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 9, September 2015

Survey of Data Retrieval for Decentralized DTN

Nikita Bankhele, Priya Deshmukh, Chandrakant Gawande, Mangesh Manake

Student, Dept. of Computer Engineering, Savitribai Phule Pune University, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

Student, Dept. of Computer Engineering, Savitribai Phule Pune University, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

Student, Dept. of Computer Engineering, Savitribai Phule Pune University, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

Head, Dept. of Computer Engineering, Savitribai Phule Pune University, Dr. D. Y. Patil Institute of Engineering & Technology, Ambi, Pune, India.

ABSTRACT: Frequent partitions and stopping network connectivity hampers the mobile nodes, e.g. in military areas. DTN's (Disruption Tolerance Networks) like technologies are found to be emerging as successful solutions for wireless devices which are carried by soldiers. Here by exploiting external storage nodes, these devices are used for communicating with each other and access the secret information. Limitations are enforcement of policies authorization and policies update for safe data retrieval. To handle control issues CP-ABE (Ciphertext-Policy Attribute-based Encryption) is promising cryptographic solution. With the involvement of CP-ABE in decentralized DTNs privacy and security problem a rises. Attribute revocation, coordination of attributes issued by various authorities and key escrow. Review or survey is done on the data retrieval scheme using CP-ABE for decentralized DTNs.

KEYWORDS: Access Control, Attribute-Based Encryption (ABE), Disruption-Tolerant Network (DTN), Multi-Authority, Secure Data Retrieval.

I. INTRODUCTION

In many military network models, connections of wireless devices carried by soldiers. These connections may be disconnected by hampering some factors, jamming or mobility, particularly when it works in a hostile environment. Where the links in between intermediate nodes may be opportunistic, unsurprisingly connectable, or occasionally connected, there does not always exist an end-to-end path between a host and a destination spot. The research community has future architecture to allow nodes to communicate with each other in these extreme networks in environments, are known as DTNs (Disruption-Tolerant Networks). Several DTN techniques [3] [5] [14] have been projected. Typically, the source node's message may need to wait in the intermediate nodes for an extensive amount of time when there is no connection to the final destination. After the connection is ultimately established, the message is delivered to the destination node. Other regular users (mobile node) can access the necessary information quickly and efficiently because there are some 'storage nodes' that is also called as the mobile node in the network where valuable data is stored or replicated. So that it is very necessary in many military applications to increase requirements, protecting confidential data. To protect and important the confidential data stored in the storage nodes or routed through the network some security-critical application is to design.

In many cases, it is enviable to provide differentiated access services in a way that information/data approach policies are defined over user attributes or rules, which are managed by key authorities. For example, in a DTN (military), a commander can store secret information in the node, which should be accessed only by members of "Battalion 6" or a participant in 'Area3'. In this case, this is area reasonable assumption that multiple or various key

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 9, September 2015

authorities are likely to manage their dynamic attributes (own Dynamic attributes) for soldiers in their deployed echelons (region), which could be frequently changed (e.g., attribute representing the current location of moving soldiers) [2] [5] [6]. Several current solutions follow the some traditional cryptographic-based approach, here contents before being stored are encrypted in storage nodes, and the decryption keys are distributed to the user (authorized user) We refer to this DTN architecture where multiple authorities issue and manage their attribute (own attributes) keys inside. Thus, to provide fine-grain access control, we need to design a scalable solution.

In this paper, we describe a CP-ABE based encryption method that provides fine-grained access control. A CP-ABE scheme, each user is associated with a set of attributes. Attribute depends encryption an Encryptor will associate encrypted information with a set of attributes. An authority will issue users different private key. Where user's private key is associated with an access a structure over attributes. If the key authority is adjusted by adversaries when deployed in the enemy environments, it could be a potential risk (threat) to the information (Data) secrecy or privacy especially when the data is highly confidential. Even in the multiple-authority systems as long as each key authority has the whole privilege to generate their attribute keys with their own master confidence. Since such a key generation mechanism based on the single or particular master secret is the basic method for most of the asymmetric encryption systems such as the attribute-based encryption protocols, and also identity based encryption protocol, CP-ABE is a pivotal open problem of removing escrow in single or multiple-authority. The last challenge is the coordination of attributes issued by different authorities. It is very hard to define fine-grained access policies over attributes issued by different authorities as users get their own master secrets by various authorities since they manage and issue attribute keys to users independently. The different authorities generate their attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as 'n-out-of-m' logic, cannot be expressed in the previous schemes, which is a very implementable and generally required access policy logic.

II. LITERATURE SURVEY

It is necessary to decide the time factor, economy *n* company strength before developing the tool. After these things 'r' satisfied, then next steps is to decide which language and operating system can be used for developing the tool. In the above consideration 'r' taken into account for before developing proposed system.
Attribute-based encryption comes in two flavours following area: (I). Key-Policy ABE (KP-ABE). (II).Ciphertext-Policy ABE (CP-ABE).

- KP-ABE (Key-policy ABE): In KP-ABE allows to the Encryptor simply gets to label a ciphertext with a set of attributes. The key authority selects a policy for each user that decides which cipher-texts he can decrypt and issues the key to each user by embedding the policy into the user's key.
- CP-ABE (Cipher-text policy Attribute-based encryption): In CP-ABC keys and ciphertexts are reversed. The Encryptor choose an access policy to encrypt the cipher-text, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE since it enables encryptors such as a commander to choose an access policy on attributes and to encrypt secret data under the access structure via encrypting with the corresponding public keys or attributes.

i. ATTRIBUTE REVOCATION: Solutions proposed to distribute a new set of keys to valid users after the expiration and append to each attribute an expiration date (or time). Two main limitations with periodic attribute revocable ABE schemes. The security degradation problem in conditions of the backward and forward secrecy. The users such as soldiers may change their attributes frequently that scenario must considerable. Example attributes like position or location move are must consider.The other problem is scalability. All of the non-revoked users can update their keys when the key authority periodically announces a key renew material by unicast at each time-slot. This outcome in the '1_affects' issue. Wholly non-revoked users who distribute the attributes, are affected by this particular update on attribute. This could be a restricted access for both the key authority and all non-revoked users. The immediate key revocation can be done by recalling users using ABE that supports negative clauses. To do so,user identities recalled one just adds conjunctively the AND of negation. But this solution still is fairly lacking efficiency performance. This system will cause the overhead O(R) group elements1 additively to the size of the ciphertext and O (log M) multiplicatively to the size of private key over the original CP-ABE system of Bethencourt*et al.* [10], where is the highest size of revoked attributes set. Golle *et al.* [12] system only works when the number of attributes related to a ciphertext is exactly fifty percent of the universe size which a user revocable KP-ABE scheme.

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 9, September 2015

ii. KEY ESCROW: Generally of the existing ABE schemes are constructed in the structural design where a single trusted authority has the authority to generate the whole private keys of users with its master secret information [13] [14] [3] [11]. Accordingly, the key escrow difficulty is ingrained such that the key authority has right to decrypt every ciphertext addressed to users in the system by generating their secret keys at any instance. A scattered KP-ABE scheme proposed solves the key escrow difficulty in a multi authority system. In this approach, all (put out of joint) attributes authorities are participating in the key generation protocol in scattered way such that they can't pull their data and link multiple attribute sets, belong to the same user. The performance degradation the limitation of this fully distributed approach. Since there is no admin authority with master secret information, all attributes authorities need to communicate with each other in the system to generate a user's secret key.

iii. DECENTRALIZED ABE: Huang *et al.*[9] and Roy *et al.* [4] For decentralized CP-ABE schemes, multi - authority network environment is used. They achieved a gathered access policy over the attributes issued by different authorities by simply encrypting data several times. The limitation of these approaches is effective and self-expression of access policy. For example, when a commander encrypts a top secret mission to soldiers under the policy ("Battalion 2" AND ('Area 3'OR 'Area 4')), it cannot be expressed while each "Area" attribute is managed by different authorities, since simply multi encrypting approaches can by no means express any general" n-out-of-m " logics (1-out- of- m).

III. PROPOSED ARCHITECTURE

Here, we have proposed the architecture for above technique. The sender is given with a key from key authorities to gain access and send the data. The data is sent in encrypted form to storage node. Only users having same authorized key is allowed to access the data via data retrieval process from storage node.

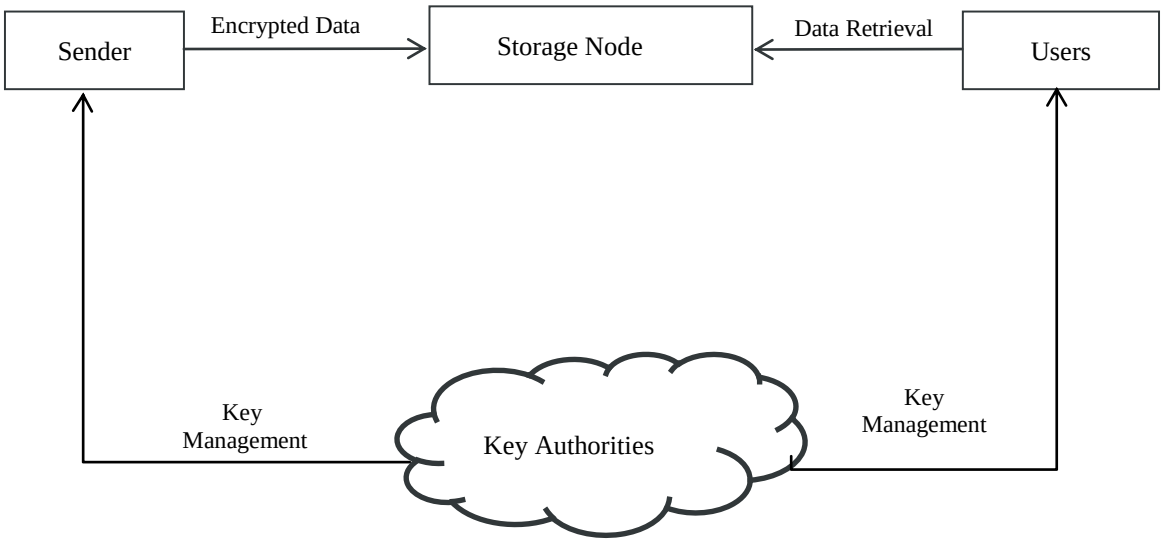

Fig.1. Proposed Architecture of secure data retrieval in a Disruption-Tolerant Network

IV. CONCLUSION

In this paper, we have reviewed the DTNs. We have also given the architecture for Secure Data Retrieval in DTS's. We have also recommended the good one to be selected while using DTNs. Further, we have elaborated previous work and future scope.

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 9, September 2015

V. FUTURE SCOPE

The proposed scheme features having following achievements:-

i. Immediate attributes revocation boosts up the forward or backward secrecy of secret information by minimizing the windows of vulnerability.
ii. Using any monotone access structure, encryptors can define a fine-grained access policy under attributes issued from any chosen set of authorities.
iii. An escrow-free key issuing protocol can solve the problem of key escrow by exploiting the characteristic of the decentralized DTN architecture.
iv. Hence, users need not to be required to trust the authorities fully in order to protect their data which is being shared.
v. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the remedial scheme.

VI. ACKNOWLEDGEMENT

The authors are thankful to researchers, publishers. For making the availability of their resources & publications. Teacher's guidance is equally responsible for this paper. We are also thankful to college authorities for providing us basic facilities and equipment which requires. Finally, we would like to extend heartfelt gratitude to friends, family members for their support and encouragement.

REFERENCES

1. Junbeom Hur, and Kyungatae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks," in Proc. IEEE,ACM, 2014
2. S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
3. M. Chuah and others. Enhanced disruption and fault tolerant network architecture for bundle delivery (EDIFY). In Proceedings of I IEEE Infocom, 2006
4. J. Burgess and others. Maxprop: Routing for vehiclebased disruption tolerant networks. In Proceedings of IEEE Globecom, 2005.
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. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application,"inProc. WISA, 2009, LNCS 5932, pp. 309–323.
7. N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.
8. 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.
9. A. Lewko and B. Waters, "Decentralizing attribute-based encryption", Cryptology Print Archive: Rep. 2010/351, 2010.
10. J. Bethencourt, A. Sahai,and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321–334.
11. 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.
12. P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp. Identity Trust Internet", 2008,pp. 26–35.
13. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in Proc. ACM Conf. Comput. Commun. Security", 2007, pp. 456–465.
14. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in Proc. ASIACCS, 2009.
15. M. M. B. Tariq and others. "Message ferry route design for sparse ad hoc networks with mobile nodes", In Proceedingsof ACM Mobihoc, 2006p.343–352.

BIOGRAPHY

Nikita Bankhele, Student pursing B.E in Computer Engg. from Savitribai Phule Pune University, Department of Computer Engg., Dr. D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, India.

Priya Deshmukh, Student pursing B.E in Compute Engg. from Savitribai Phule Pune University ,Department of Computer Engg., Dr. D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, India.

Chandrakant Gawande, Student pursing B.E in Computer Engg. from Savitribai Phule Pune University ,Department of Computer Engg., Dr. D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, India.

Asst. **Prof**. **Mangesh Manake** from Savitribai Phule Pune University , Head, Department of Computer Engg., Dr. D. Y. Patil Institute of Engg. & Tech., Ambi, Pune, India.