IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 5, May 2016

Secure Data Retrieval Using Access Policies in Ciphertext Policy Attribute Based Encryption

Navaneetha A R[1], Sushant Mangasuli[2]

Alva's Institute of Engg &Tech, Mijar, Moodbidri, Karnataka, India[1, 2]

Abstract: Mobile nodes in military environments like a arna or a hostile region are doubtless to suffer from intermittent network property and frequent partitions. Disruption-tolerant network (DTN) technologies are getting no-hit solutions that enable wireless devices carried by militia to speak with one another and access the steer. Several militia applications need multiplied protection of confidential knowledge together with access management ways that are cryptographically enforced. Attribute-based secret writing (ABE) may be a promising approach that fulfils the wants for secure knowledge retrieval in DTNs. However, the matter of applying the ABE to DTNS introduces many security and privacy challenges. Since some users might modification their associated attributes at some purpose key revocation for every attribute is critical so as to form systems secure. Cipher text policy attribute-based secret writing (CP-ABE) may be a promising scientific discipline answer to the access management problems. However, the matter of applying CP-ABE in suburbanised DTNs introduces many security and privacy challenges with relevancy the attribute revocation, key escrow. Here, we have a tendency to propose a secure knowledge retrieval theme victimization CP-ABE for suburbanised DTNs wherever multiple key authorities manage their attributes severally. We'll offer the way to apply the planned mechanism to firmly and with efficiency manage the confidential knowledge distributed within the DTN.

Keyword: Disruption-tolerant networks, Cipher text policy attribute-based secret writing.

I. INTRODUCTION

In several military network eventualities, connections of wireless devices carried by troopers could also be quickly disconnected by ECM, environmental factors, and quality, particularly once they operate in hostile environments. Disruption-tolerant network (DTN) technologies have become no-hit solutions that enable nodes to speak with one another in these extreme networking environments [1]-[3].

Typically, once there's no end-to-end association between a supply and a destination combine, the messages from the supply node may have to attend within the intermediate nodes for a considerable quantity of your time till the association would be eventually established. The storage nodes in DTNs wherever knowledge is hold on or replicated such solely approved mobile nodes will access the mandatory info quickly and expeditiously. Several military applications need enhanced protection of confidential knowledge as well as access management strategies that are cryptographically implemented [6]-[7].

In several cases, it's fascinating to produce differentiated access services such knowledge access policies are outlined over user attributes or roles, that are managed by the key authorities. For instance, in a very disruption-tolerant military network, a commander might store a guidance at a storage node, that ought to be accessed by members of "Battalion 1" in agency are collaborating in "Region a pair of." During this case, it's an inexpensive assumption that multiple key authorities are doubtless to manage their own dynamic attributes for troopers in their deployed regions or echelons, that may well be oftentimes modified (e.g., the attribute representing current location of moving soldiers). We have a tendency to seek advice from this DTN design wherever multiple authorities issue and manage their own attribute keys severally as a decentralized DTN.

The construct of attribute-based cryptography (ABE) [11]-[14] could be a promising approach that fulfils the necessities for secure knowledge retrieval in DTNs. ABE options a mechanism that allows associate access management over encrypted knowledge victimization access policies and ascribed attributes among personal keys and ciphertexts [13]. Especially, ciphertext-policy ABE (CP-ABE) provides a climbable method of encrypting knowledge such the encryptor defines the attribute set that the rewriteor has to possess so as to decrypt the ciphertext. Thus, totally users are allowed to rewrite different items of information per the safety policy. However, the matter of applying the ABE to DTNs introduces many security and privacy challenges. Since some users might modification their associated attributes at some purpose (for example, moving their region), or some personal keys may be compromised, key revocation (or update) for every attribute is critical so as to create systems secure. However, this issue is even tougher, particularly in ABE systems, since every attribute is conceivably shared by multiple users. This means that revocation of associated attribute or any single user in an attribute cluster would have an effect on the opposite users within the cluster. Another challenge is that the key written agreement downside. In CP-ABE, the key authority generates personal keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority will rewrite each

DOI 10.17148/IJIREEICE.2016.4593

ciphertext addressed to specific users by generating their attribute keys [16]. If the key authority is compromised by adversaries once deployed within the hostile environments, this might be a possible threat to the information confidentiality or privacy particularly once the information is very sensitive. The key written agreement is associate inherent downside even within the multiple-authority systems as long as every key authority has the complete privilege to come up with their own attribute keys with their own master secrets.

Since such a key generation mechanism supported the only master secret is that the basic technique for many of the uneven cryptography systems like the attribute- based mostly or identity-based cryptography protocols, removing written agreement in single or multiple-authority CP-ABE could be a polar open downside. The last challenge is that the coordination of attributes issued from totally different authorities.

Once multiple authorities manage and issue attribute keys to users severally with their own master secrets, it's terribly onerous to outline fine-grained access policies over attributes issued from totally different authorities. For instance, suppose that attributes “role 1” and “region 1” are managed by the authority A, and “role 2” and “region 2” are managed by the authority B. Then, it's not possible to come up with associate access policy ((“role 1” OR “role 2”) AND (“region 1” or “region 2”)) within the previous schemes as a result of the OR logic between attributes issued from totally different authorities can not be enforced. This can be because of the very fact that the various authorities generate their own attribute keys victimization their own freelance and individual master secret keys.

II. RELATED WORK

ABE comes in 2 flavours referred to as key-policy ABE (KPABE) and Ciphertext-policy ABE (CP-ABE). The conception of attribute-based cryptography (ABE) [11] may be a promising approach that fulfils the wants for secure knowledge retrieval in DTNs. ABE options a mechanism that allows associate access management over encrypted knowledge mistreatment access policies and ascribed attributes among non-public keys and cipher texts. Especially, Ciphertext-policy ABE (CP-ABE) provides a climbable means of encrypting knowledge such the encryptor defines the attribute set that the decoder has to possess so as to decrypt the Ciphertext [10]. In KPABE, the encryptor solely gets to label a Ciphertext with a collection of attributes. The key authority chooses a policy for every user that determines that cipher texts he will decode and problems the key to every user by embedding the policy into the user’s key. However, the roles of the cipher texts and keys square measure reversed in CP-ABE. In CP-ABE, the Ciphertext is encrypted with associate access policy chosen by associate encryptor, however a secret's merely created with relevancy associate attributes set [8].

KP-ABE it allows write in codeors like a commander to settle on associate access policy on attributes and to encrypt confidential knowledge beneath the access structure via encrypting with the corresponding public keys or attributes [5], [9].

Attribute Revocation: Solutions planned to append to every attribute associate expiration date or time and distribute a replacement set of keys to valid users once the expiration.

Key Escrow: Most of the present ABE schemes square measure created on the design wherever one trustworthy authority has the ability to come up with the complete non-public keys of users with its master secret info. Thus, the key written agreement downside is inherent such the key authority will decode each ciphertext addressed to users within the system by generating their secret keys at any time. A distributed KP-ABE theme planned solves the key written agreement downside during a multi authority system. during this approach, all (disjoint) attribute authorities square measure taking part within the key generation protocol during a distributed means such they can not pool their knowledge and link multiple attribute sets happiness to an equivalent user.

Decentralized ABE: A combined access policy over the attributes issued from totally different authorities by merely encrypting knowledge multiple times. the most disadvantages of this approach square measure potency and quality of access policy.

III. CP-ABE SCHEME FOR DTNS

In this paper, we have a tendency to implement associate attribute-based secure information retrieval theme exploitation CP-ABE for redistributed DTNs. The planned theme options the subsequent achievements. First, immediate attribute revocation enhances backward/ forward secrecy of confidential information by reducing the windows of vulnerability. Second, encryptors will outline a fine-grained access policy exploitation any monotone access structure beneath attributes issued from any chosen set of authorities. Third, the key written agreement drawback is resolved by associate escrow-free key supplying protocol that exploits the characteristic of the redistributed DTN design.

The 2PC protocol deters the key authorities from getting any master secret info of every different specified none of them may generate the entire set of user keys alone. Thus, users don't seem to be needed to totally trust the authorities so as to guard their information to be shared. confidentiality and privacy will be cryptographically implemented against any curious key authorities or data storage nodes within the planned theme.

A. Advantages

1) Information Confidentiality: Unauthorized users WHO don't have enough credentials satisfying the access policy ought to be deterred from accessing the plain information within the storage node. additionally, unauthorized access from the storage node or key authorities ought to be additionally prevented.

DOI 10.17148/IJIREEICE.2016.4593

2) Collusion-Resistance: If multiple users interact, they will be ready to rewrite a ciphertext by combining their attributes though every of the users cannot rewrite the ciphertext alone.

3) Backward and forward Secrecy: within the context of ABE, backward secrecy implies that associated user WHO involves hold an attribute (that satisfies the access policy) ought to be prevented from accessing the plaintext of the previous information changed before he holds the attribute. On the opposite hand, forward secrecy secrecy implies that associated user WHO drops an attribute ought to be prevented from accessing the plaintext of the next information changed when he drops the attribute, unless the opposite valid attributes that he's holding satisfy the access policy.

IV. NETWORK ARCHITECTURE

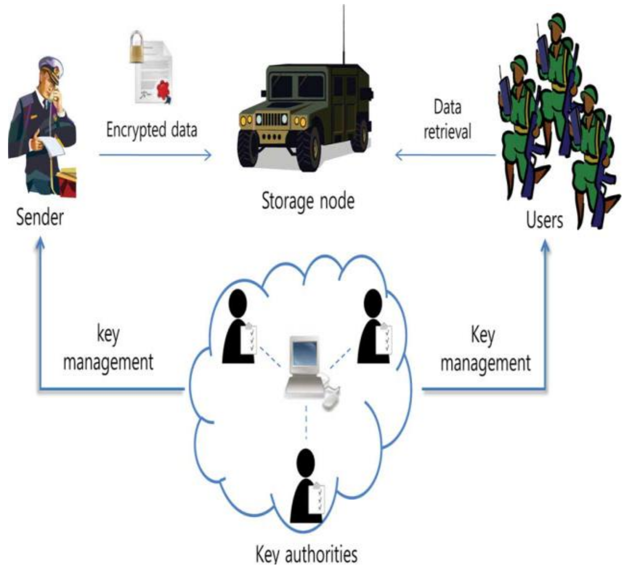

Fig1. Architecture of secure data retrieval in a disruption-tolerant military network

A. System Description and Assumptions: Fig. 1 shows the architecture of the DTN. As shown in Fig. 1,the architecture consists of the following system entities.

1) Key Authorities: they're key generation centers that generate public/secret parameters for CP-ABE. The key authorities carries with it a central authority and multiple native authorities. We have a tendency to assume that there are secure and reliable communication channels between a central authority and every federal agency throughout the initial key setup and generation part. Every federal agency manages totally different attributes and problems corresponding attribute keys to users. They grant differential access rights to individual users supported the users attributes.

2) Storage node: this is often associate entity that stores information from senders and supply corresponding access to users. It should be mobile or static.

3) Sender: this is often associate entity who owns confidential messages or information (e.g., a commander) and needs to store them into the external information storage node for simple sharing or for reliable delivery to users within the extreme networking environments. A sender is chargeable for shaping (attribute based) access policy and implementing it on its own information by encrypting the info underneath the policy before storing it to the storage node.

4) User: this is often a mobile node who needs to access the info keep at the storage node (e.g., a soldier). If a user possesses a group of attributes satisfying the access policy of the encrypted information outlined by the sender, and isn't revoked in any of the attributes, then he are ready to decipher the ciphertext and procure the info.

Since the key authorities are semi-trusted, they must be deterred from accessing plaintext of the info within the storage node; meantime, they must be still ready to issue secret keys to users. So as to understand this somewhat contradictory demand, the central authority and therefore the native authorities have interaction within the arithmetic 2PC protocol with master secret keys of their own and issue freelance key elements to users throughout the key issuance part. The 2PC protocol prevents them from knowing every other's master secrets in order that none of them will generate the entire set of secret keys of users one by one. Thus, we have a tendency to take associate assumption that the central authority doesn't conspire with the native authorities.

B. Threat Model and Security Requirements

1) knowledge confidentiality: Unauthorized users World Health Organization don't have enough credentials satisfying the access policy ought to be deterred from accessing the plain knowledge within the storage node. Additionally, unauthorized access from the storage node or key authorities ought to be conjointly prevented.

2) Collusion-resistance: If multiple users conspire, they will be ready to decode a ciphertext by combining their attributes albeit every of the users cannot decode the ciphertext alone [11]–[13]. As an example, suppose there exist a user with attributes and another user with attributes . They may achieve decrypting a ciphertext encrypted below the access policy of ("Battalion 1" AND "Region 2"), albeit every of them cannot decode it separately. We do not want these colluders to be ready to decode the key info by combining their attributes. We tend to conjointly take into account collusion attack among curious native authorities to derive users keys.

3) Backward and forward Secrecy: Within the context of ABE, backward secrecy means any user World Health Organization involves hold an attribute (that satisfies the access policy) ought to be prevented from accessing the plaintext of the previous knowledge changed before he holds the attribute. On the opposite hand, forward secrecy means any user World Health Organization drops an attribute ought to be prevented from accessing the plaintext of the next knowledge changed when he drops the attribute, unless the opposite valid attributes that he's holding satisfy the access policy.

DOI 10.17148/IJIREEICE.2016.4593

V.CONCLUSION

DTN technologies have become roaring solutions in military applications that permit wireless devices to speak with one another and access the lead dependably by exploiting storage device nodes. CP-ABE could be a climbable science resolution to access management and to secure information retrieval problems. during this project, Associate in Nursing economical and secure information retrieval methodology victimisation CP-ABE for decentralised DTNs wherever multiple key authorities manage their attributes severally has been enforced. The inherent key written agreement downside is resolved specified the confidentiality of the keep information is secure even underneath the hostile setting wherever key authorities may well be compromised or not totally trustworthy . additionally, the fine-grained key revocation may be in serious trouble every attribute cluster.

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, pp. 1–11.

[2] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in Proc. IEEE MILCOM, 2006, pp. 1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, “Mesage ferry route design for sparse ad hoc networks with mobile nodes,” in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] S. Roy andM. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2007, pp. 1–7.

[6] 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, pp. 29–42.

[7] 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.

DOI 10.17148/IJIREEICE.2016.4593