GRAPHICAL PASSWORD AUTHENTICATION BY USING IMAGE

Punna Srilatha
Assistant Professor
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
psrilatha191@gmail.com

Theerdhala Ramesh
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
trameshvarma2000@gmail.com

Vemula Preethi
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
vemulapreethi987654321@gmail.com

Tadepalli Ganesh
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
ganeshtadepalli1@gmail.com

Vanam Saiteja
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
vanamsaiteja1@gmail.com

***Abstract*—The usage of alphanumeric usernames and passwords is the most popular computer authentication technique. It has been established that this approach has serious disadvantages. Users frequently choose passwords that are simple to guess, for instance. On the other side, a password that is difficult to guess is frequently also difficult to remember. Some researchers have created authentication techniques that use a graphical password to solve this issue. It is an authentication method that functions by asking the user to choose from a set of photos that are presented in a graphical user interface (GUI), in a particular order.**

***Index Terms*—Information Security,Authentication,sql yog, ,SpringToolSuite4 - Shortcut,Graphical Password.**

I. INTRODUCTION

A computer security system's weakest link is frequently regarded as human factors. Authentication, security operations, and creating safe systems are the three main areas where human computer interaction is crucial, according to Patrick et al. The authentication issue is the main concern here. User names and text passwords are the most popular form of computer authentication. The weaknesses of this approach are widely understood. The inability to recall passwords is one of the key issues. According to studies, consumers prefer using short or simple-to-remember passwords. Unfortunately, it is equally simple to guess or crack these passwords.

In a recent Computerworld news item, it was reported that the security team at a large corporation performed a network password cracker and discovered roughly 80of the passwords in under 30 seconds. On the other side, complicated passwords can be challenging to remember. Studies have shown that users tend to write down their passwords or reuse them across other accounts since they can only recall a finite number of passwords.

Alternative authentication techniques, such biometrics, have been utilised to overcome the issues with conventional username and password authentication. But in this essay, we'll concentrate on a different option: utilising images as passwords.

It has been suggested that graphic password schemes could replace text-based ones since people tend to recall images more readily than words; psychological research back up this claim. Text is typically harder to recall or recognise than images. A graphical password scheme may also have a larger possible password space than text-based schemes, making it more resistant to dictionary attacks if the number of possible images is sufficiently big. There is rising interest in graphical passwords as a result of these (said) benefits. Graphical passwords have been used on mobile devices and ATMs in addition to workstation and online log-in apps. .

II. LITERATURE SURVEY

Numerous studies on the idea of a graphical password have been conducted over the past ten years. Blonder invented the first graphical password method. The security and usability metrics are kept in balance, and the attacks are thwarted to the greatest extent possible. The following categories apply to graphic password techniques:

Recognition-based Techniques: In this, the user must choose a predetermined number of images from a collection of randomly chosen photos as a password for registration and then must identify (recognize) each of those images to be authenticated.

Recall-Based Techniques: In these methods, the user is required to duplicate (recall) an action they took earlier on during the registration phase. There are two categories. Purely Recall-Based Methods Techniques Based on Cued Recall .

(a) PassdoodleTechnique: It is a handwritten image or text that is typically drawn with a stylus on a touchscreen.

(b) The user will design a picture on a 2D grid using the design-A-Secret (DAS) technique in this case. The drawing's order is used to store the coordinates of a grid that the image occupies. The user will recreate the identical image for authentication. The user is verified if the drawing contacts the same set of coordinates on the 2D grid.

(c) Signature Technique: In this case, the user records his or her signature as a password upon registration, and authentication is carried out by having the user redraw the same signature using the mouse.

III. RELATDED WORK

The usage of alphanumeric passwords is the most common method for gaining access to computer systems. However, individuals have trouble memorizing long, random-looking passwords. Instead, they provide insecure, brief, and easy passwords. Text passwords are coded phrase or series of letters and numbers that are used to authenticate users and grant them access to resources.

Cons:

1. It's challenging to remember passwords.
2. simple to recall -¿ simple to figure out
3. difficult to remember/hard to guess
4. Open to attacks such as dictionary and brute force assaults. Numerous solutions have been put forth. One of the answers is a graphic password..

IV. PROPOSED SYSTEM

It has been suggested that graphic password schemes could replace text-based ones since people tend to recall images more readily than words; psychological research back up this claim. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices. Benefits: It provides defence against password dictionary assaults, which have long posed a serious security risk to a variety of online services. Additionally, it provides defence against relay attacks, which pose a growing danger of getting through Captcha's security.

V. SYSTEMS IMPLEMENTATION

o Visual Password
o Authentication using Captcha
o Avoiding and Countering Guessing Attacks
o Underlying Captcha Security

A. DESCRIPTION OF THE MODULES:

o Visual Password :

With the help of this module's authentication and security features, users can access the information that is displayed in the Image System. The user must first have an account in order to access or search the details; otherwise, they must register.

o Authentication using Captcha :

In order to prevent online dictionary attacks, we utilise both Captcha and a password in this module's user authentication protocol, which we refer to as Captcha-based Graphical Password Authentication protocol. Unless a valid browser cookie is retrieved, the Captcha-based Graphical Password Authentication protocol-protocol requires completing a Captcha challenge after entering a valid pair of user ID and password. The user has a chance to successfully complete a Captcha challenge for an invalid user ID and password combination before being denied access.

o Avoiding and Countering Guessing Attacks : A password guess examined in an unsuccessful trial of a guessing attack is judged to be incorrect and disqualified from following trials. With more tries, the number of indeterminate password guesses declines, increasing the likelihood of discovering the password. Traditional methods for creating graphical passwords try to increase the effective password space to make passwords more difficult to guess and so necessitate more tries in order to fight guessing assaults. A brute force assault can always find the password in a graphical password scheme, regardless of how secure it is. In this study, we distinguish between two types of guessing assaults: human guessing attacks use a manual trial and error method, whereas automatic guessing attacks use an automatic trial and error approach. Transactions must also have a transaction ID and a sufficient date to be valid. Hyperledger Fabric protects against the network controller having access to change those two variables, ensuring the authenticity of the created transaction.

o Underlying Captcha Securiv:

The core of the Captcha-based Graphical Password Authentication protocol is computational intractability in object recognition in Captcha-based Graphical Password Authentication images. Most evaluations of Captcha security that have been done so far were case-by-case or used an approximation.

VI. ALGORTHM

Here is a simple algorithm for using pictures as passwords in a graphical password authentication scheme:

Picture Selection: The user selects a set of pictures from a predefined set or uploads their own pictures to create a personalized set of pictures for use as passwords. The set of pictures should be large enough to provide sufficient password space and should be diverse enough to avoid easily guessable patterns.

Picture Creation: The system generates a grid of pictures from the selected set of pictures. The user then selects a pattern or sequence of pictures as their password. The pattern could

be as simple as clicking on a single picture or as complex as drawing a specific path across multiple pictures.

Password Storage: The system stores the selected pattern or sequence of pictures as the user's password. The password may be stored in a hashed or encrypted form to protect against unauthorized access.

Password Verification: When the user attempts to authenticate, the system presents the grid of pictures again and asks the user to recreate their selected pattern or sequence of pictures. The system then verifies if the recreated pattern matches the stored password. If the pattern matches, the user is granted access; otherwise, the authentication fails.

Password Reset: In case the user forgets their picture password, the system may provide an option for password reset. This could involve selecting a new set of pictures and creating a new password or using other authentication factors, such as email verification or answering security questions.

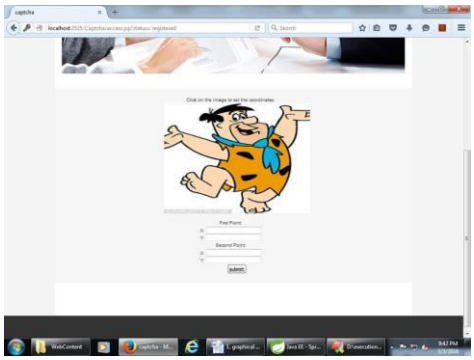
Security Measures: To enhance security, the system may implement additional measures, such as limiting the number of login attempts, detecting and blocking brute-force attacks, and periodically prompting users to update their picture password.

User Education: It is crucial to educate users about the importance of choosing diverse and complex pictures, not sharing their picture password with others, and regularly updating their picture password to maintain security.

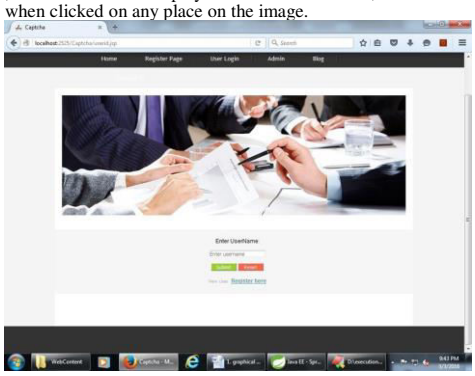
It is important to note that the implementation of a graphical password authentication scheme should also consider other security factors, such as encryption, secure storage of passwords, and regular security audits to identify and address vulnerabilities. Additionally, user feedback and usability testing should be conducted to ensure that the graphical password scheme is user-friendly and effective in improving security compared to traditional text-based password methods.

Test cases can be seen in here on the website that we have created

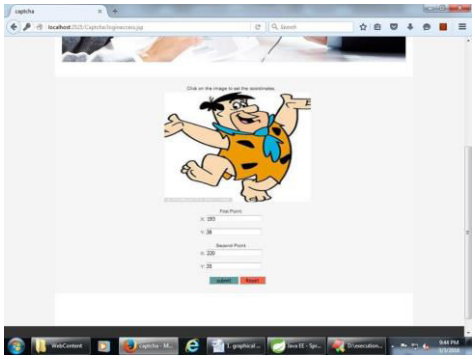
This is the registration form and also where we can enter the capcha of our liking.



Here we are going to select two places on the image ,where the axis are displayed one after the Other , when clicked on any place on the image.



After registering we will again login to our account by entering the details



After selecting the places, the coordinates of the location where we have clicked on the image Will be shown in the bottom of the screen by x and y axis.

VII. FUTURE SCOPE

Enhanced User Experience:

Image-based authentication can provide a more intuitive and user-friendly experience compared to traditional text-based passwords. Future developments could focus on further enhancing the user experience by leveraging advances in computer vision, machine learning, and augmented reality. For example, users may be able to create graphical passwords by selecting and manipulating images in 3D space, using gestures or voice commands to interact with images, or incorporating personalized images from their social media accounts.

Multi-Factor Authentication:

Graphical password authentication can be combined with other authentication factors to create multi-factor authentication (MFA) systems, which offer increased security. For example, image-based authentication could be combined with fingerprint or facial recognition, voice recognition, or other biometric authentication methods to create more robust and secure authentication systems. This could provide an additional layer of security to protect against various attacks, such as brute force attacks, dictionary attacks, and phishing attacks.

Adaptive and Context-Aware Authentication:

Future developments in graphical password authentication could focus on creating adaptive and context-aware authentication systems that dynamically adjust the authentication process based on various contextual factors, such as the user's location, device, behavior, and time of day. For example, the system could adapt the images presented for authentication based on the user's previous authentication behavior or adapt the level of difficulty of the authentication challenge based on the user's location or the perceived risk level.

Integration with Emerging Technologies:

Graphical password authentication could be integrated with emerging technologies to create new authentication methods or enhance existing ones. For example, image-based authentication could be combined with blockchain technology to create decentralized and distributed authentication systems that are resistant to tampering and fraud. Image-based authentication could also be integrated with Internet of Things (IoT) devices, wearable devices, or smart devices to provide secure and convenient authentication for these devices.

Accessibility and Inclusivity:

Future developments in graphical password authentication could focus on improving accessibility and inclusivity for users with disabilities. For example, research could be conducted on how to create graphical passwords that are more accessible for users with visual impairments or motor impairments. This could include techniques such as using audio cues, haptic feedback, or alternative input methods to enable users with disabilities to create and authenticate graphical passwords effectively.

VIII. ACKNOWLEDGMENT

The authors would like to thank the anonymous authors for their time and effort reviewing this paper

IX. CONCLUSION

The use of graphical passwords as an alternative to conventional text-based passwords has gained popularity during the past ten years. We have undertaken a thorough analysis of the graphical password approaches that are currently in use in this work. The two categories of graphic password methods used nowadays are recall-based methods and recognition-based methods. Although the primary defence of graphical passwords is that they are easier to remember than text-based passwords, there is currently little data to back up this claim due to the paucity of user studies. According to our preliminary investigation, standard attack techniques like brute force search, dictionary attack, or malware are less effective at cracking graphical passwords. However, because graphical password systems have not yet been widely adopted, the weaknesses of graphical passwords are still not completely recognised.

X. REFERENCES

1. "PassPoints: Design and longitudinal evaluation of a graphical password system" by Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), 2012.

2. "PicshaPass: A picture-based graphical password authentication system" by M. S. S. S. Bharathi and V. C. Patil. In Proceedings of the International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017.

3. "Image-based authentication: A survey" by R. Dhamija and A. Perrig. In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2000.

4. "On the design and security of graphical passwords" by Dirk Balfanz, Drew Dean, and Edward Felten. In Proceedings of the USENIX Security Symposium, 2004.

5. "Graphical passwords: A survey" by Sonia Chiasson, Alain Forget, Elizabeth Stobert, and Robert Biddle. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2007.

6. "Usable graphical password scheme" by Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2007.

7. "Gaze gestures for authentication: A proof of concept study with smart glasses" by Sophie Stellmach, Florian Alt, and Albrecht Schmidt. In Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI), 2017.

8. "A hybrid password-authentication scheme based on color recognition" by J. Chung and J. Cho. In IEEE Transactions on Consumer Electronics, 2013.

9. "ReCAPTCHA: Human-based character recognition via web security measures" by L. von Ahn, M. Blum, N. J. Hopper, and J. Langford. In Science, 2008.

10. "Security of graphical passwords: An evaluation of the state of the art" by P. C. van Oorschot, A. Salehi-Abari, and R. Biddle. In ACM Computing Surveys, 2012.

11. "ClickGesture: A novel graphical password scheme using touch gesture" by S. S. Kanhere, V. C. Patil, and M. S. S.
S. Bharathi. In Proceedings of the International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2016.

12. "iPwd: An image-based graphical password authentication scheme using color visual cryptography" by S. S. Kanhere, V. C. Patil, and M. S. S. S. Bharathi. In Proceedings of the IEEE Conference on Computing, Analytics and Security Trends (CAST), 2017.

13. "GridPix: A novel graphical password scheme using grid-based images" by G. K. Venayagamoorthy, D. Glowacki, and M. A. Hsieh. In Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA), 2007.

14. "User authentication using on-screen graphical passwords" by R. Dhamija and A. Perrig. In Proceedings of the USENIX Security Symposium, 2000.

15. "Design and evaluation of a shoulder-surfing resistant graphical password scheme".