International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-4, March 2023

Implementation of Graphical Password Authentication

Ranjini K, Abhi Raj, Ayush Kumar, Noor Poonia, Shambhavi Jhala

Abstract. A graphical password is a security feature. Among a given set of images, the user is asked to choose a password of their choice, which must be in a specific order. This is carried out via a graphical user interface (GUI), and for this reason, the process is often referred to as graphical user authentication. Generally, alphanumeric passwords, which are sometimes case-sensitive and may include special characters, are used. Hence, it is the most popular password authentication technique. This approach, though, has demonstrated substantial disadvantages. For ease of use and memorability, users frequently select passwords that can be easily guessed. However, a complex password will increase the likelihood of forgetting it. Researchers have developed authentication techniques that utilise photos as a password to address the issue of low security. In this paper, we address the issue of low security and present our proposed solution to this particular problem, which is based on the idea that people can remember images more effectively than text.

Keywords: ReactJS, Django, JavaScript

I. INTRODUCTION

During the early days, a text password was the only proposed method of computer authentication. Initially, text passwords were used for the authentication system. The user must always create different passwords for different systems, which should be both memorable and difficult for attackers to guess. However, text passwords are vulnerable to hacking techniques such as dictionary attacks, brute force attacks, and phishing attacks. Additionally, it is challenging for users to remember more than one text password for multiple websites.

Later on, token-based password authentication systems and biometrics were introduced as alternatives to text passwords, but again, there were drawbacks, as they require extra hardware setup and cost to set up a new system.

Finally, a graphical password authentication system was introduced as an alternative to these methods because it is inexpensive and easy to use.

Manuscript received on 26 February 2023 | Revised Manuscript received on 05 March 2023 | Manuscript Accepted on 15 March 2023 | Manuscript published on 30 March 2023.

*Correspondence Author(s)

Prof. Ranjini K, Assistant Professor, Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore (Karnataka), India.

Abhi Raj*, Undergraduate Scholar, Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore (Karnataka), India. Email ID: iabhi.raj24@gmail.com

Ayush Kumar, Undergraduate Scholar, Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore (Karnataka), India.

Noor Poonia, Undergraduate Scholar, Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore (Karnataka), India.

Shambhavi Jhala, Undergraduate Scholar, Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore (Karnataka), India.

Additionally, psychological studies suggest that users can recall graphical passwords more effectively than text passwords.

For the most part, there are two types of graphical password techniques: [1] Graphical Techniques based on Recognition, and [2] [5] Recall-based Graphical Method.

In methods based on recognition, the user must authenticate themselves by selecting one or more pictures from the ones they selected during registration. Recall-based approaches require the user to recall a process that was performed during registration.

II. PROBLEM STATEMENT

A user may find it challenging to remember numerous passwords of varying types from several websites. These passwords are also exposed to outside attacks. We offer a graphical password authentication solution that allows users to select graphical elements in a specific order, rather than establishing and maintaining a password, to provide users with both security and flexibility.

III. NOVELTY OF IDEA

It can be tough to remember long and complex passwords, let alone for so many different websites. To simplify the login process, users can create passwords in the form of pictorial representations that adhere to a specific pattern using a graphical password procedure, which they can then use to log in to the system. Enterprises can enhance the security and reliability of their system while also preserving a higher level of confidentiality. It also becomes nearly impossible to commit cybercrimes, such as dictionary attacks and brute force attacks.

IV. PROPOSED SOLUTION

We provide a secure way to enter passwords. Our solution is to build a business-to-business product which allows users to enter their passwords in the form of graphical objects [6]. Users will have to remember the pattern they chose for the pictures to log in. This provides a secure way to log in, as cyber-attacks are significantly reduced, and the chances of shoulder surfing are also much lower. Our product offers multi-layer authentication, including both text-based and image-based options, as well as the implementation of a zero-trust model.

V. IMPLEMENTATION AND METHODOLOGY

Our approach utilises Django and React.js. A JavaScript-based framework called ReactJS makes it simpler to develop interactive designs. ReactJS is the framework we chose since it makes it easier to

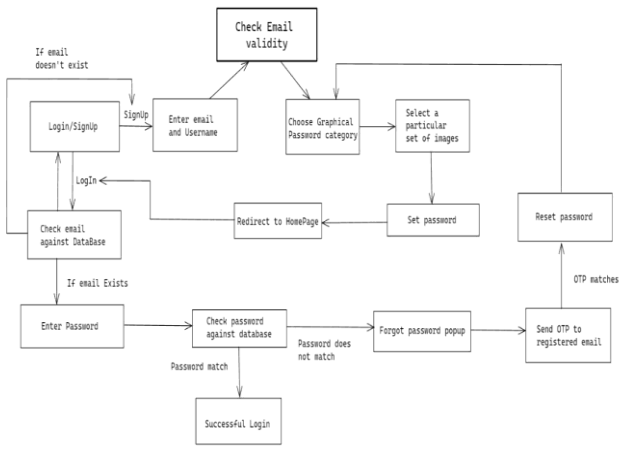
build reusable code and render and update our website quickly as needed. Django, on the other hand, is a high-level Python web framework that promotes quick development and spick-and-span style. We chose Django because it is highly scalable, fast, and safe.

Our product allows users to:

i. To register a user with a username, Email ID, and a graphical password
ii. Only an authorized person with the correct password can login.
iii. Users can be prevented from attacks while using text passwords such as Brute force, Shoulder Surfing, Spyware, Hidden Camera, and Phishing.
iv. Users can reset their user ID and password.
v. Upon multiple unsuccessful login attempts, it sends an email to the user informing them about a possible Brute force attack.

VI. BACKGROUND

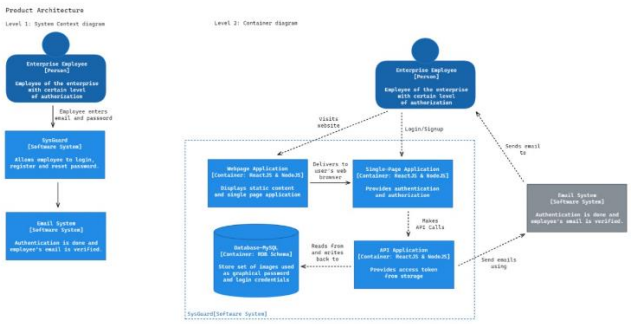
Paper Title / Author's Name	Conference / Journal Name and Year	Technology / Design	Results shared by the author	What you infer
1. Implementation of Graphical Password Authentication Technique for Security Using Cued Click Point Algorithm: Mr. Shantanu Rangiri, Prof. K. R. Ingole	IJRASET Journal for Research in Applied Science and Engineering Technology, 2022 We take an image as input from the user at the time of registration and put a quid point. Quid point is the selected part of the image which the user chooses [3]	We take an image as input from the user at the time of registration and put a quid point. The selected point is the part of the image that the user chooses.	So, we arrived at a successful conclusion that is both simple to remember and difficult to foresee. There are ways to make passwords that are more approachable for humans using graphic password schemes.	We were successful in concluding, which is simple to remember yet difficult to predict. You can make passwords that are easier for people to remember by using graphical password schemes.
2. Graphical Password Authentication System: Pathik Nandi, Dr. Preeti Savant	Ijraset Journal for Research in Applied Science and Engineering Technology, 2022 [4]	There are three alternatives presented to users who attempt to reach the Homepage: sign up, log in, and learn about the developer. The user must select the 'Register' option if they have not already registered.	To have a sound system, high security and good usability is required. To protect against various attacks, a higher level of protection can be provided for text-based passwords by incorporating colour and image-based passwords.	Adding a layer of security to text-based passwords in the form of graphical passwords will enhance the system's security.
3. Web-based Graphical Password Authentication System : Abhijith S, Sreelekshmi K U, Soja Sam, T T Samjeevan	International Journal of Engineering Research & Technology (IJERT), 2021	The server setup is done using XAMPP. SQL is utilized to collaborate with databases. On the client side, a PHP framework called CodeIgniter is used.	Users must type their passwords to authenticate themselves, making it simple for anyone to discover these passwords. To resolve this issue, a shoulder-surfing-resistant authentication method was suggested.	To establish a safe and graphical password authentication system, we need an authentication method that requires the user to follow a separate set of instructions, rather than asking them to enter their passwords.
4. Secure Graphical Password Authentication System. Rajguru Dipali, J Walunj Jyoti, Jadhav Jayashree, HandeReshma	Ijraset Journal for Research in Applied Science and Engineering Technology, 2021	A randomised pictorial grid is used in place of a physical keyboard.	The success possibility of shoulder surfing and keylogger spyware can be minimised.	It was proposed that a secure graphical password system be implemented, which offers resistance to the proposed schemes of shoulder surfing, spyware, and accidental login.



[Fig.1: Workflow]

Additionally, our product adheres to the zero-trust model, a security framework that requires all users—whether inside or outside the organisation's network—to be first authenticated, authorised, and continually validated for security configuration and posture before gaining access to applications and data.

Our product's support for multifactor authentication, a layered strategy for data and application security, is another crucial feature. This approach requires a system to request that a user supply a combination of two or more credentials to prove their identity before granting access.



[Fig.2: Product Architecture]

VII. ANALYSIS AND RESULT

A. Application

Every day, we use digital devices that require us to go through an authentication process. A straightforward authentication technique is the graphical password. Therefore, we are moving toward using it everywhere, including at the desktop and application development levels. Several programmes that now employ graphical password authentication mechanisms are:

i. Mobile Device
ii. Web Application
iii. System for file locks
iv. Desktop Security Setting
v. Enterprise Application
vi. Zero Trust Application

B. Security Analysis

Graphical password systems have two levels; they provide significant protection against attacks such as brute force attacks and dictionary attacks. This system will be shoulder-surfing resistant, making it difficult for a person to guess the password. Its password selection is broad. We utilised three levels of security authentication for this project:

The first step is to verify the text-based password.

The second step is authentication based on a colour pattern.

The third step is authentication based on graphical images.

VIII. CONCLUSION AND FUTURE WORK

We are increasingly incorporating digital devices into our daily lives. We are now able to understand the authentication procedure due to digital devices. Security must include validation, which is accomplished through authentication. Shoulder surfing attacks could occur if the authentication process is carried out in public. In both authentication systems, randomisation offers good security against shoulder surfing. Compared to other authentication techniques, the graphical password authentication method is more valuable and secure. However, there is still room for improvement in the suggested solutions for the shoulder surfing problem. The text-based password system can also be strengthened with the help of this approach. Including multifactor authentication will help with this cause.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. A. S, S. K U, S. Sam and T. Samjeevan, "Web-based Graphical Password Authentication System", *International Journal of Engineering Research & Technology*, vol. 9, no. 7, p. 4, 2021. [Accessed 13 September 2022]. https://www.ijert.org/research/web-based-graphical-password-authentication-system-IJERTCONV9IS07007.pdf
2. P. Nandi and D. Savant, "Graphical Password Authentication System", *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, no. 4, pp. 1759-1765, 2022. Available: 10.22214/ijraset. 2022.41621. https://doi.org/10.22214/ijraset.2022.41621
3. M. Rangari and P. Ingole, "Implementation of Graphical Password Authentication Technique for Security Using Cued Click Points Algorithm", *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, no. 4, pp. 1476-1479, 2022. https://doi.org/10.22214/ijraset.2022.41416 .
4. *Ijariie.com*, 2022. [Online]. Available: http://ijariie.com/AdminUploadPdf/SECURE_GRAPHICAL_PASSWORD__AUTHENTICATION_SYSTEM_ijariie1872.pdf. [Accessed: 13- Sep- 2022].
5. Sharayu S. Ganorkar1, Prof. H. V. Vyawahare 2 "Review Paper on Graphical Password Authentication Techniques "Volume 5, Issue 03, March -2018. https://www.irjet.net/archives/V5/i2/IRJET-V5I207.pdf
6. P. R. Devale Shrikala, M. Deshukh and Anil B. Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme", International Journal of Soft Computing and Engineering, Vol. 3, Issue 2, May 2013. https://www.ijsce.org/wp-content/uploads/papers/v3i2/B1528053213.pdf