

# Graphical Password Authentication

**Dr. Yokesh Babu <sup>[1]</sup>, Arunesh Gour, Shailesh Goswami**

<sup>[1]</sup> Associate Professor

Department of IoT

School of Computer Science and Engineering

Vellore Institute of Technology

Vellore (632014), Tamil Nadu, India

**Dr. Sathyaraj R.**

HOD

Department of Information Security

School of Computer Science and Engineering

Vellore Institute of Technology

Vellore (632014), Tamil Nadu, India

Email: [yokeshbabu.s@vit.ac.in](mailto:yokeshbabu.s@vit.ac.in), [arunesh.pratap2022@vitstudent.ac.in](mailto:arunesh.pratap2022@vitstudent.ac.in)

## Abstract

Passwords are universal. They are used in almost all authentication systems. Generally, password refers to text based passwords which are very common. They have their pros and cons. We use passwords almost everytime we want to log in to websites, apps, services, etc. Though this seems very easy and simple task, but for many, this is not. Generally people from non-technical background, life – experienced, mentally challenged and many others find it difficult and complex

to use this authentication, be it due to the increasing length and complexity of passwords, inability to remember them, multiple sites requiring password, each one having different rules and policies for password or unable to operate the UI due to complex procedures, so on and so forth. To address such issues, numerous researches have been conducted to replace text – based passwords with graphic based so as to solve this issue. These researches brought numerous designs on the table to make passwords less complex, allowing people to memorize them easily. But in the process, they increased the complexity of the input (or using) to a level that though the concept and benefits are worth it but the UI became a challenge instead. To solve the issue, this paper tries to find and implement a basic, viable and practical mechanism by analysing some of the existing researches.

## **Keywords**

Graphical Password Authentication (GPA), JavaScript, graphical password box, universal, UI, graphic picker, virtual tablet, library, text – based and graphic – based passwords.

## **Introduction**

Passwords are a basic yet powerful method for various authentication systems. These are used for various purposes like authenticating a user to a website, application, or service, providing one – time tokens for accessing certain services, securing a database, encryption, cryptography, etc.

Generally, when we talk about passwords, we assume it to be simply text – based, but passwords come in variety depending upon their user interfaces (UI). These are:

- Text – based (something you know).
- Biometric (something you are).
- Physical key (security key) based (something you have).
- Graphic – based (something you know).

### Text – based passwords

Text – based passwords are universal and most common, basic form of authentication.

These are used everywhere, be it on websites, applications, mobile devices, laptops, old devices, web services, web tokens, etc.

These take input using a text box from frontend and are ready to use directly at the backend.

### Biometric passwords

These require the use of special hardware to take user input. User input is in the form of biometric – fingerprint, iris scan, or any other form where the frontend captures user input as a special data, sends it to the backend which processes the input and stores it in another format, and uses different technique to authenticate users.

These are very limited in use owing to the fact that each of these require use of special hardware which itself is expensive based on the requirements.

### Security key

This is a physical key based password where the password is the physical drive itself.

Here, the frontend is the physical interface where the drive mounts to the device which then communicates to the backend of authentication mechanism to prove its identity automatically. Here, the frontend and backend automatically manages the authentication.

But since these keys are very expensive, they are rarely used by general public, even though they are more secure and user friendly.

### Graphic – based passwords

These are the type of passwords where the user input is taken using images, shapes, or in general graphics. Here, the user picks up images, draws patterns, arranges items, etc based on the mechanism implemented.

This type of password is easy to remember, shoulder smurf proof, brute force proof, dictionary attack proof, etc, but can be defeated in terms of usability due to its complex user interface.

## **Methodology**

### Existing research

Many researches have been carried out in the recent times to replace existing text – based passwords with graphics – based passwords in order to address the needs of some section of society. The target of such researches are to reduce the complexity of passwords to a level where it is easy to memorize but at the same time difficult to crack, so that life – experienced, mentally challenged, and other users can use without difficulties.

Each of the existing research proposes various methods (mechanisms) to make graphic based password authentication system more robust and user friendly, and for this they use a coupled system comprising frontend and backend modules which work together to make it a success.

But, while doing so, even if their user interface (UI) appears clean and simple, its implementation is complex from the developer's perspective. The developer not only has to configure the frontend, but also has to use the provided backend which might break existing functionalities, increase the resource usage, or introduce risks.

### Problem statement

To mitigate the issues of existing researches, such as coupled backend and frontend, non-universality, complex implementation and user interface, while still keeping the benefits of both text – based and graphic – based passwords.

### Proposed solution

We have come up with a decoupled, frontend (UI) only solution which works similar to text – based password boxes.

It takes user input in form of both text and graphics, where the texts are rendered normally, but graphics are combinations of shape and color (from a limited set), entered exactly as text – based password, that is, in order. From above input, it generates a password string, which can be used in any way depending on the developer be it treated as a normal text – based password, be it converted to another format using regular expressions, or using any other mechanism at the backend, thus allowing a wide range of possibilities by not restricting to a specific mechanism and implementation.

Also, the frontend is supplied as a library which is of plug-n-play type, thus eliminating the need for further configuration, but does not stop one from customizing it for their needs.

It comes with a graphical password box which shows current password state similar to text – based ones, a password picker (virtual tablet) to enter graphic input (combination of shape and color) and also allows user to enter password using normal keyboard with some keys mapped as special keys to allow graphic input directly without the need to open password picker (virtual tablet). And for developers, it allows to get the password string using ‘get\_password’ api.

#### Extension / future work

The proposed solution uses a very basic yet simple approach, which might not seem to stand up with current standards. But, this is just a basic demonstration of how to make a user and developer friendly graphical password box which can be extended later to implement various mechanisms like alignment – based, arrangement – based or mixed approaches.

#### **Result and discussions**

The current version of proposed solution is still under development and currently allows only a limited subset of user inputs like shapes, colors, texts due to the issue with representation of shapes and colors using built-in methods. Though by using external methods the development will speed up but it will make a significant impact on its usability.

Currently, it is able to take user input using virtual tablet (graphic picker) and directly from keyboards, but is not yet moulded in a library format, which inhibits plug-n-play model. But with further development these issues will be solved.

For now, the beautified wireframes of the implementation are depicted through the figures below.

User  
Login


---

A wireframe of a login screen. It features a light gray background. At the top, there is a white rounded rectangle labeled "Username". Below it is another white rounded rectangle labeled "Graphical Password" with a small grid icon to its right. At the bottom, there is a dark purple rounded rectangle with the word "LOGIN" in white capital letters.

*Figure 1: GPA box in login screen.*

User  
Login

---



Select shape




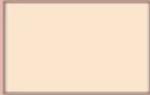




Figure 2: Graphic picker expanded – shape selection (step 1).

User  
Login

---



Select color











  


Figure 3: Graphic picker expanded – color picker; box showing current state – square selected in step 1.

User  
Login

---

A user login form with a light gray background. At the top is a white rounded rectangle labeled "Username". Below it is a horizontal bar containing a small dark red square on the left and a small purple rectangle on the right. Underneath this bar is a light red rectangular area labeled "Select shape" in black text. Inside this area are four yellow shapes: a rectangle, a square, a circle, and a triangle. At the bottom of the form is a dark purple rounded rectangle with the word "LOGIN" in white capital letters.

Figure 4: GPA box showing shape and color for 1<sup>st</sup> entry and expanded graphic picker.

User  
Login

---

A user login form with a light gray background. At the top is a white rounded rectangle labeled "Username". Below it is a horizontal bar containing five colored shapes: a dark red square, a blue rectangle, a red triangle, a teal triangle, and a teal circle. To the right of these shapes is a small gray rectangle with two vertical lines inside. At the bottom of the form is a dark purple rounded rectangle with the word "LOGIN" in white capital letters.

Figure 5: GPA box showing multiple entries, with graphic picker collapsed.



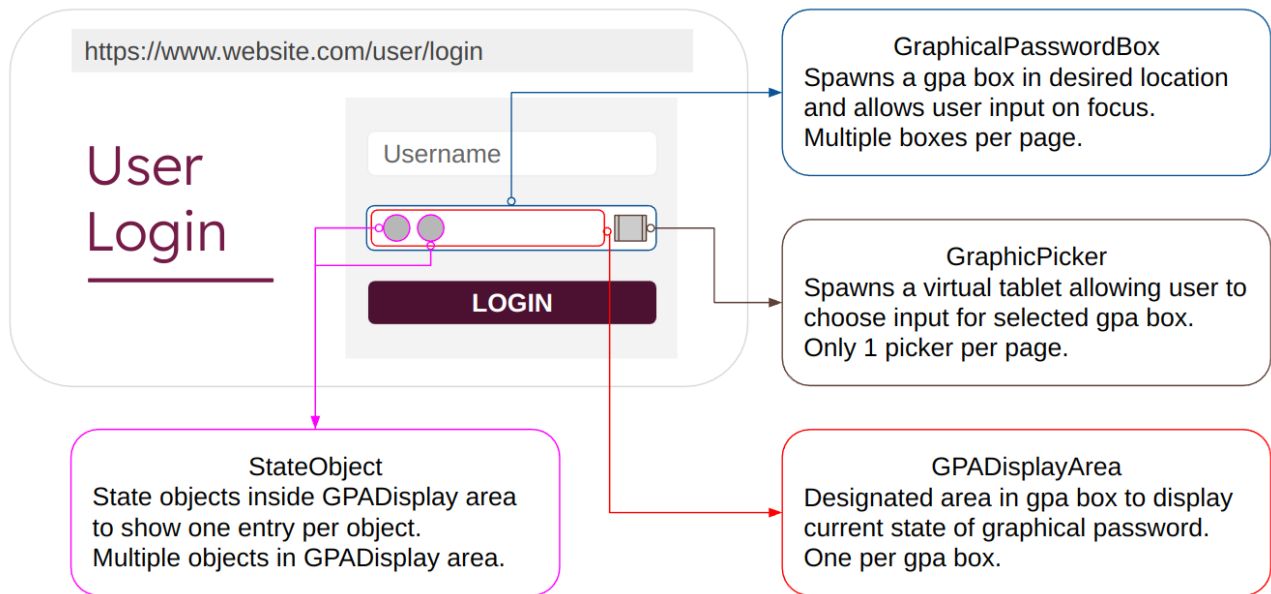


Figure 6: Graphical password box with illustrated parts.

## Conclusion

The solution proposed in this paper takes a unique approach to address current issues and manages to bring best of both worlds. Also with the progress in its development, the solution aims to add a new box – graphical password box to all systems and making it a de-facto standard in near future owing to its capability to allow graphic – based passwords as well as text – based passwords without altering the usability or working of currently implemented systems.

## References

- Danish, A., Sharma, L., Varshney, H., & Khan, A. M. (2016). Alignment based graphical password authentication system. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference On, 2950–2954.
- Abraheem, A., Bozed, K., & Eltarhouni, W. (2022). Survey of Various Graphical Password Techniques and Their Schemes. 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), 2022 IEEE 2nd

International Maghreb Meeting of the Conference On, 105–110. <https://doi.org/10.1109/MI-STA54861.2022.9837719>

Agarwal, G., Singh, S., & Indian, A. (2011). Analysis of knowledge based graphical password authentication. 2011 6th International Conference on Computer Science & Education (ICCSE), Computer Science & Education (ICCSE), 2011 6th International Conference On, 588–591. <https://doi.org/10.1109/ICCSE.2011.6028707>

Assal, H., Imran, A., & Chiasson, S. (2018). An exploration of graphical password authentication for children. International Journal of Child-Computer Interaction, 18, 37–46. <https://doi.org/10.1016/j.ijcci.2018.06.003>