, 2010.
4. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.Eurocrypt, 2005, pp. 457–473.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

5. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access controlof encrypted data," in Proc.ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

6. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321–334.

7. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.

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

9. M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp. 515–534. [10]. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT '04),Lecture Notes in Computer Science. Springer Verlag, 2004.

10. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

11. Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.

12. Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

13. B. Balamurugan and P. Venkata Krishna, "Extensive Survey on Usage of Attribute Based Encryption in Cloud", in Proceedings of Journal Of Emerging Technologies In Web Intelligence, VOL. 6, NO. 3, 2014, pp.263-272

14. S.Revathi and A.P.V.Raghavendra, "Advanced Data Access Scheme in Disruption Tolerant Network", in International Journal of Innovative Research in Computer and Communication Engineering. Vol. 2, Issue 10, October 2014, pp.6207-6212.