# Password Authentication using Pass Matrix to Avoid Shoulder Surfing

**PRATHYUSHA REDDY THUMMA**

*Engineer, (B.Tech), Information Technology, Kakatiya Institute of Technology and Sciences, Affiliated under Kakatiya University, Warangal, Telangana, India.*

---

**Abstract -** *Password in terms of general texts, images are used for computer, mobile applications regularly. This general, easy, convenient password cannot hold computer security and data privacy. This kind of approach usually tends to Shoulder Surfing. Applications are accessed anywhere anytime for remote server locations to local host. These general passwords can be accessed by unusual user by many means of methods and can breech the user's data. To overcome this problem, we propose an authentication system using pass-matrix. With the given login credentials provided by the user a nxn matrix is generated which covers alpha-numeric combinations. Generated alpha-numeric grid changes on time intervals. Pattern oriented selection and time changing event of grid generation makes the attacker have no clue to obtain the original password. With development of protype it is proven to resist shoulder surfing at better rate.*

***Key Words***: **Authentication, remote server, shoulder-surfing, pass-matrix, alpha-numeric**

## 1. INTRODUCTION

Accessing a particular application or obtaining few Database related information requires credentials which is formulated as "Authentication". This helps the Admin to evaluate the right user to access the data. Traditionally, there are formats like alpha-numeric, visual, biometrics, voice recognition.

Authentication through alphanumeric can have some requirements to be satisfied and hard to remember the toughest passwords. Authentication by Biometrics, visual recognition is very expensive and complex to handle.

To overcome this, password by using Pass-Matrix is proposed to build complex security for user's data. Graphical Password is created with inter-linked pattern with alpha-numeric characters.

Passwords with Pass matrix is an authentication technique in which we use (nxm)matrix to register a pattern with the valid user name. The user in the login session is asked to provide username and the alphanumeric combinations in the grid which matches the pattern drawn during the registration process. This grid value changes with time interval and cannot be reentered after a particular time. The external user who sees this combination expects the password to be the present time grid value. But the actual password is alphanumeric grid value which matches the registered pattern.

## 2. RELATED WORK

**1. Cryptanalysis of Password Authentication Schemes: Current Status and Key Issues Sandeep K. Sood', Ani! K. Sarje2 and Kuldip Singh" 1,2,3 Department 0/Electronics & Computer Engineering Indian Institute of Technology Roorkee, India e-mail: ssooddec, sarjefec, ksconfcn}@iitr.ernet.in**

Password is the most commonly used technique for user authentication due to its simplicity and convenience. The main advantage of passwords is that users can memorize them easily without needing any hardware to store them. Efficient password authentication schemes are required to authenticate the legitimacy of remote users over an insecure communication channel. In this paper, we presented the survey of all currently available password-based authentication schemes and classified them in terms of several crucial criteria. This study will help in developing different password-based authentication techniques, which are not vulnerable to different attack scenarios. Two- and three-party key exchange protocols require secure authentication mechanism for achieving the required goals and satisfying the security requirements of an ideal password-based authentication scheme. Smart cards, which are used in financial transactions require highly secure authentication protocols. Keywords: Password; Authentication protocol; Two- and three-party key exchange protocol; Smart card; Dictionary attack.

**2. Graphical Password Authentication ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. guravsm292@gmail.com Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India. lgleena90@gmail.com Prathamey K. Rane computer Department Mumbai University MCET Ratnagiri, India. prathamey@gmail.com Nilesh R. Khochare Computer Department Mumbai University RMCET Ratnagiri,India. nileshkhochare@gmail.com**

Graphical(Mutating) password is one of the alternative solutions to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally, cloud is provided with this graphical password authentication.

## 3. RELATED WORK

Providing a strong efficient password is a tough task to handle with the increasing data. As data is growing at exponential rate, the classification of data and various methodologies are used to protect the data. This various classification has made password authentication to be grouped into various classes.

In general, the graphical password techniques can be classified into 3 categories:

1. Recognition-based
2. Recall-based graphical techniques using AI technique.
3. Hybrid Scheme

A brief description of above mention classification:

### 1. Recognition-based:

Recognition based technique is also known as Cogno-metric System which used to deal with the image portfolios of iimages registerd by the user. This is basically used to deal with the password techniques where attribute are given prefernce on images.

### 2. Recall-based graphical techniques using AI technique:

It is based on invariant pass points in which user can specify the secret path to join the pass points and create a new specific password.

### 3. Hybrid Scheme:

Hybrid Scheme is complex and more efficient one to deal with as it is mixture of two or more Graphical Passwords. It enhances the performances as it overcomes the problems like Spyware, Shoulder-Surfing etc.,

## 4. SAFETY

Safety with the defined Graphical(Mutating) Password authentication encrypts the pattern-based password with alphanumeric details which are not permanent.
Mutating Password Authentication provides safety from the following threats:

1. Spy-ware attacks
2. Shoulder surfing attacks
3. Brute force attacks
4. Dictionary attacks

## 5. PROPOSED SYSTEM

The main objective of the proposed method is to design a secure login interface which is resistant to shoulder-surfing attack by providing the 8 X 8 size grid to select alphanumeric characters during the login phase. For resistance, transpose operation for columns is applied for every character selected during login sessions to prevent from guessing attack. The registration and login sessions of the proposed authentication technique are designed to be simple and as easy to use as possible by the user. And the two sessions look similar to each other.

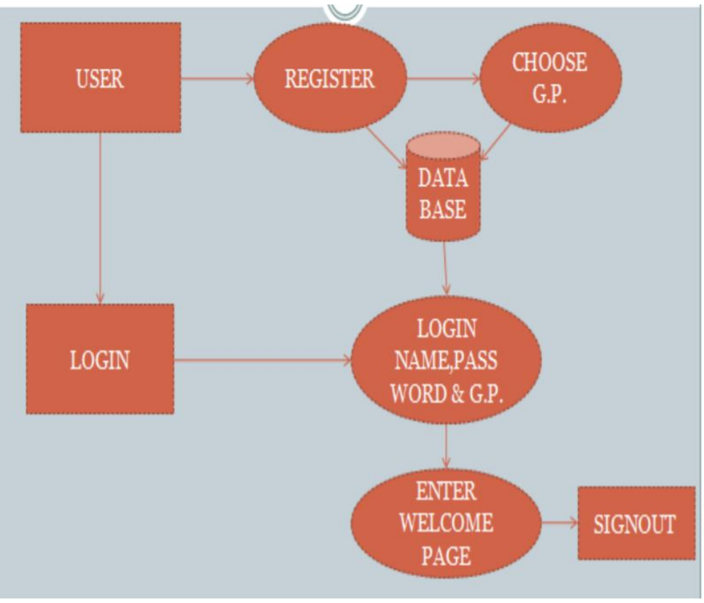


FIG:01

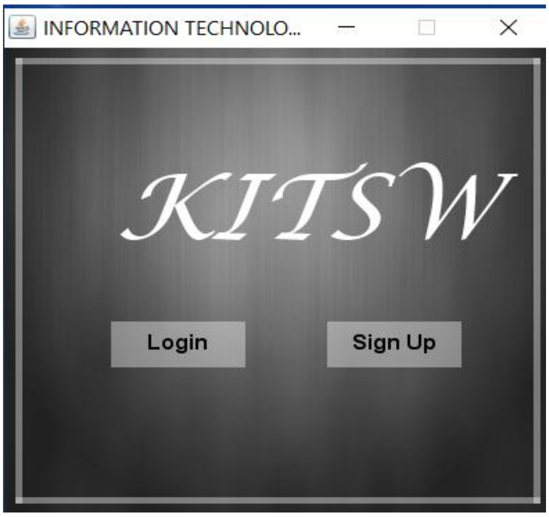
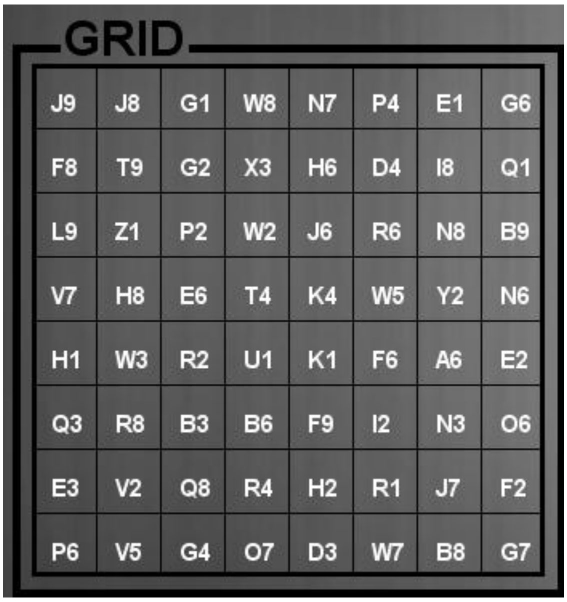


FIG: 02



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| J9 | J8 | G1 | W8 | N7 | P4 | E1 | G6 |
| F8 | T9 | G2 | X3 | H6 | D4 | I8 | Q1 |
| L9 | Z1 | P2 | W2 | J6 | R6 | N8 | B9 |
| V7 | H8 | E6 | T4 | K4 | W5 | Y2 | N6 |
| H1 | W3 | R2 | U1 | K1 | F6 | A6 | E2 |
| Q3 | R8 | B3 | B6 | F9 | I2 | N3 | O6 |
| E3 | V2 | Q8 | R4 | H2 | R1 | J7 | F2 |
| P6 | V5 | G4 | O7 | D3 | W7 | B8 | G7 |

FIG: 03

The above shown grid is time recurring alpha-numeric grid which changes for a given time. We are supposed to enter the password which matches the pattern while we have entered during registration.

## 6. CONCLUSIONS

Textual Passwords are easy to guess and get data from the users and is weak to protect. Many of the researchers found that it is not effective to use for highly confidential data.

Password authentication using pass matrix to avoid shoulder surfing ensures the security for any non - authenticated user to get the credential information easily. This method can be implicated for any application by linking to the databases, for database for only admin can get data without breech of data, for transactions in open platforms such as ATM's etc.,

Graphical(Mutating) Password protects from security attacks like Brute force attack, Shoulder Surfing attack, Dictionary attack etc., Even with wide range of security advantages Graphical Passwords are not evenly used due to high maintenance, storage issues etc.,

## REFERENCES

[1]. F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in Proceedings of the 11th international conference on mobile and ubiquitous multimedia, 2012, p. 13.
[2]. H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.Y. Cheng, "A shoulder surfing resistant graphical authentication system," IEEE Transactions on Dependable and Secure Computing, vol. PP, 2016.
[3]. X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in 21st annual Computer security applications conference, 2005.

## BIOGRAPHIES

**PRATHYUSHA REDDY THUMMA**, Dept of IT, Kakatiya Institute of technology and Sciences, Affiliated under Kakatiya University.