Volume 3, Issue 5, May-2016, pp. 237-240 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Secure Data Retrieval for Decentralized Disruption Tolerant Military Networks

[1]SHUBHAM P. VERMA ,[2] MAMTA S. MAHAJAN,[3] KALYANI M. ZAWAR, [4]TIPUSULTAN S. TADAVI

[1,2,3,4]Dept. of Computer Engineering,SSBT COET, Bambhori,Jalgaon, Maharashtra

shubhamvrm880@gmail.com, mamtamahajan811@gmail.com, Kalyanizawar09@gmail.com, Tipusultan0209@gmail.com

Abstract:- A battlefield or a hostile region are partitions in military environments . Intermittent network connectivity is major problem in such environment. Frequent partitions are there. A true and easy solution is Disruption-tolerant network DTN technologies. To interact with each other people in a military environment carries devices that are wireless. The confidential information is accessed by these devices and they command reliably by exploiting external storage nodes. DTN is very successful technology in these networking environments. When there is no wired connection between a source and a destination device, the information from the source node may need to wait in the middle nodes for a huge amount of time until the connection would be correctly established. ABE is one of the challenging approaches which is attribute-based encryption that satisfies the requirements for retrieving secure data in DTNs. An appropriate way of encryption of data is given by Cipher text Policy ABE (CP-ABE) .Decryption should possess an attribute set which was used during encryption in order to decrypt the cipher text. Hence, multiple users may be allowed to decrypt different parts of data according to the security policy.

Keywords – DTN, ABE, cipher text policy

1. INTRODUCTION

Passwords are used for access control, authentication and authorization. The password is selected by the user which can be both graphical and text based passwords. Users chooses memorable password, unhappily it means that the passwords should follow certain patterning that are very easy for assuming to the unknown person. The usability issues occur while allowing passwords to the user randomly, means user cannot remember the random passwords. Huge number of graphical password systems has been produced; text-based passwords suffer with both usability and security problem. We know that the human mind is good at remembering and recalling images than text, graphical passwords .For the authentication purpose the password method is very common Method. This passwords used for safely login to emails over internet, transferring of files and sharing of data and information. Password causes some drawbacks like forgetting the password, having less characters or very weak password, etc. So to secure all application and data, we have to provide a secure and strong authentication in the military areas as we are using passwords. Graphical password technique is the new technique introduced to provide high or strong authentication .The drawback of alphanumeric password is dictionary attack. Graphical password technique enhances the password techniques.

Graphical password technique is used as an alternative to the alphanumeric password. As human brain can capable of remembering the images, pictures so this technique is designed to overcome the drawbacks and weakness of the traditional technique. The shoulder surfing problem and usability problem are the main

drawbacks for the present graphical password technique. Even though graphical passwords are difficult to break and guess, though, the issue of how to design the authentication systems which have both the usability and security elements is still another example of what making the challenge of Human Computer Interaction (HCI) and security communities.

2. RELATED WORK

In the existing system, a empirical study of pass faces is carried out by Brostoff and sasse, which explains how a graphical password recognition system generally works. Blonder-style passwords are based on cued recall. In a single image, a user clicks on several previously chosen locations to log in. As implemented by Passlogix Corporation, in an image the user chooses several predefined regions as his or her password. The user has to click on the same regions in effect to log in, alternative to pass points, cued click points (ccp) is proposed. Rather than clicking on five points on one image users click one point on each of 5 images in ccp. It offers cued-recall and to alert instantly to valid users that if they have made a mistake when entering their latest click-point the visual cues are introduced. It also makes attacks based on hotspot analysis more challenging. Next-image is showed as a result of each click, in Effect leading by clicking on their sequence of points users down a "path". An incorrect path is there whenever there is a wrong click, with a certain hint of authentication failure only after the final click. Users select their images only to the extent that their click-point commands the next image. By disallowing user choice and assigning passwords to users the predictability problem can be solved, since users cannot easily remember such random passwords this usually leads to usability issues. Number of graphical password systems have been generated, researches shows that text-based passwords suffers with both usability and security problems. File sharing is done after authentication. In existing system, sharing of file is done with less security. As files are send to the military officers. There should be the high security given to that file. There is no such technique available which is used to secure the file by using the cryptography and graphical password. So our proposed system provides the secure file sharing in the military networks by using the graphical password technique and also catches the external attacks.

3. PROPOSED WORK

In this paper, an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs is proposed. Following are the achievements given by the proposed system. First, by reducing the windows of vulnerability, backward/forward secrecy of confidential data is enhanced by attribute revocation. Second, using any monotone access structure under attributes issued or expressed from any chosen set of authorities, encryptions can define a fine-grained access policy. Third, the problem of key escrow is determined through an escrow-free key issuing protocol that utilize the characteristic of the decentralized DTN architecture ,.By executing a secure two-party computation (2PC) protocol among their own master secrets with the key authorities, the key issuing protocol generates and issues user secret keys . The 2PC protocol deters the key authorities from retrieve any master secret information of each other such that the whole set of user keys alone is not generated by anyone. Thus, in order to protect their data to be shared users are not required to fully trust the authorities. The privacy and data confidentiality can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

3.1 Advantages:

1. Data confidentiality: In the storage node unauthorized or unwanted person who do not have enough authorization satisfying the access policy should be prevented for accessing the plaintext. In addition, from the storage node or key authorities unauthorized access should be also prevented.

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

3. Backward and forward Secrecy: In the circumstances of ABE, backward secrecy means that any user who comes to hold an attribute (that access policy is satisfied) should be deterred from accessing the plaintext of the previous data exchanged before he holds the attribute. Whereas, forward secrecy means that any user who drops an attribute should be deterred from accessing the plain text of the successive data exchanged after he drops the attribute, unless the other authentic attributes that he holds satisfy the access policy.

3.2. Challenges:

The problem of applying CP-ABE in decentralized disruption tolerant networks introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

3.3. Implementation:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it‟s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

3.3.1 Modules:

1. Key Authorities
2. Storage Nodes
3. Sender
4. User

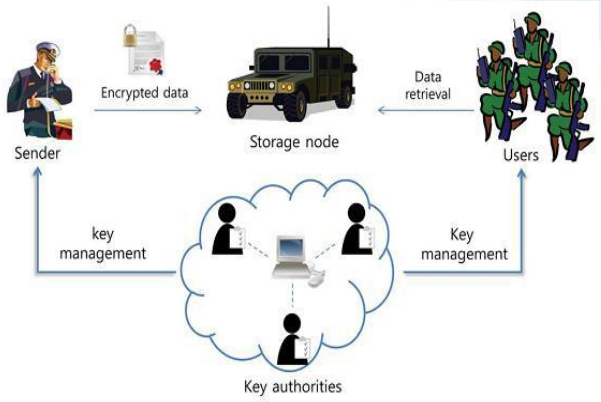

Fig 1.2: System Architecture and Module collaboration

3.3.2 Modules Description:

1. Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users‟ attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible.

2. Storage Nodes: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted that is honest-but-curious.

3. **Sender:** This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4. **User:** This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

4. CONCLUSION

Our project is not the unique one, but is an Endeavour attempt to have a precise scenario of what the terms “secure data retrieval for decentralized disruption

tolerant military network" is meant to be and its implementation as well on which we are currently working. As stated before, our proposed system can enhance the security of military network by using CP-ABE Technique. It is a scalable cryptographic solution to the access control and secures data retrieval issues. In this paper, an secure and efficient data retrieval method using CP-ABE for decentralized DTNs where attributes are separately manage by multiple key authorities is proposed. The inherent key escrow problem is resolved which guarantees the confidentiality of the stored data even under the hostile environment, where key authorities are not fully trusted or might be compromised. In addition, for each attribute group the fine-grained key revocation can be done. We demonstrate how to apply the proposed mechanism to efficiently and securely manage the confidential data distributed in the disruption- tolerant military network.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp.1–6.

[3] 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*, 2006, pp. 37–48.

[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[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] 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.*, 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[8] 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.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular

