Efficient and Secure Information Retrieval for Decentralized Disruption Tolerant Military Networks

G.Saidivya[#1], C.Rajendra[*2] , V.Sreenatha sharma[#3]

[1]*Department of CSE, ASCET, Gudur*

[2] *Department of CSE, ASCET, Gudur*

[3]*Department of CSE , ASCET, Gudur*

[1] divyasai.g@gmail.com

[2] srirajendra.c@gmail.com

[3] villariss@gmail.com

***Abstract--*In the transformation of data opening in military systems, the security constraints have serious issues. In order to retrieve the data secured and efficiently we use the CP-ABE. Cipher text-policy attribute based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The problems of key Escrow, Revocation and co-ordination are discussed and we demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. The overall monitoring of the system is and uses of analysis are discussed.**

***Key Words-* Attribute Based Encryption (ABE), Security, Disruption Tolerant Network (DTN), secure data retrieval**

I. INTRODUCTION

In several military network situations, connections of wireless devices carried by soldiers are also briefly disconnected by jamming, environmental factors and quality, particularly once they operate in hostile environments. Disruption-tolerant network (DTN) technologies are getting made solutions that permit nodes to speak with one another in these extreme networking environments. Typically, once there is no end-to-end association between a supply and a destination pair, the message 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. Roy and chuah [2] introduces storage nodes in DTNs where ever information is hold on or replicated specified solely approved mobile nodes will access there required data quickly and expeditiously. Several military applications need developed protection of confidential information together with access management strategies that are cryptographically implemented. In several cases, it is fascinating to supply differentiated access service specified information access policies decide over user attributes or roles that are managed by the key authorities. For instance, during a disruption-tolerant military network, a commander might store lead at a storage node, that ought to be accessed by members of “Battalion 1” who are join in "Region two". During this case, it is an affordable assumption that multiple key authorities are acceptable to manage their own dynamic attributes for soldiers in their deployed regions or echelons that can be often modified (e.g., the attribute representing current location of moving soldiers) [4]. We check with this DTN design wherever multiple authorities issue and manage their own attribute keys severally as a decentralized DTN. The conception of attribute based encryption (ABE) may be a promising approach that fulfils the wants for secure knowledge retrieval in DTNs [5].

ABE options a mechanism that allows associate access management over encrypted knowledge victimization access policies and ascribed attributes among non-public keys and cipher texts. Especially cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting knowledge such them encrypt or defines the attribute set that the decode or has to possess so as to decrypt the cipher text. However, the matter of applying the ABE to DTNs introduces many security and privacy challenges. Since some users may convert their associated attributes at some purpose (for example, moving their region) [6], or some non-public keys could be compromised, key revocation (or update) for every attribute is critical so as to form systems secure. However, this issue is even harder, particularly in ABE systems, since every attribute is conceivably shared by multiple users (henceforth, we have a tendency to check with such a set of users as associate attribute group).

This suggested that revocation of associated attribute or any single user in an attribute cluster would have an effect on the opposite users within the cluster. May be, if a user joins or leaves associated attribute cluster, the associated attribute key ought to be modified and decentralized to all or any the opposite members within the same cluster for backward or forward secrecy. It should end in bottleneck throughout rekeying procedure or security degradation thanks to the windows of vulnerability if the previous attribute secret is not update immediately. Another challenge is that the key escrow 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 [8]. Thus, the key authority will rewrite each cipher text addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries once deployed within

Selected paper: International Conference On Computing (NECICC-2k15)

the hostile environments, this might be a possible threat to the information confidentiality or privacy particularly once the information is extremely sensitive. The key escrow agreement is associate degree inherent downside even within the multiple-authority systems as long as every key authority has the full privilege to get their own attribute keys with their own master secrets. Since such a key generation mechanism supported the single master secret is that the basic method for many of the uneven cryptography systems akin to the attribute-based mostly or identity based cryptography protocols, removing written agreement in single or multiple-authority CP-ABE could be a important open problem.

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 is terribly onerous to outline fine-grained access policies over attributes issued from totally different authorities. To illustrate, suppose that attributes “role 1” and “region 1” area unit managed by the authority A, and “role 2” and “region 2” area unit managed by the authority B. Then, it is not possible to get associate degree 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't be enforced. This can be because of the actual fact that the various authorities generate their own attribute keys exploitation their own attribute keys exploitation their own freelance and individual master secret keys.

II. LITERATURE SURVEY

S. Roy and M. Chuah [2] Planned CP-ABE system for DTNs, they used two kinds of encoding techniques at the side of CP-ABE. Within the first technique, the information is encrypted mistreatment interchangeable key encryption. Then the result is subjected to CP-ABE encoding. In the second technique, the information are encrypted employing key encoding key (KEK) and so KEK are encrypted mistreatment CP-ABE. They also extended CP-ABE methodology to support static and dynamic attributes.

D. Huang and M. Verma [4] Planned a theme within the multi authority network surroundings referred to as decentralized Cipher text-policy Attribute-based encryption (CP-ABE). They achieved a combined access policy by encrypting the information multiple times over the attributes issued from multiple authorities.

A. Lewko and B. Waters [5] Planned multi authority attribute based mostly encoding methodology. This methodology consists of multiple authorities that they manage completely different attributes of user.

J. Bethencourt, A. Sahai and B.waters planned secure information access management methodology referred to as cipher text policy attribute based mostly encoding. In previous technique like just in case of attribute based mostly encoding. In previous techniques like just in case of attribute based mostly encoding method the policies are outlined with secret keys of users and therefore the information are keep within the storage highly in secured. But here, encrypting information, owner can outline some policies over encrypted data and it will be keep within the storage node. In order to urge encrypted information that is keep within the storage node, the decrypt or must satisfy the policies.

A. Boldyreva, V. Goyal, and V. Kumar [7] here the encoding are done supported the identity of users by mistreatment trustworthy authority. The most advantage of this system is that the users do not have to be compelled to have public keys and is secure technique.

Chase and S. M. Chow [8] given a distributed key-policy Attribute-based encoding (KP-ABE) scheme that solves the key written agreement drawback in an exceedingly multi authority system. During this theme, participating to get attribute keys mistreatment the key generation protocol in an exceedingly distributed method such they can't collect their information and acquire attribute sets that are happiness to an equivalent user.

Chase [9] here multiple authorities concerned in generating the non-public keys of users and user uses key-policy technique where ever policies are outlined over the non-public keys of user for social control of encrypted information and thus this methodology provides reliable access to data users.

III. ACTUAL WORK

A. Implementation of ABE:

The idea of Attribute based encryption writing could be a guaranteeing approach that satisfies the conditions for secure information recovery in DTNs. ABE characteristics a system that empowers a right to achieve entrance management over scalable access approaches and attributable qualities among personal keys and cipher texts. The difficulty of applying the ABE to DTNs presents a number of security and protection challenges. Since a number of users could correct their connected qualities sooner or later (for instance, moving their district), or some personal keys is also listed off, key repudiation (or redesign) for every one characteristic is prime keeping in mind the top goal to create frameworks secure.

This infers that renunciation of any property or any single shopper during a characteristic gathering would influence alternate shoppers within the gathering. Case in point, if a user joins or leaves a attribute assemble, the connected characteristic key have to be compelled to be modified and decentralised to the assorted elements within the same gathering for retrograde or forward mystery. It is going to originate bottleneck amid rekeying technique or security corruption owing to the windows of impotence if the past characteristic secret is not overhauled quickly.

B. Limitation of Existing System

i) The difficulty of applying the ABE to DTNs presents a number of security and protection challenges. Since a number of users might exchange their connected properties sooner or later (for instance, moving their area), or some personal keys is also bargained, key renunciation (or upgrade) for every one attribute is key with a particular finish goal to form frameworks secure.

ii) But, this issue is considerably additional hard, significantly in ABE frameworks, since each characteristic is presumably important by different users (hereafter, we tend to touch to such a gathering of shoppers as a high quality gathering).

iii) Another take a look at is that the key written agreement issue. In CP-ABE, the key power creates personal keys of shoppers by applying the powers skilled mystery keys to clients connected set of properties.

iv) The last take a look at is that the coordination of traits issued from distinctive powers. At the purpose once numerous power supervised and issue ascribes keys to shoppers freely with their skilled mysteries, it is tough to characterize fine-grained access arrangements over traits issued from distinctive powers.

C. *Working Procedure for CP-ABE*

In this paper, we tend to propose associate an attribute-based secure knowledge retrieval theme victimisation CP-ABE for localised DTNs. The planned theme options the subsequent achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential knowledge by reducing the windows of vulnerability. Second, encryptions will outline a fine-grained access policy victimisation any monotone access structure beneath attributes issued from any chosen set of authorities. Third, the key written agreement downside is resolved by Associate in Nursing escrow-free key supply protocol that exploits the characteristic of the localised DTN design. The key supply protocol generates and problems user secret keys by activity a secure two- party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from getting any master secret info of every alternative specified none of them might generate the total set of user keys alone. Thus, users don't seem to be needed to totally trust the authorities so as to guard their knowledge to be shared. Confidentially and privacy will be cryptographically implemented against any curious key authorities or data storage nodes within the planned theme.

D. Advantages

i) *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, unauthorised access from the storage node or key authorities ought to be conjointly prevented.

ii) *Collusion-resistance*: If multiple users conspire, they will be able to rewrite a cipher text by combining their attributes albeit every of the users can't rewrite the cipher text alone.

iii) Backward and forward Secrecy: Within the context of ABE, backward secrecy implies that 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 implies that any user World Health Organization drops an attribute ought to be prevented from accessing the plaintext of the next knowledge changed once he drops the attribute, unless the opposite valid attributes that he is holding satisfy the access policy.

E. challenges

The problem of this method is to outline Cipher text-policy attribute based encryption (CP-ABE) may be a promising solution to the access management problems. However, the matter of applying CP-ABE in decentralised DTNs introduces many security and privacy challenges with reference to the attribute revocation, key escrow, and coordination of attributes issued from totally different authorities.

F. System Architecture

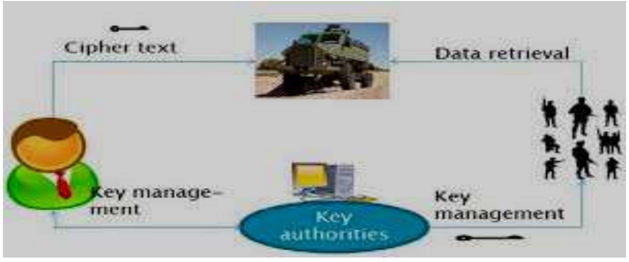

Fig1: Architecture of secure data retrieval for decentralized disruption tolerant network.

1. Key Authorities: They are key generation centres that generate public/secret parameters for CP-ABE. The key authority carries with it a central authority and multiple native authorities. We tend to assume that there square measure secure and reliable communication channels between a central authority and every local authority throughout the initial key setup and generation part.

Every bureau manages completely 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 an entity that stores knowledge from senders and supply corresponding access to users. It should be mobile or static. Like the previous schemes, we tend to additionally assume the storage node to be semi-trusted that's honest-but-curious.

3. Sender: This is Associate in nursing entity World Health Organization owns confidential messages or knowledge and needs to store them into the external knowledge storage node for simple sharing or for reliable delivery to users within the extreme networking environments.

A sender is liable for shaping (attribute based) access policy and imposing it on its own knowledge by encrypting the info below the policy before storing it to the storage node.

4. User: This is a mobile node World Health Organization needs to access the information keep at the storage node (e.g., a soldier). If a user possesses a collection of attributes satisfying the access policy of the encrypted knowledge outlined by the sender, and is not revoked in any of the attributes, then he are going to be able to decipher the cipher text and acquire the information.

IV. CONCLUSION

We proposed an efficient and secure data retrieval method using CP-ABE for decentralized Disruption Tolerant Networks (DTN) where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. The overall monitoring system also enhances the security and betterment of the system.

REFERENCES

[1] Brent Waters Cipher text-policy attribute-based encryption: An expressive efficient and provably secure realization cryptologyprint archive ,report 2008 /290, 2008. http: //eprint .iacr.org/

[2] S. Roy and M. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[3] 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.

[4] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.

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

[6] J. Bettencourt, A. Sahai, and B. Waters, "Cipher text- policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[7] Boldyreva, V. Goyal, and V. Kumar, "Identity based encryption with efficient revocation," in Proc. ACM Conf. Compute. Common. Security, 2008, pp. 417–426.

[8] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

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