Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 549-556, April-June 2018

# A Shoulder Surfing Resistant Graphical Authentication System

G Abinaya[1], Prabha T[2], Sudha C[3], Deepika C[4] and Kokila R[5]

[1]*Assistant Professor, Department of Information Technology, V.S.B Engineering College, Karur.*
[2,3,4,5]*Students, Department of Information Technology, V.S.B Engineering College, Karur.*

*Article Received: 01 March 2018* *Article Accepted: 09 April 2018* *Article Published: 28 April 2018*

ABSTRACT

Authentication based on passwords is used largely in applications for computer security and privacy. However, while we choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. For user convenient they choose either easy or meaningful password instead of arbitrary numeric characters for easy memorization. With the help of web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. It leads to exposing passwords to shoulder surfing attack. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, an authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks is proposed. With the help of one-time login indicator, Pass Matrix concept doesn't give opportunity for hackers to figure out the password even they conduct multiple camera and video based attacks. Along with pass-matrix we have implemented dynamic virtual keyboard. Virtual Keyboard authentication has helped users to protect their username and passwords from being captured by key loggers, spyware and malicious bots. We have designed a virtual keyboard that is generated dynamically each time the user access the web site. In virtual keyboard, the keys get shuffled for every clicking event. The key position will be hidden so that attacker standing behind couldn't see the password which is pressed by user. This approach proposed makes the usage of virtual keyboard for user's security and makes it hard to identify authentication details.

## 1. INTRODUCTION

In ancient days, we used a textual password while we are logging into any authentication based website. Textual password consists of upper- and lower-case letters and numbers. It doesn't provide a secured login into the network. Network affected by the shoulder surfing and the key loggers attack. Using video capturing and camera snapshot the attacker can stole our identity details. Even though we have virtual keyboard, the keys are highlighted while we pressing it. With the help of malicious key logging software, the screenshot recording will be done while keys are highlighted. It is vulnerable to the user as well as network. It will be overcome by shuffling the keys which is present in the keyboard. And we can set a image cell as password by using pass matrix. It will secure our sensitive information like username, password, PIN and personal identity.

## 2. BACKGROUND AND RELATED WORK

There are lot of research on password based on authentication has been done in the literature. Among all of these proposed schemes, from this paper focuses mainly on the graphical-based authentication systems along with a virtual keyboard shuffling. It defines that the keys will be hidden and shuffled after we pressed a password key by using fisher Yates shuffling algorithm. To avoid the shoulder surfing and key logger attack, we introduced the above concepts. We need to choose image. After the image is accepted to split into 7*11 matrixes, we need to specify the cell to set as password. After the cell is selected as password, login indicator will be generated based on cell which is selected. At initial stage we need to create with a username. To avoid key loggers attack while we typing username and other authentication based, keys are shuffled by using above mentioned algorithm.

The following lists the research problems we would like to address in this study:

1. The problem of how to perform authentication in public so that shoulder surfing attacks can be alleviated.
2. The problem of how to increase password authentication mechanism than that of the traditional PIN.
3. The problem of how to efficiently search exact password objects during the authentication phase.

## 3. PROBLEM STATEMENT, ATTACK MODEL, ASSUMPTIONS

### *3.1 PROBLEM STATEMENT*

Nowadays there are lot of mobile devices and web services, users can access their personal accounts in the network to make communication like sending and receiving confidential business emails and posting videos and images in the cloud or revoke money from their e-bank account anytime and anywhere. While logging into these services in the public, they may expose their passwords while login into the services.

People who decided to hack our identity can watch the whole authentication procedure through video cameras and surveillance equipment, or even a reflected image on a window. Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to one's assets.

### *3.2. ATTACK MODEL*

#### *3.2.1. key logger attack*

It involves in capture a user's entire keyboard strokes while we choose the password and other personal information

#### *3.2.2. Shoulder Surfing attack*

The people who is looking over victims shoulders while they are sitting in front of terminals

#### *3.2.3. Password Cracking*

Recovering the passwords of a particular user id by applying various possibilities

#### *3.2.4. Screenshot Capturing*

Take screenshot while we choose the password in the virtual keyboard and save it as image file when key is pressed by user in the public network.

### *3.3 ASSUMPTIONS*

In this paper, we are discussing about the solution for which is enlisted in attacks. We have certain assumptions in this study:

1. Any communication between client and the server should be protected by avoiding malicious network attacks.
2. The user can login into the web services or any authentication based services without surfing passwords

## 4. PROPOSED SYSTEM

To overcome the security weakness in traditional PIN method and to protect the user identities while they are logging into any of network based system services. The security will be provided by using two main concepts. That are,

1. Pass Matrix
2. Shuffling of keys in virtual keyboard

### *4.1. PASSMATRIX*

Pass Matrix overcome the disadvantages and threats while we choosing textual password. At first stage user need to give their username for identification. Then we need to choose image cell as password after image has been spitted into 7*11 matrix. It contains three modules.

That are,

1. Image Discretization Module
2. Horizontal And Vertical Axis Control Module
3. Login Indicator Generator Module

Pseudo Code for Pass Matrix:

Pass Matrix Registration Phase Pseudo code

1. when user enters a unique username
2. for i in number of images do
3. choose an image
4. chosen image is discredited into m*n grids
5. choosing 1 square/cell from discretized image
6. if 1 square/cell chosen
7. then
8. send username, chosen image, chosen square/cell to the server
9. save it in the database
10. Complete registration
11. End if

Pass Matrix _Authentication Phase Pseudo code

1. when user inputs username & password
2. if valid(username & password)
3. then
4. login Indicator Generation
5. if verifying the shifting of horizontal &vertical bar matches the login indicator

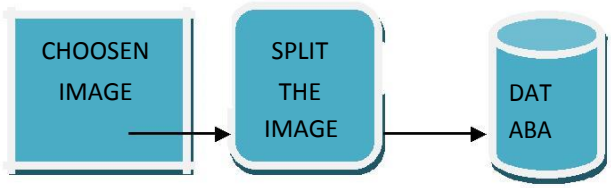
6. then Login Success
7. else
8. print invalid login
9. end if
10. else
11. print invalid username or password
12. end if

### *4.1.1. Image Discretization Module*

At this stage, the user creates an account which contains a username and a password. The password consists of only one pass-square per image for a sequence of n images. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if Pass-Matrix is applied to authentication The user has to choose images from a provided list as pass-image. Then the user will pick a pass-square or each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set. This module divides each image into squares, from which users would choose one as the pass-square. An image is divided into a 7 * 11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations. Hence, in this implementation, a division was set at 60-pixel intervals in both horizontal and vertical directions, since 60 pixels is the best size to accurately select specific objects.

### *4.1.2. Registration phase for Pass Matrix:*


Image Discretization Module:




4.1.2. Login Indicator Generator Module

It triggers a onetime login indicator that consist of many recognizable characters (such as alphabets and numbers) or visual materials (such as colours and symbols) for users to register their details in authentication phase. In this

implementation, characters A to G and 1 to 11 for a 7 _ 11 grid is used. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called.

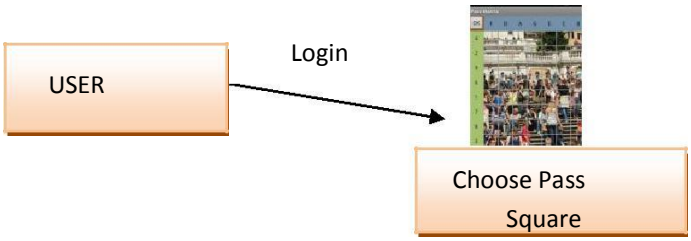
The generated login indicator can be given to users visually.

### *4.1.3. Horizontal and Vertical Axis Control*

Module:

It consists of two axis, includes two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. This control module provides drag function for users to control both bars. Users can drag either bar to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the user's pass-square.

Module Diagram




### *4.2. Shuffling of keys in virtual keyboard*

It involves in protecting our user personal information while we press keys in virtual keyboard while typing the details. It includes two modules followed by above Pass Matrix modules.

C# pseudo-code that implements generic Fisher-Yates shuffle using System;

```
class Program
    {
    /// <summary>
    /// Used in Shuffle(T).
    /// </summary>
    static Random _random = new Random();
    /// <summary>
    /// Shuffle the array.
    /// </summary>
    /// <typeparam name="T"> Array element type.</typeparam>
```

```
/// <param name="array">Array to shuffle.</param> static void Shuffle<T>(T[] array)
{
int n = array.Length; for (inti = 0; i< n; i++)
{
// NextDouble returns a random number between 0 and 1.
//  ... It is equivalent to Math.random() in Java. Intr=i + (int)(_random.NextDouble() * (n - i)); T t = array[r];
array[r] = array[i]; array[i] = t;
}
}
static void Main()
{
{
Int[] array = { 1, 2, 3, 4, 5, 6, 7, 8, 9 }; Shuffle(array);
foreach (int value in array)
{
Console.WriteLine(value;
}
}
{
string[] array = { "A","B","C"}; Shuffle(array);
foreach (string value in array)
{
Console.WriteLine(value);
}
}
}
}
```

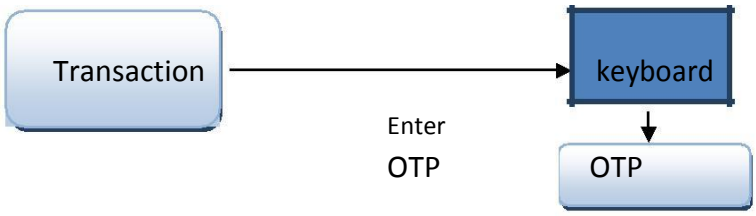
***4.2.1. Dynamic Virtual & Shuffled Keyboard Layout:***

This element the virtual keyboard design is generated. A virtual keyboard provides the best way to give input. The keys are hidden when the user clicks a particular key. After the release of mouse click, the keys are visible.

Since the keys are hidden after user presses the hide keys button, even if the screen shot is recorded it would make no sense to the attacker. For example for the same password “abdg” the screen capture would record the following things. This makes no sense to attacker and user password is thus secure. We shuffle the keyboard after every click. As a result if a person is standing behind to spoof the password over the shoulder, he cannot remember the password since the layout and arrangements of alphabet change after every click. Also noting the coordinates

would be of no help since even if the position is noted, the next click would again reshuffle the keyboard. Thus if "v" was currently at position (3, 1), the next click would have some other alphabet at the same position (3, 1).

### *4.2.2. TRANSACTION MODULE:*

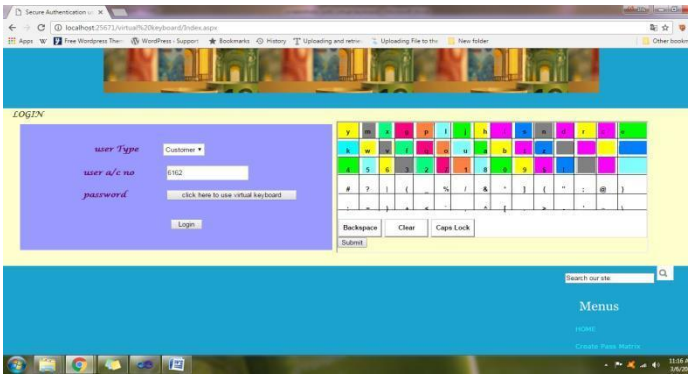


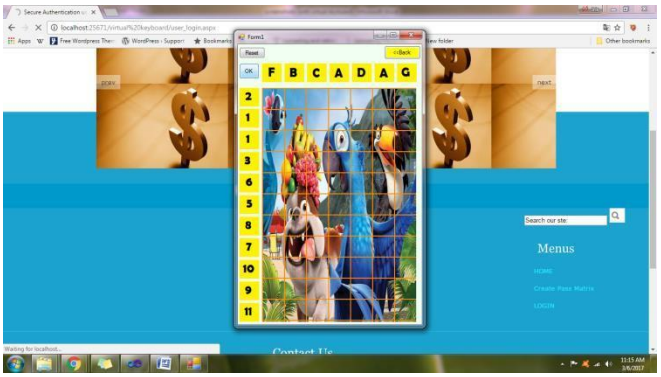

Transaction of amount will be completed by One Time Password. It will be verified to make secure transaction. The database server stores all of the information.

## 5. CONCLUSION

To overcome the disadvantages of textual password we proposed the graphical password in a banking sector as a real time scenario. Graphical password and a virtual keyboard shuffling method is used to protect the traditional password attacks while we using textual password. Our proposal system overcomes the disadvantages of textual password attacks. Due to encryption of our data additional security will be provided.

Sample output figure:



**REFERENCES**

[1] A shoulder surfing resistant graphical authentication system, hung-min sun, shiuan-tungchen, jyh-haw yeh and chia-yuncheng .

[2] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.

[3] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical password- including ISRN Communications and Networking, and International based user authentication with free-form doodles," IEEE Transac- Journal of Security, Advances in Information Sciences and Service

[4] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[5] Oakley and A. Bianchi, "Multi-touch passwords for mobile program committee members of many international conferences. He device access," in Proceedings of the 2012 ACM Conference on Ubiq- was the honor chairs of 2009 International Conference on Computer and ubiquitous Computing, ser. Ubi Comp'12. New York, NY, USA: ACM, Automation Engineering, 2009 International Conference on Computer.

[6] H. Zhao and X. Li, "S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme," in Advanced Information Networking and Applications Workshops, 2007, AINAW'07.

[7] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.