Enhancing data security in DTN using 2PC protocol & 2Phase key technique

(PRITESH SONI, SIDDHESH PANDE, PANKAJ SHARMA, ANIKET SHRIMAWALE)

(DEPARTMENT OF COMPUTER ENGINEERING, SKN-SITS COLLEGE OF ENGINEERING, SAVITRIBAI PHULE PUNE UNIVERSITY, INDIA)

ABSTRACT

Mobile nodes in military 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 soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. This paper proposes a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. It demonstrates how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords: *Reverse circle cycle encryption, DTN, Key escrow, CP-ABE, Data tampering*

1. INTRODUCTION

In the hostile environment of military network, connections suffer frequent problems such as temporary connections, jamming, mobility, snoofing, etc. Disruption tolerant network (DTN) is the success full approach to communicate in such harsh networking conditions. Disruption Tolerant Networking (DTN) operates by implementing a store-and forward communication model between mobile users and carrier entities where a user delegates the carrier a task, the carrier stores it locally and whenever service connectivity is available tries to accomplish it, successively notifying the user of the task output next time they encounter again.in a battlefield DTN, a storage node may have some confidential information which should be accessed only by a member of 'Battalion 5' or a participant in 'Mission 4'. Several current solutions 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 conventional pairwise key or group key primitives. Thus, we still need to design a scalable solution that can provide fine-grain access control. In this paper, we describe a 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. Attribute-based Encryption (ABE) systems where encryption and decryption are determined by the attributes of the data and the recipients. An ABE cryptosystem is designed to enable fine-grained access control of the encrypted data. It allows the encryptor to attach attributes or policies to a message being encrypted so that only the receiver(s) who is (are) assigned compatible policies or attributes can decrypt it. Formally, the attributes can be considered as Boolean variables with arbitrary labels, and the policies are expressed as conjunctions and disjunctions of attribute variables.

CPABE uses multiple attributes of user to generate private keys. It makes use of master private key and one public key to encrypt and decrypt message. In reverse circle cipher arbitrary reversal factor coupled with arbitrary variable key length. Reverse circle cipher is capable of exploiting the benefits of confusion and diffusion because it uses reverse transposition and circular substitution. Input received by the system.

2. Organization of Paper:

While starting with literature survey we will discuss the proposed system with architecture and its test results. Then conclusion derived from the approaches we used and future scope of enhancement. At the end references used for preparing this paper are shown.

3. Literature Survey:

[1]CP-ABE scheme uses to unique specifications: (1) It use the attributes which are changing over time and dynamic. (2)The feature of revocation. [5] states that CP-ABE is designed to handle the flexible fine-grained access control like the authorized users will only be able to access the encrypted contents and each user will help in generating user's private key by incorporating the set of attributes it got.

[2]States that the CP-ABE provides efficient revocation as CP-ABE scheme is enhanced than before. The revocation problem which was earlier a big problem in public key encryption scheme is well studied concept in CP-ABE [5]. In the past several years have seen efficient revocation of certificates have been an active topic. CP-ABE considers expressive access control, efficient distributing and data confidentiality.

[3]Evaluation is followed by analysis of three aspects of designing CP-ABE: (1) User secret keys are associated with different set of attributes rather than for individual characteristics by the system manager. The fuzzy identifier thus is able to apply system revocation on a specific user. (2)Individuality of a node is defined by several common attributes and thus set of attributes or attributes cannot exclude misbehaving users with high accuracy. (3)The system shares some common attributes with non-revoked users though the system needs to be secure against collision attack from revoked users.

[4] States the study of feasible revocation operation in CP-ABE scheme: unique identifier revocation, attribute set revocation and single attribute revocation.

Attribute Based Encryption (ABE)

Implementation makes it possible for users to encrypt and decrypt messages based on their attributes. This paper focuses on implementing and designing ABE schemes with fast decryption algorithm. It needs constant number of pairing to decrypt a message in ciphertext provided by unbounded key-policy ABE (KP-ABE). It allows each user to tweak their settings independently for decryption in spectrum, from GPSW (i.e. slow decryption and short keys) to KP-ABE (i.e. fast decryption, longer keys).

4. Proposed System:

In this section, we describe our framework for handling secure data transaction in military disruption tolerant network system using strong network cipher techniques with the below mentioned steps as shown in figure 1.

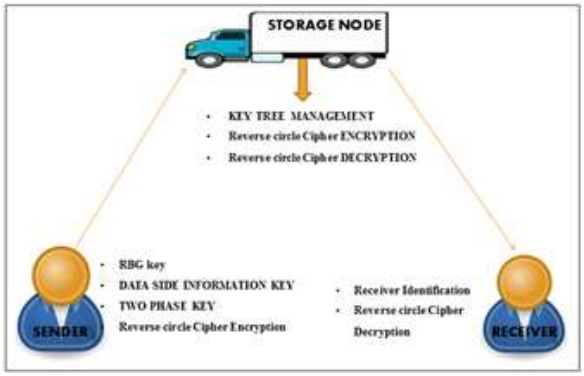

Fig -1: Architecture

Step 1: This is the most primitive step where all the data of the respective sender is been encrypted using Reverse circle cipher encryption with random key and then send to the storage node for its temporary storage .

Step 2: Here in this step one of the key of two phase key is been created using RBG mode using java security random key class.

Step 3: Here Random private key is generated using the random key generation for the data side information. This is shown as below.

ALGORITHM 1: RANDOM KEY GENERATION

Input: Set U = {u1, u2, u3…..un}

Output: Random Key (Rk)

Step 0: Get the User side information attribute set U

Step 1: Convert all the attributes to String type

Step 2: Concatenate all the String to get a single String

Step 3: Get the auto incremented User ID as I

Step 4: x=ID mod 7

Step 5: for i=0 to String length

Step 6: Fetch xth character from the String

Step 7: Continue till 7 characters are selected

Step 8: concatenate all the 7 characters

Step 9: return key

Step 10: Stop

(A) Random Key Generation

$$f(x) = \sum_{i=0}^{n} Ui \quad \text{.....(1)}$$

f(x) = side information concatenation function

n=no of attributes

Ui =side information attribute

Pk=P(f(x)) .....(2)

Pk= private key

P (f(x))= random key generation function

Step 4: Here in this step data send to the receiver is been stored in the storage node for the said time. And then this data is been allow to alter by the key authorities. And then this data is been delivered to the receiver using two phase commit protocol in the WLAN setup.

Step 5: This is the final step of the proposed model where the sender data is been encrypted using strong encryption technique of reverse circle cipher. Where the data is been divided into blocks which are been indexed to send for the further rotation based on the index value. Then each n character is been rotated based on the index value of the block. This cipher technique produces strong encryption technique over the network and this can be shown in the below algorithm

ALGORITHM 2: REVERSE CIRCLE CIPHER

Step 0: Start

Step 1: Get Input String S

Step 2 : Initialize a String ENC as empty

Step 3: Divide the string S in N blocks of size 10 characters

Step 4: for I =1 to N

Step 5: Let String BS =10 character of each block

Step 6: rotate block with I characters in clock wise

Step 7: for i=1 to 10

Step 8: substitute each character

Step 9: Replace character

Step 10: End of inner for

Step 11: ENC=ENC+BS

Step 12: End of Outer for

Step 13: Stop

Fig -2: Selection of Tab

Fig -3: Data browser tab where data can be uploaded to data server.

Fig -4: Key authority registration

5. Result and Discussion:

To show the effectiveness of the proposed system some experiments are conducted on java based windows machine using Netbeans as IDE in the wireless distributed LAN environment. And a developed system is put under hammer in many scenarios to prove its authenticity as mentioned in below tests.

5.1 Key Space Complexity

Key space is playing a vital role in the complete scenario as space required for the keys are always needed to be linearly dependent on the number of generated keys, which is successfully achieved by our system as shown in the figure 5

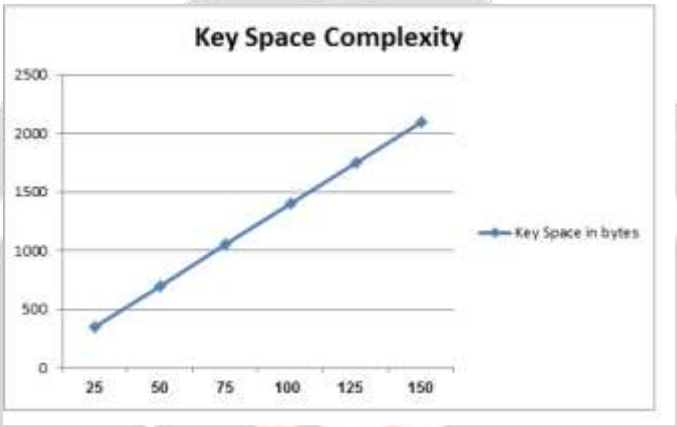

Fig -5: Key Space Complexity analysis

5.1 Character assignment for Encryption

The graph in figure 6 is drawn between the number of file character that are being used for the encryption and decryption v/s number of different characters that are using by the algorithm. Here in the above graph proposed system of key exposure system in web uses the character to encrypt while each rotation is being happened, this takes less characters to replace than of the most recent encryption models.

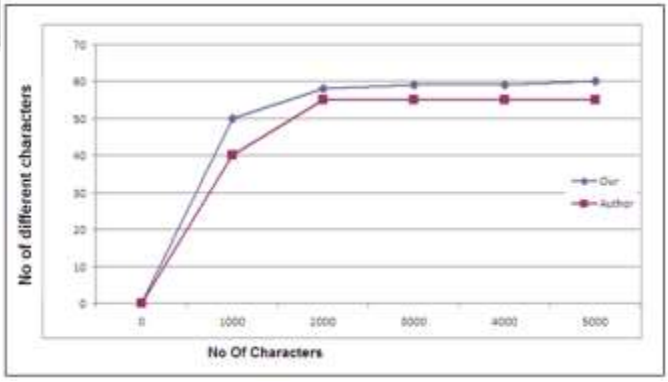

Fig -6: No of File character v/s No of Using different characters for the encryption and decryption

6. Conclusion:

All the respected studies in this paper clearly indicates many flaws in the existing systems. So to counter attack this, proposed system performs a detailed research on DTN, reverse circle cipher encryption, ABE, CP-ABE.

DTN technologies are becoming reliable and authenticated solutions in military applications that allow accessing the secret information without making storage nodes placed externally and communication between wireless devices vulnerable. CP-ABE is a scalable cryptographic solution for retrieving the confidentiality of data and provide access control. Using CP-ABE for secure data retrieval and making the system efficient where attributes are managed by multiple key authorities independently is the proposed concept of this paper. Under the hostile environments where key authorities might be compromised or not fully trustworthy the key escrow problem is fully resolved. In addition, fine-grained key revocation can be done for each attribute group.

7. References:

[1] "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Vipul Goyal, Omkant Pandey, Brent Waters, International Journal of network security, vol.15, July 2007.

[2] "Attribute-Based Encryption with Fast Decryption", Susan Hohenberger and Brent Waters, Theor.comp.sci.,422:15-38,2013.

[3]"Study of Various Cryptographic Algorithms", Mini Malhotra, Aman Singh,International Journal of Scientific Engineering and Research(IJSER), Vol. 1 issue 3, Nov. 2013.

[4] "Attribute-Ba sed Encryption With Verifiable Outsourced Decryption", Junzuo LaiDeng, R.H.Chaowen Guan , Jian Weng, Information forensics and security, IEEE transaction, vol. 8 issue 8, July 2013.

[5] "Secure data retrieval based on ciphertext policy attribute based encryption system for DTNs", S. Roy, M. Chauh, Lehigh University, 2009.

[6] " Ciphertext policy attribute based encryption", Waters B., Sahai A., Bethencourt J., IEEE Symposium on security and privacy, pp. 321-334, 2007.

[7] " Ciphertext policy attribute based encryption with anonymous access policy", Cheung L., K. Kuppusami,17th ACM conference on communication security, 2011.

[8] " Limitations of key Escrow in Identity based Schemes in Ad-Hoc networks", Hoeper K., Guang Gong, Security and privacy for emerging areas in communication network, IEEE, pp 403-405, Sept. 2005.

[9] "How to solve Key escrow problem in proxy Re-encryption from CBE to IBE", Ke Niu, Xu An Wang, Minqing Zhang, 1st International workshop on Database technology and applications, IEEE, pp 95-98, April 2009.

[10] "Reverse Circle Cipher for personal and network security", Ebenezer R.H.P, Isaac, Joseph H.R. Isaac, J. Visumathi, IEEE symposium on computer and communication security, 2013.

[11] "Enforcing reverse circle cipher for Network security using Multirotational Technique", Sajjade Zeba S., Gupta Aruna K., International journal of Advanced Research in computer science and software engineering, Vol. 4 Issue 3, March 2014.