ISSN: 2278-0181
Vol. 3 Issue 2, February – 2014

3D Password – More Secure Authentication Scheme

Tejal M. Kognule[1], Monica G. Gole[2], Priyanka T. Dabade[3], Sagar B. Gawde. [4]
[1,2,3,4]*Department of Computer Engineering, P.V.P.P.C.O.E, Sion, Mumbai.*

***Abstract*— In this paper, we propose and evaluate our contribution which is a new scheme of authentication. This scheme is based on a virtual three-dimensional environment. Now the passwords are based on the fact of Human memory[3]. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling[1]. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password.**

Keywords*— *Authentication, graphical passwords, multifactor, textual passwords, 3-D passwords, 3-D virtual environment.

I. INTRODUCTION

Authentication is the process of validating who you are to whom you claimed to be. In general, there are four human authentication techniques:

1. What you know (knowledge based).
2. What you have (token based).
3. What you are (biometrics).
4. What you recognize (recognition based).[4]

Textual passwords are the most common authentication techniques used in the computer world. Textual password has two conflicting requirements: passwords should be easy to remember and hard to guess.

Klein [3] acquired a database of nearly 15,000 user accounts that had alphanumerical passwords, and stated that 25% of the passwords were guessed using a small, yet well formed dictionary of (3×106) words. Even though the full textual password space for 8- character passwords consisting of letters and numbers is almost(2×1014) possible passwords, by using a small subset of the full space, 25% of the passwords were guessed correctly. This fact is due to the user's carelessness in selecting their textual passwords and to the fact that most users do not select random passwords.

Many graphical passwords schemes have been proposed. The strength of graphical passwords comes from the fact that users can recall and recognize pictures more than words. Most graphical passwords are vulnerable for shoulder surfing attacks[1], where an attacker can observe or record the legitimate user's graphical password by camera. Currently, most graphical passwords are still in their research phase and require more enhancements and usability studies to deploy them in the market

Token based systems such as ATMs are widely applied in banking systems and in laboratories entrances as a mean of authentication. However, tokens are vulnerable to loss or theft. Moreover, the user has to carry the token whenever access required.

Many biometric schemes have been proposed. Each biometric recognition scheme is different considering consistency, uniqueness, and acceptability. Users tend to resist some biometrics recognition systems due to its intrusiveness to their privacy.

Both recall based & recognition based authentication techniques having some drawbacks & limitations when they are used separately or used single authentication scheme at a time[2]. To overcome these drawbacks & limitations of previously existing authentication schemes. We have introduced a new authentication scheme which combines both textual as well as graphical. The 3D password has alarge number of possible passwords because of the highnumber of possible actions and interactions towards everyobject and towards the three dimensional virtual environment

3D Password Overview: The three dimensional password (3D password) is a new authentication methodology that combines recognition, recall in one authentication system[4]. The idea is simply outlined as follows. The user navigates through a three dimensional virtual environment. The combination and the sequence of the user's actions and interactions towards the objects in the three dimensional virtual environment constructs the user's 3D password. Therefore, the user can walk in the virtual environment and type something on a computer that exist in (x1, y1, z1) position, then walk into a room that has a image gallery, selects any image exist in position (x2, y2, z2) from it. The combination and the sequence of the previous two actions towards the specific objects construct the user's 3D password. Users can navigate through a three dimensional virtual environment that can contain any virtual object.

Virtual objects can be of any type. We will list some possible objects to clarify the idea[1].

An object can be:

1. A computer that the user can type in
2. A white board that a user can draw on
3. Any Graphical password scheme
4. Any real life object
5. Any upcoming authentication scheme

3D Password Selection and Inputs: Consider a three dimensional virtual environment space that is of the size G×G×G. Each point in the three dimensional environment space represented by the coordinates (x, y, z) $\in$ [1..G] × [1..G] ×[1..G][2]. The objects are distributed in the three-dimensional virtual environment. Every object has its own (x,y,z) coordinates. Assume the user can navigate and walk through the three-dimensional virtual environment and can see the objects and interact with the objects. The input device for interactions with objects can be a mouse, a keyboard, styles, a card reader, a microphone …etc.

User actions, interactions and inputs towards the objects and towards the three-dimensional virtual environment are mapped into a sequence of three-dimensional coordinates andactions, interactions and inputs. For example, consider a user navigates through the three-dimensional virtual environment and types "AB" into a computer that exists in the position of (13, 2, 30).The user then presses the login button. The representation of user actions, interactions and inputs towards the objects and the three-dimensional virtual environments can be represented as the following:

(13,2,30) Action = Typing, "A",
(13,2,31) Action = Typing , "B",
(20,6,12) Action = Clicking on picture from gallery.
(30,6,20) Action = Clicking on another picture from gallery.

Two 3D passwords are equal to each other when the sequence of actions towards every specific object are equal and the actions themselves are equal towards the objects.

As described earlier, three-dimensional virtual environments[2] can be designed to include any virtual objects. The first step in building a 3D password system is designing the three-dimensional virtual environment. The selection of what objects to use, locations, and types of responses are very critical tasks. The design affects the strength, usability and performance of the 3D password. Fig 1 shows an experimental three-dimensional environment.

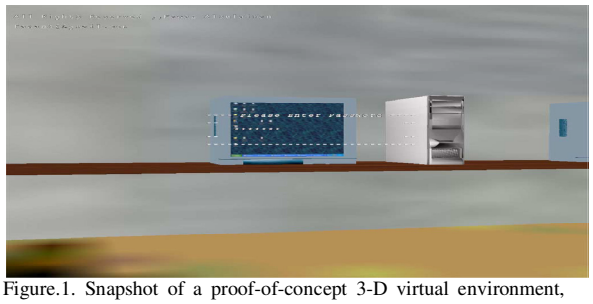

Figure.1. Snapshot of a proof-of-concept 3-D virtual environment, where the user is typing a textual password on a virtual computer as a part of the user's 3-D password.[6]

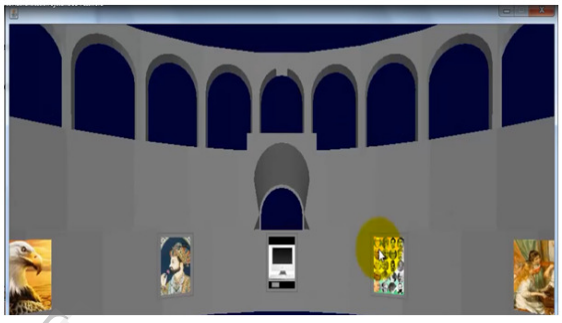

Figure.2.Snapshot of three-dimensional virtual environment which is image gallery

A virtual art gallery that consist of 20 pictures and computer where users can navigate and interact with virtual objects by either typing textual password on virtual computer with the help of keyboard or selecting any number of images in any sequence from image gallery.

II. METHODOLOGY

Proposed System: Proposed authentication scheme is combination of many other authentication schemes together. 3D password is combination of both recall-based (i.e. textual password, etc) & recognition based (i.e. graphical password). so that 3D password is multifactor & multi password authentication[2] scheme. Refer Fig 3:

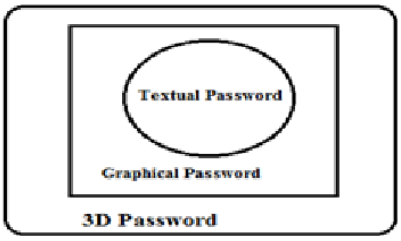

Figure.3. Multifactor authentication scheme

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February – 2014

For authentication with 3D password a new virtual environment is introduced called as 3D virtual environment where user navigate, moving in 3D virtual environment to create a password which is based on both the schemes. We don't use biometric scheme because biometric having some major drawbacks (like hardware cost is more)[1]So that we have not included biometric authentication in our 3D password scheme. Because biometric authentication is efficient over shoulder surfing attacks. But other attacks are venerable & easy on biometric authentication. Also inclusion of biometric may leads to increasing the cost of scheme & more hardware parts needed.

Objective of proposed system :

- To provide more secure authentication technique than existing one.
- To design & develop more user friendly[2] & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
- To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password.etc).
- New scheme should be combination of recall-, recognition -, biometrics-, and token based authentication schemes

Architectural study: This section tell about that how to create 3D password & what are different schemes[4] used to form a complete 3d password.. 3D password is multi-factor & multi password authentication scheme. So that many password schemes like textual password, graphical password, biometric etc. password schemes can be used as a part of 3D password. Choosing of different schemes are based on category of user who are going to use this scheme to their system. Fig.3 shows state diagram of 3D password creation.

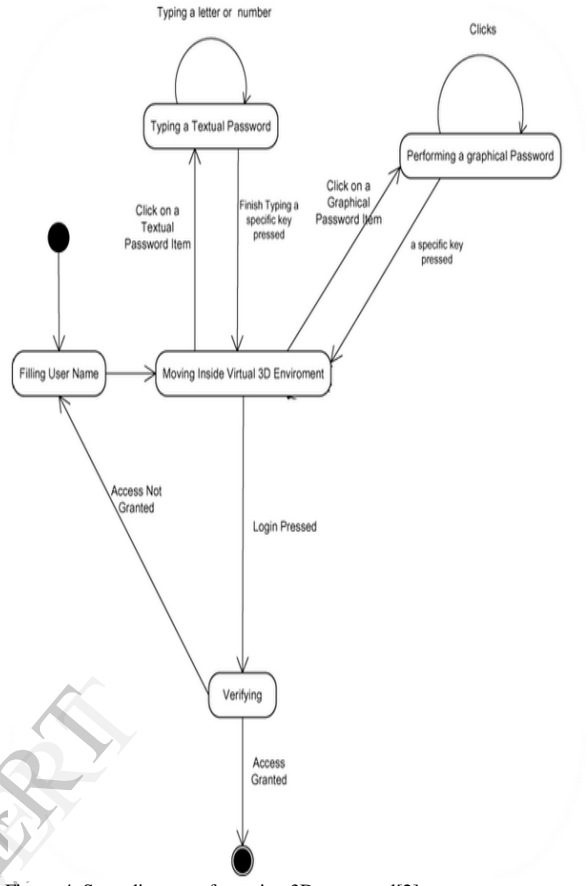

Figure.4. State diagram of creating 3D password[2]

3D virtual environment: In this multi-factor authentication scheme the basic building block used is 3D virtual environment. 3D virtual environment is created inside a 2D screen, refer fig.5. 3D environment is a real time scenario seen by peoples in day to day life which is created virtually in 3d virtual environment. We can use any real time object as a environment like any room or village but for simplicity we suggest to use small environment like room.

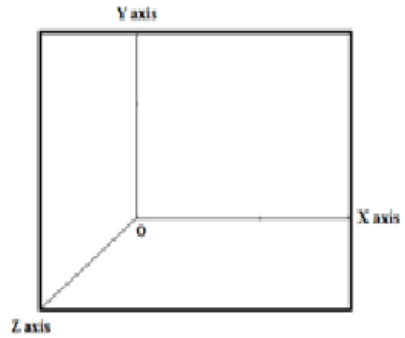

Figure.5. 3D environment under 2D screen [1]

For selecting the sequence of objects (i.e. points) we have used a very simple, easy & efficient algorithm called as convex hull algorithm. The 3d quick hull algorithm is used. & also the points selected are stored in the form of 3d co-ordinate(x, y, z) in a simple text file. Some design guidelines related to 3d environment such[3]

- Virtual environment selected in such a way so that it is similar to real life object.
- Every object is unique & distinct from other.
- Virtual environment size should be considered [1]

Working of 3D password scheme:

(A)Registration

1. When new user register, first enter the all details which give in registration form.
2. Then user will enter into the virtual environment enter textual password and select images from multiple images .
3. This all interactions stored in database in encrypted format.

(B)Authentication

1. Enter username and password.
2. Click the images in proper sequence.
3. All interactions fetch from database then compared one by one.

Then access granted to authorized user for access applications.

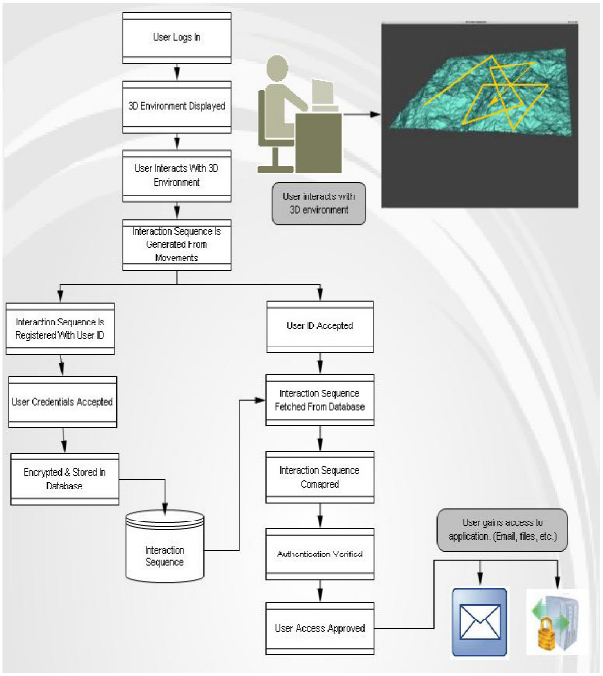

Figure.6.working of 3d password scheme

Authentication Schemes: In this system, we use multiple authentication schemes for give access of data or any system for authorized user and also the security for any system or data[4]. Following schemes are used in this system.

(A)Text Authentication

In this scheme, we use simple Username and Password for Authentication. When register the new user, save all detail information of that user and also save Username and Password of that user as per user's choice in Registration Database. This Password is stored in database in encrypted format using Message Digest 5 Algorithm. When user log's in, first enter the Username and Password then system check the new Username and Password is same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

Algorithm used in this System for Encryption Message Digest 5 (MD5)

1. The MD5 algorithm accepts a message as input and generates a fixed length output which less than the length of input message.
2. The output is called a hash value or message digest.
3. The MD5 algorithm is mostly used for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."

To compute the message digest of the message five steps are performed as following :

1. Append Padding Bits
2. Append Length
3. Initialize MD Buffer
4. Process Message in 16-Word Blocks
5. Output

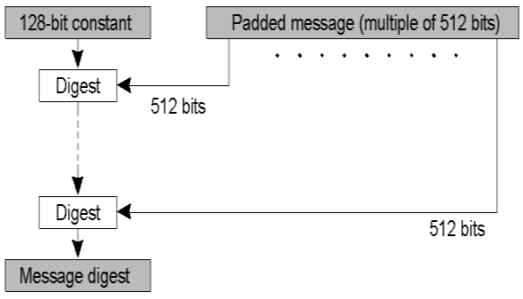

Figure.7. Working of MD5

(B) Graphical Authentication

In this scheme, we use images for Authentication. When register the new user, User will perform the actions in virtual environment by selecting any number of images in any sequence from image gallery. that is pixel values in sequence which stored in 3D Coordinate Database. This click points are also stored in database in encrypted format using Message Digest 5 Algorithm.

When user log's in, first select the proper image sequence with the help of mouse then system checks that sequence of input points are same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

Database Design:

The database which has been created from this system consists USER registration. The detailed information in every table is shown in following table:

Table.1. Registration Database

USER ID	EMAIL ID	PASSWORD	SECRET QUESTION	SECRET ANSWER
ABC	3dpwd@gmail.com	123456ABC12	What is your favorite teacher Name	XYZ

Table.2. 3D Coordinates Database

USER ID	3D CO-ORDINATE			PASSWORD
ABC	X	Y	Z	123456ABC12
	10	20	50	
	40	30	70	

According to concept we have built an experimental three dimensional virtual environment that consist of many objects. Objects initially have two kinds of responses to reactions, they are, objects that accept textual passwords and objects that accept graphical passwords.

1. computer that accept textual passwords
2. 20 pictures that the users can click on, anywhere in the picture, as a part of their 3D password

Experimental Virtual 3-D Environment: In our experiment, we have used WPF (Windows Presentation Foundation)[5] with Visual Studio 2010 to build the 3-D virtual environment. The design of the experimental 3-D virtual environment represents an image gallery that the user can walk through and is depicted in Fig. 2.

System is divided into Registration module i.e. user is require to register first of all. That is it requires filling all the necessary personal information such as User id, Email ID, Password, Perform 3D password in 3D virtual environment, Secret Question and its answer. And for as Proposed scheme the confidential details are as User id, the text password field named as Password and the 3D password field is recorded after you selecting one of the environment and in that environment you are require to select random sequence of images as a 3D Password. The Registration process is shown in Fig 3.

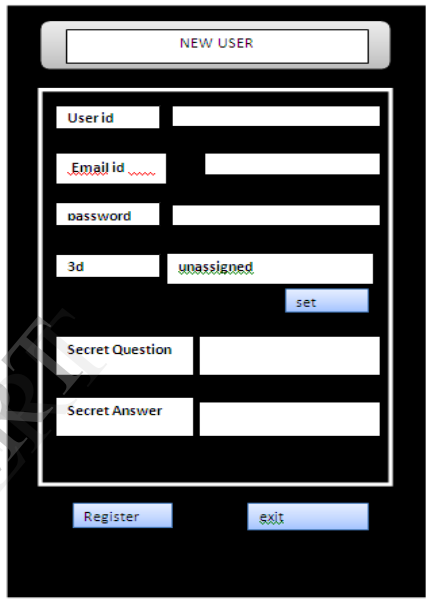

Figure.8. Registration

The next module is Login. In this module it Require to fill the necessary information such as User id, password can be filled. After user the selecting the environment and after that in that environment user is require to select the random sequence of images as a 3D Password that user has selected at the time of registration, if the selected image sequence at the login time is equal to the selected image sequence at the time of registration then and then only the authentication is valid otherwise authentication is failed. The text password field indicates where user is require to give the text password. It also noted that the text password field is also very important because this filed is also checked in database i.e. text password at the time of registration and the text password at the time of login. If the username, Recorded data, and the text password are matches with respect to Registration time and that the user entered at the login time then and then only the authentication is valid. The Login process is shown in Fig 9:

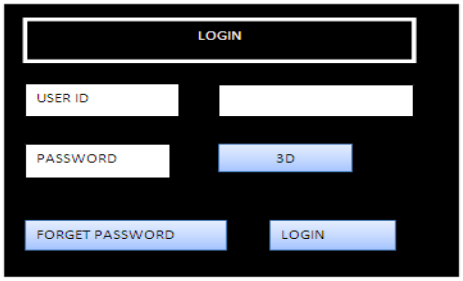

Figure.9. Login

The Fig 2. Shows one of the environments for the authentication purpose for our proposed scheme i.e. Graphical password authentication scheme based on image gallery.

III. CONCLUSION

In the proposed scheme i.e. 3D password Authentication scheme is combination of Textual and Graphical Password authentication Scheme based on image gallery here the user having the choice to select minimum one and maximum N number of images, therefore the user is having the flexibility to select the any kind of password i.e. sequence of selecting images from gallery. Security is achieved because only legal user is known that what kind of images are selected and in what sequence.

There are pros and cons while applying this authentication scheme[7]. The challenges that one has to face while processing are:

1. Difficult for blind people to use this technology.
2. Requires sophisticated computer technology.
3. A lot of program coding is required.

Every coin has two sides. The advantages of this approach are:

1. Provides security.
2. This 3D password can't take by any other person.
3. 3D graphical password has no limit.
4. Password can change easily.
5. Implementation of the system is easy.
6. Password can remember easily.
7. This password helps to keep lot of personal details

The motivation of this work is to have a scheme that has a huge password space while also being a combination of any existing, or upcoming, authentication schemes into one scheme.

REFERENCES:

[1] A Novel 3D graphical password schema-Fawaz A Alsulaiman and Abdulmotaleb El Saddik, IEEE 2011

[2] Secure Authentication with 3D Password(IJESIT 2013)

[3] Daniel V.Klein. Foiling the Cracker: A Survey of, and Improvement to Passwords SecurityGreg E. Blonder, Graphical Password, United State Patent 5559961

[4] A Novel 3D Graphical Password Schema, IEEE 2006

[5] Book on WPF in action with visual studio2010

[6] Videos are taken from the following link https://www.youtube.com/watch?v=XKsrLLIxICQ

[7] Graphical Password Authentication Scheme Based On Color Image Gallery (IJEIT 2011)

[8] Integration of Sound Signature in 3D Password Authentication System