Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 2, 2016
ISSN: 2455 - 7528

# Security Analysis of 3D Password Based Authentication System

Kapil Kumar [#1], Dinesh Goyal [*2]
M.Tech Scholar[#1], Assistant Professor[*2]
Suresh Gyan Vihar University, Jaipur, India[#1,*2]
[1]en.kjangir@gmail.com
[2]dgoyal@gyanvihar.org

**Abstract**—

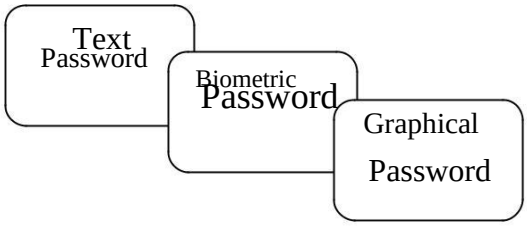
***Access to any automated system is most often based on the use of textual or alphanumeric passwords. However, mostly end users have difficulty to remembering a password that is long and random-appearing. Instead, they generally use short, simple, and insecure passwords. Graphical passwords can be designed to try to make passwords more memorable and easier for the end users to use and, therefore, system will be more secure. Using a graphical password or 3D password, users click on images rather than type alphanumeric characters. We have designed a more secure multi-layer password framework for textual, biometric as well as graphical password system. In this paper we give an idea about the proposed system. Here we deal its security characteristics, and the empirical study carried while the development and comparing the system with normal textual or alphanumeric password protected system.***

*Keywords*— ***Graphical password, texture password, 3D password, biometric password***

## I. INTRODUCTION

3D or graphical passwords based system was first proposed by Blonder in 1996 [1]. In his description of the concept an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated.

Authentication of a person's identity is a very old but still a challenging problem. There are three common ways which are used for authentication. First one is based on what a person's possession such as keys, identity cards, identity number etc. Second way of authentication is based on what a person knows or remembers knowledge such as passwords, PIN number etc. Third way of authentication is based on what a person carries, i.e. the features of a human being like biometrics. There are chances that the items which are under possessions may be lost and knowledge may be forgotten. But this is not the case with biometrics. Limitations of these three methods can be overcome if we make use of all three methods in a single system. The main driving force behind biometrics based authentication getting more and more popularity day-by-day [2]. The purpose of using a biometrics is to provide a mechanism to recognize a person with the help of his/her own features and to eliminate the use of much inconvenient ways of recognition which are based on ID card, password, physical keys etc. This proposed system is a multifactor authentication scheme, and can combine all existing authentication schemes into a single 3D virtual environment. This 3D virtual environment contains several objects or items with which the user can interact. We are using three layer methods which has texture, biometric and graphical password.



Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 2, 2016
ISSN: 2455 - 7528

Figure 1: Three Layer of Authentication

Texture based password is basically a recall based techniques which require the user to repeat or reproduce the secret text that user created before. Textual Passwords should be easy to remember for usr but at the same time hard to guess by another. This scheme has a drawback as it can guess correctly by using brute force dictionary.

Many biometric schemes have been proposed earlier such as face recognition; fingerprints, palm prints, hand geometry, voice recognition, iris recognition, and retina recognition etc. Each biometric recognition scheme has its advantages and disadvantages based on different factors. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic [3]. Graphical password is based on the idea that users can recall and recognize pictures more than any text of number. Currently most of the graphical password are in the research phase and require more enhancement and usability studies to develop them in the market.

## II. PROPOSED METHOD

In this section, we proposed a multilayer authentication scheme that combines the advantages of three different authentication schemes. We try to justify the requirements of current security issues for authentication on different platforms. The new scheme should provide secrets that are easy to remember and very difficult for intruders to guess.

*Layer1*

At the first layer of authentication we used texture password as intialially as recall method. This layer is based on knowledge level or we can say what the user knows. Passwords have been used with computers since the earliest days of computing. Basically it has a LOGIN command that requested a user password. "After typing PASSWORD, the system turns starts working. To log in, at the client side is ensured by the use of text password, and that text password has to be entered by ensuring by applying of special characters. Therefore, security at Layer1 is ensured by use of text password which is a usual approach with normal login scheme.

*Layer2*

At the second layer of authentication we used graphical password scheme for final access of the system. Graphical password is based on the concept that users can recall and recognize pictures more than words. Graphical password scheme were basically introduced to decrease the human memory burden to remember text-based password. In a virtual visual environment a particular pattern of images or clues can easily be recognized. In some cases of graphical passwords are susceptible only due to shoulder surfing attacks, where an attacker can observe or record the valid user graphical password by camera. We tried to use a virtual environment where multiple objects are there, which need to be organizing in a particular manner can only authenticate the user. The coordinates of combining objects are used to create a number by calculating the average distance between theses coordinates. If we we have three objects in one environment as p1(x1, y1), p2(x2, y2) and p3(x3, y3) and their distances are d1,d2 and d3 then value will be average of d1,d2 and d3. In the market most of the graphical password are in the research phase and require more enhancement and usability studies to develop them in the market.

*Layer3*

At the third layer of authentication we used biometric password as face recognition scheme. This is recognition based scheme as it require user to pick and memorize some of a given set of pictures of their face. At the time of authentication

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 2, 2016
ISSN: 2455 - 7528

system must have to match face of user with multiple images of their face taken in different angles and distances.

## III. SECURITY ANALYSIS

To analyze and understand how far our authentication scheme is secure, we consider all possible attack techniques. We need to study whether our proposed authentication scheme is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune, we then have to find the countermeasures that prevent such attacks. In this section, we try to cover most possible attacks and whether the attack is valid or not. Moreover, we try to analyze system performance to assure for these attacks one by one as:

*Brute force attack*

In the first layer where texture based passwords taken for authentication have space to generate all combinations of character and numerals. But it is difficult to do this attack on graphical passwords .We believes it is harder for this attack to succeed for next two layer and their all efforts will not work on biometric and graphical passwords. Generally recall based password is more secure then recognition based techniques when it comes to brute force attack.

*Guessing*

It is very tough to get graphical password by using any human interaction method. Instead user must consous when he/she enters the graphical password for system authentication.

*Social Engineering*

This attack practically impossible in graphical passwords as keyboard input is not involved so words in dictionary can’t be used to crack the password.

*Spyware attack*

This type of attack is not possible on graphical passwords. Screen recording is possible but there are no such spywares till date to detect graphical password. Instead user must concern as text based passwords can be stolen using key loggers applications or devices.

## IV. WORKING ENVIRONMENT

At very first step in the processing of image indexing, using MATLAB 7.9.1 where to start with a command RUN M-file. It has basically two modules, first is to register the user credentials and another is to login layers for accessing the system.

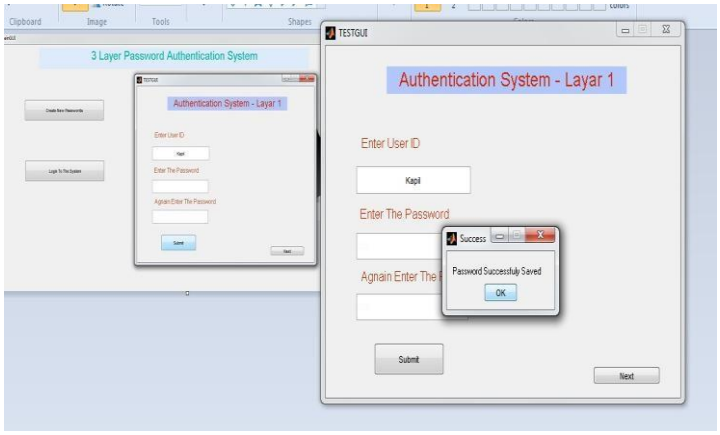



Figure 2: Layer 1 of Authentication

At the layer 1 of authentication we used texture password as recall method. Passwords have been used with computers since the earliest days of computing. Basically it has a LOGIN command that requested a user password. "After typing PASSWORD, the system turns starts working to the next layer.

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 2, 2016
ISSN: 2455 - 7528


Figure 3: Layer 2 of Authentication

At the layer 2 of authentication we used graphical password scheme for final access of the system. Graphical password is based on the concept that users can recall and recognize pictures more than words. In a virtual visual environment a particular pattern of images or clues can easily be recognized as shown in the fig. 3. The coordinates of combining objects are used to create a number by calculating the average distance between theses coordinates. If we we have three objects in one environment as p1(x1, y1), p2(x2, y2) and p3(x3, y3) and their distances are d1,d2 and d3 then value will be average of d1,d2 and d3.

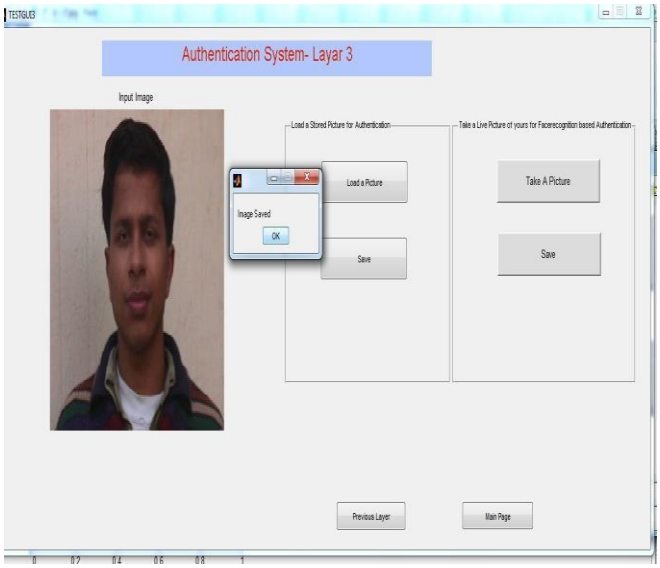



Figure 4: Layer 3 of Authentication

At the layer 3 of authentication we used biometric password as face recognition scheme. This is recognition based scheme as it require user to pick and memorize some of a given set of pictures of their face. At the time of authentication system must have to match face of user with multiple images of their face taken in different angles and distances.

After successful login at layer 3 the system finally authenticates the user and redirect to the system to be access as shown in the fig. 5.

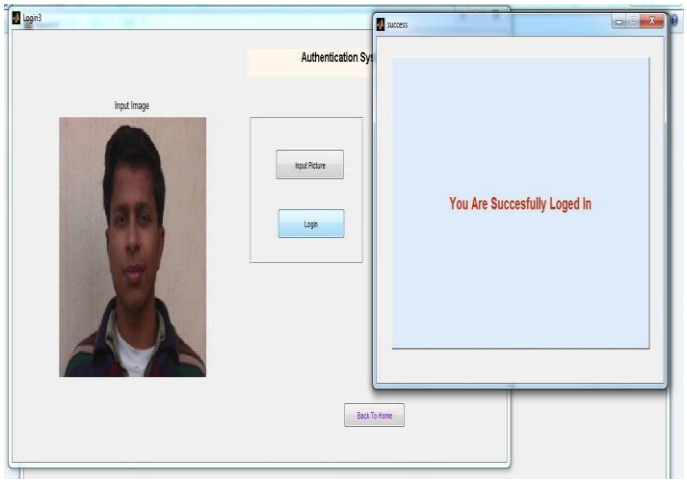



Figure 5: successful login screen

## V. EXPERIMENTAL RESULTS

In this section we evaluate the proposed method of 3 layer authentication system using multiple layers. For implementation we used MATLAB 7.9.1. The performance evaluation of the system carried out on various real users under different conditions. The proposed method expressed here in this paper is tested on 100 different users and the success rate is received to 98% so this result shows the high efficiency of this method.

We have have compared our proposed Layers with each other as taken one layer protection , two layer protection and three layers of protection one by one. At every layer the level of security

increasing as presented in the comparison graph in figure 4. Therefore as whole 3 layer of security improves the system security up to desirable extend.

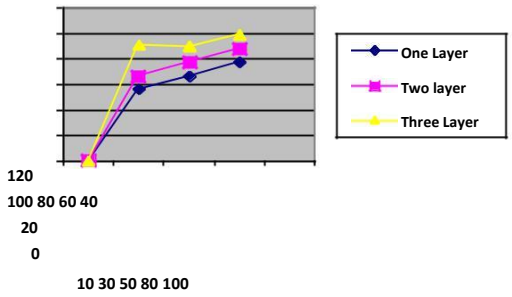



Figure: 4 Comparison Graph

## VI. CONCLUSION

In this paper we tried to show a robust method for the best result in this system and success rate of 98 %. There are many authentication schemes in the current era. Some of them are based on user's physical and behavioral properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Moreover, there are some other important authentication schemes that are based on what you have, such as smart cards. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, as mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be applicable for commercial use.

## REFERENCES

[1] Alsulaiman, F.A.; El Saddik, A., "Three- for Secure, "*IEEE Transactions on Instrumentation and measurement*", vol.57, no.9, pp 1929-1938.Sept. 2008

[2] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, An association-based graphical password desigu resistant to shoulder surfing attack', International Conference on Multimedia and Expo (ICME), IEEE.2005

[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.

[4] Jansen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices", NISTt NISTIR 7030, 2003

[5] Nari Kannan; "How to catch some next big things and lose others" Online: http://blogs.ittoolbox.com/bi/entrepreneur/archives/000574.asp March 2004.

[6] Sobrado, L and Birget, J. "Grap hical Passwords", The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004