International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 5, October 2012 www.ijcsn.org ISSN 2277-5420

Graphical User Authentication for E-Transaction

[1]Dr. Manish Manoria, [2]Ankur Jain

[1]Director, Truba Institute of Engg. and Information Technology, Bhopal, M.P. , INDIA

[2]Department of CSE, Truba Institute of Engg. and Information Technology, Bhopal, M.P. , INDIA

Abstract

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. Recently, E-transactions have become an important tool to carry out financial transactions besides the orthodox banking transactions. They are increasingly being used to make payments, access bank accounts and facilitate other commercial transactions. In view of their increased importance there is a compelling need to establish ways to authenticate user during E-transactions. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the orthodox authentication system and may be more convenient for the user. Our scheme is resistant to Phishing attack and many other attacks on graphical passwords. This scheme is proposed for E-transactions used to make payments and commercial transactions etc.

Keywords *- E-transactions, Graphical Passwords, Authentication, Security*

1. Introduction

Most initial computer applications had no or at best, very little security. This continued for a number of years until the importance of data was truly realized. Until then, computer data was considered to be useful, but not something o be protected. When computer applications were developed to handle financial and personal data, the real need for security was felt like never before. They are increasingly being used to make payments, such as at retail shops, public transport, paid parking areas and also to access the bank accounts via internet. While accessing bank accounts via internet it is necessarily essential that user should first authenticated. Authentication should be reliable, secure and resistant to all the possible attacks. During E-transactions it is essential that user should authenticate before any money transaction.

In this paper, considering the problems of text based password systems, we have proposed a new graphical password scheme which has desirable usability for E-transaction authentication. Our proposed system is new graphical passwords based hybrid system which is a combination of recognition and recall based techniques and consists of two phases. During the first phase called Registration phase, the user has to first select his username and a textual password. Then objects are shown to the user to select from them as his graphical password. After selecting the user has to draw those selected objects on a screen using device. Then in the last step select the pictures for recognition based system. During the second phase called Authentication phase, the user has to give his username and textual password, then give his graphical password by drawing it in the same way as done during the registration phase and then recognized and identify the images selected during the registration phase. If they are drawn correctly the user is authenticated and only then he/she can access his/her account.

TABLE I

PRIMARY CONCERNS IN WIDESPREAD ACCEPTANCE OF GRAPHICAL PASSWORDS FOR USER AUTHENTICATION

a)	*Security:* It is hard to break and obtain graphical passwords using the traditional attack techniques and phishing website because it uses images.
b)	*Reliability:* It is more reliable than other authentication technique because it does not depend on human parts and cards; they are less reliable because authentication is depended on elements.
c)	*Password space:* Infinite password space.
d)	*Attacks:* Resistant to possible attacks due to its complexity.

2. Classification of Current Authentication Methods

Recently, events of thefts, hacking, phishing and unauthorized access; authentication process has become more important for an individual and organization to provide an accurate and reliable means of authentication. Currently the authentication methods can be broadly divided into three main areas. Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication.

A. Token Based Authentication

Two-factor authentication is a security process in which the user provides two means of identification, one of which is

typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it.

B. Biometric Based Authentication

Biometric authentication has been widely regarded as the most foolproof - or at least the hardest to forge or spoof. Since the early 1980s, systems of identification and authentication based on physical characteristics have been available to enterprise IT[10]. These biometric systems were slow, intrusive and expensive, but because they were mainly used for guarding mainframe access or restricting physical entry to relatively few users, they proved workable in some high-security situations. A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamic. Biometric identification depends on computer algorithms to make a yes/no decision. It enhances user service by providing quick and easy identification.

C. Knowledge Based Authentication

Knowledge-based authentication (KBA) is an authentication scheme in which the user is asked to answer at least one "secret" question. It include both text based and picture based passwords (Graphical Password Based System). Knowledge-based authentication (KBA) is based on “Something You Know” to identify you for example a Personal Identification Number (PIN), password or pass phrase. It is an authentication system in which the user is asked to respond at least one "secret" question. KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics.

TABLE II

CLASSIFICATION OF GRAPHICAL PASSWORD BASED SYSTEM

a) *Recognition based Systems:* In this system (Searchmetric/Recognition Systems) user has to recognize the previously registered image for the authentication Research shows that it is possible for the majority (90%) of users to remember their password after one or two months[7].
b) *Pure Recall based Systems:* In this system (Drawnmetric/Recall Systems) user has to draw a copy of something that he/she drawn or produce earlier during the registration stage.
c) *Cued Recall based:* This system is also known as Iconmetric system. Pre-determined image put in front of the user on a screen and user should be point to one or more predetermined positions on the image (tap regions) in a predetermined order as a way of point out his or her authorization to access the resource.
d) *Hybrid Systems:* This system is typically a combination of two or more systems.

3. Previous Work

Dhamija and Perrig [2] proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program (Fig 1). Later, the user will be required to identify the preselected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

“Passface” is a technique developed by Real User Corporation. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces (Fig 2). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures [1].

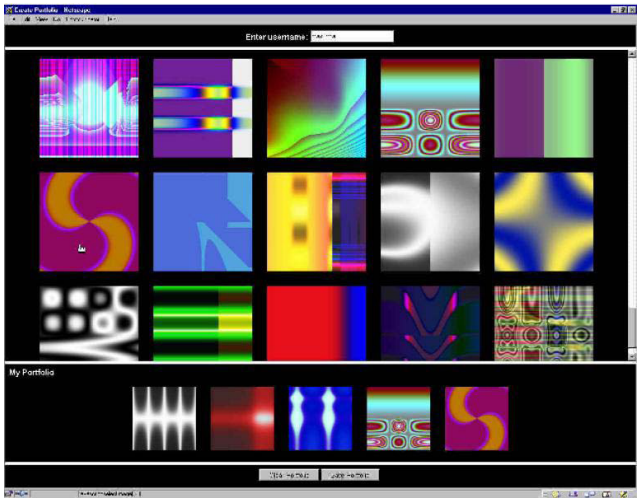

Fig.1. Random Images used by Dhamija and Perrig

Fig.2. an example of Pass faces

Thorpe and van Oorschot [3] further studied the impact of password length and stroke-count as a complexity property of the DAS scheme. Their study showed that stroke-count has the largest impact on the DAS password space. The size of DAS

password space decreases significantly with fewer strokes for a fixed password length. The length of a DAS password also has a significant impact but the impact is not as strong as the stroke-count. To improve the security, Thorpe and van Oorschot proposed a "Grid Selection" technique. The selection grid is an initially large, fine grained grid from which the user selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password (Fig 3). This would significantly increase the DAS password space.

Jermyn [5], et al. proposed a technique, called "Draw- a - secret (DAS)", which allows the user to draw their unique password (Fig 4). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

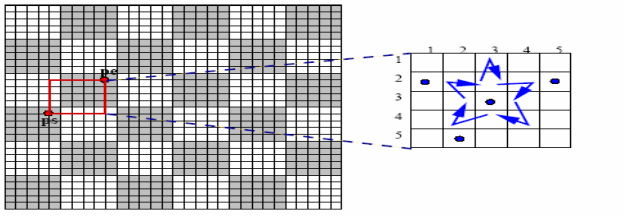

Fig.3 user selects a drawing grid (Thorpe and Oorschot)

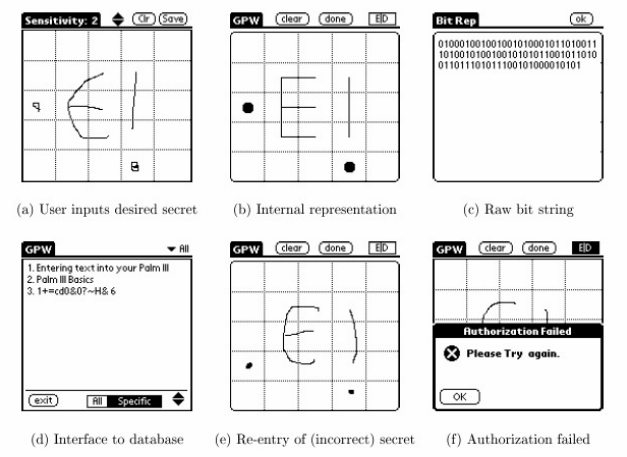

Fig.4 Draw-a-Secret (DAS) technique proposed by Jermyn

4. Problem Formulation

Till now the work done over graphical passwords is for mobile devices and touch screen systems (i.e. PDA)[4]. We are supposed to develop the system that will be used for E-transactions and helpful in authenticating the user during transactions.

There are many problems with each of the graphical based authentication methods which are to be analyzed and to solve. If we talk about the bank transactions, confidential data and financial information it needs an authentication system which is reliable, secure and usable. There is a compelling need to establish ways to authenticate people during transactions. Computer systems and the information they store and process are valuable resources which need to be protected. Computer security systems must also consider the human factors such as ease of a use and accessibility [6].
Now it is a need to have secure authentication system. So we have proposed a new hybrid graphical password based system, which is a combination of textual, recall and recognition based techniques that offers many advantages over the existing systems and may be more secured for the user. It is a three step authentication process for user authentication which is more secure and convenient to use.

Recently, it has seen that graphical based password system are not using during bank transaction. It is more secure than the orthodox transaction system.

So, we are developing the graphical password system that can be useful for E-transaction authentication.

5. Proposed System

It is a three step process to authenticate the user, take time more than any other process but for banking transactions, accounts, financial data, high profile system and confidential data it is acceptable. It will be provided on choice of user to use this particular authentication system for access the system and allow doing transactions in banking. This authentication process is resistant to phishing attack. Setting up a phishing website to obtain graphical passwords would be more time consuming. To get proper environment of particular authentication system and bluff the user is a difficult task in such a secure banking environment.

Significantly neither trespasser can use the confidential data nor do the transaction in banking. It is suggested that in banking transactions this authentication system used before the transaction request. So it will secure the amount from any accidental transaction or trespasser.

A. Working of Proposed System

Our proposed system comprises of 2 phases, First phase is registration phase and Second phase is the authentication phase.

Registration Phase

Proposed system is new graphical passwords based hybrid system which is a combination of textual, recall and

recognition based techniques and consists of two phases. During the first phase called Registration phase, the user has to first select his username and a textual password. Then objects are shown to the user to select from them as his graphical password. After selecting the user has to draw those selected objects on a screen using device. Then in the last step select the pictures for recognition based system (Fig 5).

It is suggested that user selects the password carefully. After selecting the password see it sensibly to remember it.

Algorithm: Registration

1. Enter Username (U_r) (If exists Enter New Username)
   {U_r: It is a set of characters.}
2. Now user selects the desired text password (T_r).
   {T_r: It is a set alphabets, characters and etc.}
3. Draw a Secret (DAS_r) for producing recall based password.
   {DAS_r: It is combination of Dot Pattern produce by user.}
4. User selects the images (I_r) from the various categories of images for recognition based password.
   {I_r: It is a set of images selected for authentication by user in a definite order}
5. Registration complete.

Authentication Phase

During the second phase called Authentication phase, the user has to give his username and textual password, then give his graphical password by drawing it in the same way as done during the registration phase and then recognized and identify the images selected during the registration phase. If they are drawn correctly the user is authenticated and only then he/she can access his/her account (Fig 6).

Algorithm: Authentication

1. Enter Username (U_a) (If not valid enter valid username.)
   {U_a: It is the username given during registration.}
2. Now user enters the text password (T_a). (If not verified enter valid text password)
   {T_a: Text password selected during registration.}
3. Draw the DAS_a.
   {DAS_a: It is combination of Dot Pattern produced by the user during registration.}
4. Selects the images (I_a) from the various categories of images for recognition based password.
   {I_a: It is a set of images selected during registration by user in a definite order.}
5. If successful than.
6. Authentication Complete.

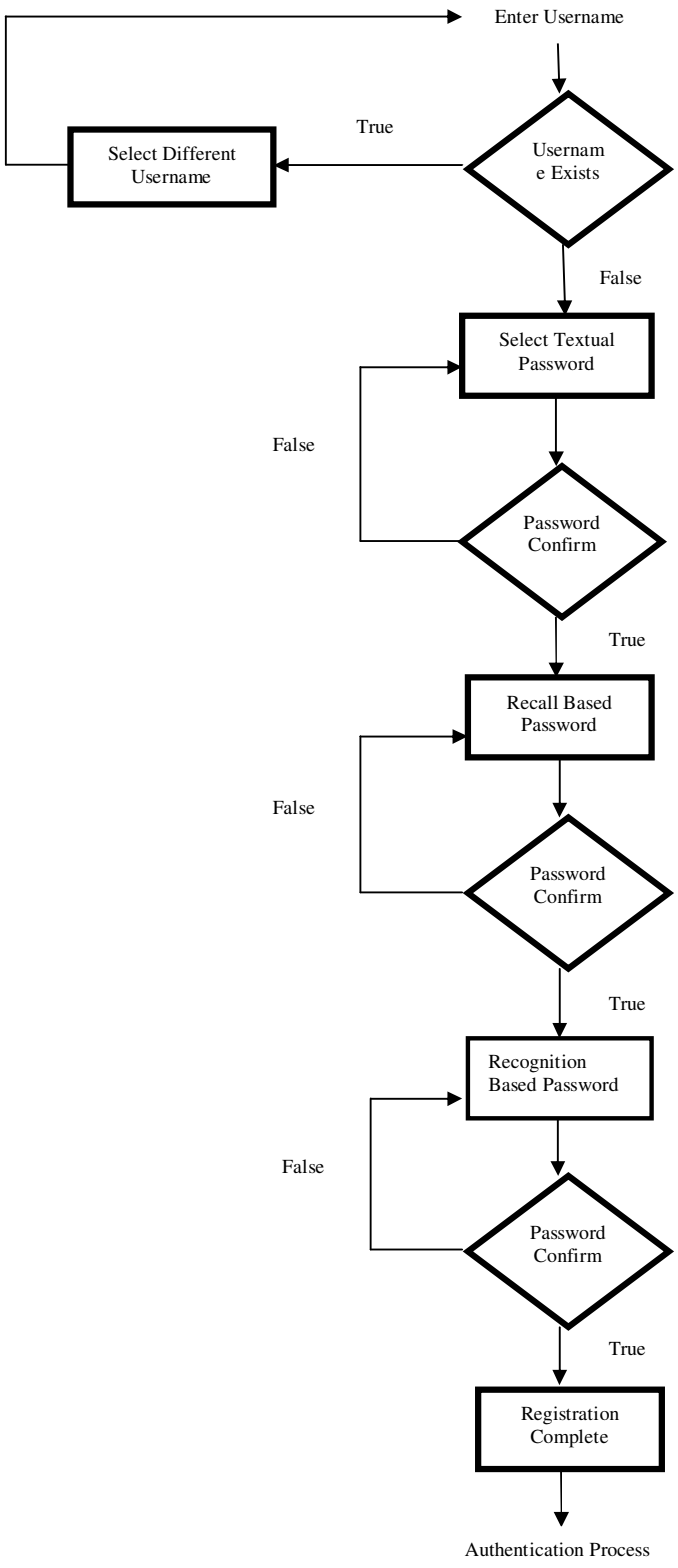

Fig. 5 REGISTRATION PHASE

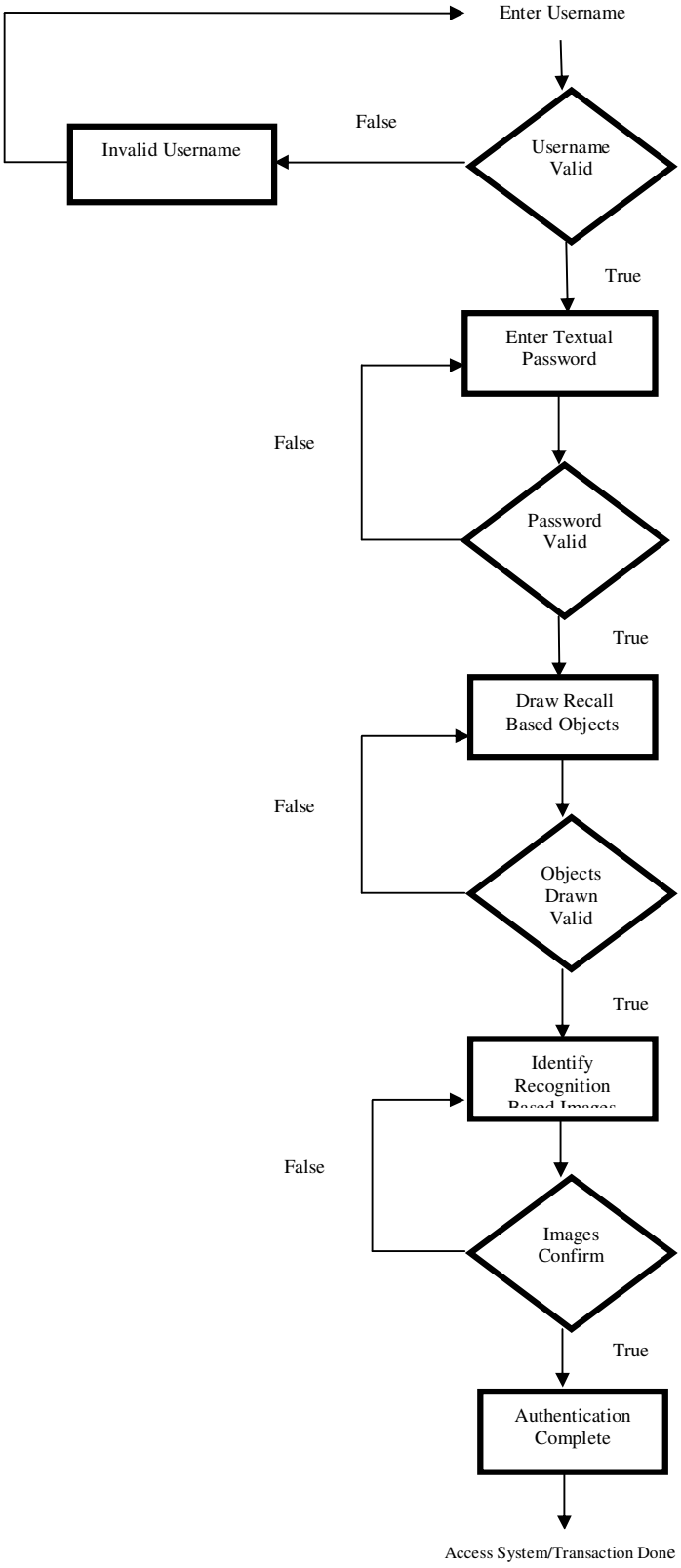

Fig. 6 AUTHENTICATION PHASE

6. Comparison of Proposed System With Existing Schemes

Our system is different from other existing system.

Comparing to the existing system, our system is designed for E-transaction authentication. We have used Dot Pattern in recall based and different categories of images in recognition based. Also we believe that as compared to human faces, objects are easier to remember which are in daily use. Our system has very good technique for restoring password.

In Three steps, while users' text password part can still be stolen by phishing, obtaining their graphical password parts is more difficult: without knowledge of users' image profiles, the phisher does not know what images to present in order to extract a graphical password.

7. Implementation and Analysis

Implementation of proposed system requires ease of use, such as ease in registration, authentication and forgot password. So concerning with these facts we develop a system which is user friendly as well as secure over an insecure channel such as the Internet. Security and Memorability are two major issues of this E-transaction graphical authentication system. Following are the details of evaluation of memorability (also evaluate the accuracy) and Security of the proposed system.

A. Implementation

For implementing this system an application is required to authenticate the user in three steps. We developed an application, first to register the user and then authenticate the user with the mention details during registration. In implementation of the system it is necessary that the authentication is secure and easy to perform. For secure authentication we are using server-side authentication for secure transaction because bank servers are secure from outside world in both ways physical as well as logical.

As per the proposed scheme, we have to implement two phases one for registration and second one is authentication.

Set of variables used in Registration (R) and Authentication (A):

R: $\{U_r, T_r, DAS_r, I_r\}$

A: $\{U_a, T_a, DAS_a, I_a\}$

In registration phase first user will enter email id, it will become a user id for authentication. Using email id for username (U_r) will be useful in forgot password and selects the desired text password (T_r). In the next step Dot Pattern (DAS_r) will be selected by user, in dot pattern [N x N] matrix (where N=5) is given, user will draw its desired password, sequence matter in this dot pattern and in the last step user will selects the images (I_r) for completing the registration phase.

In authentication phase user will enter username (U_a) and if exists than proceed to enter text password (T_a). If text password will entered successfully then user will proceed to draw the dot pattern selected during the registration. Successful draw of pattern (DAS_a) allow proceeding and selects the set of images. Successful selection of images (I_a) will authenticate the user for E-transactions.

B. Analysis

After implementation of the system, it is necessary to check the reliability, security and memorability of the system. These are the major factors for the analysis of the system.
As the authentication is knowledge based the reliability of the system is very high. The system has not depended on any element like human parts, cards and token etc. So the reliability of the system is very high. Accuracy of the system is also a concerned. In this system tolerance factor is negligible due to its design. It does not need tolerance during input of password. So due to negligible tolerance it is less vulnerable to attack. This also increases the reliability of the system.

TABLE III
COMPARITIVE STUDY OF DIFFERENT AUTHENTICATION SYSTEM WITH PROPOSED SYSTEM ON VARIOUS FACTORS OF RELIABILITY

Authentication System	Biometric		Token Based		Knowledge Based	
Factors	Finger Print	Voice Recognition	Card	ID Chip Card	Graphical System	Proposed System
Wear & Tear	Yes	No	Yes	Yes	No	No
Noise	Yes	Yes	Yes	Yes	Yes	No
Accuracy	Low	Very Low	Above Average	Above Average	High	Very High
Tolerance	High	Very High	Average	Below Average	Depends on the System	Negligible

To break Graphical Passwords is quite hard. As such there are no reports on cracking the graphical passwords. Although our proposed system includes three different passwords to authenticate the user, all the steps of authentications have their own complexity and security. For security purpose we have used server side authentication. By using this particular technique first we verify the user id if exists than proceed to enter the passwords and process continue till all three steps successfully completed in the given no. of attempts.

Memorability is one of the major issues in Graphical Authentication System as user has to remember images and drawings which they had selected or drawn during the registration. So to make it easy we have used Draw a Secret in which user has to draw a pattern in 5x5 Dot Matrix. In image selection we are using three categories which are easy to remember because they are used in daily life like Flowers, Fruits and Monuments. At last if user is unable to login than Forgot Password facility is also available in which the password information is directly sent to the registered email id of the particular user.

TABLE IV
SECURITY OF PROPOSED AUTHENTICATION SYSTEM WITH VARIOUS FACTORS

Password Type	Length	Combinations	Attempts	Security
Text Password (T)	20 Characters	Very Large no. of combination	3	Large no. of combination gives huge password space as well as number of attempts secure from any type of Guessing and Brute Force attacks
Draw A Secret (DAS)	5 x 5 Square Matrix	$2 \times [NxN]^N$	3	Draw of pattern has a sequence in its password, it makes the password space double and make it secure against the spyware and sequence in password prevents it from phishing
Image Selection (I)	30 Images in 3 Categories	1000	3	Three attempts provide the security of 99.7%. Image recognition is safe from dictionary attacks , shoulder surfing attacks and phishing

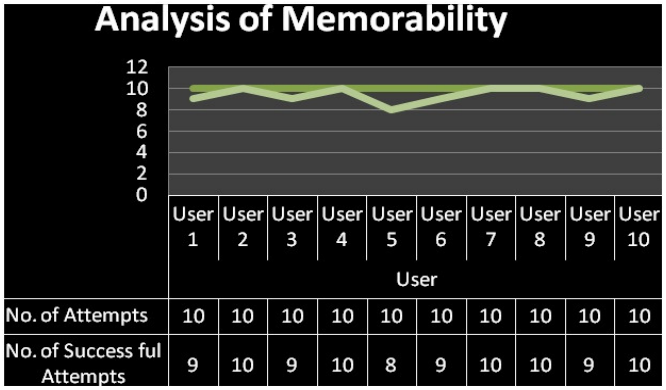

Fig. 7 Showing the Analysis of Memorability

8. Discussions and Conclusion

The core element of computational trust is identity. Currently many schemes and techniques are available for authentication. There is a growing interest in using pictures as passwords rather than text passwords. So we have proposed hybrid graphical based password authentication system for E-transaction. The major advantage of the proposed scheme is that we have a secure authentication system for E-transaction. It is achieved by using hybrid graphical password based system. In fact, this particular system needs not to be depended on any elements (like cards or human parts etc.) for authenticating the user it increases the reliability and accuracy of the system. By using the elements of daily life (image categories like fruits, flower and monuments) in the scheme increases the memorability of the system. Forgot password is also the provided feature in the system to increase the memorability.

The proposed hybrid graphical authentication is highly secured under the various attacks of the graphical passwords persona. Server side authentication secures the passwords from

intruders. The three steps of authentication make it secure and safe. Password space and combination is very large which makes it secure against various attacks. It is extremely necessary to have a secure authentication system for E-tran sactions. So we proposed our authentication system during E-transaction. Possible extension to this work is to use encryption techniques in passwords to increase security. Efficient elements are needed to increase the memorability of graphical passwords.

References

[1] Xiaoyuan Suo, Ying Zhu and G. Scott. Owen, "Graphical Passwords: A Survey", Proceedings of the 21st Annual Computer Security Applications. IEEE. 463-472; 2005.

[2] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.
[3] J. Thorpe and P. C. V. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in *Proceedings of the 13th USENIX Security Symposium.* San Deigo, USA: USENIX, 2004.

[4] Mohammad Sarosh Umar and Mohammad Qasim Rafiq, "A Graphical Interface for User Authentication on Mobile", IARIA, 2011, pp. 69–74, ACHI 2011.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The Design and Analysis of Graphical Passwords", in Proceedings of 8th USENIX Security Symposium, pp. 1-14, 1999.

[6] Sreelatha Malempati and Shashi Mogalla, "A Well Known Tool Based Graphical Authentication Technique", CCSEA 2011, CS & IT 02, pp. 97–104, 2011.

[7] Arash Habibi Lashkari, Abdullah Gani, Leila Ghasemi Sabet and Samaneh Farmand, "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids", Scientific Research and Essays Vol. 5 (24), pp. 3865-3875, 18 December, 2010.

[8] Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, "A Graphical Password Based System for Small Mobile Devices", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

[9] ARASH HABIBI LASHKARI, SAMANEH FARMAND, DR. ROSLI SALEH and Dr. OMAR BIN ZAKARIA, "A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009.

[10] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2, JUNE 2010

Dr. Manish Manoria is currently working as the Director of Truba Institute of Engineering & Information Technology, Bhopal. He is having a vast experience in the field of Computer Science and Academics. He has guided a number of Projects and Dissertations for M. Tech. Students, as well as for UG Students. He has completed his Engineering (Honors) in Computer Technology, Master of Engineering (Honors) in Computer Engineering and Ph. D. in Computer Science Engineering.

Ankur Jain has done his Engineering from Shree Institute of Science & Technology, Bhopal (RGPV) in Information Technology Branch. He is having an Experience of 1 Year in Academics, worked as an Assistant Professor (CS/IT) in People's College of Research & Technology, Bhopal. Currently, he is pursuing M.Tech. (Final Semester) in Computer Science Engineering Branch from Truba Institute of Engineering & Information Technology, Bhopal (RGPV). His areas of interest are Security, Object Oriented Programming, Operating Systems, Data Base Management Systems, etc. His topic for research is Graphical User Authentication.