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 11, November 2015

An Approach to Secure Data in Disruption Tolerant Network

Mayuri Gourkhede, Neha Titarmare

M.Tech Student, Dept of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

Assistant Professor, Dept of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

ABSTRACT: Mobile nodes in secured environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by individuals to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. The concept of attribute-based encryption (ABE) is a promising approach that fulfils the requirements for secure data retrieval in DTNs. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. Data can be easily hacked by third person if they have the key credentials with them. To overcome the drawback of existing system we planned to proposed a system where data will be transferred securely in DTN from one end to other end with respect to parameters like geo-location, valid timestamp and ip-address.

KEYWORDS: Access control, attribute-based encryption(ABE), disruption-tolerant network(DTN), secure data retrieval.

I. INTRODUCTION

Disruption Tolerant Networks utilize the mobility of nodes. The nodes can move anywhere at any time. Due to the intermittent connectivity it is very difficult to maintain end-to-end connections.[12] An end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic, predictably connectable, or periodically connected. To allow nodes to communicate with each other in these extreme networking environments, recently the research community has proposed a new architecture called the disruption tolerant network (DTN). Several DTN routing schemes have been proposed[1,2]. Typically, the source node's message may need to wait in the intermediate nodes for substantial amount of time when there is no connection to the final destination. After the connection is eventually established, the message is delivered to the destination node.

Roy [13] and Chuah [5] introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced [14]. A DTN is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet [5]. DTNs accommodate the mobility and limited power of evolving wireless communication devices. DTNs overcome the problems associated with intermittent connectivity, long or variable delay, asymmetric data rates, and high error rates by using store-and forward message switching.

Attribute-based encryption (ABE) is a promising approach that fulfils the requirements for secure data retrieval in DTNs. Especially, Cipher text-Policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text [14]. As an example, in a battlefield DTN, a storage node may have some confidential information which should be accessed only by a member of 'Battalion 6' or a participant in 'Mission 3'. Several current solutions [15,16] follow the traditional cryptographic-based approach where the contents are encrypted before being stored in storage nodes, and the decryption keys are distributed only to authorized users. In such approaches, flexibility and granularity of content access control relies heavily on the underlying cryptographic primitives being used. It is hard to balance between the complexity of key management and the granularity of access control using any solutions that are based on the

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 11, November 2015

conventional pair wise key or group key primitives. Thus, we still need to design a scalable solution that can provide fine-grain access control.

CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt [9]. The aim is to secure data in DTN. Data can be easily hacked by third person if they have the key credentials with them so our proposed approach is to overcome the drawback of existing system we planned to proposed the system where data will be transferred securely in DTN from one end to other end with respect to parameters geo-location, valid timestamp and ipaddress.With the help of CP-ABE scheme we propose a system such that data should be secure in DTN. A CP-ABE scheme consists of the following four algorithms:[3,13]

1. Setup: This is a randomized algorithm that takes a security parameter as input, and outputs the public parameters *PK* and a master key *MK*. *PK* is used for encryption and *MK* is used to generate user secret keys and is known only to the central authority.
2. Encryption: This is a randomized algorithm that takes as input a message *M*, an access structure *T*, and the public parameters *PK*. It outputs the cipher text *CT*.
3. KenGen: This is a randomized algorithm that takes as input the set of a user (say *X*)'s attributes *SX*, the master key *MK* and outputs a secret key *SK* that identifies with *SX*.
4. Decryption: This algorithm takes as input the cipher text *CT*, a secret key *SK* for an attribute set *SX*. If *SX* satisfies the access structure embedded in *CT*, it will return the original message.

II. RELATED WORK

In paper [1] author introduces how a content-based information retrieval system can be designed for DTNs. There are three important design issues, namely (a) how should data be replicated and stored at multiple nodes, (b) how should a query be disseminated in sparsely connected networks, (c) how should a query response be routed back to the querying node. In paper [2] author introduces in a distributed system the user can access the data if user can posses a certain set of attributes,sometimes the server can trusted so that time the data cannot be stored securely. Cipher text-policy-ABE control the complex structure on the encrypted data and store in securely. They secure the data against collusion attacks. In paper [3] author introduces routing messages are intermittent connected nodes but routing in such environment are difficult because peers have little information in a partition network and transfer opportunities of peers in lower duration.MaxProp, a protocol 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. MaxProp on simulated topologies and show it performs well in a wide variety of DTN environments. In paper [4] author introduces traditional ad hoc routing protocol do not work in a intermittently connections so that the path cannot exist in the network. Store and forward approach is proposed for DTN.With the help of this message ferrying. So we assume a special node for ferrying the messages. We design a node density based routing that allows regular nodes to volunteer to be message ferries when there are very few nodes around them ensure the feasibility of continued communication. In paper[5] author introduces that the attribute based encryption for secure the data, in this paper proposed that the multiauthority attribute based encryption system. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that react their attributes. In paper[6] author introduces traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In this paper, we introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. In paper [7] author introduces disruption tolerant network is a different type of wireless network. It is a intermittently connected mobile network. It also has a limitation in network resources. The DTN allows transmission only if it is in the transmission range. Because of this limitation there is a chance of dropping the received packets by the selfish or malicious nodes. Finally this leads to attacks. Many approaches are proposed to solve the problems which are occurred in DTN so that a survey is proposed by referring some approaches that are used to overcome different problems in the Disruption Tolerant Network.

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 11, November 2015

EXISTING SYSTEM:

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 ciphertext,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.[17] 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.

III. PROPOSED WORK

Data can be easily hacked by third person if they have the key credentials with them. To overcome the drawback of existing system we planned to proposed the system where data will be transferred securely in DTN from one end to other end with respect to parameters geo-location, valid timestamp and ipaddress.

PROPOSED ARCHITECTURE:

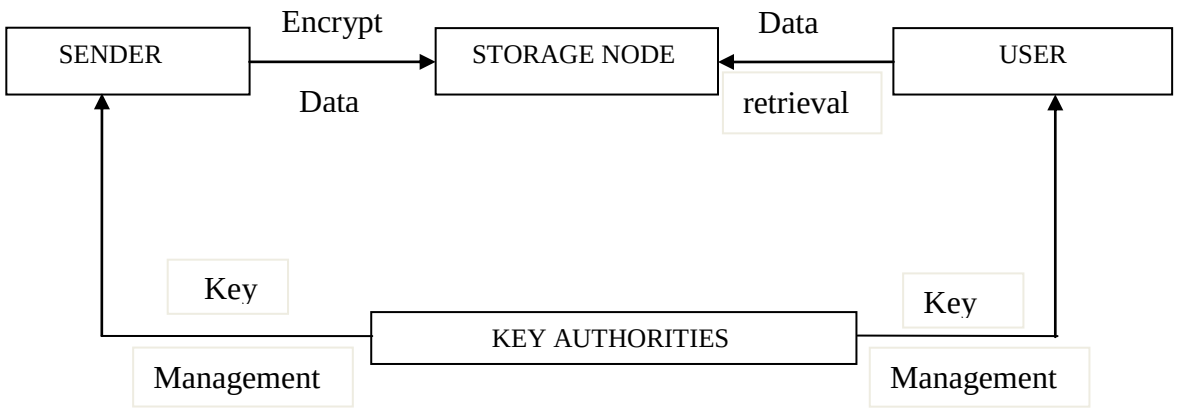

Fig. Shows the proposed architecture of DTN

The description of module are as follows:

1. Key Authorities :

They are key generation centres that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

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 11, November 2015

2. Storage node :

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [17]. Similar to the previous schemes, we also assume the storage node to be semi-trusted, that is honest-but-curious.

3. Sender :

This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4. User :

This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the cipher text and obtain the data.

IV. RESULTS

It is expected that the proposed approach should be secure the confidential data and transferred securely from a source node to a destination node with respect to parameters like geo-location, valid timestamp and ip-address.

V. CONCLUSION AND FUTURE WORK

Our project is not a unique one but DTN concept is very useful for securing the confidential data from sender to receiver and it is used in many applications such as military application, commercial application, scientific application etc.The future work is how to construct a cipher text policy attribute-based encryption scheme which would have both:the flexible delegation and attribute revocation properties, without involving a Mediator in the system Architecture.

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. M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*,2007.
4. J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007.
5. A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptology ePrint Archive: Rep. 2010/351, 2010.
6. M. Pirretti, P. Traynor, P. Mc Daniel, and B. Waters, "Secure attribute based systems," in Proc. ACM Conf. Comput. Commun. Security, 2006.
7. S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Survey., vol. 35, no. 3, pp. 309–329,2003.
8. L. Cheung and C. Newport, "Provably secure cipher text policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
9. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded cipher text policy attribute based encryption," in Proc. ASIACCS,2009
10. M. Chase and S. S. M. Chow, "Improving privacy and security in Multiautority based attribute based encryption " in Proc. ACM Conf. Computer. Commun. Security, 2009.
11. A Survey of Secure Data Transfer in Disruption Tolerant Network in International Journal of Advanced Research I computer and communication Engineering by E K Girisan1, Shidha S2.
12. D.S.Delphin Hepsiba, S.Simla Mercy, S.Prabu," Secured Data Forwarding Technique in Disruption Tolerant Networks-Survey"in international Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014.
13. 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.
14. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated cipher text-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

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 11, November 2015

15. M. K. et al. Plutus: scalable secure file sharing on untrusted storage. In *Proceedings of ACM Usenix*, 2002.
16. A. Harrinton and C. Jensen. Cryptographic access control in a distributed file system. In *Proceedings of ACM SACMAT*, 2003
17. Junbeom Hur and Kyungtae Kang, *Member, IEEE, ACM.* IEEE TRANSACTIONS ON NETWORKING VOL:22 NO:1 YEAR 2014.

BIOGRAPHY

Ms. Neha Titarmare Assistant Professor in the CSE Department, Rajiv Gandhi College of Engineering and Research, Nagpur, India. She has received Master of Technology (M.Tech.) degree. She's research interests are in Wireless Networking.