iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43658

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Authentication by Grid Image Pattern

Raghul K[1], Suriya Prakash R[2], Thossi Bala V[3], Mr. T. N. Sudhahar[3]
[1, 2, 3]*Department of Computer Science and Engineering, Agni College of Technology, Chennai, India*
[4]*Assistant Professor, Department of Computer Science and Engineering, Agni College of Technology, Thalambur*

Abstract: ***This paper tries to point out flashy topics in an authentication system that works by having the user select from images, in a specific pattern (order), presented in a Graphical User Interface (GUI). So that the graphical password approach is called Graphical Image Authentication (GIA). The most common authentication method is to use alpha-numerical passwords. For example user tends to choose passwords that can be easily guessed on the other hand, if a password is difficult to guess then it is often difficult to remember. To overcome this problem of low security, Authentication methods change from images to passwords. Because humans can remember visuals (patterns) better than text, graphical password schemes have been offered as a feasible replacement to text-based systems. Visual patterns, rather than specific images, are easier to remember.Patterns are general easier to remembered or recognized than text. This early study implies that many graphics in graphical password systems may support memorability.***

Keywords: Authentication, Pattern based authentication, Click points, Grid images, Graphical passwords.

I. INTRODUCTION

A password is a secret that is used to verify your identity. In computer and communication systems, passwords are the most prevalent technique of identifying users. Only the user is intended to know about it. A graphical password is an authentication technique that requires the user to choose from a set of images given in a certain order in a graphical user interface (GUI). As a result, the graphical-password method is also known as graphical user authentication (GUA). Human factors are frequently seen as a computer security system's weakest link. Security operations, designing secure systems, and authentication are three significant areas where human-computer interaction is vital, according to Patrick. User authentication is an important and fundamental component in most computer security systems, and we will focus on it here. Biometrics is one of the most common authentication methods used to address the issues with traditional username-password authentication. However, we'll look at another option: employing visual patterns as passwords. According to a recent computing world news report, a significant company's security team conducted a network password cracker and found around 80% of the passwords within 30 seconds. Passwords that are difficult to guess or break, on the other hand, are often difficult to remember. According to studies, because users can only recall a limited amount of passwords, they tend to write them down or reuse passwords across multiple accounts. Alternative authentication methods, such as biometrics, have been employed to overcome the shortcomings with traditional username password authentication. However, in this paper, we will look at another option: utilising photographs as passwords. Furthermore, if the number of possible pictures is large enough, a graphical password scheme's possible password space may exceed that of text-based schemes, implying that it will be more resistant to dictionary assaults. Because of these (supposed) benefits, graphical passwords are gaining popularity.

II. LITERATURE SURVEY

TITLE 1: A Color Image Authentication Scheme With Grayscale Invariance.
AUTHOR: Jason Lin
YEAR: 2020
DESCRIPTION: Color picture authentication is a technique for detecting manipulated areas on photographs. Existing comparable works evaluated their performance based on the marked image's visual quality and detection capacity, but grayscale invariance was overlooked. Many applications in image processing, including as edge detection, colour masking in Photo shop, and e-ink display, required the colour image to first be converted into a grayscale image before any further post-processing. If the grayscale value of the produced image and the original image differs, the post-processed image may produce different results. As a result, keeping the grayscale value constant has become a major concern. A grayscale-invariance colour image authentication algorithm is presented in this paper. We recommended embedding the authentication code in two of the three major colour channels and adjusting the third to correct the grayscale value distortion. The visual quality of the marked images reached an average 33.26 dB peak signal-to-noise ratio (PSNR) while giving sufficient detect ability when each four bit authentication code was embedded into two colour channels, according to the experimental results.

TITLE 2: Image Based Authentication System
AUTHOR: Pintu R Shah
YEAR: 2013
DESCRIPTION: Because of its simplicity and ease, username and password are the most often used authentication system. However, it has some flaws, such as people choosing weak passwords, users exposing their passwords, and so on. This compromises the organizations security stance. As a result, we propose a new authentication mechanism based on images. According to research, using images for some applications may be more successful in terms of security and convenience of use. This is due to the fact that humans are better at recognizing photos than passwords. We describe a new image-based authentication system that may be used alone or in conjunction with existing character-based authentication systems to improve security and usability. We integrated the aforementioned mechanism with the present authentication system (username and password). We conducted the user survey. Seventy users, including students and staff, evaluated the system and provided feedback. One of the significant findings was that 97 percent were able to register with the system and 94 percent were able to successfully authenticate with the system after the analysis. This article presents and discusses the results of user input.

TITLE 3: Image Based Authentication Using Zero-Knowledge Protocol
AUTHOR: Zarina Mohamad, Lim Yan Thong, Aznida Hayati Zakaria, Wan Suryani Wan Awang
YEAR: 2018
DESCRIPTION: User authentication is one of the most pressing issues in information security today. When utilizing text-based strong password schemes, there is a lot of security, but remembering those solid passwords is often difficult, so people write them down on a piece of paper or save them in their smart phone. Graphical User Authentication (GUA) or simply image-based Password is an alternative to text-based authentication that is based on the idea that humans remember visuals better than text. This method makes it simple for people to create and remember passwords. However, one of the major problems that GUA is dealing with is a shoulder surfing attack that can record users' mouse clicks and eavesdropping. In this research, we present a new technique that uses the zero-knowledge protocol to solve the eavesdropping and shoulder surfing attacks and improve system security. Users confirm they know the graphical password without sending it via the zero-knowledge protocol. In other words, the user does not divulge the password to others or give it to the verifier. Hackers attempting to eavesdrop the password will be unsuccessful because the password is neither transferred over an insecure channel such as the Internet nor revealed. As a result, it is a secure method of preventing interception by other parties or adversaries. This project will produce a safe authentication method that is also user-friendly.

III. EXISTING SYSTEM

Graphical User Authentication (GUA) is a type of password authentication that uses a graphic or a picture as the password. Graphical Authentication Techniques are classified into three types in most publications published between 1995 and 2020, which are Pure Recall Based, Cued Recall Based, and Recognition Based. All of these solutions work on the same principle of authenticating users using a graphic-based technique. To be specific, with a graphical user authentication system, a user must select a memorable image as his password in order to login or authenticate.

The nature of the picture process and the exact sequence of click locations influence the process of selecting memorable images or graphical passwords. Images with significant content should be used to improve the user's memory because meaning for random objects is weak. Users must replicate their passwords without being offered any reminders, clues, or gestures in the Pure Recall-based Technique.

Although this category is simple and convenient, consumers appear to have trouble remembering their passwords. Users in the Pass Point system can easily and rapidly establish a valid password, but they have greater difficulty remembering it than alphanumeric users. For newbies, the practice requires more trials and time to complete. However, this approach takes longer to log in than the alphanumeric method.

The fundamental purpose and most crucial requirement of a user authentication process is security. Similarly, various ways exist primarily to challenge the system's authentication. As a result, schemes must be assessed in terms of their vulnerabilities and susceptibility to various assaults, because no system can guarantee complete security. Shoulder surfing refers to getting a user's password by direct observation when the user is not employing adware or external recording equipment. Shoulder surfing assaults are vulnerable to the majority of graphical password schemes.

A. Disadvantages Of Existing System

1) It's difficult to recall more similar images.
2) Choosing a pattern in a single image is difficult and memory-intensive.
3) It takes longer to log in using this way than it does using the alphanumeric method.

IV. PROPOSED SYSTEM:

The most extensively used authentication techniques are knowledge-based strategies, which include both text-based and picture-based passwords. Recognition-based graphical techniques and recall-based graphical techniques are two types of picture-based techniques.A user is shown with a series of photos using recognition-based approaches, and the user passes authentication by recognizing and identifying the images he or she selected at the registration step. A user is prompted to recreate anything that he or she generated or selected earlier during the registration stage using recall-based techniques.

We use click point patterns coupled with graphical images in the suggested system to solve the problem that emerges from password sharing and selection. As a result, the system seeks to achieve the following:

1) Authentication should not be relied on accurate password remember.
2) Make password sharing and writing tough.
3) Ensure a positive user experience.

It's also a known truth that humans remember patterns faster than they recall words or images, and that they can recognize patterns despite distractions and keep them over time.

A. Advantages of the Proposed System

1) Adds an additional layer of security to the existing system, making it more secure.
2) The user must provide the password as well as click point patterns to log in, which prevents password sharing. Pattern sharing is tricky.
3) Defends against brute force attacks. After three failed attempts, the user's account is locked. Administrators have the ability to unlock this.
4) Bots cannot be attacked automatically.
5) Remove the potential of using an intersection attack to deduce the user's click points pattern.

V. METHODOLOGY

The user must first create an account using the graphical password approach. For registration, users must provide information such as their name, email address, and graphical image pattern. A graphical image pattern is a set of grid pictures from which the user must choose images in a pattern. There are 36 grid photos in our procedure; the minimum number of grid photographs required for authentication is four. In general, patterns are easier to recall or recognize than words. As a result, rather than employing photos, we use the pattern as an input. The user must then log into the system and select the image pattern that they chose during the registration procedure. The user will successfully login and gain access to the system if the click point pattern is picked or in the correct sequence, which is where the password is hidden.

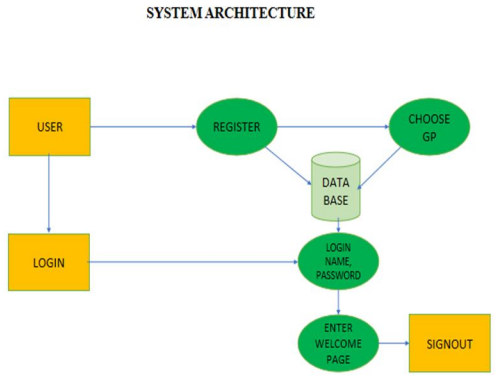


Fig. 1.System Architecture

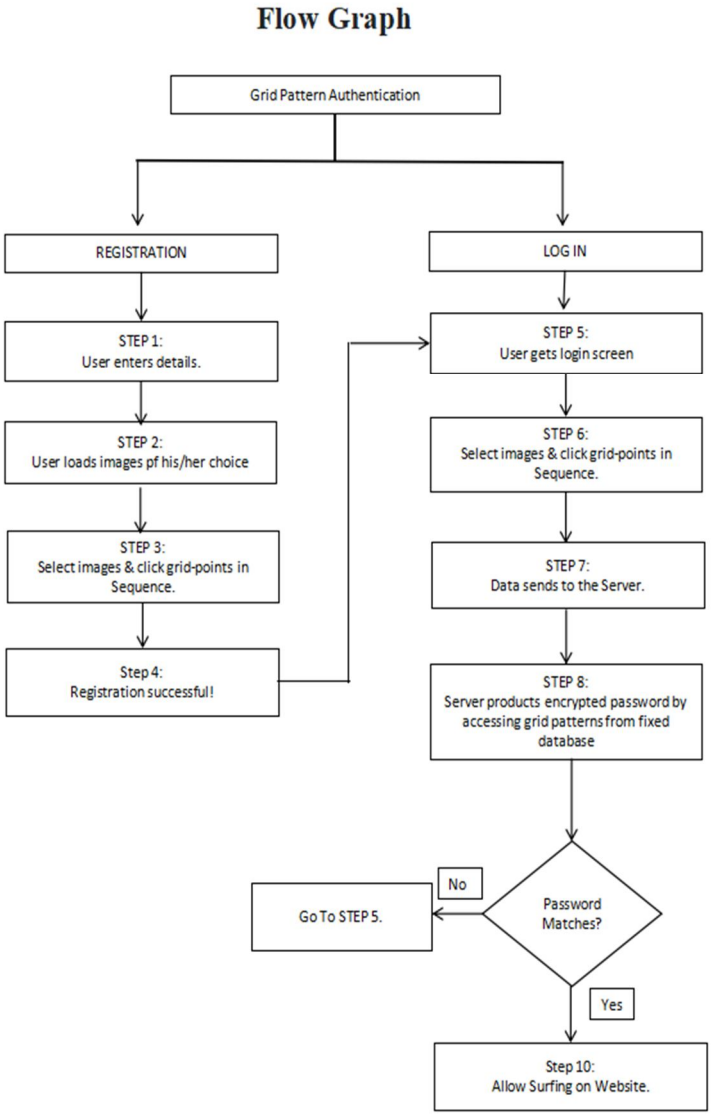


Fig. 2.Flow Graph

VI. OUTPUT

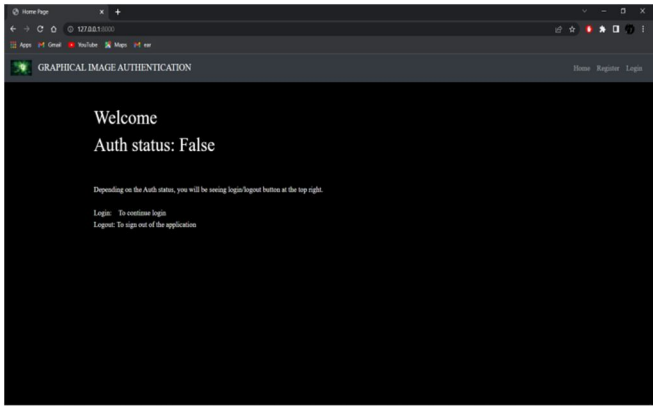


Fig. 3.Home Screen

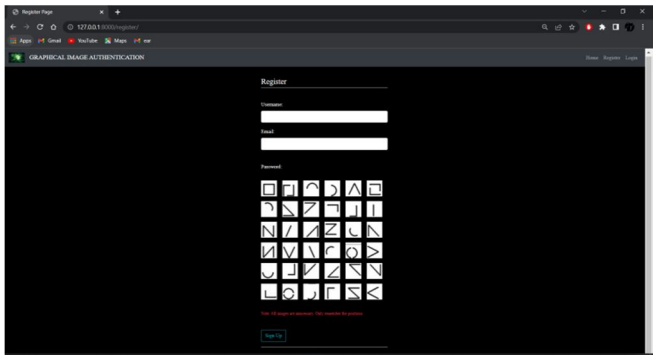


Fig. 4.Register Screen

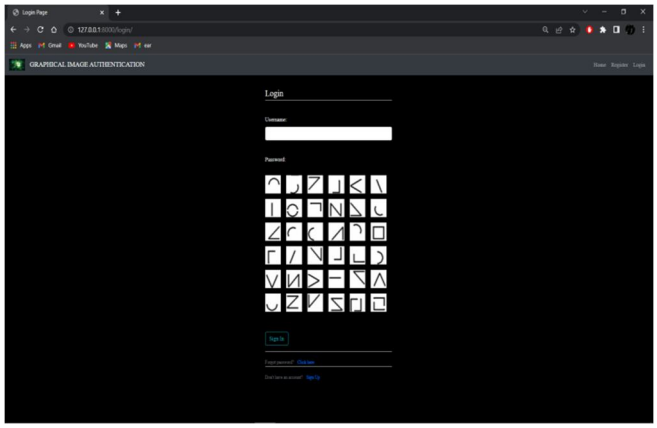


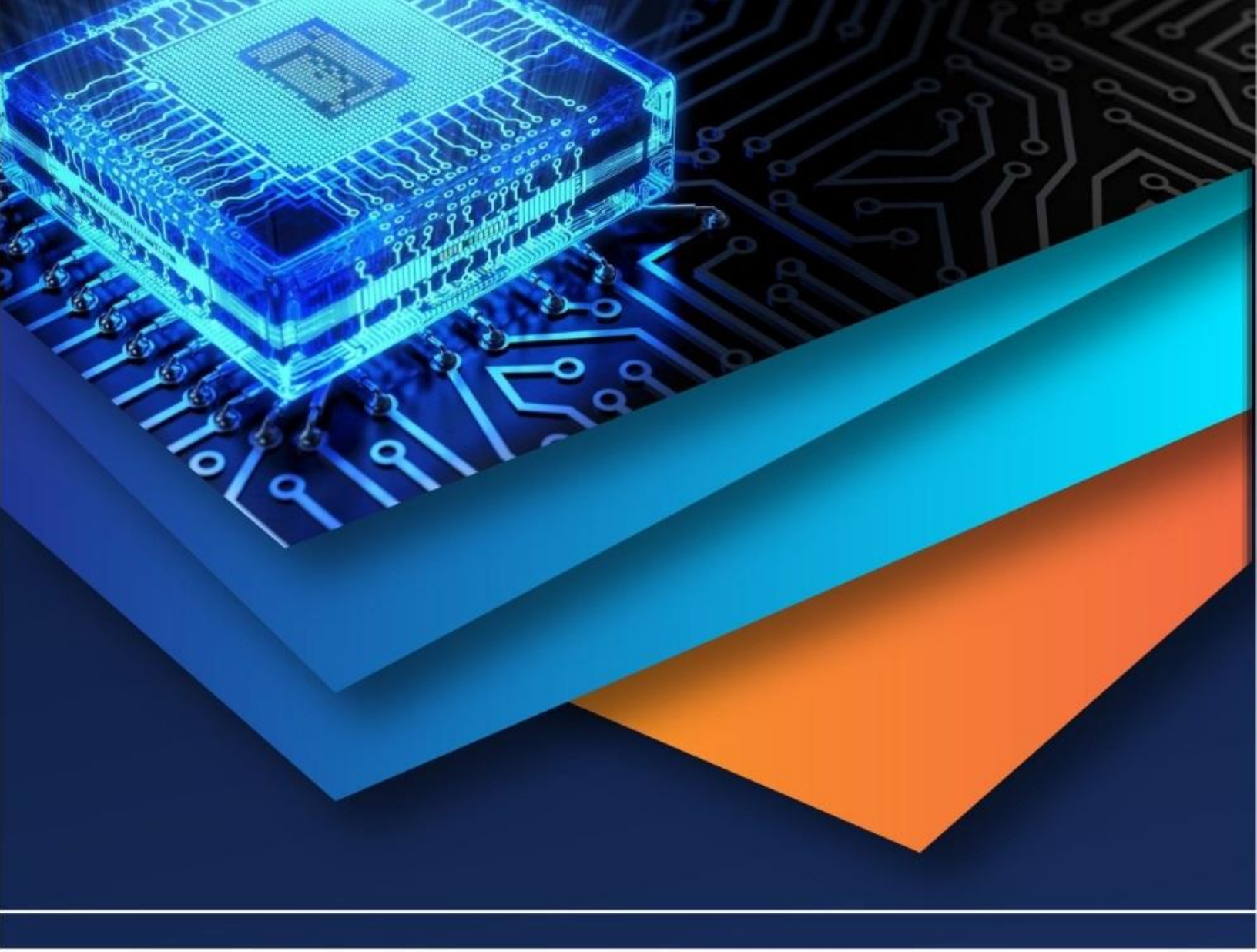
Fig. 5.Login Screen

VII.CONCLUSION

This project was created for information security. We used a grid picture click points pattern instead of a standard alphanumeric password. This is a user-friendly module that makes it simple to establish and remember passwords. There are several ways to guess a numeric password, but this method surpasses all of them. If the user fails to login three times, the account will be locked, and the user will receive an email with instructions on how to unlock the account. To be more explicit, in order to login or authenticate with a graphical user authentication system, a user must choose a memorable image as his password. A user authentication process's primary goal and most important need is security. It's also well knowledge that humans recall patterns faster than words or images, and that they can recognise patterns despite distractions and retain them over time.

REFERENCES

[1] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 2013).
[2] IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING VOL.9 NO.2 YEAR 2012.
[3] IEEE Transactions on dependable and secure computing Vol.9 No.2 Year 2012.
[4] R. Biddle, S. Chiasson, and P. van Oorschot, Graphical passwords: Learning from the first twelve years, ACM Computing Surveys (to appear), vol. 44, no. 4, 2012.
[5] World Research Journal of Human-Computer Interaction ISSN: 2278-8476 & E-ISSN: 2278-8484, Volume 1, Issue 1, 2012.
[6] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
[7] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops).Ft. Lauderdale, Florida, USA., 2003.
[8] K. Gilhooly, "Biometrics: Getting Back to Business," in Computer world, May 09, 2005.
[9] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33,pp. 168-176, 2000.
[10] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402
[11] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13thUsenix Security Symposium. San Diego, CA, 2004.
[12] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176,2000



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY