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 4, April 2016

Secure and Efficient Data Retrieval in Disruption-Tolerant Military Network

Aws Khaleel Ibrahim , Prof. Mohammed Tajuddin

M.Tech Student (Computer Network Engineering), Department of Computer Science and Engineering

Dayananda Sagar College of Engineering, Bangalore, India

Associate Professor, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, India

ABSTRACT: Disruption-tolerant network (DTN) improvements are becoming more fruitful results that remote devices can easily conveyed by the officers and access the secret information or data or summon dependably by way of abusing outside potential or storage nodes. Consequently a new methodology to furnish communication between others successfully and confidentiality of information is provided by dominant officers like superior officers or commander. The methodology is known as Disruption-Tolerant network (DTN). However, the difficulty of making use of CP-ABE in decentralized DTNs introduces manychallenges regarding safety and privacy.Our system is having integrated key feature of Hierarchicalattribute based encryption (HABE) and cipher text policyattribute based encryption (CP-ABE) system, so as to achieve high performance and fine grained access.

KEYWORDS: *ruption-Tolerant network (DTN);*

I. INTRODUCTION

Military environment is adverse and turbulent one.Thus, functions strolling on this environment needs more security to defend their data access and managetheir cryptographic ways. For communication to occur a node must be created and a connection situated between the node and the neighbour nodes in this networking environment should be established, but if there's no connection between the source and the destination the message from the source node may need to wait relying on when the connection might be eventually established [1].

The attribute-based encryption (ABE) concept is a promising process that fulfils the requisites in DTNs for the purpose of secure data retrieval. ABE points a mechanism that makes it possible for an access control over encrypted data making use of access policies and ascribed attributes amongst confidential keys and ciphertexts. Notably, ciphertext-policy ABE (CP-ABE) provides a scalable method of encrypting information in such way that the encryptor defines the attribute set that the decryptor needs to possess with in order to be able to decrypt the ciphertext [2].

The key authorities cannot be trusted as they are semi-trusted, and hence they should be deterred from gaining access to plaintext of the information present in the storage node; in the meantime, they should be still competent to issue users' secret keys also.

Secure retrieval of information is done using CP-ABE for decentralized Disruption-tolerant Networks.Attributes can be manipulated independently by multiple key authorities. A disruption-tolerant army community is carried out to manipulate the exclusive information distribution in a comfortable and efficient manner [6].

In this paper, we combined the concept hierarchical attribute-based encryption and cipher text policyattribute based encryptionin order to achieve secure data retrieval.

Challenges that applied in DTNs are: i) the issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related attributes sooner or later (for instance, moving their area), or some private keys may be bargained, key renouncement (or upgrade) for each one trait is fundamental with a specific end goal to make the frameworks secure.

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 4, April 2016

ii) However, this issue is significantly more troublesome, particularly in ABE frameworks, since each one characteristic is possibly imparted by different clients (hereafter, we allude to such a gathering of clients as a quality gathering)

iii) The otherchallenge is the key escrow issue. In CP-ABE, the key authority creates private keys of clients by applying the authority'smaster secret keys to clients' related set of attributes.

II. RELATED WORK

Many different functions tend to establish short time multicast groups for the supply of secure messages. Incredibly scalable result for dynamic multicast setup with a gaggle of members can be carried out by a novel design that enhances the technique of Ciphertext policy attribute-based encryption (CP-ABE) scheme. Attributes of the community are good covered under any situations of powerful attacks. The complexity of the scheme in phrases of the ciphertext dimension o(n) may be very gigantic the place n is the quantity of attributes within a community and it's unbiased of the size for each group [7].

Proxy re-encryption (PRE) algorithm allows the semi-reliable on proxy for changing the ciphertext into the originaltext. Negative attributes, multi-value attributes are supported with the aid of bringing out the ciphertext policy attribute based proxy re-encryption (CP-AB-PRE) scheme. Hence, a new access coverage centered on the access constructions of LSSS matrix was proposed in CP-AB-PRE scheme for non-interactivity, and encryptorsare allowed to analyse whether or not the ciphertext can be re-encrypted with the aid of making use of the access policy [8].

In Attribute-based Encryption (ABE) scheme attributes play a most important position and general public key generation is the major responsible of these attributes to encrypt the information and determines the access coverage to manipulate the access of the customers. Access structure of user's private key and cipher text-policy is Access policy. ABE scheme is carried out to decrease the conversation overhead within the internet and fine-grained having access is provided to manage the customers within the cloud environment [9].

A secure protocol is offered for information interchange which utilizes cross symmetric and uneven scheme for the interchange of initial informationwhich hides the information. Disruption tolerant system technology offers the special explanations to permit the conversation between the wireless instruments and to provide the access control of the secret information. An inclusive self-configured and secured set of directions is processed by using the scheme to share the security services and grants a new benefit that examining their reliable region [10].

Various applications have a tendency to establish temporary multicast organizations for the delivery of comfy messages. Tremendously scalable solution [1] for dynamic multicast setup with a bunch of individuals is finished by a novel design that upgrades the method Ciphertext policy attribute-based encryption (CP-ABE) scheme. Attributes of the network are well included under any instances of powerful assaults. The complexity of the scheme in context of the ciphertext size o(n) could be very large the place n is the quantity of attributes inside a community and it's independent of the scale for each and every group.

Proxy Re-Encryption (PRE) algorithm concede the semi-relied on proxy for converting the ciphertext into the plain textual content. Multi-value attributes, bad attributes are supported via introducing the ciphertext policy attribute based proxy re-encryption (CP-AB-PRE) scheme [3]. For this reason, a brand new entry coverage established on the access constructions of LSSS matrix is proposed in CP-AB-PRE scheme for non-interactivity and allows for the encryptors to investigate whether the ciphertext can also be re-encrypted via utilizing the entry policy.

III. METHODOLOGY

Ciphertextpolicy attribute-based encryption can also be viewed as a generalization of identity-based encryption. So similar to identification-based encryption process, there is a mastersecret keyand there is a single public key that can be used to make more limited number of private keys. Nevertheless, CP-ABE is more flexible than undeniable identification-centered encryption, in that it enables difficult principles specifying which personal keys can decrypt the cipher texts. The private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt[4].

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 4, April 2016

Figure 1: Secure Data Exchange with CP-ABE Approach

The ciphertext policy attribute-based encryption (CP-ABE) dependson how attributes and policy are associated with cipher texts and users' decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a client's decryption secret is related to set of attributes.

Data confidentiality: Unauthorized users who would not have enough credentials satisfying theaccess policyshould be deterred from getting access to the plain data in the storage node. Additionally, unauthorized access from the storage node or key authorities will have to be also prevented.

Sender: that is an element who claims confidential messages or information (e.g., a commandant) and wants to store them into an outer storage for simplicity of imparting or for accountable conveyance to clients within the strong systems administration circumstances. A sender is in command of characterizing (attribute based) accesspolicy and authorizing it all by myself know-how through scrambling the dataunder the access policypriorto storing it into the storagenode.

User: this is a versatile user that needs to get to the information stored in the storagenode (e.g., a fighter). In the case, a usermust have a set of attributesthat fulfils the policy to access the encoded data characterized by the sender.

Assigning various privileges to user according to the role they play in a top to bottom approach in an organization is the Hierarchical implementation. Organizations will be having various departments, all departments are controlled by central authority and each department has its head as local authority manipulate the entire workers working at his lower level. This is known as hierarchical implementation [3].

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 4, April 2016

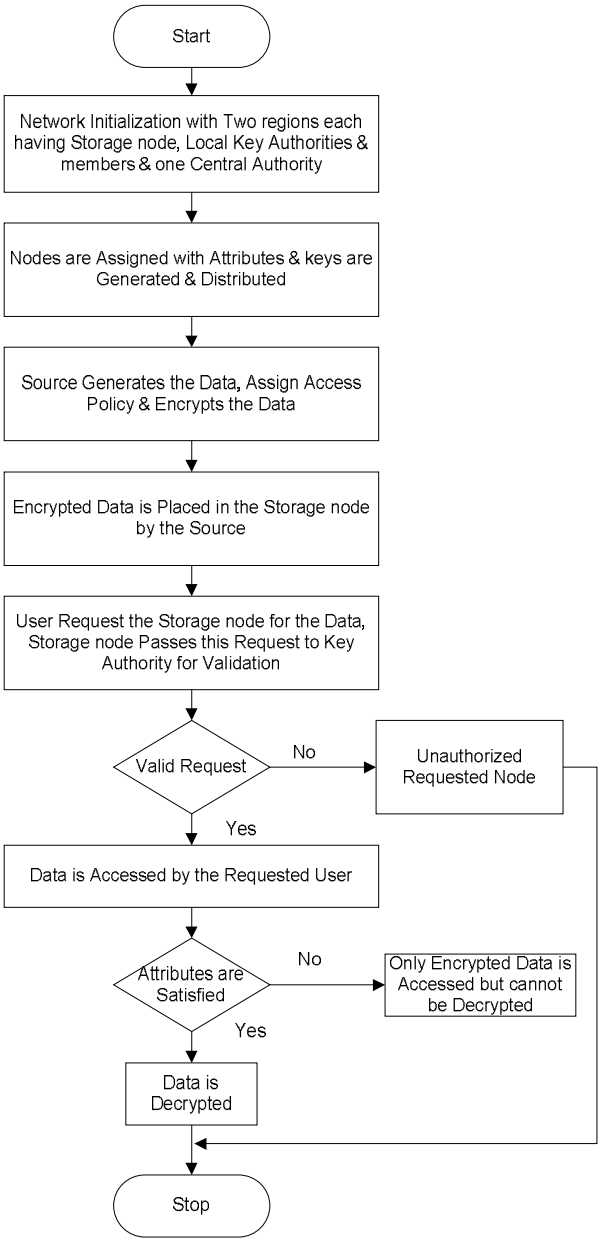

Figure 2: Flowchart of the Proposed System

The following four steps are steps of the CP-ABE: Setup, Key Generation, Encryption and Decryption.

Setup: The algorithm does not take any input apart of security parameter implicitly and it generates master key (MK) and public parameters (PK).

Key generation (MK,S): This step takes master key (MK) and attributes set S as input parameters and generates a private key (SK). The algorithm first selects the random $r \in_R Z_p$ and for each attribute j belongs to attribute set S. it generates a random r_j . Then it computes the key as in eq. (1).

$$SK = \left(D = g^{\frac{\alpha+\gamma}{\beta}}, \forall j \in S: D_j = g^r H(j)^{r_j}, D_j^i = g^{r_j}\right) \quad (1)$$

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 4, April 2016

Encrypt (PK,A, M): The public parameters PK, a message M, and an access structure A over the universe of attributes are considered as input parameters.The algorithm will encrypt M and generates ciphertext CT in such a way that a user possessing certain set of attributes that satisfies the access structure will be in a position to decrypt the message. Expect that the ciphertext implicitly contains A.

The ciphertextis then constructed by giving the tree access structureT and is computed as in eq. (2)

$$CT = \left(T, C = Me(g,g)^{\alpha s}, C = h^{s}, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H\left(att(y)\right)^{q_y(0)}\right) \quad (2)$$

Decrypt(PK,CT,SK): The ciphertext CT and the public parameters PK are given as input which involves an access structure A, and a personal key SK, which is a confidential key for a collection S of attributes. The algorithm will decryptthe ciphertext and return a message M only if the set S of attributes satisfies the access structure A.

IV. RESULTS

The concept of hierarchical is added along with CP-ABE technique. In this approach only valid user having certain attributes can access the data and each user has its own privilege. The user having certain privileges can decrypt the data.

Energy consumption: is the average energyrequired for sending 1 bit of data from source node to destination node. Energy consumption is calculated as eq.(3).

$$E = \left(\sum_{k=1} E_{transk} + \sum_{k=1} E_{Rxk}\right)/N \quad (3)$$

Here E_{transk} and $E_{Rxk}$are the energy consumption ofreception and transmission of node K. N indicates thenumber of data packets (in bits) which are successfully reached thedestination. Figure 4 shows comparison graph of Energy consumption

Packet delivery ratio: the ratio of the number of delivered data packet to the destination by the total number of sent packets. Which is given by the following relation:

$$PDR = \frac{\sum Number\ of\ packet\ received}{\sum Number\ of\ packet\ send}$$

The greater value of packet delivery ratio means the better performance of the protocol. The figure 4 shows the graph of packet delivery ratio.

Figure5 shows the total communication cost that the sender orthe storage node needs to send on a membership change in eachmulti-authority CP-ABE scheme. It includes the cipher-text andrekeying messages for non-revoked users. Communication cost is measured in bits.

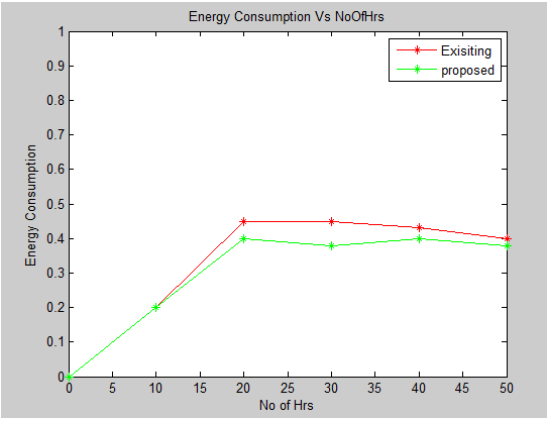

Figure 3: Comparsion of Energy Consumption with existing system.

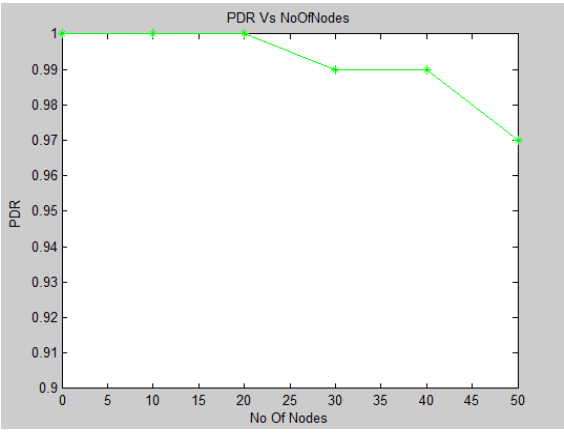

Figure 4: Graph of PDR.

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 4, April 2016

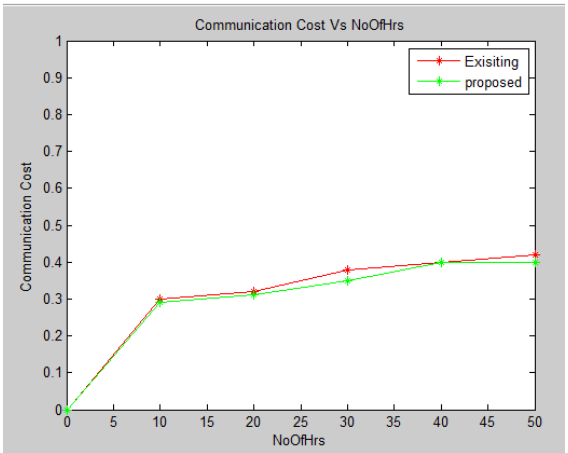

Figure 5: Comparsion of Communication Cost with existing system..

TABLE 1: COMPARISON TABLE FOR ENERGY CONSUMPTION

No.of Hrs	0	10	20	30	40	50
Existing System	0	0.2	0.45	0.45	0.43	0.4
Proposed System	0	0.2	0.4	0.38	0.4	0.38

TABLE 2: COMPARISON TABLE FOR COMMUNICATION COST

No. of Nodes	0	10	20	30	40	50
Existing system	0	0.30	0.32	0.38	0.4	0.42
Proposed system	0	0.29	0.31	0.35	0.4	0.4

V. CONCLUSION

DTNs are becoming very successful solutions for military applications that enables wireless devices to communicate with each other and access the confidential information reliably by availing external storage nodes. CP-ABE is a scalable cryptographic technique to the access control and secure data retrieval issues. In this dissertation, an efficient and secure data retrieval scheme using CP-ABE is proposed for decentralized military DTNs in which multiple key authorities manage their attributes separately. Our proposed system offers the few features: (1) excessive performance; (2) fine-grained access management; (3) scalability. Our CP-ABE scheme in DTN technologies is becoming victorious solutions in in military environments and navy purposes that enable wireless instruments to keep up a correspondence with each other and access the private know-how reliably by exploiting external storage nodes.

REFERENCES

[1] Miss. Arshiya Tabassum R.A.Khan, Miss. Ashwitha Reddy, "Securing DataRetrieval for Decentralized Disruption-Tolerant Military Networks (DTNs) using Cipher text-Policy Attribute-Based Encryption", International Journal of Engineering Research and Applications, 2015.

[2] Korra Bichya, "Secure Information Recovery for Decentralized Interruption Tolerant Defense Data Network", International Journal of Computer Engineering In Research Trends Volume 1, Issue 3, pp 119-126, 2014.

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 4, April 2016

[3] D. N. Rewadkar1 , V. S. Dhumal, "Hierarchical CP-ABE Scheme Implementation on Amazon EC2 cloud", International Journal of Science and Research (IJSR), Volume 3 Issue 7, 2014.
[4] Dr. Ananthi Sheshasaayee and K. Geetha, "An Efficient Presentation of Attribute Based Encryption Design in Cloud Data", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, 2015.
[5] Gubbala Siva Krishna, D Ramesh, "Attribute Based Secure Military Data Retrieval System for Decentralized Disruption Tolerant Networks", International Journal of Science Engineering and Advance Technology, Vol 3, No 12 (2015).
[6] B. Bhuvaneshwaran and A.Vijay, "Distribution of Secured Data Retrieval using Efficient Tolerant Military Network", Journal of Recent Research in Engineering and Technology, Volume 2 Issue 2 2015.
[7] Shucheng Yu, KuiRen, Wenjing Lou, "Attribute-based on-demand multicast group set up with membership anonymity", SciencedirectComputer Networks, pp 377–386, 2010.
[8] Keying Li, "Matrix Access structure Policy used in Attribute-Based Proxy Re-encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 2, November 2012.
[9] Cheng-Chi Lee, Pei-Shan Chung, and MinShiang Hwang," A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013.
[10] G.Mallika, Dr.P.Kuppusamy, "Protected records rescue for decentralized disruptiontolerant networks", International Journal of Science and Engineering Research (IJ0SER), Vol 2 Issue 10 October -2014.