Password Protection for Online and Offline Data

Prof. Kirti Rajadnya[1], Prathamesh Pasalkar[2], Vaishnavi Birhade[3], Prashant Sargar[4]

[1]*Professor Kirti Rajadnya, Information Technology, Shivajirao S. Jondhale College of Engineering, Dombivli, Mumbai, India*
[2]*Student Prathamesh Pasalkar, Information Technology, Shivajirao S. Jondhale College of Engineering, Dombivli, Mumbai, India*
[3]*Student Vaishnavi Birhade, Information Technology, Shivajirao S. Jondhale College of Engineering, Dombivli, Mumbai, India*
[4]*Student Prashant Sargar, Information Technology, Shivajirao S. Jondhale College of Engineering, Dombivli, Mumbai, India*

Abstract- *User authentication and password protection is one of the most important topics in information security. Authentication is the process to allow users to confirm his or her identity to a Web application. Password authentication is most widely used authentication mechanism for web applications. The password should be protected from various attacks. The most common computer authentication method is to use alphanumerical usernames and passwords. This method has significant drawbacks. Major issues in alphanumeric passwords are forgetting password, stolen password, weak password etc. The technology has been developing at a rapid rate in the past three centuries. We are getting modernized by making everything digitalized by the growth of technology.*

To protect the personal account, we have created a prototype of three level password protection system. In this system, fist level contains simple alphanumeric password combinations. In second level of authentication, the RGB colour code pattern is used and in third level graphical password is used i.e. face detection and recognition. The user will have to go through the all three levels for successful authentication. This 3 level password system will provide high security to the system. As the data becomes more confidential the security threats will simultaneously increase. For this reason, we have to provide a better security for authentication of data and accessing it.

Multilevel password protecting system will help us to protect the information. It will help us to overcome the vulnerabilities. By adding the extra levels in authentication, we can provide an enhanced security to the system.

***Key Words*: Authentication, alphanumeric password, RGB colour patter, Face detection and recognition, multilevel, security**.

1. INTRODUCTION

User authentication is main component of currently used security systems. There are so many user authentication systems such as knowledge-based system, token-based systems and biometrics. In today's systems alphanumeric password system, I used most prominently for user authentication. Biometrics systems can also be used but this system is hard to develop and it requires specialized devices.

Most of the time token base password authentication system is used with knowledge based password. For example, ATM authentication, which requires combination of token i.e. a bank card and a secret pin. Knowledge base password is used most frequently for user authentication. In this paper we focus to develop a prototype which contains multilevel authentication.

Knowledge based passwords have number of shortcomings. Mostly user uses simple and meaningful password which are vulnerable to attackers. Sometimes user uses complex and arbitrary passwords but it becomes difficult to remember. User can remember only limited number of passwords; sometimes user uses same password for different purpose.

One approach to improve the authentication is to use multilevel password authentication system although it is quite tedious but it provides enhances security. In multilevel password protection system, there are three basic level of authentication. In first level user will use simple alphanumeric password. The second level contains the RGB colour code pattern. The human brain can remember the colour pattern more easily than the alphanumeric passwords. Third level contains the face detection and recognition where user need not to remember any kind of combination.

The password protection system will ensure the security. Although it is a lengthy process of authentication but at the same time it is more secure. It is developed to overcome all kind of vulnerabilities.

2. LITERATURE SURVEY

Current authentication methods can be divided into three main areas:

- Token based authentication

- Knowledge based authentication
- Biometric base authentication

Token based authentication: - (something you have) it includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.).

Knowledge based authentication system: - (something you know) it includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category.

Biometric base authentication: - (something you are) It includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

By combining two or three factors from these three categories, a multi-factor authentication is crafted. Multi-factor authentication is preferred, as it is much more difficult for an intruder to overcome. With just a password, an attacker only has to have a single attack skill and wage a single successful attack to impersonate the victim. With multi-factor authentication, the attack must have multiple attack skills and wage multiple successful attacks simultaneously in order to impersonate the victim. This is extremely difficult and, thus, a more resilient logon solution.

Table 1: Literature Survey

Literature survey	
Sr. no	**papers**
1.	Wenjian Luo, Yamin Hu, Hao Jiang, and Junteng Wang [7] has done the work on alphanumeric password. In the paper "Authentication by Encrypted Negative Password" first, the received plain password from a client is hashed through a cryptographic hash function (e.g., SHA-256). Then, the hashed password is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password (abbreviated as ENP) using a symmetric-key algorithm (e.g., AES). **Advantages:** **1.** ENP only needs to select a pair of cryptographic hash function and symmetric-key algorithm without the need for extra elements (such as salt), which indicates that our scheme is programmer-friendly. 2. The cryptographic hash function and symmetric encryption make it difficult to crack passwords from ENPs. **Disadvantages:** 1. It is not resistant to shoulder surfing attack. 2. If the size of hashed password is large it is not efficient.
2.	Dhamija and Perrig [3] proposed a graphical authentication scheme based on the Hash Visualization technique in the paper "Deja Vu: A User Study Using Images for Authentication". In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. 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. **Advantages:** 1. Authentication is quiet easier due to the use of images and it does not use a traditional approach of alphanumeric password. **Disadvantages:** 1. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. 2. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.
3.	I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin [4] proposed a technique, called "Draw - a - secret (DAS)" in paper "The Design and Analysis of Graphical Passwords". 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. **Advantages:** 1. There no need to store graphical database at server

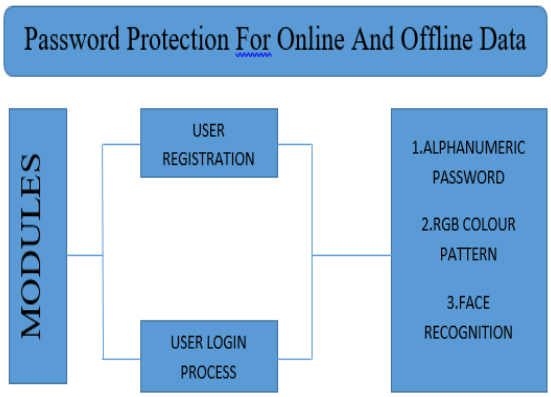
	side. 2. Grid is simple object there are no extra displays are needed. **Disadvantages:** 1. During authentication the sequence can be changed or grids may be different as it is a drawing.
4.	Blonder [2] designed a graphical password scheme in "Graphical passwords" in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords. **Advantages:** 1. This method of recalling the images in order to authenticate is more convenient. **Disadvantages:** 1. It is not resistant to brute force attack and shoulder surfing.
5.	Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget [1] has proposed a PassPoint technique in "Modeling user choice in the PassPoints graphical password scheme". A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. A user can click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence **Advantages:** 1. User had to click on the predefined image at predefined region. PassPoint algorithm overcomes this by selecting any natural image and having as many click points as possible which make the system more secure. **Disadvantages:** 1. Time consuming. 2. Difficult to memorize the click points, thus number of trials is required for authentication
6.	J. Thorpe and P. C. v. Oorschot [5] has proposed a grid selection technique in the paper "Towards Secure Design Choices for Implementing Graphical Passwords". Grid selection algorithm is also a pure recall-based authentication technique. It overcomes the disadvantages of DAS system i.e. with respect to password space and stroke count. The user is required to select a small region from a large rectangular grid. This region gets zoom in on selection, and then he is required to draw the password pattern. **Advantages:** 1. Larger password space as compared to DAS Algorithm. **Disadvantages:** 1. The disadvantage is that user cannot remember the exact stroke order. 2. If user is not familiar with the input devices (mouse, joystick, etc.) then the technique is difficult to use.
7.	Sonia Chiasson, P.C. van Oorschot, and Robert Biddle [6] has proposed a cued-click point authentication method in a paper "Graphical Password Authentication Using Cued Click Points". In 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. **Advantages:** 1. CCP provides greater security than PassPoints because the number of images increases the workload for attackers. 2. Performance is very good in terms of speed, accuracy, and number of errors. **Disadvantages:** • It is not resistant shoulder surfing. • If attackers can accurately predict the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built.

3. IMPLEMENTATION

Password protection for online and offline data is a multilevel password authentication system. In this project various password authentication systems have been proposed at each level. It can be used as password for folder lock, web-driven applications, desktop lock etc. At first level alphanumeric password is used in which the user password is encrypted by the MD5 algorithm. The next level is implemented by using RGB colour pattern.

In this level user has to select memorable colour pattern. At the third level there is face recognition system.

System Architecture:



Hardware Specification

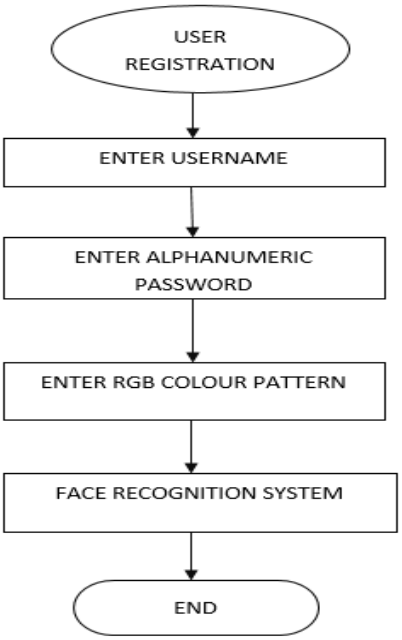
Processor : Intel Pentium IV Main
Processor speed : 3.00GHz
Memory : 512 MB
RAM Hard Disk : 80GB
CD Drive : 52X

Software specification

Operating System: Windows 2000/XP
Language used : Python
Tools : NETBEANS IDE,
MYSQL SERVER,

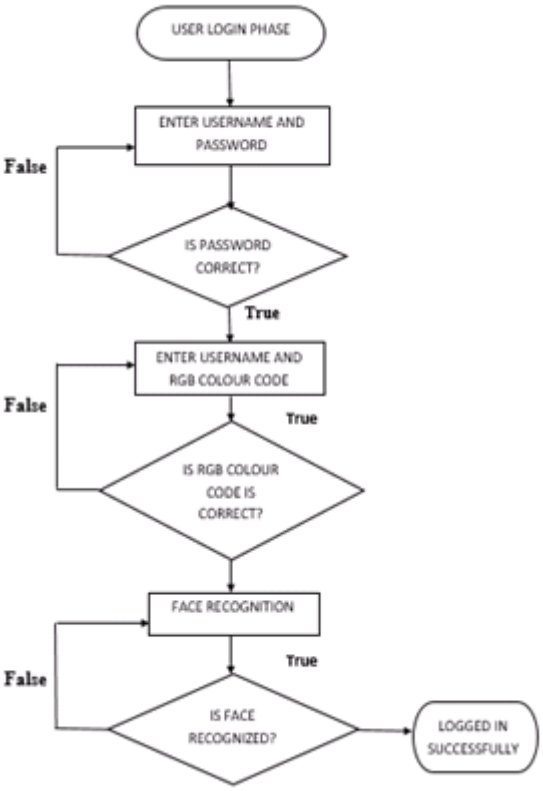
The system is divided into two phases; Registration phase and Login phase. The user will register himself at first level by using alphanumeric password then user will register himself at second level by using RGB colour pattern and at the third level users face will be stored to database as a password. In this way user will be registered to the system successfully. in a registration phase the system will require the username and email address along with-it user has to submit the alphanumeric password. User's data will be safely stored into the data base and password will be encrypted by using MD5 algorithm in order to provide security.

After the first level user will be directed towards the second level where user has to submit his/ her RGB colour pattern. The RGB colour pattern provided by the user will also be encrypted. After the successful registration of passwords the user has to register himself at third level which is face detection. At this level system will capture the user's face and the dimensions of face will be stored in a database.



For the login, user has to submit the username and appropriate passwords to the system. At very fist level user will have to submit Username along with the alphanumeric Password. The system will authenticate the user and only authorised user can access the system. User has to submit the correct password Combination. The user will be directed towards second level if and only if he/she will able to provide a correct password at first level. At second level user should submit the correct RGB colour pattern code. The system will check whether the password matches with the password which was registered previously in a database. If the pattern matches, then only user can move forward. At very last level of login phase the system will capture the user's face and the system will try to match it with previously saved dimensions in order to authenticate the user if it matches correctly the user will gain authenticate access to the system.

Although it seems a tedious and lengthy but it is an effective way to provide the security to the information.



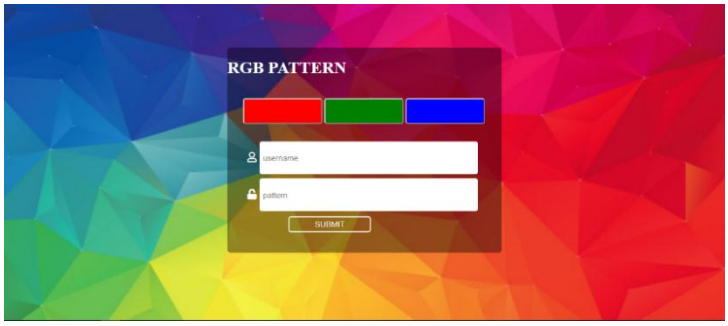
So basically, user makes use of a primary username password key-pair to log into his account. Then he is required to re-authenticate himself by providing a secondary password. The only advantage that in case a user left his account open by mistake or someone knows the primary username and password, and then they won't be able to do anything.

4. RESULT

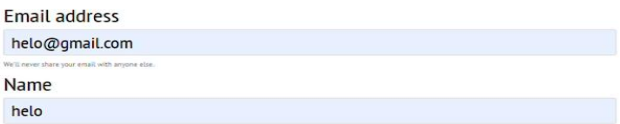
Followings are the webpages we developed while working on our project

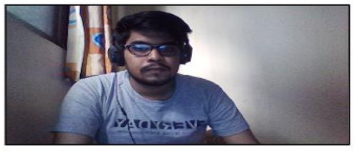
Registration page

Login page



RGB pattern





Face recognition and detection page

The project cane be divided into four steps

1. Registration of user, It consists of 2 sub steps
   - Fillings personal information
   - Creating an RBG Pattern
   - Uploading picture of user for facial recognition
2. Login using user's registered email
3. Reentering the RGB he/her created while registration process
4. Using the Face-detection system to get access to user's confidential data

5. CONCLUSION

An important usability and security goal in authentication systems is to help users to select better passwords and thus increase the effective password space. The password protection for online and offline data scheme shows promise as a usable and memorable authentication mechanism. We have developed a system

which is based on multilevel authentication method. We developed a three-level authentication system. The developed system is resistant to various attacks like shoulder surfing, guessing, dictionary attack and brute force attack. The system has three layers' alphanumeric password, a colour pattern and finally the graphical password i.e. face recognition system. This will provide high security to the applications.

REFERENCES

[1] Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget, Modeling user choice in the PassPoints graphical password scheme, Pittsburgh, Pennsylvania, USA, July 18 - 20, 2007.

[2] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[3] Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[4] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[5] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.

[6] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, Graphical Password Authentication Using Cued Click Points, Dresden, Germany, September 24 - 26, 2007.

[7] Wenjian Luo, Yamin Hu, Hao Jiang, and Junteng Wang, Authentication by Encrypted Negative Password, IEEE, 07 June 2018.