International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 12 | Dec 2024 www.irjet.net p-ISSN: 2395-0072

GraphiSecure: Revolutionizing Authentication through Visual Passwords

[1]Aishwarya khune, [2]Shruti More, [3]Sanika Pawar, [4]Anuradha Narkhedkar, [5]Kshitija Awad, [6]Amruta Adwani, [7]Dr.Ms. S. P. Pawar

[1,2,3,4,5,6] *UG Students, Department of Computer Science and Engineering , SVERI's College of Engineering, Pandharpur, Maharashtra , India*
[7] *Associate Professor , Department of Computer Science and Engineering , SVERI's College of Engineering, Pandharpur, Maharashtra , India*

ABSTRACT

In the current digital era, security is still a top priority. The GraphiSecure: Revolutionizing Authentication with Visual Password project presents a multi-level, extremely secure solution that improves on conventional password protection by utilizing visual patterns and color combinations. Three levels of security are combined in this system. An image-based password, a distinctive color pattern, and a conventional alphanumeric password are included in the package. Adding another layer of protection makes it harder to get in. The architecture of the system makes it easy to integrate with other web apps and give both developers and end users strong security options.

KEYWORDS

AES Encryption, Brute Force Attack Mitigation, Color Pattern Authentication, Cybersecurity in Authentication, Graphical Password Authentication, Image Pattern Machine, Human Memory and Visual Authentication, Multi-Factor Authentication (MFA), Multi-Level Authentication Systems, Password Security Algorithms, Persuasive Cued Click-Points (PCCP), Recall-Based Authentication, Recognition-Based Authentication, SHA-256 Hashing, Shoulder Surfing Attack Prevention, Temporary Data Storage in Browser Memory, User-Friendly Authentication Techniques, Usability in Authentication Systems, Authentication Vulnerabilities, Secure Session Management

I. INTRODUCTION

The rapid growth of digital technologies has led to an increase in online transactions, communication, and data storage. Significant security concerns have been introduced by the digital revolution[1][2].Text-based passwords have been shown to be inadequate due to their vulnerability to various attacks.

The limitations of traditional passwords have become apparent in recent years. Weak passwords are easy to compromise by brute-force attacks, while strong passwords are difficult to remember and lead to password fatigue. Password reuse and recycling make it easier for attackers to gain access to sensitive information [3]. To address the limitations, researchers have looked at alternative approaches. The human brain's ability to recognize and recall visual patterns is what makes visual passwords promising[5].

II. LITERATURE SUVERY

In Dec 2009 author H. Gao proposed graphical password scheme using color login. In this color login uses background color which drop login time. Possibility of accidental login is high and word is too short. The system. developed by Sobrado is bettered by combining textbook with images or colors to induce session watchwords for authentication. Session watchwords can be used only formerly and every time a new word is generated. The advantages of this system is that it reduces the login time, session watchwords are also generated to ameliorate security. The disadvantage of this system is that it the possibility of accidental login is high and word is too short(1).

In this paper M. Sreelatha proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four couples of colors and 8 * 8 matrix will be displayed. As the color standing given by the user, the word will induce. First color shows row number and second shows column number of the grid. The disbenefit of this system is cutting element is the first letter of the word. The user has to study the standing and order of the colors. So it becomes truly agitated to user. The benefit of this system is that it's flexible and simple to use(2).

A hybrid graphical word-grounded system is proposed, combining both recognition and recall-based approaches. This system offers several advantages over traditional methods and is more user-friendly. In this system, users draw an object, which is then stored in a database linked to their unique username. The objects can be symbols, characters, shapes, or everyday objects. Users can also draw

pre-selected objects on a touch-sensitive screen using a mouse. The system performs preprocessing, followed by stroke coupling and scaling. The next step is sketch simplification, and three distinct features are extracted from the drawn sketch. The final step is hierarchical matching. A key feature of this system is its integration of recognition and recall methods, which provides greater flexibility. However, the complexity of tasks such as preprocessing and stroke integration could be seen as potential weaknesses of the system.

The authors introduced a system that combines colors and text to create session passwords. In this approach, passwords are used only once per session and are no longer valid once the session concludes. The system incorporates two types of session password schemes: a pair-based textual authentication method and a color code-based authentication method. In the pair-based textual authentication scheme, users provide their credentials.

Authentication schemes aim to give secure access while addressing implicit vulnerabilities. One similar system is the grid- grounded textual authentication scheme. In this approach, druggies register by creating a word with specific character conditions. During login, a 6x6 grid is displayed, filled with aimlessly arranged figures and rudiments that change with every login attempt. druggies must reconstruct their word grounded on the dyads of characters they registered before. Another system is the color- grounded authentication scheme, where druggies calculate on colors to produce their word. During the enrollment phase, druggies give their details and rank different colors, which are also used for authentication. While this system enhances security, it can occasionally lead to crimes if druggies misremember their credentials. To address similar challenges, an OTP- grounded system is used. This system generates a one- time word(OTP) that's transferred to the stoner's registered mobile number via messaging services. The OTP contains details about specific particulars in an image shown during login. druggies must authenticate by clicking on the correct particulars in the image grounded on the OTP.

The primary thing of this system is to help shoulder surfing attacks, where bushwhackers essay to steal credentials by observing the stoner during login. It also offers protection against wordbook attacks, brute force attempts, and guessing attacks, enhancing overall security. Advantages and Limitations Provides robust security by precluding shoulder surfing and other attacks. Dynamic interfaces make it delicate forbushwhackers to prognosticate patterns. Limitations druggies must click directly within specific areas of the image and follow the correct sequence, which can occasionally lead to crimes. By combining grid-grounded, color- grounded, and OTP- grounded authentication ways, this system provides a high position of security while addressing colorful vulnerabilities.[4]. The authors have proposed four graphical word systems. Traditional textual- grounded watchwords have been extensively used for authentication for numerous times. While they offer several benefits, they also have certain limitations. As a result, ultramodern graphical word ways have been classified into four orders recognition-grounded, pure recall- grounded, cued- recall- grounded, and mongrel- grounded systems.

In the recognition- grounded approach, druggies must study a set of images during the word creation phase. When logging in, they're needed to identify their chosen images from a group of baits. These images can include faces, icons, everyday objects, or abstract art. On the other hand, the pure recall- grounded system requires druggies to flash back the images or outlines they created or named on a grid during enrollment . druggies generally draw their word on either a grid or a blank oil.

The cued- recall system is analogous to the pure recall-grounded system, with the addition of cues to help memory. In this system, monuments are handed to help druggies recall their word.the grid which they have created or selected during registration phase. In this system the user usually draws. their password either on grid or on blank canvas. The cued- recall based system is similar to recall system but it is recalled with cueing. In this system remainders are send to the user to reproduce the password accurately. The Hybrid system is

The authors introduced a scheme aimed at addressing the issue of shoulder surfing. This system presents a novel click-based color password method called Color Click Points (CCP). It combines elements of Pass-Points, Pass Faces, and Stories. A password in this system consists of a sequence of colors, with each color associated with a specific click-point. The next color displayed depends on the previous click-point. Additi

III. PROPOSED METHODOLOGY

The approach for creating GraphiSecure centers around a multi-layered authentication system that combines visual and textual component

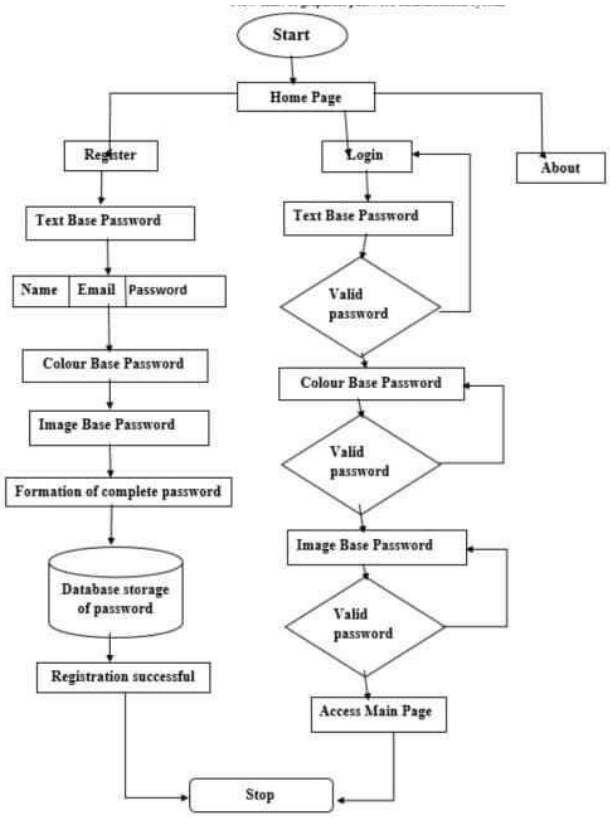

fig 1 : Block Diagram

The proposed solutions involve the use of randomized input zones, the creation of dynamic decoys, and the integration of multimodal systems that combine graphical passwords with biometric authentication.Technological Enhancements

This flowchart represents a registration and login process using a multi-factor authentication system:

1. **Start**: The user begins by navigating to the homepage.

2. **Registration Process**:he user opts to register by creating a text-based password. They also provide their name, email, and password, while setting up additional security layers: a. A color-based password b. An image-based password The complete set of passwords, including all layers, is stored securely in the database. Once done, the registration is successfully completed.

3. **Login Process**:The user selects the login option and enters their text-based password. If correct, they proceed to the color-based password.

4. Upon successful validation of the color-based password, the user moves on to the image-based password. If that is also correct, access to the main page is granted.

1**. About Section**: This section offers details about the system and its features.

2. **End**: The process concludes when the user either finishes or exits the operation.

IV. ALGORITHMS

1. **Hashing Algorithm:**

    1. When a user sets a password, it is processed through a hashing algorithm such as SHA-256, which transforms it into a fixed-length string. The original password is not stored; instead, only the hashed version is saved for security purposes. During the login process, the password entered by the user is hashed again and compared with the stored hash to authenticate the user

    2. .User Registration:

        a. The user chooses a visual password, such as a series of image selections.

        b. The system generates a hash with a unique salt and securely stores it.

    3. **Login**:

        a. The system hashes the entered password with the stored salt and compares it to the stored hash.
        b. Matching hashes authenticate the user.

2. Recognition-Based:

In this approach, users recognize and choose an item or pattern they have previously seen from a set of options. The system then verifies the selection to authenticate the user.

1. Registration Phase:

1. The user picks a series of visual elements from a pre-established library or a randomly generated selection.
2. These chosen elements form the user's "visual password."
3. The system assigns unique identifiers or feature vectors to the selected elements using a recognition-based algorithm, securely storing .

2. Authentication Phase:

1. The system displays a grid of visual elements, which includes the user's previously chosen images along with decoy images.
2. The user identifies their original selections from the grid.
3. The algorithm compares the user's chosen images with the stored identifiers to confirm the user's identity.

3. Recall-Based:

1. In this method, users must recall and reproduce a piece of information, such as a password or pattern, without relying on external cues. This approach depends on recall memory, which can be more challenging for users but is generally more secure.

1. Registration Phase:

1. The user selects a series of visual elements (e.g., images or icons) from a predefined or random set, creating their "visual password."
2. The system assigns unique identifiers to these elements using a recognition algorithm and securely stores them via hashing and salting.

2. Authentication Phase:

1. The user tries to recall and replicate their password by performing the same pattern or sequence they created during registration.
2. The system compares the reproduced input with the stored representation to verify its accuracy.

V. RESULTS AND DISCUSSION

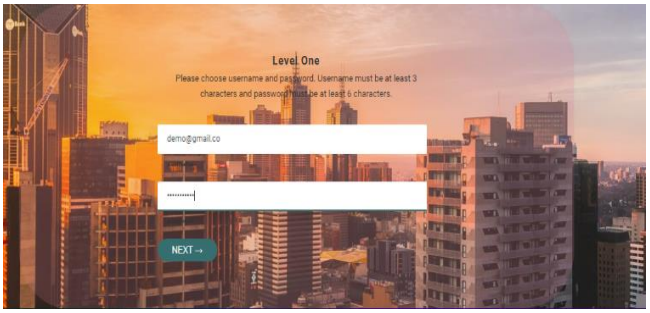

Fig 2 : Authentication Level 1

Step 1 of the GraphiSecure project, a basic login system using a username and password is implemented, laying the groundwork for security. This method guarantees that only authorized users can access the system, serving as a preliminary measure before introducing more advanced authentication techniques, such as visual passwords. By starting with a familiar and essential security practice, this approach facilitates a smooth transition for users as they progress to more innovative authentication methods in subsequent steps.

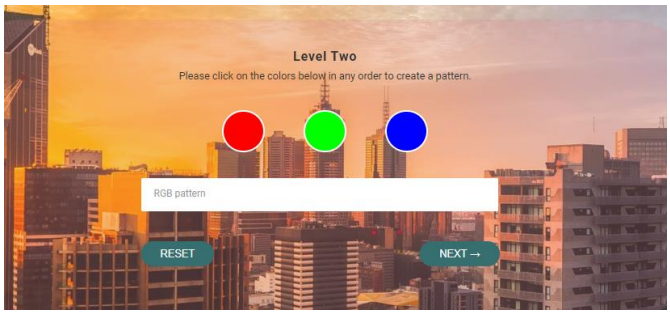

Fig 3:Authentication Level 2

Step 2 of the GraphiSecure project introduces RGB color pattern authentication, marking a major progression in user authentication. By shifting from conventional password systems to visual patterns, this method improves both security and the user experience. It allows users to design personalized and memorable authentication methods, while also setting the stage for future advancements in secure account access.

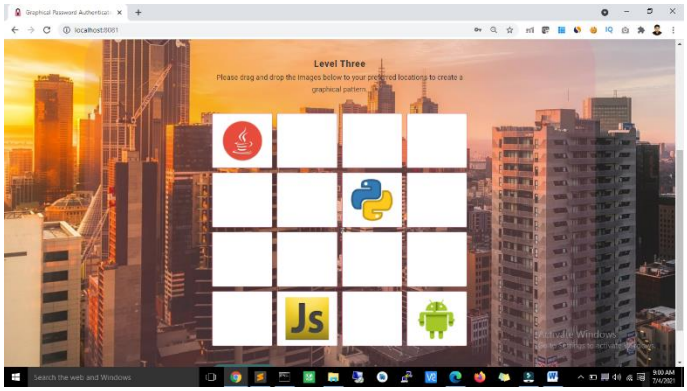

Fig4:Authentication level 3

Step 3 of the GraphiSecure project introduces grid-based drag-and-drop authentication, combining visual, spatial, and interactive security techniques. By having users create and recall patterns using movable elements within a grid, this method improves security and provides a more memorable, user-friendly alternative to traditional passwords. This multi-faceted approach makes it considerably harder for unauthorized users to access an account, even if they are familiar with aspects of the system from earlier steps.

VI. CONCLUSION

In this extended abstract, we aim to enhance the user-friendliness of our authentication system while implementing a mature and efficient Shoulder Surfing Resistant Mechanism. We have explored both text-based and graphical-based systems, focusing on reducing the cognitive load for users in remembering passwords. Given the rapid technological advancements in recent years, it is clear that system security will play a central role in the future. As a result, graphical passwords may become a key component of authentication systems moving forward.

VII. FUTURE SCOPE

The future development of GraphiSecure includes various enhancements to bolster both security and usability. Biometric authentication, such as fingerprint or facial recognition, could be integrated to provide an extra layer of security. Additionally, context-aware authentication could be implemented, adapting security measures based on factors like the user's location, device, and behavior. Machine learning may be incorporated for improved pattern recognition, enabling the system to evolve and optimize according to user interactions. Furthermore, blockchain technology could be used to enable decentralized authentication, enhancing overall security.

REFERENCES

1. Dec 2009, H. Gao proposed paper on "graphical password scheme using color login".

2. In May 2011, M. Sreelatha proposed Hybrid Textual Authentication Scheme.

3. Er. Aman Kumar, Er. Naveen Bilandi, Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India "Graphical Password Based Authentication Based System for Mobile Systems".

4. Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Computer Engineering, RTM nagpur university, M.I.E.T Bhandara, "Password Authentication Using Text and Colors".

5. Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, KJ Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".

6. Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, KJ Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".

7. In 2017 Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa, Department of Information Technology Vidyalankar Institute of Technology, Mumbai, "Color Shuffling Password Based Authentication".