PATTERN-BASED GRID AUTHENTICATION SYSTEM

Mr. Rushikesh Dhanorkar[1], Mr. Saurabh Belsare[2], Ms. Janhavi Tikar[3], Ms. Ranjita Gharami[4], Mr. Novhel Rahangdale[5], Prof. Jayant Andhakari[6]

[1]*First Author Computer Science & Eng. & Tulsiramji Gaikawad-Patil College of Engineering & Technology*
[2]*Second Author Computer Science & Eng. & Tulsiramji Gaikawad-Patil College of Engineering & Technology*
[3]*Third Author Computer Science & Eng. & Tulsiramji Gaikawad-Patil College of Engineering & Technology*
[4]*Fourth Author Computer Science & Eng. & Tulsiramji Gaikawad-Patil College of Engineering & Technology*
[5]*Fifth Author Computer Science & Eng.& Tulsiramji Gaikawad-Patil College of Engineering & Technology*
[6]*Sixth Author (Assistant Professor) Computer Science & Eng.& Tulsiramji Gaikawad-Patil College of Engineering & Technology*

---***---

Abstract - The purpose of this document is to enlist the software requirements and specifications for the "pattern-based grid authentication system" which will be a new added feature to the authentication framework. User authentication is an indispensable part of secure system. Traditional authentication methods have been proved to be vulnerable to different types of security attacks. artificial intelligence is being applied to crack textual passwords and even CAPTCHAs are being dismantled within a few attempts. Existing classical authentication such as textual passwords and pattern-locks are prone to various attacks. The most popular textual-based password system is prone to shoulder surfing attacks. Another popular authentication method which is pattern lock scheme method, is widely used on mobile devices. However, numerous research studies show that users choose patterns from a small space which makes them vulnerable to a variety of attacks such as guessing attacks, shoulder-surfing attacks and smudge attacks. By this project, we will allow users to use a recall-based pattern-grid authentication system that is an advancement over these traditional systems. Our system will help in preventing user's personal assets from being stolen by their adversaries and provide an easy safe and secure way to login to any site.

1.INTRODUCTION

This project will be an added feature to the existing authentication system. Moreover, the traditional and most commonly used way of authentication i.e. The textual password is prone to dictionary attack, brute force attack and shoulder surfing attack. In this project, a pattern-based grid authentication will be developed to overcome this problem and eliminate these attacks. This project also serves the purpose of having One Time Password with no network medium like SMS/Email.

The Pattern-based grid authentication system provide pattern-based login systems to their users. The system will allow users to draw a pattern over a 3 ╳ 3 grid on the web page using their mobile phones or computer devices during registration. Whenever a user wishes to authenticate, he is presented with a random alphanumeric challenge grid. The user then enters the characters in the cells that correspond to the registered Pattern. This recall-based technique asks the user to reproduce something that the user has created earlier during the registration stage. Recall based usually requires the user to interact with the system in some cognitively meaningful manner.

1.1 Product Function

1. The user will be able register into the system.
2. User can draw a pattern on the 3 ╳ 3 grid as his password.
3. Users can login into the system using their authorized username and a recall-based password by entering the characters in the random grid according to their pattern. Services are delivered to the authorized recipient if the credentials entered are appropriate.
4. To eliminate various authentication attacks like shoulder surfing attacks, guessing attacks, shoulder-surfing attacks and smudge attacks.
5. This project also serves the purpose of having One Time Password with no network medium like SMS/Email.

1.2 User Classes and Characteristics

User class: The user class contains attributes pertaining to users such as username, email, pattern password.

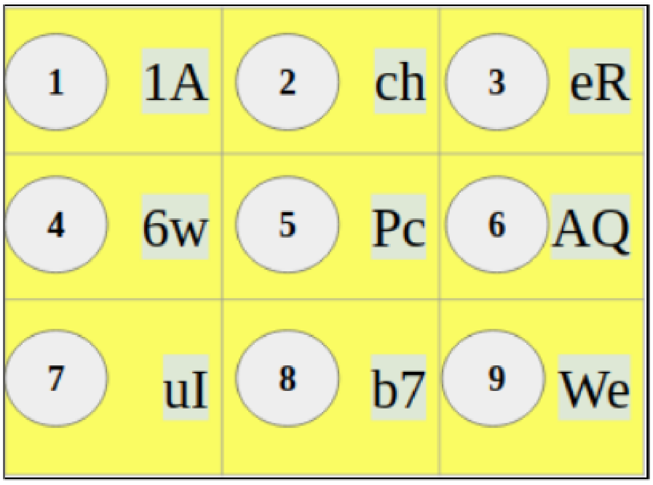
Pattern Type Class: The pattern type class can be used to customize the size of the pattern grid.

Randomization class: Randomization class is used to generate a randomized sequence of alphanumeric characters to be displayed in the pattern grid.

2. System Features.
1.Pattern Lock Module
2.Random Alphanumeric Grid Generation Module
3.User Registration Module
4.User Login
5.Reset pattern
6.Forget pattern

3. Random Alphanumeric Grid Generation Module
Registration is done using a 3 × 3 grid pattern. The selected ordered sequence of positions will be stored in the database as password for the user. During Login, a recall-based technique is used wherein the user will see a 3 × 3 grid of randomly generated characters. The user has to enter these characters in

a text input field based on the original pattern password and not actually draw the pattern again. Recall based technique asks the user to reproduce something that the user has created earlier during the registration stage. Recall-based technique usually requires the user to interact with the system in some cognitively meaningful manner. The user is required to remember their password pattern strokes that they choose during registration. The important thing for the user is to remember back the pattern sequence that they choose because, during login, they need to enter the textual password based on their sequence of pattern passwords. Access to the system is granted only when the users can recall back their pattern password and enter it correctly.



1 1A	2 ch	3 eR
4 6w	5 Pc	6 AQ
7 uI	8 b7	9 We

Randomization of the grid characters plays an important role over here. Every time the user makes a request to the login page a unique grid with random characters must be generated. This unique grid must be in a way mapped with the original password to check the original pattern-based password once he/she tries to login. This random password must also be a minimum of 8 characters long and a combination of digits, alphabets both lowercase and uppercase to increase the number of permutations and combinations and eliminate attacks like brute force etc.

Rules for generating random sequence characters:

1.Each box of the grid has 2 characters.
2.Characters can be either lowercase or uppercase alphabets or digits.
3.The character sequence is not repeated.

Algorithm:

1. Create a function say stringGenerator() which returns a random string of length equal to 2.
2. The function will use a character array of randomly placed lowercase, uppercase and digits to generate the string.
3. Create a string array of size 9 for all the 9 grid boxes indexed accordingly when request is made to the login page.
4. Loop until all 9 indexes of string are filled.
5. Start Loop.
6. Call stringGenerator().
7. Check if the generated string is already present.
8. If not present, save it in the string array.
9. End Loop if the array is completely filled.
10. Send the String array as a response.

These random grid characters will be generated on the server-side and sent to the client-side when a request is made. These characters will be randomized for every new request to the login page. This will ensure that the one-time password functionality.

4. Flow Charts.

4.1 Use Case Model
4.2 Sequence Diagram

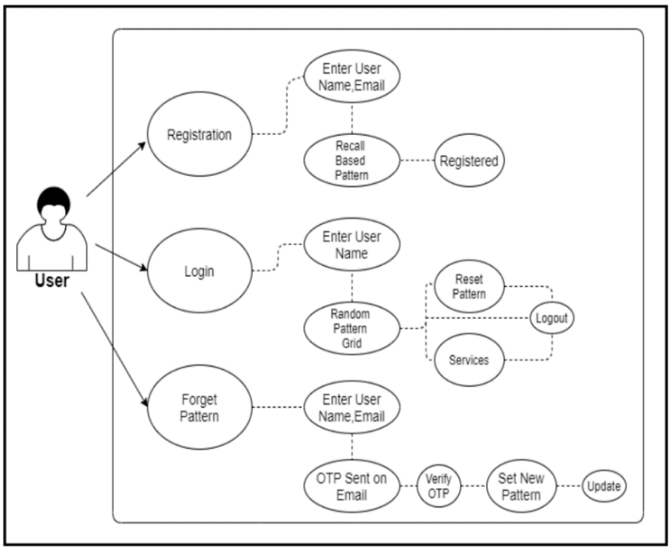


Fig- Use case model

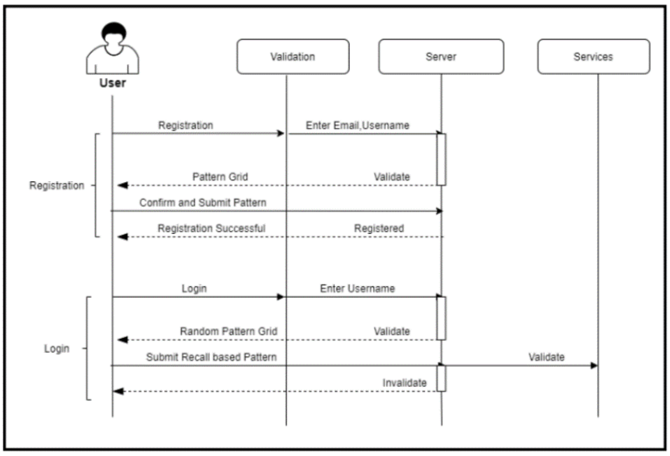


Fig- Sequence Diagram

5. CONCLUSION

The pattern-based grid authentication system represents a significant advancement over traditional authentication systems. By leveraging the power of patterns and grids, this innovative approach offers enhanced security and usability for users. One of the key strengths of the pattern-based grid authentication system is its resistance to common attacks such as brute force, shoulder surfing attack and dictionary attack. The large number of possible pattern combinations and the requirement to accurately replicate the pattern on the grid make it extremely difficult for unauthorized individuals to gain access. Moreover, the pattern-based grid authentication system offers a more intuitive and user-friendly experience.

Overall, the pattern-based grid authentication system's blend of enhanced security and user-friendly design positions it as a promising advancement in the field of authentication, paving the way for a more secure and convenient digital future.

6. REFERENCES

[1] R. Syahputri and K. S. Chan, "A new pre-authentication scheme for IEEE 802.11i wireless LAN network," International Journal on Advanced Science, Engineering and Information Technology, vol. 1, pp. 342-346, 2011.

[2] N. S. Joshi, "Session passwords using grids and colors for web applications and PDA," International Journal of Emerging Technology and Advanced Engineering, vol. 3, pp. 248-253, May 2013.

[3] S. M. S. Tabatabaeifar, M. Lashkargir, S. Taghizadeh, and H. K. Tafti, "Colour fusion in face authentication system based on visible and near infrared images," International Journal on Advanced Science, Engineering and Information Technology, vol. 1, pp. 376- 380, 2011.

[4] M. Singhal and S. Tapaswi, "Software tokens based two factor authentication scheme," International Journal of Information and Electronics Engineering, vol. 2, pp. 383-386, May 2012.

[5] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identityauthentication system using fingerprints," Proceedings of the IEEE, vol. 85, pp. 1365-1388, Sep. 1997A