iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.49669

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 11 Issue IV Apr 2023- Available at www.ijraset.com

Click and Session based Captcha as Graphical Password Authentication Process using AI Technology

Ms. Kowsalya[1], Mr. Yogalingam[2], Mr. Sanjay Prasath[3], Mr. Surya Prakash[4]
Department of CSE, Erode Sengunthar Engineering College, Perundurai, Erode-638 057

Abstract: ***Graphical passwords, two-factor authentication, and other ways are just a few of the many options we have for authentication. Text based protection. Codes are susceptible to a variety of assaults, including dictionary attacks. As a result, as part of the authentication procedure, in addition to the usual alpha-numeric password, we also utilise pictures with captchas. It also fixes the problems with the pass points of graphical password systems. Automated Turing Test for Computers and Humans that Is Completely Public (CAPTCHA) Users who have successfully authenticated must pass a test in order to access their individual mail accounts. Accounts that put the secrecy, reliability, and privacy of data at risk are attacked by bots and other malicious software. This was stopped by the invention of CAPTCHA.***
Keywords: Captcha, Validation, CaRP, Graphical Password, Speculating Assults.

I. INTRODUCTION

In our daily lives, security is of utmost importance. Early systems primarily utilised text passwords, which are quite lengthy passwords are challenging to remember. "Completely Automated Public Apart" is known as CAPTCHA. A bot is a malicious programme that can do automatic operations across a network, which causes trouble for the network. One such defence against these harmful software programmes like Bots is CAPTCHA Many people use names, phone numbers, or any other easy to remember phrase, but they are particularly susceptible to hacking. We must create passwords that are difficult for hackers to guess in order to protect our data and information.

A graphic password is one that uses graphics for security and can be used for hot zones, pass points, etc. The usage of captcha at the next level of the advanced approach allowed for the separation of humans from bots. In situations where Captcha challenges were intended to be completed by humans, CaRP can be utilised to prevent relay attacks. If CaRP and dual view technologies are used together, shoulder surfing attacks can also be avoided. . As a password, users are required to click on the image or any portion of it, and these points or images are then saved as a graphical password. Every viewer sees a different version of these photos. Along with the standard user password, the newly produced graphical password is utilised. Access credentials Login credentials help protect the university's networks and shared information systems (user IDs and passwords). In most cases, access passwords are a crucial component of personal computer security.

Typically, offices are open, communal places, making physical access to computers difficult. cannot be fully under control. If the software allows it, you should think about creating passwords for any particularly sensitive programmes installed on your computer (such as data analysis software) in order to secure it. snooper's eye protection Here on the medical campus, we deal with every aspect of clinical, scientific, educational, and administrative data, therefore it's critical to take every precaution to limit data accessibility to unauthorised people. antivirus programmes Antivirus software that is current and well configured is crucial. Although our network machines have server-side antivirus programmes, you still require client-side antivirus software (your computer). you still require client-side antivirus software (your computer).

II. OBJECTIVE

The goal of the project is to demonstrate several captcha and graphical password strategies that may be used to safeguard any network application. to provide a dependable system and to stop various security assaults. Implementing a new picture captcha system to defend against spyware attacks is one of the system's goals. The majority of internet systems use it. Only three attempts at login are permitted with this system. When a user tries to log in to the system more than three times, the system can block that user's id.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

III. MOTIVATION

The usage of alphanumeric usernames and passwords is the most popular computer authentication technique. To access accounts or restricted areas of a website, you are required to remember username/password combinations using this authentication mechanism. Protocols for password authentication fall short when they are not taken seriously. This entails creating challenging passwords and preserving confidentiality.

IV. LITERATURE REVIEW

A. Related work

Images were employed in graphical password schema and other authentication methods, such as pass points hot spot, as passwords for authentication. Images were utilised one after another to unlock; this preserves the clickthrough pattern on the pictures. To verify user clicks, utilise pass logic. For recognition-based methods, photo dummies must be identified. Face recognition is one of the methods of authentication listed by Pass faces. The faces are organised into grid parts and recorded in the database, with the grid sections being noted for confirmation. When the sections match the authentication time, they are accepted; otherwise, they are rejected. Users frequently select passwords that are simple to remember, have patterns, and are therefore susceptible to brute-force dictionary attacks when using text based password schemes. This prompts us to wonder if users' propensity to select memorable passwords makes other password types (such graphical ones) also vulnerable to dictionary attacks. For systems where passwords are generated exclusively from a user's memory, we provide a method to foresee and model several such classes. Our theory states that these classes specify weak password subspaces exploitable by attack dictionaries. This method is used in conjunction with cognitive research on the retention of user-generated graphical passwords.

V. EXISTING SYSTEMS

The most noteworthy early invention is Captcha, which separates human users from computers by posing a challenge—a riddle, really—that is difficult for computers but simple for people. Today, captcha is a common Internet security method used to prevent bots from abusing online email and other services. To prevent bots from misusing online email and other services, captcha is currently a common Internet security mechanism. These drawbacks, which include being difficult to grasp, inaccessible to people with disabilities, time consuming to decipher, and technically troublesome with particular browsers, may be significantly improved with the inclusion of artificial intelligence. Due to severe distortion or a higher degree of complexity, some of the photos are unreadable because the letters are overlapping.

A. Dis Advantages of existing

In comparison to the widespread use of cryptographic primitives based on challenging arithmetic problems, this paradigm has only had a limited amount of success.

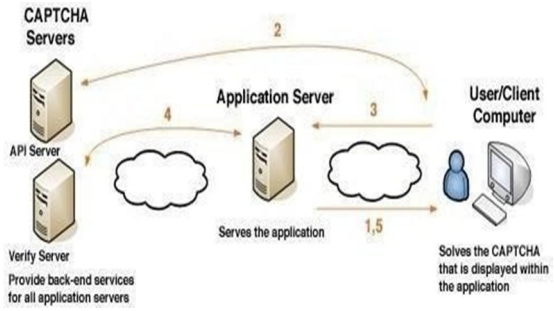
VI. PROPOSED SYSTEMS

By employing photos (captcha) We have one of the passwords as provided an additional authentication technique to distinguish between bots and people and to prevent supercomputers from being hacked. Here is a security-related addition to the general registration process. Discussing image authentication under graphics Graphical passwords, captcha in a picture format, and making it one of authentication, threats have all been taken into consideration. Our graphical password system is built on a combination of text and image passwords. For the login to be successful, the user must choose the appropriate image from the ones they already selected during registration. implementing the recognition-based CaRP Click Text technique, is done to increase security. Click Text offers clients additional security because it is an upgraded version of CaRP if a password is forgotten, chosen using a click based system, the puzzle is In addition to having distorted graphics, it is also more challenging to finish. CaRP is a captcha-enabled graphical password system. When used in conjunction with dual view technology, CaRP can stop shoulder-surfing attacks as well as online guessing attempts and relay attacks.

A. Advantages of proposed

CaRP provides defence against password dictionary attacks, which have long posed a serious security risk to a variety of online services. Additionally, CaRP provides defence against relay attacks, which are a growing danger to defeat Captcha security. By decoding a click based graphic CAPTCHA, any spyware entering a webpage will have a very difficult time doing so. The suggested system is protected from spyware attacks.

VII. ARCHITECTURE DIAGRAM



VIII. MODULES

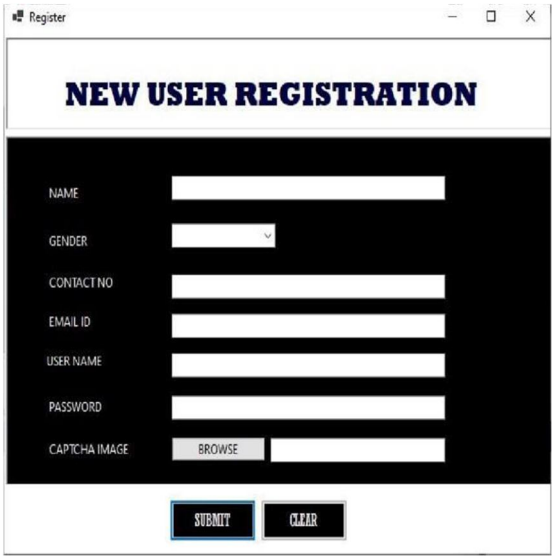
1) Graphical Password
2) Captcha in Authentication
3) Overcoming Thwart Guessing Attacks
4) Security Of Underlying Captcha

A. User Registration

In this module, users must authenticate themselves in order to access the informationdisplayed in the image system. Users must have an account in order to access or search the details;otherwise, they must register. General information, such as the user's name, email address, user name, and password—all alphanumeric—are requested on this page. After providing this information to the server, the pageredirects to the captcha selection page, where theuser must choose a captcha from a list of fake images; however, we've only included a few for simplicity.

B. User Login

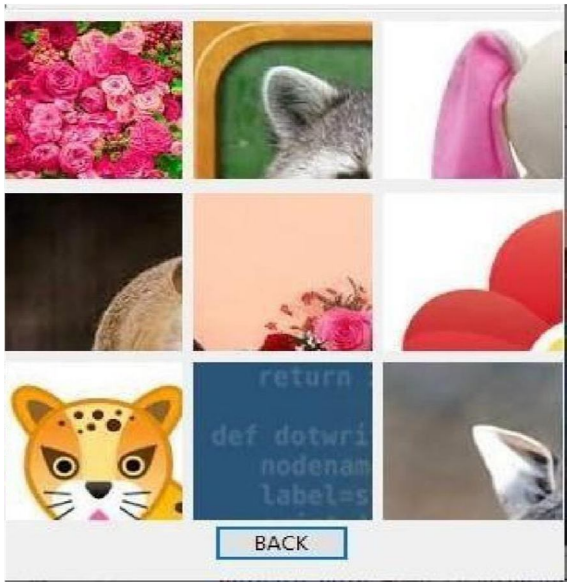
This module defends against online dictionaryattacks by utilizing both Captcha and a password in a user authentication protocol we call Captcha based Password Authentication (CbPA). If a validbrowser cookie is not obtained after entering a valid pair of user



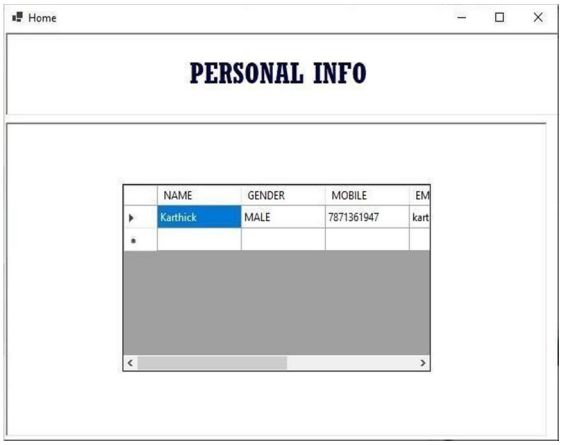
ID and password, the CbPA protocol demands solving a Captcha challenge. If the user enters an erroneous user ID and password, there is a chance that You mustcomplete a Captcha puzzle to gain access. No matter how secure a graphical password scheme is, the password can always be found by a brute force attack. In this paper, we distinguish two types of guessing attacks. automatic guessing attacks apply an automatic trial and error process but S can be manually constructed whereas human guessing attacks apply a manual trial and error process.

C. Overcome Thwart Attack

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 forms of guessing attacks: automated and human. Automatic guessing attacks use an automatic trial and error procedure, although S can be manually created. No theoretic security model has been established yet. Object segmentation is considered computationally expensive, combinational-hard problem, which modern text Captcha is always based on the image based captcha.



The core of CaRP is computational intractability in object recognition in CaRP images. Most evaluations of Captcha security that have been done so far were case-by-case or used an approximation. Theoretical security models have not yet been developed. Modern text Captcha techniques rely on object segmentation, which is regarded as a computationally expensive technique. If the user's chosen captcha matches his account, a welcome page displays; otherwise, an error is presented, and the user can log out using the link at the right top of the page. For the users, this module displays the data that is available in the database. When we use this form of captcha-based protection, the attacker cannot grab the data or file. The user has access to all information and vital documents.

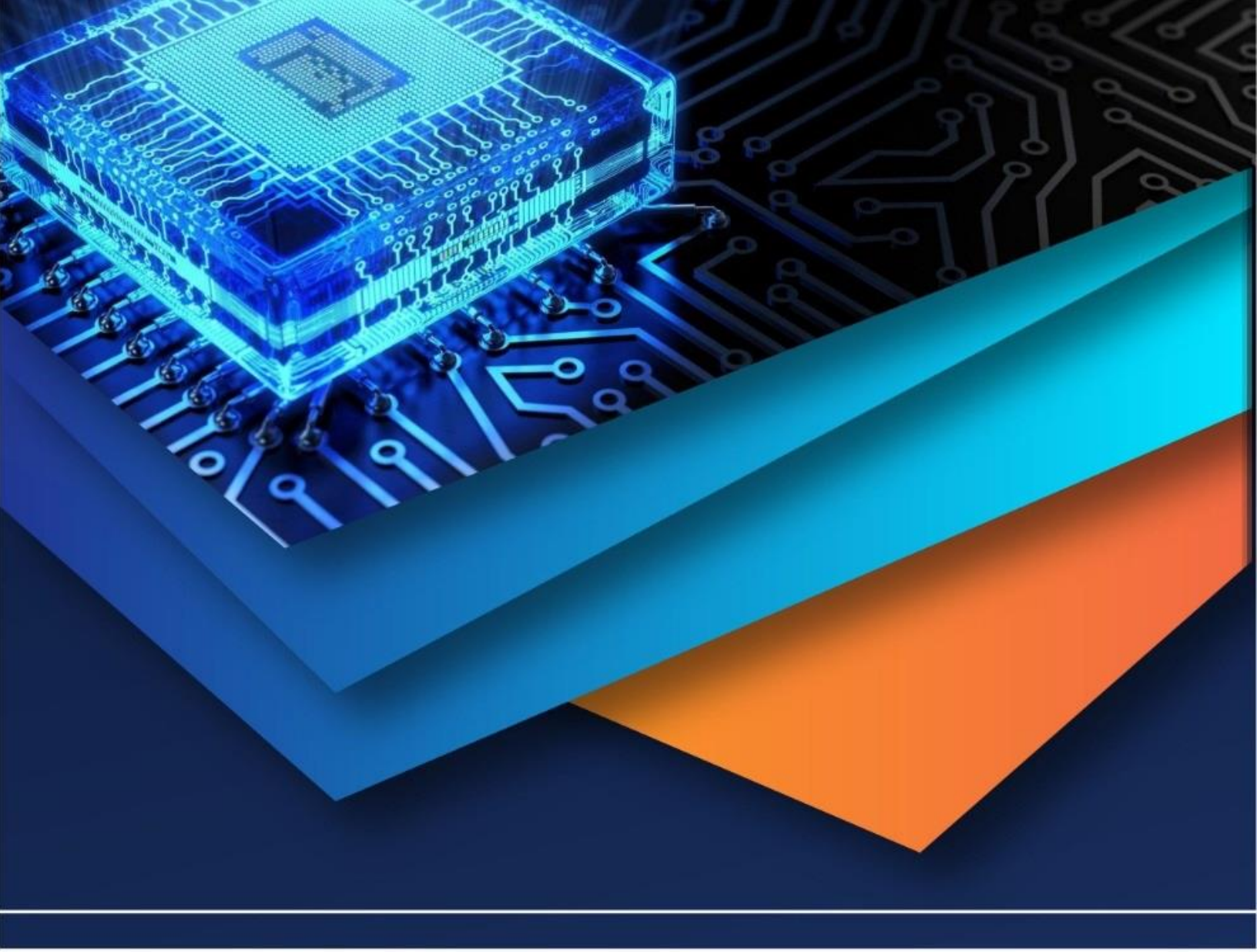


IX. CONCLUSION

Users benefit from CAPTCHA since it helps users recall images for a long time and stops botsfrom attacking accounts. This aids security in a variety of ways, and the front-end interface should also have a more appealing design and a larger database storage space for photos. By means of this project, a graphic captcha is incorporated into our project. The results of our usability research of the two CaRP methods we have used are promising. For instance, Click Text and Animal Grid received higher user satisfaction ratings from participants than Pass Points and a text password and Captcha combination. The password memorability of Animal Grid and Click Text was better than that of conventional text passwords. However, using images with various levels of difficulty dependent on the user's login history and the login device might further increase the value of CaRP.

REFERENCES

[1] Khan, &A. G. Chefranov, “A new secure and usable captcha-based graphical password scheme,” In International Symposium on Computer and Information Sciences, Springer, Cham., September, 2018, pp. 150- 157.
[2] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, “Enhancing security behaviour by supporting the user,” Comput. Secur., vol. 75, pp. 1–9, 2018
[3] Y. W. Chow, W. Susilo, & P. Thorncharoensri, “Captcha design and security issues," In Advances in Cyber Security: Principles, Techniques, and Applications, Springer, Singapore, pp. 69-92, 2019.
[4] Zahra Noury , Mahdi Rezaei, “Deep-CAPTCHA: a deep learning based CAPTCHA solver for vulnerability assessment” IEEE Transactions June 2020.
[5] Ning Yu, and Kyle Darling, “A Low-Cost Approach to Crack Python CAPTCHAs Using AI-Based Chosen-Plaintext Attack”, Applied Sciences 16 May 2019.
[6] C. Shi, X. Xu, S. Ji, K. Bu, J. Chen, R. Beyah and T. Wang, ”Adversarial CAPTCHAs,” in arXiv preprint arXiv:1901.01107., 2019.
[7] Chenghui Shi, Xiaogang Xu, Shouling Ji, Kai Bu, Jianhai Chen, Raheem A. Beyah, and Ting Wang. Adversarial captchas. CoRR, abs/1901.01107, 2019
[8] M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, and P. Wang, “Research on deep learning techniques in breaking text-based captchas and designing image-based captcha,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 10, pp. 2522–2537, 2018.
[9] B. Togookhuu and J. Zhang, “New graphic password scheme containing questions-background-patternand implementation,” Procedia Comput. Sci., vol. 107, pp. 148–156, 2017.
[10] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, “Enhancing security behaviour by supporting the user,” Comput. Secur., vol. 75, pp. 1–9, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY