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. 4, Issue 9, September 2016

A Survey on Data Security in Military Networks using CP-ABE where Multiple Key Authorities Manage their Attributes Separately

Sumit Hirve, Komal Khatavkar, Vishakha Karande, Richa Mehta

Assistant Professor, Dept. of Computer Engineering, M.E.S College of Engineering, Pune, India

UG Student, Dept. of Computer Engineering, M.E.S College of Engineering, Pune, India

UG Student, Dept. of Computer Engineering, M.E.S College of Engineering, Pune, India

UG Student, Dept. of Computer Engineering, M.E.S College of Engineering, Pune, India

ABSTRACT: The mobile nodes in military environment are likely to suffer from many network connectivity problems. The DTN provides a solution by allowing mobile nodes to interact with each other in secure manner. In this scenario the major problems are the enforcement of authorization policies and secure data retrieval. The CP-ABE (cipher text policy-attribute based encryption) ensures secure retrieval of data in DTNs and guarantees cryptographic approach for access control issues. Hence if hacker hacks the message he cannot know which data has been transferred. In this paper we have discussed about disruption tolerant network and many more issues regarding to data retrieval.

KEYWORDS: Access control, Cipher text policy attribute based encryption (CP-ABE), Disruption tolerant network (DTN), Secure data retrieval, Two-party computation (2PC) protocol, Key authority

I. INTRODUCTION

The current Internet service model's design is based on a few assumptions such as (a) between a source and destination pair there is an end to-end path and (b) between any node pair there is a low roundtrip latency. However in some military networks these assumptions do not hold .In battlefield ad-hoc networks, wireless components carried by soldiers operate in virulent and warlike environments where jamming, environmental factors and mobility may cause temporary disconnections, intermittent connectivity with one another.

In such scenario, the end to end path may not exists between source and destination pair. The links between intermediate nodes may suffer from periodic network connectivity or they may be predictably connectable, opportunistic. Disruption tolerant network (DTN) allows these nodes to communicate with each other in such extreme environmental conditions [9]-[11]. When there is no end to end connection between the source and destination nodes, the messages sent by the source node may need to wait for some amount of time in the intermediate nodes until the connection is established. Once the connection is established, the messages are delivered to the destination node. In DTNs there are storage nodes where data is stored or replicated temporarily. Only authorized mobile nodes can access this data. In military network data security is most important. There is a need to design an access control method in order to protect the highly classified data stored in the storage nodes or which is routed through the network. For example, in a battlefield DTN, a storage node may have some highly classified data which should be accessed only by a member of 'Battalion 3' who are participating in 'Mission 2'. Traditionally in cryptographic-based approaches, the contents are encrypted before storing them in storage nodes and the decryption keys are given only to authorized users. In such approaches, the flexibility and granularity of content access control relies on the underlying cryptographic primitives being used. So we will be referring to DTN architecture in which multiple authorities issue and manage their own attribute keys independently.

DOI: 10.15680/IJIRCCE.2016. 0409104

CP-ABE based encryption scheme is being described in this paper. It provides fine-grained access control. In a CP-ABE scheme, user's private key is generated based on set of attributes specified by sender. Only those users can decrypt the contents that are encrypted under an access policy whose attributes match the access policy. It provides a scalable way of encrypting the data. Applying ABE to DTNs introduces several security and privacy issues and challenges. Due to portability of some users or hubs (moving from one region to other) private keys of users might be compromised. The alternative to this is key renouncement for each characteristic through which it may accomplish security. In ABE systems, this issue is very challenging and effortful because each attribute is shared by many users. Suppose if a user associates with or sanctions from an attribute group, the associated attribute key should be varied and distributed again to all the other members in the same group .If not updated immediately it may create a problem during rekeying procedure or security degradation. Another issue is the key escrow problem. In CP-ABE, the key authorities are responsible for generating private keys of users. If the key authorities are conciliated by attackers when utilized in the hostile environments, this could be a potential threat to the confidentiality of data. The end challenge is the coordination of attributes broadcasted from different authorities. When multiple key authorities issue manage and attribute keys to users independently it difficult to define fine-grained access policies over attributes issued from different authorities.

II. RELATED WORK

[1.] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data: Sahai and Waters introduced the concept of Attribute-Based Encryption (ABE). There are two types of ABE schemes: Key-Policy ABE scheme (KP-ABE) and Cipher text Policy ABE scheme (CP-ABE). The main problem with KP-ABE is that only the encryptor can figure the content with some characteristic set and the key power keeps up some gateway arrangements. This key can be utilized by the receiver to decrypt the message. These roles are transposed in CP-ABE, the cipher texts is encrypted with a gateway arrangement by encryptor and key is made by an arrangement of aspects. So CP-ABE is more adaptable for DTNs as compared to KP-ABE [21].

[2.] Key revocation: Bethencourt et al. and Boldyreva et al. first proposed key revocation mechanisms in CP-ABE and KP-ABE. Their solution is to affix an expiration date or time to each attribute and distribute a new set of keys to valid users after the expiration. These intermittent trait recoverable ABE plans have two noteworthy problems. One problem is with respect to security fraudulency i.e. forward and in reverse mystery and the other is versatility problem [4].

[3.] Client revocation: A client revocable KP-ABE instrument was proposed by Golleet al. The issue of this plan is that it works just if the number of traits are half of the universe size [15].

[4.] Disruption- Tolerant Networking: K. Fall and M. Loubser presented a study of DTN protocol design-related issues and proposed the Delay-Tolerant Networking architecture as a solution to the DTN inter-operability problem. Few problems raised in other issues such as error detection, custody transfers, congestion control, buffer management, addressing, fragmentation, naming and binding were left untouched by them [17]-[18].

[5.] Decentralized ABE scheme: Huang et al. also proposed a decentralized ABE scheme in multi authority environment which accomplished a combined access policy over attributes issued by different authorities using a simple encryption algorithm [6].

[6.] Scalable Secure File Sharing: Plutus explained the mechanisms to 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 [16]. Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

III. PROPOSED WORK

DTN based correspondence systems are becoming more prominent specially appointed systems and are being sent in military applications to permit remote impromptu gadget to convey proficiently. Data needs to be dependably transmitted between the sender and recipient, so key administration assumes an essential part in giving information classification and security. CP-ABE based arrangements are extremely adaptable as compared with other cryptographic methodologies. In this paper we have proposed an effective and adaptable CP-ABE based methodology which can be used for secure information retrieval in military networks that work on DTN advancements.

IV. METHODOLOGY

The system architecture of DTN is as shown in figure given below. It consists of four main modules as follows:

1. Sender
2. Storage node
3. Receiver
4. Key authorities

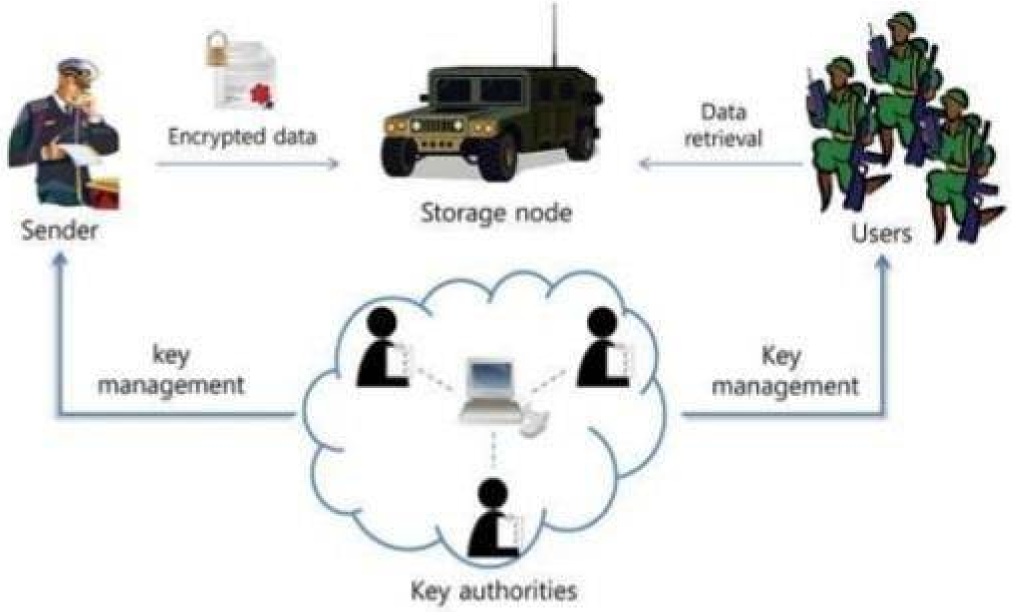

Figure 1: System architecture for DTN military network

1) **Sender**: Sender can be a commander who wants to send the data to the battalion. This data is stored in the storage node for easy sharing. Sender encrypts the data using the access policies.
2) **Storage Node**: Storage node receives the data from the sender, stores it and provides it to the receiver when needed. This node resides between sender and receiver. This node may be mobile or static. Storage node is semi-trusted.
3) **Receiver**: Receiver can be a soldier or battalion. It can access the data stored at storage node only if the receiver possesses a set of attributes that satisfy the access policy of encrypted data specified by the sender.
4) **Key Authorities**: Key authorities consists of central authority and many local authorities. We consider that the communication channels between central authority and each local authority during key generation is reliable and secure. Key authority generates public or secret parameter for CP-ABE. Each local authority is responsible to manage

different authorities. It also issues corresponding attribute keys to receivers. We assume that key attributes are true or loyal to their work but curious.

Key authorities are not allowed to access the plain text of data in the storage node but they can still issue a secret keys to receivers. As a contradictory requirement central authority and local authorities engage in the arithmetic 2PC protocol (2 Phase Commit protocol). This protocol prevents central authority and local authorities from knowing each other's secret key.

V. EXPECTED OUTCOME

Our proposed system is intended to enhance the security of military networks by using CP-ABE mechanism. It also aims to securely and efficiently manage the highly confidential and classified data distributed in the disruption- tolerant military network. Even if the storage server is untrusted the encrypted data can be kept confidential. Also our methods are secure against many types of attacks.

REFERENCES

1. Kaushik, Varadharajan, Rajarathnam, "Multi-user Attribute Based Searchable Encryption", IEEE 14th International Conference,Vol. 11, pp. 47-54, 2013.
2. Eric, Luis, Shigeo, Ana, Teruya and Francisco, "Software implementation of an Attribute-Based Encryption scheme", IEEE Transactions on Computers,Vol. 10, pp. 75-81, 2015.
3. Lu, Mario, Tuan Le, Vince, Haik, "Community Aware Content Retrieval in Disruption-Tolerant Networks", 13th Annual Mediterranean Ad Hoc Network Workshop,Vol. 8, pp. 19-23, 2014.
4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy,Vol. 11, pp. 47-54, 2007.
5. Xinlei,Zhang,Eve,Mihaela,"PerformanceEvaluationof Attribute-BasedEncryption:TowardDataPrivacyintheIoT",IEEECommunication andInformationSystemsSecuritySymposium,Vol. 9, pp. 34-40, 2014.
6. D.HuangandM.Verma,"ASPE:Attribute-basedsecurepolicyenforcementinvehicularadhocnetworks,"AdHocNetwork,vol.7,no.8,pp.1526–1535,2009.
7. Han,Jiang,Yang, "TheRevocableAttributebasedEncryptionScheme for SocialNetworks",IEEEInternational SymposiumonSecurityand PrivacyinSocialNetworksand Big Data,Vol. 5, pp. 46-51,2015.
8. JunbeomHurandKyungtaeKang,SecureDataRetrievalforDecentralizedDisruption-TolerantMilitaryNetworks,IEEE/ACMtransactionsonnetworking,vol.22,no.1,February2014.
9. J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in Proc. IEEE INFOCOM, Vol. 11, pp. 1–11, 2006.
10. S M. Chuah and P. Yang, "Node density- based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, Vol. 6, pp. 1–6, 2006.
11. D 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, Vol. 5,pp. 37–48, 2006.
12. G A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351,Vol. 9, pp. 22–28. 2010.
13. 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, Vol. 3, pp. 89–98, 2006.
14. ShuaiMa,Yang Cao, "Capturing Topology in Graph Pattern Matching" 38th International Conference on Very Large Data Bases August 27th - 31st 2012, Istanbul, Turkey. Proceedings of the VLDB Endowment, Vol. 5, No. 4, pp. 54-59, 2012.
15. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf.Comput. Commun. Security, Vol. 4, pp. 456–465, 2007.
16. 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.,Vol. 5, pp. 73–79, 2003.
17. K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Intel Research Berkley,Vol. 11, pp. 67-74, 2003.
18. M. Loubser, "Delay Tolerant Networking for Sensor Networks," SICS Technical Report, ISSN 1100-3154,Vol. 8, pp. 33–41, January 2006.
19. SribhashyamSathvik and K.M.V Madan Kumar, ―A Strategic Review on Cipher Text Policy Attribute Based Encryption‖. 2650-2654, Vol. 2, pp. 97–106, December 2014.
20. M. Chase, ―Multi-authority attribute based encryption, in Proc. TCC, LNCS 4329, Vol. 7, pp. 515–534, 2007.
21. VipulGoyal, Omkant Pandey, Amit Sahai and Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data" *ACM CCS*, Vol. 10, pp. 48–56, *2006*..