Attribute Based Secure Data Retrieval System for Decentralized Disruption Tolerant Military Networks

Sagar L. Khairnar[1]
Comp Dept. BVCOERI
Nashik, India.
sagar.khairnar1169@gmail.com

Gayatri V. Patil[2]
Comp Dept. BVCOERI
Nashik, India.
gayatripatil.18@rediffmail.com

Pooja D. Bankar[3]
Comp Dept. BVCOERI
Nashik, India.
poojabnkr@gmail.com

Pooja P. Bharade[4]
Comp Dept. BVCOERI
Nashik, India.

Hemant D. Sonawane[5]
Comp Dept. BVCOERI
Nashik, India.
hd.sonawane@gmail.com

***Abstract*—** There are partitions in military environments such as a battlefield or a hostile region. They are likely to suffer from intermittent network connectivity. They are having frequent partitions. Disruption-tolerant network DTN technologies are is a true and easy solutions.DTN is a Disruption-tolerant network.It allows devices which are wireless and carried by peoples in a military to interact with each other. These devices access the confidential information or command reliably by exploiting external storage nodes. In these networking environments DTN is very successful technology. 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 intermediate nodes for a large amount of time until the connection would be correctly established. one of the challenging approach is a ABE. That is attribute-based encryption which fulfills the requirements for secure data retrieval in DTNs. The concept is Cipher text Policy ABE (CP-ABE).it gives a appropriate way of encryption of data. the encryption includes the attribute set that the decryption needs to possess in order to decrypt the cipher text. Hence, Many users can be allowed to decrypt different parts of data according to the security policy.

Keywords- *Military Networks, Encryption, Decryption, DTN, CP-ABE.*

*****

I. Introduction

For authentication, authorization and access control passwords are used. The password is selected by the user is predictable. This happens with both graphical and text based passwords. Users chooses memorable password, unfortunately it means that the passwords follow the predictable patterns that are very easy for guessing to the attacker. While allowing passwords to the user randomly the usability issues occurs, means user cannot remember the random passwords. There are number of graphical password systems has been developed; text-based passwords suffer with both security and usability problems. we well know that the human brain is better at remembering and recalling images than text, graphical passwords.

The password method is very common method for the authentication purpose. This passwords used for safely login to emails over internet, sharing of data and transferring of files. Password causes some drawbacks like forgetting the password, very weak password or having less characters etc, So to secure the data and all application we have to provide a strong authentication as we using passwords in the military areas. So to provide high or strong authentication the new technique is introduced called as graphical password technique. The drawback of alphanumeric password is dictionary attack. So the graphical password technique improves the password techniques.

So the as an alternative to the alphanumeric password graphical password technique is used. As human brain can capable of remembering the images, pictures so this technique is designed to overcome the weakness and drawbacks of the traditional technique. The main drawbacks for the current graphical password schemes are the shoulder surfing problem and usability problem. Even though graphical passwords are difficult to guess and break, Nevertheless, the issue of how to design the authentication systems which have both the security and usability elements is yet another example of what making the challenge of Human Computer Interaction (HCI) and security communities.

II. OBJECTIVES

To maintain the security in the military for sending the file the graphical password technique and the DTN technology is an efficient method. So this system is efficient and provides high security. Necessity for easy access and plan for rapid action, communication between military officers and security of data, fast and effective file sharing with strong security.

III. PROBLEM STATEMENT

Various graphical password schemes have been proposed as alternatives to text-base passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope speakers of any language.We propose and examine the usability and security of Cued Click Points (CCP), a cued-recall graphical password technique. Users click on one point per image for a sequence of images. The next image is based on the previous click-point. We present the results of an initial user study which revealed positive results. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to Pass Points saying that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. We also suggest that CCP provides greater security than Pass Points because the number of images increases the workload for attackers or a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security.

Alphanumeric password technique is traditional technique. Humans can remember pictures better than alphanumeric characters. To overcome the traditional password technique graphical password technique is used. To send the file securely in military (Defense, Air force, Navy), there is a need of high security to the file.

IV. EXISTING SYSTEM

In the existing system, Brostoff and sasse carried out an empirical study of passfaces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, the user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions in effect, cued click points (ccp) is a proposed alternative to pass points.

In ccp, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in Effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image.

While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems have been developed, Study shows that text-based passwords suffers with both security and usability problems After authentication there is a file sharing. In existing technology, file sharing is done with less security. As there is sending the file to the military officers. there should be the high security provide to that file. There is no such technique used to secure the file by using the graphical password and the cryptography. So our proposed system provides the graphical password technique and the secure file sharing in the military networks and also catches the external attacks.

V. PROPOSED SYSTEM

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptions can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

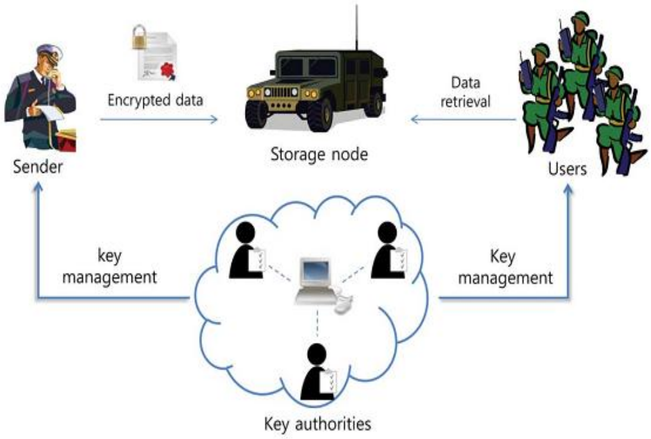
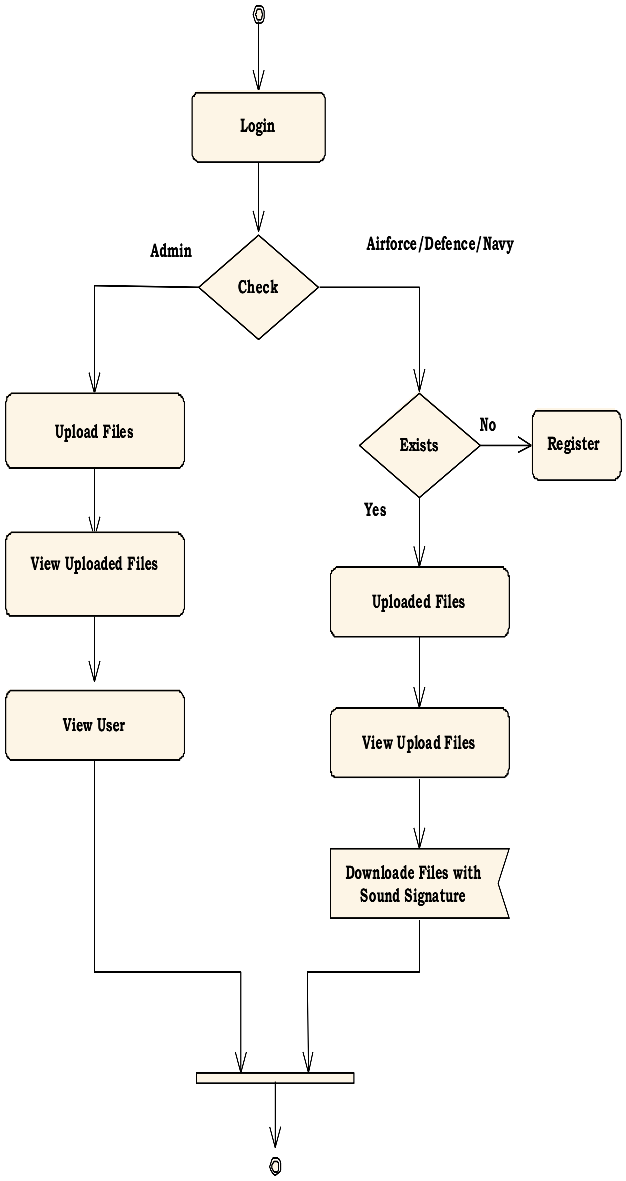


Figure 1: System Architecture

- Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.
- Collusion-resistance: If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.
- 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.

VI. ACTIVITY FLOW



VII. MODULES FOR DEVELOPMENT

A. VECTOR MODULE:

1. *Create User profile Vector(master):*

While registration of user information, the user id, sound frequency or time and tolerance are getting for creating master vector.
Master vector :
(User ID, Sound Signature frequency, Tolerance)

2. *Create Detailed Vector*

To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.
Detailed Vector - (Image, Click Points)

3. *Compare User Profile/login Vector:*

Enters User ID and select one sound frequency or time which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.

4. *Upload/Download Module:*

Admin, defense, navy and air force are going to upload secret file between them. They can share the uploaded files. User (defense, air force and navy) uses sound signature for download files. System showed very good Performance in terms of speed, accuracy, and ease of use. In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice the profile vector is created.

B. USER MODULE:

1. 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.

2. Soldier (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 cipher text and obtain the data.

C. ADMINISTRATOR MODULE:

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 node :

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.

CONCLUSION

We have proposed a novel approach which uses sound signature to recall graphical password click points. No previously developed system used this approach this system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text**.** In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network

ACKNOWLEDGMENT

It is my pleasure to express my knowledge to my respected sir Mr. H. D. Sonawane, Computer Engineering, BVCOE&RI, Nashik for his valuable guidance, inspiration and continues support. This paper could not be success without secure algorithm done which help to understand the necessity for this paper.

REFERENCES

[1] *Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.*

[2] *Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.*

[3] *Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.*

[4] *Cranor, L.F., S. Garfinkel. Security and Usability. O'Reilly Media, 2005.*

[5] *R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.*

[6] *A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.*

[7] *D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.*