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 8, August 2016

Tolerant Military Network

Dandawate Puja Baban[1], Bajare Sneha Mahad[2], Pradhan Sudipta Debansu[3], Bhagwat Shital Ramdas[4]

Department of Computer Engineering, Institute of Knowledge College of Engineering, Pimple Jagtap, India[1]

Department of Computer Engineering, Institute of Knowledge College of Engineering, Pimple Jagtap, India [2]

Department of Computer Engineering, Institute of Knowledge College of Engineering, Pimple Jagtap, India [3]

Department of Computer Engineering, Institute of Knowledge College of Engineering, Pimple Jagtap, India [4]

ABSTRACT: Military security implies the capability of a nation-state to defend itself, or deter military aggression. Alternatively, military security implies the capability of a nation-state to enforce its policy choices by use of military force. The term "military security" is considered synonymous with "security" in much of its usage. One of the definitions of security given in the *Dictionary of Military and Associated Terms*, may be considered a definition of "military security". The scope of military seciurity has expanded from conventional forms of conflict between nation-states to fourth-generation warfare between a state and non-state actors. In Militray Environment ,they are suffer intermittent network connectivity. So we are using the DTN(Disruption Tolerant Network) that allows the wireless network for military application to communicate each other and also soldiers can access confidential data by utilizing storage node in battlefield or hostile region to distress form the intermediate network connectivity and achieve secure data or some command by reliable to explore from external node. The most challenging thing in this cases are enforcement of authorized policies. Ciphertext-policy attribute-based encryption is a reliable cryptographic solution to access control problems. In this paper, by using CP-ABE for decentralized DTNs we define how to secure data and retrieval scheme where multiple key authorities manage their attributes independently and avoid the key escrow ,revocation, Coordination of attributes issued from different authorities. Scalability is provided by CP-ABE for data encryption and decryption. For decryption to take place the decryptor has to possess some attributes that matches or corresponds with the one defined by security policy of the access control. We described that how securely and efficiency manage the confidential data by applying proposed mechanism which is distributed in the disruption-tolerant military network.

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

I. INTRODUCTION

A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. In Military secure network, they are using wireless devices connections that may be disconnected primarily by connection jam, some environment factors and mobility, mostly when they operate in hostile environments. To communicate each other easily in these extreme networking environments i,e Disruption-tolerant network (DTN) technologies are used. When there is no any end to end connection in between source and destination pair and message from source node may wait on intermediate node for a substantial amount of time until the connection would be eventually established. In author define storage nodes in DTNs where data is stored in storage node or examined that only such mobile node can access necessary information quickly and efficiently. Disruption-tolerant network (DTN) is a technology which allows the node to communicate with each other in secure manner. It is one of the successful solutions for transferring the data in network. Most of the military users use this technology for secure transfer of the data. In military applications required increased protection of confidential data with access control method that are cryptographically enforced. Many of the cases it is desirable to provide different access service like data access policies are define over the user's attributes and roles, which are managed by the key authorities. For example,in a disruption-tolerant military network, on the storage node commander may store confidential data which is access by "Battalion A" who are participating in "Region B."

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 8, August 2016

The ABE is challenging approach which is fulfill the requirement of secure data in DTNs. ABE features a by using access policies it is mechanism of enable access control over the encrypted data and ascribed attributes among private keys and cipher text. One of the important thing is ciphertexts-policy ABE (CP-ABE) provided easier way of encryptor data such that the encryptor can described the attribute keys that to be need process bydescriptor and convert into ciphertext . However the user can decrypt the data on different way for security purpose. Hence, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Transportable nodes in military environments, for example, in an antagonistic area are horizontal to practice in endure of asymmetrical system network and numerous partitions. Disruption-tolerant network (DTN) modernisms are receiving to be productive results that authorize remote device conveyed by officers to speak with one another and admit the private data or secret data or beckon unvaryingly by neglecting outside capacity nodes or storage nodes. A DTN node can forward package between two or more other nodes in one of two situations they were Routing and Equivalent Forwarding. In DTNs, data where stored or pretend such that only authorized mobile nodes can entrée the required information rapidly and efficiently. At some point some users may change their associate attributes like user change the region or some private keys might be compromised, to make system secure key updating for each attribute is necessary. However, this issue is more difficult, especially in ABE systems, since each attributes shared by each user as we study multiple groups of users as attribute groups.

This defines that revocation of attributes or any single user of attribute group can effect on other users in group. Another challenge is the key escrow problem. In CP-ABE, generate private key for user by key authorities by applying the authority's master keys to user associated set of attributes. Thus, by creating attribute key, specific user can using key attribute decrypt every cipher text. The each key authority having complete privilege for create own attribute with own master secrets, the key escrow is an inherent problem in multiple authority system. A key generation method is based on signal master key and it is the basic method asymmetric encryption system as the attribute based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

II. **RELATED WORK**

In ABE **(**attribute-based encryption) is approach that fulfils the requirements for secure data retrieval in DTNs. In these define key revocation mechanism in CP-ABE and KP-ABE .In these have two main problem. The first problem is the security degradation in terms of the backward and forward secrecy. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering these as attributes. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is re encrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a cipher text is encrypted with a policy that can be decrypted with a set of attributes (embedded in the user's keys) for users with. The problem of applying the ABE to DTNs introduces many of 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.

III. EXISTING SYSTEM

In existing system, the coordination of attributes main issued from different authorities. When multiple authorities manage and issues attribute keys to users independently with their own master secrets, it is very hard to define indivisible key over attributes issued from different authorities i,e(fine- gained acesss policies). 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, or some private keys might be compromised ,key revocation(update key) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems. So there is some disadvantage of existing system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

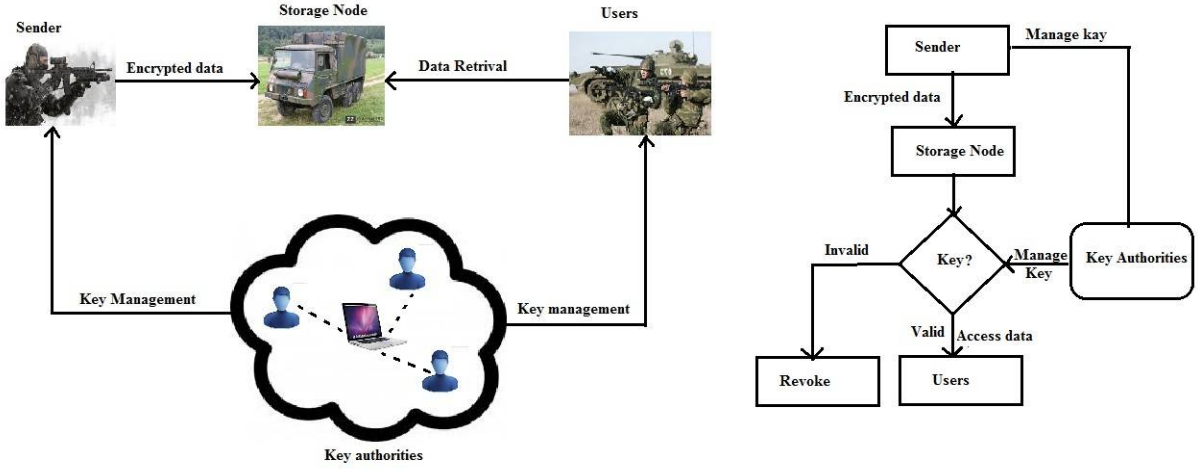
Vol. 4, Issue 8, August 2016

Disadvantages of Existing System:

1. *Attribute Revocation*:-In these ,the some key is changes that time each attribute an expiration date (or time) so after change key the key must update .
2. *Key Escrow*: The key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Author presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. One disadvantage of this fully distributed approach is the performance degradation.
3. *Decentralized ABE*: The main disadvantages of this approach are efficiency and expressiveness of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multi encrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively.

IV. PROPOSED SYSTEM

These is proposed architecture:



There are some modules :-

1.*Sender:* In these module, the user(i,e commander) sending confidentially data to the battalion. In these proposed system sender sending the data in the encrypted form by generating his own key and also he will get one key from the key authority. Hence message at commander side will be encrypted twice once by his own key and another by the key from key authority.

2.*Receiver*: In these module, the receiver receive the encrypted data from sender(i,e commander) and receiver get same key that are generate in sender side for encrypte the data and also receiver get the key from key authority. From these two key the data or message can be convert in decrypted form than receiver can get the real message or data.

3. *Storage Node:* In these module, the data or message that are in encrypte form are send by sender(i,e commander) that are stored in storage node.Whenever the receiver can take this data from storage node.

4. *Key Authority*-In these module, the key authority give the one key to the sender and another key to the receiver whenever the sender and receiver request for the key.

Advantages:

1.Data confidentiality: In these model ,the multiple key authorities do not have fully trust as well as storage node is honest .So the plain data are kept in secret from by them as well as unauthorized users.

2.Collusion –resistance: If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.

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 8, August 2016

3. Backward and forward Secrecy : In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy)should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand,forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

V. CONCLUSION

The conclusion of Remote controlling PC with Smartphone (Android mobile) Inputs from remote place with internet project is Smart phone and tablet universal remote software is usually highly customizable. As with traditional universal remotes some are programmed using the handset (phone/tablet) itself and others are programmed using a computer. remote control features, you can finally clean up your coffee table and put your extra remotes away in a drawer somewhere. Now your phone (or tablet) is your remote. At last your whole family (and even guests) will be able to figure out how to control all the different devices and inputs you have in the living room. A customizable remote control interface, where you decide exactly which buttons appear when you want them to. The dominant remotecontrol technology in home-theater applications is infrared (IR). Infrared light is also known as plain-old "heat." The basic premise at work in an IR remote control is the use of light to carry signals between a remote control and the device it's directing.

REFERENCES

[1] Noel Jerke And Michael Hatmaker "vbscripInteractive course". Published by Techmedia, ISBN NO 81-87105-55, January 1997.
[2] Scott Hawkins. “Apache Web Server Administration & E-commerce Handbook”. Published Edition Wesley Longman (Singapore) Pte Ltd, ISBN NO 81-7808-278-0, January 2001.
[3] Gerry O’Briena. “Microsoft IIS 5 Administration”. PUBLISHED By C.G.JAIN For TECHMEDIA, ISBN NO 81-7635-480-5, January 2000.
[4] Jeff Frentzen and Henry Sobotka. ”Javascript Annotated Archieves”. PUBLISHED BY TATA MC GRAWHILL TEC, ISBN NO 0-07-463612-x, January 1999.
[5] KhannaSamratVivekanandOmprakash “Email Scripting Language “. The 2008 International Conference on Internet Computing, PUBLISHED BY 2008 CSREA PRESS.
[6] Jaya BharathiChintalapati,SrinivasaRao T.Y.S, “Remote Computer Access Through Android Mobiles”, International Journal of Computer Science Issues,2012 vol.9,Issue 5,No.3
[7] Ha-Young Ko, Jae-Hyeok Lee, Jong-Ok Kim, Member, IEEE, Implementation and evaluation of fast mobile VNC Systems, IEEE Transactions on Consumer Electronics, Vol. 58, No. 4, nov 2012.
[8] H. Shen, “A high-performance remote computing platform,” Proc. of IEEE International Conference on Pervasive Computing and Communication (PerCom 2009), pp. 1-6, Mar. 2009.
[9] Justin Grover a,b,"Android forensics: Automated data collection and reporting from a mobile device", Digital Investigation 10 (2013) S12–S20, 2013