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. 2, Issue 4, April 2014

Graphical Password Authentication in ATM Systems

Prof. K. sekhkar , B. Ramakantha Reddy, A. Nageswara Rao

Professor, Dept. of CSE, S V College of Engineering, Tirupati, A.P, India

Assistant Professor, Dept. of CSE, S V College of Engineering, Tirupati, A.P, India

Professor, Dept. of CSE, S V College of Engineering, Tirupati, A.P, India

ABSTRACT: Authentication is one of the important security approaches to protect user privacy in computer based and internet based environments. Common approach for user authentication is using Personal Identification Number (PIN) and smart card. PINs are vulnerable to various attacks. Tendency of users to choose short passwords or easy passwords makes the passwords vulnerable to various attacks like hidden video recording attack, key-loggers and spyware attacks. Other alternate solution to textual passwords is graphical passwords. Graphical password has a visual element in it, like an image or pattern. There are different mechanisms for graphical authentication such as recognition based and recall based techniques. These passwords are now being used in smart phones, workplaces and login applications. Even though these graphical passwords are easy to remember and use they are not safe from shoulder surfing attack. Shoulder surfing is a major security issue in Automated teller machine (ATM) systems. Here we propose an advanced graphical password approach for ATM systems that tries to overcome the disadvantages of earlier existing approaches.

KEYWORDS: Graphical Password, Authentication, ATM System, Registration, Login

I. INTRODUCTION

Authentication is the process to give access to users to particular system and resource. There are many authentication schemes in the current state like Token based authentication, Biometric based authentication, Knowledge based authentication. User authentication is very important in information security to protect user privacy. The traditional approach used for authentication is entering the user name and passwords. The textual passwords are short and they are easy to remember and are predictable or if textual passwords are long then it is hard to remember. Users who
fail to choose and handle passwords open hole for attacks like hidden camera, spyware attack and key-loggers. These methods based on passwords and pins rely on limitations of human capacity of recollection. On the other hand many biometric authentication methods have been proposed.

In this paper focus is on a knowledge based approach using pictures as passwords. Graphical passwords have been proposed as a suitable alternative to text based schemes, as it is possible for human to remember picture better than text. The password space would be large compared to that of text based schemes which offers better resistance to attacks. Using graphical password user clicks on image to authenticate themselves rather than alphanumeric string. These graphical passwords are anticipated to be more robust than text-based passwords. Several studies have shown that humans remember images more easily compared to text. Graphical passwords hope to leverage visual information and in turn make it easier for users to select more secure passwords.

The graphical-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. The graphical password authentication method will briefly describes the difficulties users have with traditional passwords.

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. 2, Issue 4, April 2014

II. RELATED WORK

In [1] they have proposed a Graphical Password schemes resistant to shoulder surfing. In this scheme the user draws a curve across the selected images in the same order that he had selected during registration. The image grid contains decoy images to resist shoulder surfing.
In [2] the user has to draw some pattern as password and a scanner scans that pattern and registers automatically. There are two softwares, one of them guides for the user while drawing and the other does registration process
In [3] the approach is based on the capacity of users to recognise the well known faces. An image grid with three human faces in each row is displayed. The user has to specify the number of human faces that he knows is Even or Odd.
In [4] each user is given a different set of images, from which he has to select two images. The image set is based on some calculation which involves the position of characters in alphabets.
[5] Describes two approaches. One is the pair based authentication. Here the user has to select 8 pair of images. He has to match the images with its pair during authentication as well. The other approach is text based image authentication. In this a set of images are selected by the user and a character is assigned to each image. During authentication images are displayed.
In [6] the user has to select 4 single digit numbers as password and place them in a grid with 16 positions. During authentication grid with 16 positions containing numbers from 0-9 is displayed at random positions is displayed.
In [7] User finds all original pass-characters that were selected and clicks inside invisible triangles created by characters. Different session characters are entered that are chosen from inside or on the border of pass-triangles formed in previous step.
In [8] implementation of coloured keyboards is proposed. Every characters and alphabets are shuffled every time after the user clicks on the key. Before clicking on the key the user has to note down the position of the key, then he has to press a button caption “Hide Keys”, which will hide the characters. If the user clicks on the correct position of alphabets then he will be given access.

III. MOTIVATION

The following points are observed from the above related work. It illustrates the following disadvantages which led to proposal of a new graphical password approach.

AUTHOR	DRAWBACK
Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu	Curve contains even the unselected images there is a possibility that curve drawn randomly by an unknown user may contain the selected images
Salem Jebriel, Dr. Ron Poet	Shoulder surfing is the major drawback
N. López, M. Rodríguez, C. Fellegi, D. Long	If a person knows the user well he can guess the faces which are known to the user
ShraddhaM,Gurav,Leena S. Gawade ,Prathamey K. Rane,Nilesh R. Khochare	Image set contains many images, so selection of images from that large set may be difficult for the user.
M Sreelatha,M Shashi , M Roop teja,M Rajashekar and K Sasank	User has to write the corresponding character assigned to each image
Mirang Park, Yoshihireo Kita, Kentaro Aburada, Naonobu Okazaki	User has to rearrange the numbers in his password so that they come in proper positions as arranged during registration Shoulder surfing
Huanyu Zhao and Xiaolin Li	Several clicks have to be performed.
M.Agarwal, M.Mehra, R.Pawar ,D.Shah	Remembering the position of alphabets is difficult

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. 2, Issue 4, April 2014

IV. PROPOSED SYSTEM

In the proposed system we use knowledge based authentication technique which involves using pictures and a mapped text based passwords.

The graphical password technique used is recognition based method. Here the user needs to remember sequence of images that he had selected during registration. During authentication user selects correct sequence of images. Once he chooses the images correctly he is authenticated and after the transaction positions of images are altered randomly so that shoulder surfing is minimized. In addition to this it is difficult for the intruders to remember picture passwords observed by shoulder surfing.

The graphical password uses 16 images which are of 4*4 grid. Each image has unique character associated with it. For each login session the images are randomly scattered or they are shuffled across the grid.

V. WORKING METHODOLOGY

Following are the steps implemented in the proposed Graphical Password scheme.

1) Selection of image password

At the Registration phase the user is prompted to enter the user id and is presented with a 4*4 grid onsisting of 16 images. The user id is unique and the users can select few images as their password.

2) Mapping of images

All the images displayed in the grid are mapped to unique characters. On each selection of the image its corresponding character is stored in the database. On entering a unique user id and selection of password the details are stored in the database and the user gets successfully registered.

3) Shuffling of images

At the Login phase, the user enters the unique id that he had entered during Registration phase. The image grid is displayed in which the user selects the images in the same order that he had chosen at the time of Registration. On successful login the user can carry out transactions. After each login the image positions are changed randomly or the images get shuffled.

4) Transaction Process

At the Transaction phase the user can carry out transaction and collect the amount. The relevant details are retrieved from the database and are checked against user's input and appropriate action is taken. The new details get updated in the database.

VI. WORKING ALGORITHM

The graphical password approach proposed in this paper is shoulder surfing resistant. It involves using images as password that are shuffled randomly on each login. On selection of each image password it is mapped to a unique character. The algorithm for the same is given below.

Step 1: Generate two random numbers I and j
Step 2: Check if image is assigned to a button while image is assigned Move to the next button until an unassigned image is recognized
Step 3: Assign that image to the current button
Step 4: Move the character corresponding to that image into a character array. Step 5: Set the image as assigned image
Step 6: Move to choose the next image.
Step 7: Continue the steps 1 to 6 until all the buttons are assigned image./*Mapping is done when the button is clicked*/
Step 8: When button is clicked concatenate the character corresponding to the image which has been stored in the character array to the password, which is a string.

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. 2, Issue 4, April 2014

Step 9: Perform step 8 for the buttons clicked.

VII. RESULTS

During registration first step is to accept user name and user id. Window for accepting that is shown in figure 1.

Figure 1: Window to accept user id.

After accepting user id, picture grid containing 16 images is displayed. From that user has to select few images as shown in Figure 2.

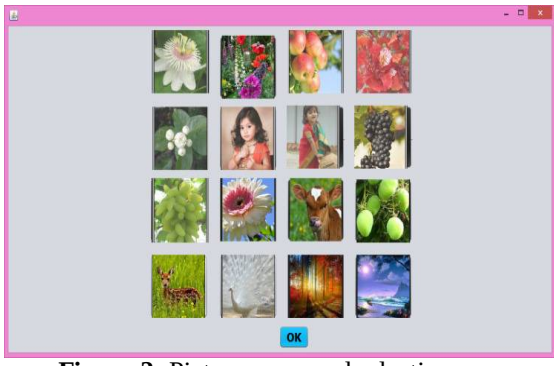

Figure 2: Picture password selection.

If the user id does not exists already, then user data and passwords are stored in the database and a message informing the user about successful registration is displayed as in Figure 3.

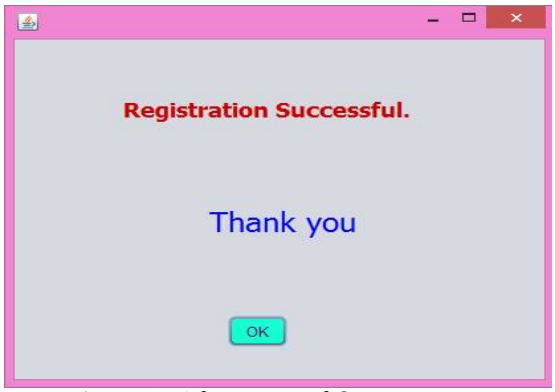

Figure 3: After successful registration.

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. 2, Issue 4, April 2014

If a user enters an id that already exists in the database (duplicate id) as shown in Figure 4 then while saving a message informing this is displayed as in Figure 5 and registration process restarts.

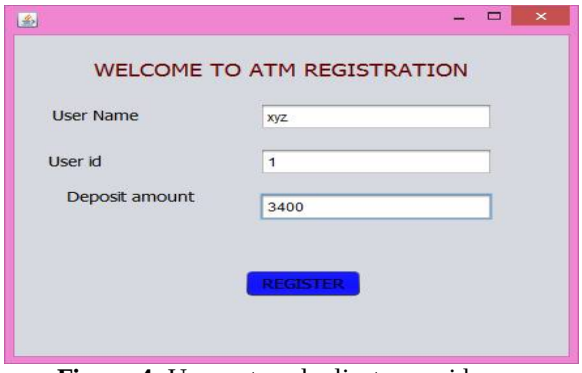

Figure 4: User enters duplicate user id.

Figure 5: Informing about duplicate user id.

At login phase user is prompted to enter the unique id that was selected during registration phase as shown in Figure 6.

Figure 6: Welcome window for login

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. 2, Issue 4, April 2014

After entering the user id the image password is selected. The images are selected in the same order as it was chosen during registration. It is shown below in Figure 7.

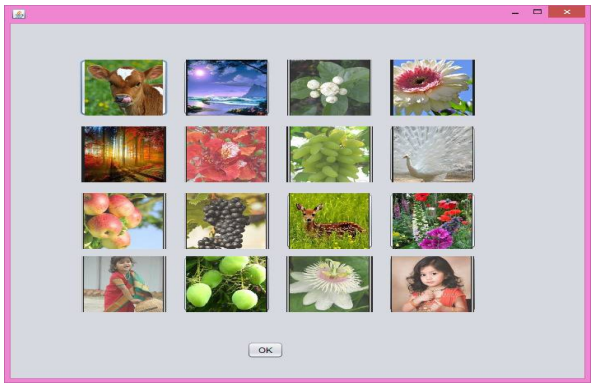

Figure 7: Read picture password.

If the login fails then a message is displayed as wrong password or id as shown figure 8 and the login process restarts as shown in Figure 9.

Figure 8: Unsuccessful login.

Figure 9: Retry logging in.

The user is given 3 attempts to enter the correct details on giving wrong input. After 3 attempts the user is blocked as shown in Figure 10.

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. 2, Issue 4, April 2014

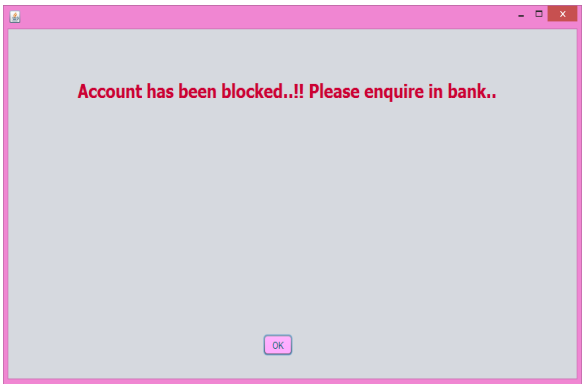

Figure 10: User has been blocked.

On successful login the transaction process starts immediately prompting the user to enter the amount. It is shown in Figure 11.

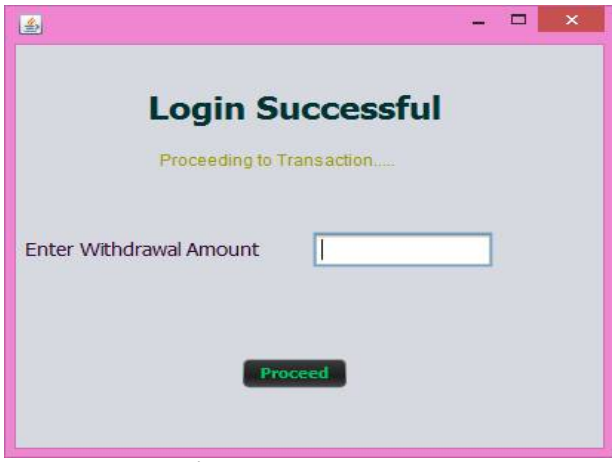

Figure 11: Transaction

The details are retrieved from the database and checked against user's input and appropriate message is displayed as in Figure 12.

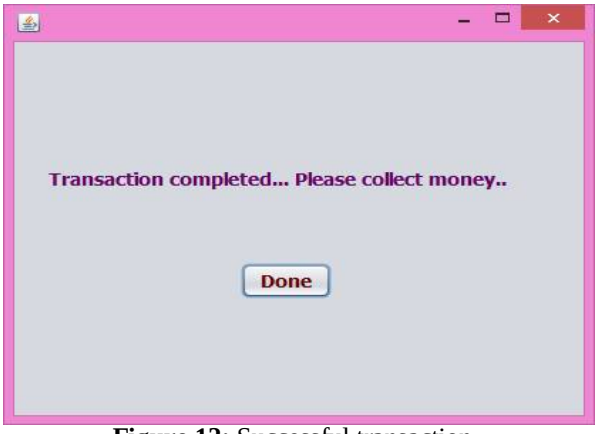

Figure 12: Successful transaction.

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. 2, Issue 4, April 2014

If the user's input doesn't meet the criteria then transaction is cancelled and it is informed to the user as shown in Figure13.

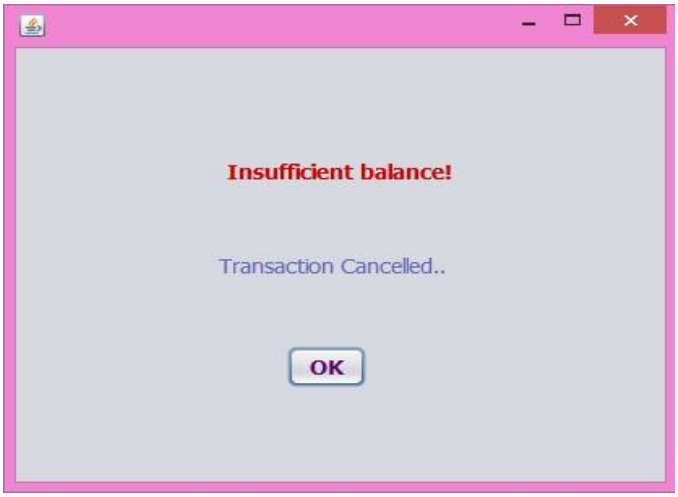

Figure 13: Cancelled Transaction

V. CONCLUSION

In this project we have used a new graphical passwords approach, this is found to be more secure than the existing approaches for minimizing shoulder surfing attack. But this approach is not resistant to hidden camera attacks. So our next work is to introduce audio password concept in addition to this graphical password. Here user has to choose one audio clip as his audio password during registration. During login user will be able to hear few audio clips in headphones which is kept in ATM room. He has to select the correct audio password along with image password.

REFERENCES

1. Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, "A New Graphical PasswordScheme Resistant to Shoulder-Surfing" 2010 International Conference on Cyberworlds.
2. Salem Jebriel, Dr. Ron Poet, "Automatic Registration of User Drawn Graphical Passwords", 2014 6th International Conference on CSIT.
3. N. López, M. Rodríguez, C. Fellegi, D. Long," Even or Odd: A Simple Graphical Authentication System", IEEE LATIN AMERICA TRANSACTIONS, VOL. 13, NO. 3, MARCH 2015.
4. ShraddhaM,Gurav,Leena S. Gawade ,Prathamey K. Rane,Nilesh R. Khochare," Graphical Password Authentication Cloud securing scheme", 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.
5. M SREELATHA, M SHASHI, M ROOP TEJA, M RAJASHEKAR and K SASANK, "Intrusion Prevention by Image Based Authentication Techniques", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590- 8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011.
6. Mirang Park, Yoshihireo Kita, Kentaro Aburada, Naonobu Okazaki, " Proposal of Puzzle Authentication Method with shoulder-surfin Attack Resistance", 2014 International Conference on Network-Based Information Systems.
7. Huanyu Zhao and Xiaolin Li," S3PAS: A Scalable Shoulder-Surfing Resistant Textual- Graphical Password Authentication Scheme", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 0-7695-2847-3/07 $20.00 © 2007.
8. M.Agarwal, M.Mehra, R.Pawar ,D.Shah," Secure authentication using dynamic virtual keyboard layout",ICWET'11 Proceedings of the International Conference & Workshop on Emerging Trends in Technology Pages 288-291 ACM New York, USA @2011.
9. Shailesh N. Sisat, "Duplicate and Fake Currency Note Tracking In Automated Teller Machine (ATM)" International journal of Electronics and Communication Engineering &Technology (IJECET), Volume 5, Issue 1, 2014, pp. 11 - 15, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.