International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey Paper on Attribute Based Encryption in Disruption Tolerant Network

Vishwajeet Mete[1], Deepali Gothawal[2]

[1]Master of Computer Engineering, D. Y. Patil College of Engineering, Akrudi, Pune, India

[2]Department of Computer Engineering, D. Y. Patil College of Engineering, Akrudi, Pune, India

Abstract: ***Mobile nodes connecting one node to another node faces some networking connectivity problem in common environment. In military network i.e in battle field are not supposed to suffer network connectivity problem. Disruption tolerant network (DTN) technologies are the solution for this problem. Attribute based encryption (ABE) gives the secure way for data delivery in Disruption Tolerant Network. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). The Cipher text-policy Attribute Based Encryption for secure data retrieval in decentralized Disruption Tolerant Networks (DTNs) where multiple key authorities manage their attributes independently. It gives an appropriate way of encryption of data, the encryption includes the attribute set that the decryption needs to possess in order to decrypt the cipher text. Hence, many users can be allowed to decrypt different parts of data according to the security policy. But concept of applying CP-ABE in DTNs introduces security and privacy problems with regard to Attribute revocation, Key escrow, Coordination of attributes issued from different authorities.***

Keywords: Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multi authority, secure data retrieval

1. Introduction

There are partitions in military environments such as a battlefield or a hostile region. They are suffering from intermittent network connectivity. They are having frequent partitions. Disruption-tolerant network DTN technologies are a true and easy solutions. DTN is a Disruption-tolerant network. It allows devices which are wireless and carried by peoples in a military to interact with each other. In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily 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 [1]–[3]. Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications. 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.

However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, he refer to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately. Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. Attribute-Based Encryption. Sahai and Waters in their seminar paper [1] introduced the concept of Attribute-Based Encryption (ABE). There are two types of ABE schemes: Key-Policy ABE schemes (KP-ABE) [10] and Cipher-text Policy ABE schemes (CP-ABE) [2, 3]. In KP-ABE, a cipher-text is associated with a set of attributes and a user secret key is associated with an access structure. A secret key holder can decrypt the cipher-text if the attributes associated with the cipher-text satisfy the access structure associated with the secret key. A related work to KP-ABE is a technique of searching on encrypted data [11][12]. In CP-ABE the idea is reversed. A cipher-text is associated with the access structure and the user secret key is associated with a set of attributes. A secret key holder can decrypt the cipher-text if the attributes associated with the secret key satisfy the access structure associated with the cipher text.

2. Related Work

2.1 Maxprop: Routing For Vehicle-Based Disruption-Tolerant Networks

Disruption-tolerant networks (DTNs) attempt to route network messages via intermittently connected nodes. Routing in such environments is difficult because peers have little information about the state of the partitioned network and transfer opportunities between peers are of limited duration. In this paper, MaxProp, a protocol used for effective routing of DTN messages. MaxProp is based on prioritizing both the schedule of packets transmitted to other peers and the schedule of packets to be dropped. These priorities are based on the path likelihoods to peers according to historical data and also on several complementary mechanisms, including acknowledgments, a head-start for new packets, and lists of previous intermediaries.

2.2 Secure Data Retrieval Based On Ciphertext Policy Attribute-Based Encryption (CP-ABE) System For The DTNs

Mobile Nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery scenarios. Disruption Tolerant Network (DTN) technologies are designed to enable nodes in such environments to communicate with one another. Several application scenarios require a security design that provides fine grain access control to contents stored in storage nodes within a DTN or to contents of the messages routed through the network. In this paper, an access control scheme which is based on the Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach is proposed. This scheme provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users. Two unique features of the scheme provide are: (i) the incorporation of dynamic attributes whose value may change over time, and (ii) the revocation feature.

2.3 Secure Data Retrieval Based On Ciphertext Policy Attribute-Based Encryption (CP-ABE) System For The DTNs

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the ciphertext is associated with an access policy over attributes. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the access policy specified in the ciphertext. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed. In this paper, we propose a mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation. This is a challenge because the primary purpose of networked storage is to enable easy sharing of data, which is often at odds with data security.

2.4 Attribute-Based Encryption For Fine-Grained Access Control Of Encrypted Data

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). He develop a new cryptosystem for fine-grained sharing of encrypted data that they call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, ciphertexts are labelled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. He demonstrates the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control.

2.5 Decentralizing Attribute-Based Encryption

In Multi-Authority Attribute-Based Encryption (ABE) system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. This system does not require any central authority. In constructing this system, the largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in this system each component will come from a potentially different authority, where assumed as no coordination between such authorities. New techniques are created to tie key components together and prevent collusion attacks between users with different global identifiers. System security can be improved using the recent dual system encryption methodology where the security proof works by first converting the challenge ciphertext and private keys to a semi-functional form and then arguing security.

2.6 Multi-Authority Attribute Based Encryption

In an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext. Sahai and Waters introduced a single authority attribute encryption scheme and left open the question of whether a scheme could be constructed in which

multiple authorities were allowed to distribute attributes [SW05]. He answer this question in the affirmative. Our scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. It can tolerate an arbitrary number of corrupt authorities. Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. The mechanisms in Plutus reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. As storage systems and individual storage devices themselves become networked, they must defend both against the usual attacks on messages traversing an untrusted, potentially public, network as well as attacks on the stored data itself. This is a challenge because the primary purpose of networked storage is to enable easy sharing of data, which is often at odds with data security. To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers. Thinking of a stored data item as simply a message with a very long network latency is a misleading analogy.

Table 2.1: Comparison based on Parameter

Parameter	Maxprop: protocol	CPABE	KPABE	Multi Authority ABE
Intermittent node	Yes	Yes	No	Yes
Cipher test	Encrypted with keys	labeled with access structure	labeled with keys	labeled with attribute
Multiple key Authority	No	Yes	Yes	Yes
Central key Authority	No	Yes	Yes	No
Data confidentiality	Yes	Yes	No	No

3. Discussions

The concept of attribute-based encryption (ABE) is a promising approach that fulfils the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

3.1 Disadvantages

- The process of applying ABE technique involves several security and privacy challenges. In order to make the system secure key revocation is done in the system.
- However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, he refer to such a collection of users as an attribute group)
- Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes.
- The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities.

3.2 CP-ABE (Ciphertext Policy Attribute-Based Encryption)

Multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bethencourt et al. [13], dozens of CP-ABE schemes have been proposed. The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model [17]. A cipher text policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Key Generation, Encryption and Decryption.

- **Setup:** The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.
- **Key Generation (MK, S) :** The key generation algorithm takes as input the master key MK and a set of attributes So that describe the key. It outputs a private key SK.
- **Encrypt (PK, A, M) :** The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. Assume that the ciphertext implicitly contains A.

- **Decrypt (PK,CT,SK) :** The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

3.3 Advantages of CP-ABE

- **Data confidentiality:** Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.
- **Collusion-resistance:** If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.
- **Backward and forward Secrecy:** In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

4. Conclusion

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. In CP-ABE, A ciphertext is associated with the access structure and the user secret key is associated with a set of attributes.

References

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in Proc. IEEE INFOCOM, 2006.
[2] M. Chuah and P. Yang, Node density-based adaptive routing scheme for disruption tolerant networks, in Proc. IEEE MILCOM, 2006
[3] S. Roy andM. Chuah, Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs, LehighCSE Tech. Rep., 2009.
[4] M. Chuah and P. Yang, Performance evaluation of content-based information retrieval schemes for DTNs, in Proc. IEEE MILCOM, 2007.
[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,Plutus: Scalable secure file sharing on untrusted storage, in Proc.Conf. File Storage Technol., 2003
[6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, Mediated ciphertext-policy attribute-based encryption and its application,in Proc. WISA, 2009.
[7] D. Huang and M. Verma, ASPE: Attribute-based secure policy enforcementin vehicular ad hoc networks, Ad Hoc Netw 2009.
[8] A. Lewko and B. Waters, Decentralizing attribute-based encryption, Cryptology ePrint Archive: Rep. 2010/351, 2010.
[9] 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.
[10] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attributebased encryption, in Proc. IEEE Symp. Security Privacy, 2007.
[11] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in Proc. ACM Conf. Comput. Commun. Security, 2007.
[12] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, Secure attribute based systems, in Proc. ACMConf. Comput. Commun. Security, 2006.
[13] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, A content-driven access control system, in Proc. Symp. Identity Trust Internet, 2008.
[14] L. Cheung and C. Newport, Provably secure ciphertext policy ABE, in Proc. ACM Conf. Comput. Commun. Security, 2007.
[15] M. Chase, Multi-authority attribute based encryption, in Proc. TCC,2007.
[16] S. S.M. Chow, Removing escrow from identity-based encryption, in Proc. PKC, 2009.
[17] Junbeom Hur and Kyungtae Kang Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks IEEE 2014.

Author Profile

Vishwajeet I Mete pursuing Master's in Computer Engineering from D.Y Patil College of Engineering. His area of interest is Networking and Information Security.

Ms. Deepali Gothawal completed her Master's in Computer Engineering from D.Y Patil College of Engineering and have UG and PG teaching experience of 10 years. Guided 13 ME students and have 11 publications in conferences and journals of National and International repute. Her area of interest is Networking.