RESEARCH ARTICLE OPEN ACCESS

Graphical Password Authentication Using Block-chain Technology

Yogita E. Patil [1], Bhavana D. Mahajan [2], Priyanka Y. Patil [3], Abhay M. Garunge [4]

Department of computer Engineering SSBT's COET Bambhori - Jalgaon.

ABSTRACT

Security is being free from danger, threat, or errors. In the case of computers and workstations, security is applied or measured through passwords. A graphical password is an authentication system that works with the help of blockchain technology by having the user select from images, in a specific order, presented in a graphical user interface (GUI). User data is stored in blockchain cloud so that it becomes almost impossible for the hacker to get into it and steal the credentials due to which user gel ultimate security advantages.

Keyboard: - Block-chain, Graphical, Password, Security, IPFS (Interplanetary File System), Authentication.

I. PROBLEM STATEMENT

Passwords have become an essential part of our daily digital life, and remembering multiple complex passwords can be a challenge for most users. To overcome this challenge, we can develop a graphical password strategy, allowing users to set passwords in the form of graphical presentations in a particular pattern. This approach can make it easier for users to remember their passwords and provide a more secure login process.

By using a graphical password system, users can select various graphical objects, such as images or shapes, in a particular order to create a unique password. This method can be more comfortable for users to remember as they can associate the images or shapes with something meaningful to them, such as a personal event or object.

Additionally, a graphical password system can be more secure than traditional text passwords as it can be challenging for hackers to guess the correct sequence of images or shapes. The system can also be designed with additional security features, such as a timeout period, to prevent brute force attacks.

In summary, a graphical password system can provide users with a more comfortable and secure login experience. By using images or shapes in a specific sequence, users can create a unique and memorable password that is harder for hackers to guess.

II. INTRODUCTION

Background: In today's world, passwords have become an essential part of our digital lives, as they are required for accessing various platforms and websites. However, remembering multiple complex passwords for different websites can be challenging for users. Therefore, there is a need for a project that can illustrate a graphical password strategy. The graphical password system will allow users to create passwords using a sequence of graphical objects, making it easier for them to remember their passwords.

The idea behind the graphical password system is to provide users with a flexible and convenient way of setting up passwords. Instead of traditional passwords, users can choose to use a sequence of graphical objects in a particular pattern. This method can help users remember their passwords more efficiently, as they can associate the images or shapes with something personal and meaningful to them.

The primary objective of the graphical password system is to make it easier for users to remember their passwords and provide a secure login process. With this system, users can create a unique and memorable password that is harder for hackers to guess, making it more secure than traditional text passwords. The system can also be designed with additional security features, such as a timeout period, to prevent brute force attacks.

In conclusion, the graphical password system can provide users with a flexible, convenient, and secure way of creating and remembering their passwords. By using a sequence of graphical objects, users can create unique and memorable passwords that are harder to guess, making it more challenging for hackers to gain unauthorized access.

Introduction: Graphical password systems have become increasingly popular as a secure and user-friendly alternative to traditional alphanumeric password systems. To use this authentication system, users must select images in a predetermined sequence presented within a graphical user interface. This approach is known as Graphical User Authentication.

Blockchain technology, which is a decentralized and shared distributed ledger that records transaction history, is often used for record-keeping, digital certification, and other administrative purposes. We can use this technology in our project to enhance modern-day data security.

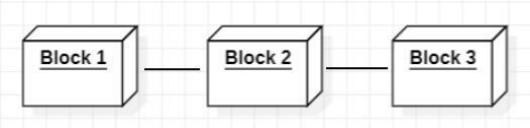
The most common method for computer authentication is through alphanumeric usernames and passwords. However, this method has significant limitations as users tend to choose passwords that are easy to interpret or guess. If a user selects a difficult password, it can become challenging to memorize. To address this issue, researchers have developed authentication methods that use images as passwords.

In our project, we use the blockchain network to store and contain graphical passwords, as the term is an immutable record of data that cannot be changed once it becomes part of the blockchain hosted on a decentralized network. This approach provides a higher level of security, as the blockchain is entirely immutable.

Considering that humans can remember images better than text, graphical password techniques have been suggested as a potential substitute for traditional image-based authentication methods. By using graphical password systems and blockchain
technology, we can develop a secure and user-friendly authentication system that is easy to remember and difficult to hack.

III. BLOCK-CHAIN TECHNOLOGY

Block-chain technology is a decentralized and distributed system that stores data in blocks linked together in a chain. It offers an alternative approach to achieving greater security by reducing vulnerabilities, providing strong encryption, and effectively verifying data ownership and integrity. The technology records information in a manner that makes it difficult or impossible to alter, hack, or cheat the system, and it can reduce security risks and eliminate fraud, thereby promoting transparency in the system. With blockchain, historical records can be kept up to date more efficiently, and the need for intermediaries can be reduced through automation. Due to its encryption features and decentralized structure, blockchain is considered a secure system that does not require intermediary fees.



BLOCK - CHAIN

IV. GRAPHICAL PASSWORD

A Graphical Password is a password system that is based on images. Users select a number of images to create their password. For instance, a user might choose different chocolates and create a specific pattern for their password, such as selecting Dairy Milk, then 5 Star, then KitKat. The next time they log in, the images will be shuffled, but they will need to follow the same pattern they used to create the password. Each time the images will be in different positions. This authentication system is difficult to crack as neither brute force nor dictionary attacks can break it. Graphical passwords are easier to remember since people remember images better than words. However, we need techniques that can be easily implemented and provide better results for this process.

V. GPA TYPES: RELATED WORK

There are various types of graphical passwords that can be used for authentication. Graphical passwords involve using images and colors to create a password. There are six main types of graphical password schemes:

A. Image-Based Scheme: In this scheme, the user selects images as their password from a grid of provided images. The user must choose the correct images in the

correct order for authentication. This is an easy-to-remember password scheme.

B. Recognition-Based Techniques: During registration, the user is presented with a set of random images from which they select a specific number of images to use as their password. During authentication, the user must recognize and select the pre-selected images in the correct order.

C. Recall-Based Techniques: In this technique, the user is not provided with any clue to recall their password. During the login phase, the user is asked to reproduce something they created or selected during the registration phase.

D. Signature-Based Scheme: This scheme uses the user's signature as their password. Signatures cannot be easily copied, and a small error in the signature can prevent access. However, this is a difficult process for users to remember.

E. Pure Recall-Based: This authentication system is difficult for users to remember, but it offers a higher level of entropy than text-based passwords. Users must draw their password on a grid or a blank canvas and redraw it to touch the listed sequence of coordinates. This is more secure than recognition-based techniques, but it is difficult for users to remember.

F. Cued Recall-Based: During the registration phase, the user selects multiple click points on an image in a specific order. The user must then select the same click points in the same order during authentication. This scheme provides hints to the user to remember their password, making it simpler than pure recall-based techniques.

VI. USED IMAGED BASED SCHEME:

WHY?

The Image-Based Scheme is based on a grid of images, similar to the Recall-Based Technique. It is neither too easy nor too difficult and is quite user-friendly. This type of password is more visually appealing, and the images are rearranged each time the user logs in, providing an added layer of security to the user's data. If a series of images is selected, a hacker would need to try each possible grouping at random. For example, if there are 100 images on each of the 9 pages in a 9-image password, there are

1009 possible combinations that could form the Graphical Password. If the system has a built-in delay of only 0.1 seconds following the selection of each image until the presentation of the next image, it would take millions of years to break into the system by hitting it with random image sequences.

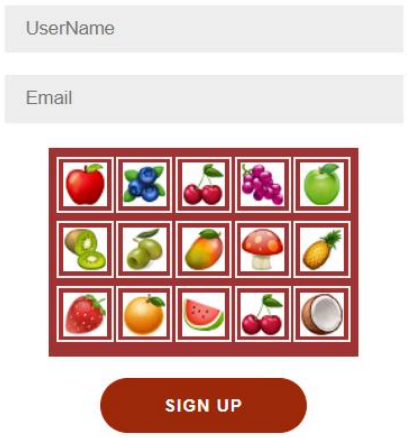


Image Based Password

Working Process:

firstly, user created account in registration page, then user enter a username, email-id, after entering user details user selected 4 or 6 number of images (Selected images are based on user choice). created account successfully. After registering, user is allowed to sign in. At the time of login user has to enter e-mail id and selected 4 or 6 number of images for password that should be matched. (i.e. exactly same as the selected
images at time of registration) sequence is matter. then after system checked and authenticate username and password, if password matched It should be sequentially correct then login successfully.in this process the text details and image based password complete data is saved in block-chain storage. Using solidity we can store our text data and image data saved in IPFS (Interplanetary File System) server. IPFS use for storing] a document, video, audio.

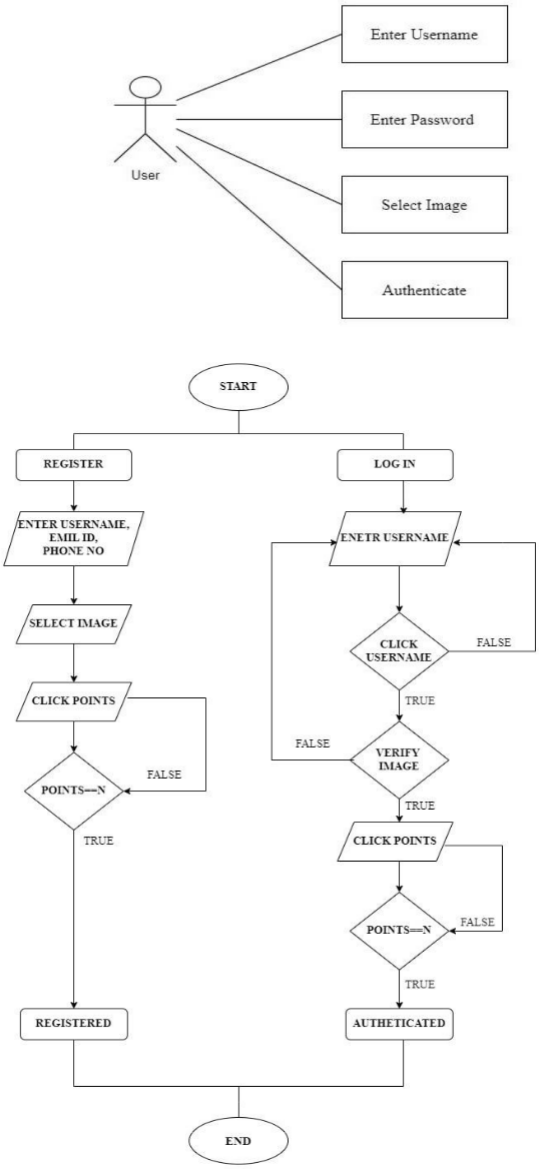


Fig. 4 Flow chart of graphical password authentication system

VII. METHODOLOGY

- The methodology of this project involves two pages for user access: register and login. If the user has not registered yet, they must click on the register option and read and agree to the terms, privacy policy, and security options provided. On the registration page, the user must provide necessary information like their username, email ID, and a text-based password. They must then select a sequence of 4 or 6 images as their password, ensuring that the order in which they select the images is remembered. After clicking on sign-up, the user's account will be created successfully.
- To login, the user must return to the login page and enter their username and image-based password. If both the text-based username and image-based password are correct, the

user will be able to log in successfully after clicking on the login button, which will authenticate the password.

- It is important to note that the project provides information about the type of security provided and has a privacy policy that the user must read before creating an account.

VIII. MOTIVE

Cyber security is a topic that is increasing in importance as the world continues to develop and rely on technology. Individuals and industries rely on their data for their daily lives and businesses. A data breach of any kind has the potential to have a several impact on those who own the data. our aim is to provide not only security but also Trust ability to user. Therefore, it is important to maintain the security. Your data has secured. But,.When Your password are secured. that' why we are using the graphical password using block-chain technology. our motive is to provide more security to user and user too trust on graphical password. cause Block-chain is Provide a trust to user.

IX. CONCLUSION

In conclusion, using blockchain technology to store and manage passwords is a secure and efficient method that makes it difficult for hackers to access. It also reduces the chances of users forgetting their passwords. The goal of this project is to develop a graphical password system that is resistant to shoulder surfing and can address the issues of weak passwords, vulnerability to dictionary attacks, and insufficient password complexity. The paper also explores blockchain-based protocols used in similar projects and aims to build a graphical password authentication system that improves security and execution.

REFERENCES

[1] Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah, "A Comparative Analysisof Consensus Algorithms for Decentralized Storage Systems," IT Professional, IEEE.
[2] https://www.ijraset.com/research-paper/graphical-password-authenticationsystem5. A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of graphical Password authentication techniques," International Journal of Computer Applications, vol. 116, no. 1, pp. 11–14, Apr. 2015.
[3] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, 2005.
[4] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication (recall-Based technique)," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.
[5] M. S. Umar and Salim Istyaq, Encoding Passwords using QR Image for Authentication, IEEE Xplore Digit. Libr., 2016.

[6] Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah, "A Comparative Analysisof Consensus Algorithms for Decentralized Storage Systems," IT Professional, IEEE.
[7] https://www.ijraset.com/research-paper/graphical-password-authenticationsystem5. A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of graphical Password authentication techniques," International Journal of Computer Applications, vol. 116, no. 1, pp. 11–14, Apr. 2015.
[8] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, 2005.
[9] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication (recall-Based technique)," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.
[10] M. S. Umar and Salim Istyaq, Encoding Passwords using QR Image for Authentication, IEEE Xplore Digit. Libr., 2016.