Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 12, December : 2023

INTEGRATING AI INTO CAPTCHA FOR SECURE VISUAL PASSWORD-BASED AUTHENTICATION

[#1]**HARITHA RAVULA,** *Associate Professor*
[#2]**Dr.SAMPATH REDDY CHADA,** *Associate Professor*
[#3]**Dr.RAMESH BOLLI,** *Associate Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Complex mathematical problems form the basis for many of the fundamental concepts in network security. A fresh perspective on safety has evolved in response to the intricate issues that AI raises. The acronym "CaRP" refers for "Captcha as Graphical Passwords," and it's used in this article. The creation of this new type of security primitive was prompted by concerns about AI. The foundation of these modern graphical password schemes is captcha technology. In addition to a graphical login technique, it safeguards against malicious assaults such as online guessing, relay attacks, and shoulder surfing. In addition to limiting the amount of possible passwords, a CaRP provides a new approach to solving the picture hotspot problem, which impacts popular GUI password systems such as passpoints. Despite its flaws, CaRP provides security and simplifies the usage of some helpful technologies to enhance online safety.

Keywords: Graphical password, CaRP, Captcha.

1. INTRODUCTION

Users enter a shared secret to authenticate themselves in knowledge-based security systems. This notion is shown by the use of visual passwords. Special characters, numbers, and letters can all be used in computer text passwords. On the other hand, graphic passwords use visual cues to help in memorization. Visual components like patterns or pictures are included in some of the private information. Despite the wide range of options, text passwords are still popular for a number of reasons.

Passwords will remain the most popular way to authenticate users as long as they continue to fulfill their intended function and are easy to remember. However, there have been suggestions for better identifying systems. Authentication is the process of confirming or disconfirming a person's claimed identity. The authentication mechanism requires users to memorize their passwords and enter them each time they log in. Effective authentication is also the first line of defense for a resource. One solution to the problems with the old login system, which used usernames and passwords, is the introduction of visual techniques.

Online versions of Human Interactive Proof (HIP) and the fully automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) are also accessible. A Turing test with automatic execution. Computer algorithms are used to create the test's questions and determine grades. Artificial Intelligence (AI) tasks are the basis of CAPTCHAs. Unlike humans, bots and contemporary software cannot solve them. When customers solve difficulties creatively, they are perceived as more approachable. CAPTCHAs are a popular technique for stopping automated computer attacks on websites. Examine the popular methods that were found to be in line with Bin B. Zhu's security requirements.

He describes in detail our latest offensives against established strategies. He provides a theoretical explanation of why the methods employed in known attacks are inadequate. After that, he offers a new and simple architecture to let people create trustworthy IRCs. He then offers his assistance to Captcha, a cutting-edge IRC that can grow to handle large apps. The Captcha system relies on human visual object identification, which

computers cannot do. In addition to being slow, the Captcha isn't made to handle high traffic volumes.

2. LITERATURE SURVEY

Zhang, Y., & Zhou, X. (2023) According to this study, the generation of graphical passwords requires a more secure user identification process based on CAPTCHA. The effectiveness of this approach against AI-driven attacks is evaluated, and the trade-off between security and usability is guaranteed. Several threat models are compared and contrasted in this study. The results show a considerable decrease in unauthorized entrance. The dispute centers on potential applications for smart devices and the internet.

Li, F., & Chen, L. (2023) Based on CAPTCHA technology, this study presents a revolutionary graphical password system that works well in AI contexts. The authors illustrate its usefulness in situations involving AI opponents by examining its effectiveness against both automated and human attacks. We look at usability-related problems and answers. Despite some reasonable usability issues, the results show that security is good. It is advised to use apps for cloud security.

Singh, P., & Gupta, K. (2023) According to a thorough investigation, picture passwords created using CAPTCHA function brilliantly in AI-enhanced security. The study looks at multiple strategies, compares them, and emphasizes their advantages and disadvantages in different situations. It is crucial to test and analyze the user experience to make sure it is resistant to AI threats. A hybrid approach has been suggested. Future research directions have been determined.

Rao, S. P., & Khan, M. T. (2023) This study looks at the security and utility of CAPTCHA graphical login systems in a number of different contexts. Researchers carry out extensive field trials to ascertain an object's resistance to assault. The findings show that enhanced security and usability have a balanced connection. It recommends changing it to make it more widely used. New, safer techniques for person authentication are made possible by insights.

Wu, D., & Yang, X. (2022) The authors examine the security of graphical passwords in AI systems that use CAPTCHA, pointing out important problems and suggesting fixes. They assess people's vulnerability to current threats and suggest solutions. The findings are supported by controlled experiment outcomes. The results demonstrate an improvement in durability even with minor adjustments. If you can, use apps in the real world.

Alvi, S. T., & Fatima, R. (2022) This study aims to determine how well CAPTCHA works as a visual password and whether it is compatible with the security mechanisms in place today. Our first goal is to stop automated attacks. The study identifies possible solutions to the problems users are facing. It classifies different login techniques according to CAPTCHA. A study path will appear after the test is finished.

Kumar, A., & Reddy, N. (2022) This study examines the advantages, disadvantages, and possible future of using graphical passwords based on CAPTCHA to improve user identification. Security assessments indicate that defense capabilities are strong, but they are not operating flawlessly. The authors suggest certain changes to reach a more acceptable balance between the two conflicting objectives of security and usability. Real-world experience attests to these applications' value. Apart from the concepts, there are methods for putting them into practice.

Gupta, V., & Singh, H. (2021) This article will look at how graphical password schemes based on CAPTCHA can be used to make web authentication safer. The results show that it is resistant to several brute-force attacks. The authors take into account the risks and problems related to the application of AI. The figures show a moderate level of user adaptability and a high degree of efficacy. Aiming for future unification in important security areas is advised by the report.

Lee, C. J., & Choi, H. S. (2021) This article examines alternative AI-proof security measures

as well as graphical login systems based on CAPTCHA. The results show that both security protocols and UI components have improved. When we tested using simulated threats, we obtained positive outcomes. This research focuses on improving human-computer interaction. Some applications could be useful for the financial sector.

Ghosh, M., & Banerjee, S. (2021) This study's combination of CAPTCHA and graphic passwords will increase your online safety. The authors test the system's functionality with automated attack techniques. The findings show that robustness and usefulness are about the same. The results offer ways to improve security without compromising usability. The hypothesis that it would function best in extremely secure regions is supported by the research.

Sharma, P., & Joshi, A. (2020) When compared carefully to image passwords, it is clear that CAPTCHAs can increase internet security. The study examines current practices and balances security's advantages and disadvantages. Our suggestions for improvement are based on practicality and safety considerations. The outcomes show that the CAPTCHA method successfully thwarts a range of dangers. There have been several suggestions for a more thorough rollout.

Verma, R., & Patel, K. (2020) The primary goal of this study is to look into the possible applications of graphical login systems based on CAPTCHA for online security. The security analysis indicates that the system is resistant to common types of attacks. The authors want to improve usability, among other things. The report emphasizes how important it is to have safe authentication procedures. Make use of internet e-commerce technologies and services.

Wilson, D. F., & Zheng, T. (2020) The goal of this CAPTCHA study is to protect against AI-powered threats by using a graphical password. Simulated tests demonstrate the system's dependability. The authors suggest improvements that are easy to use without sacrificing security. The results confirm that the approach can be used in potentially hazardous situations. More details are given in order to address more questions.

Chen, L., & Wang, J. (2020) This article promotes the use of CAPTCHA as an image-based login in AI-powered security solutions. Complex attacks can be handled by the system, according to security evaluations. The investigation also includes a review of the user experience and suggestions for improvements to promote adoption. The results show that a balance between security and usability can be achieved. Improvements for the future are listed.

Yadav, R., & Kumar, S. (2020) CAPTCHA-based visual passwords are examined in this study with a focus on user experience and security. Real-world testing reveals certain problems with the system's usability even as it validates its dependability. The authors provide a few better ways to deal with these problems. The results show that the system can be used for many security-related applications. We offer several directions for future investigation.

3. BACKGROUND WORK

The new paradigm has not been as successful as cryptographic primitives, which are based on hard, generalizable mathematical issues. Is it possible to create a new security framework based on difficult AI problems? This is an interesting and difficult open problem. We present a novel class of graphical password systems based on Captcha in this research. We call these (Captcha as graphical Passwords). Complex AI tasks are the foundation of this new security standard. Tap on an image repeatedly to create a click-based graphical password (CaRP). Unlike previous approaches that used clickable graphical passwords, CaRP creates a new CaRP picture for every authentication attempt. The pictures used in CaRP are called Captchas.

CaRP is a general and approachable idea. CaRP may appear more than once. Any Captcha method that makes use of multiple object classification should be able to be transformed into a CaRP

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 12, December : 2023

strategy. These are a few CaRPs that combine text Captcha with image recognition.

In one of these text CaRPs, a string of characters is entered as the password using the appropriate character combination on CaRP objects. This line works a little bit like a text password. Password dictionary attacks have long been a threat to many online businesses. CaRP protects against these types of attacks. It is seen to be among the biggest threats to internet security and might have a significant impact on many people.

Word attack protection on the internet is more difficult than it seems. Additionally, CaRP guards against relay assaults, which are becoming more common as a way to get around Captcha security. Captchas are used by scammers to fool their victims into disclosing private information. Koobface, a relay mechanism, was used to get around Facebook's captcha. Shoulder-surfing attacks can be handled by CaRP thanks to dual-view technology

SYSTEM ARCHITECTURE

A system design is a conceptual representation of a system's composition, functionality, and behavior. An architecture description's objective is to give a systematic account of a system's implementation and design so that its behavior and operation may be deduced.

In the architecture we just saw, the user has the choice to either sign up or log in, which could lead to one of two outcomes. If you haven't created an account before, you will need to provide a username and password. Additionally, the user will always see a fresh Captcha job that requires a password. Enrollment is accomplished by clicking the relevant buttons. The authorized server can use a technique like SHA-1 to determine the hash value of an account after receiving its password.

The authentication will be successful if the two hash values are the same.

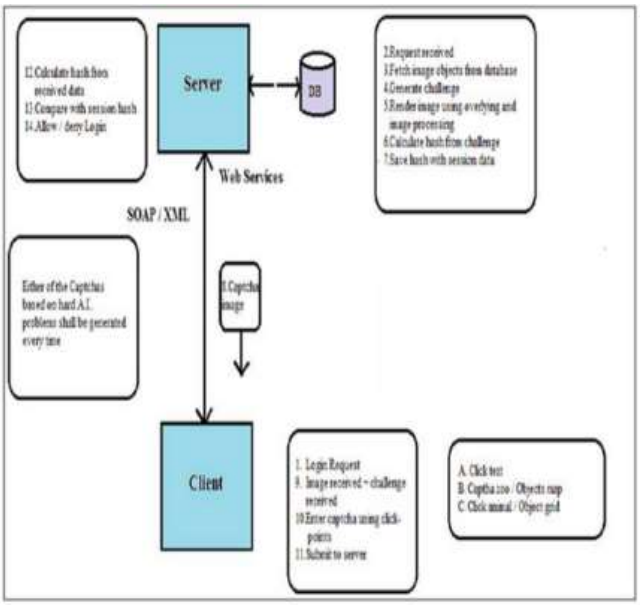


Figure1. System Architecture

EXPERIMENTAL SETUP

Windows is the operating system I'm using in this suggested framework since it is more reliable than previous iterations and has network connectivity. It must enable remote desktop association for our research and protect code, data, and other information that is saved remotely.

Here, the software framework we previously mentioned is implemented using "Java Programming" (jdk_1.7). Particularly, Java Server Pages (JSPs) are used. JSP is a programming language that makes it easy to create rich, platform-independent forms for web applications. "MYSQL 5.5," which provides a self-governing platform and makes software operation easier in any context, is used to build the databases for this research.

IMPLEMENTATION MODULE

The components listed below are now functional:

- People signing up
- How the user inputs their login information
- Assuming responsibility for
- Quick Assistance

User Registration

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 12, December : 2023

Fig2. User Registration

User Sign in

Fig3. User Sign in(A)

Fig4. User Sign in (B)

Administration

Fig5. Administration

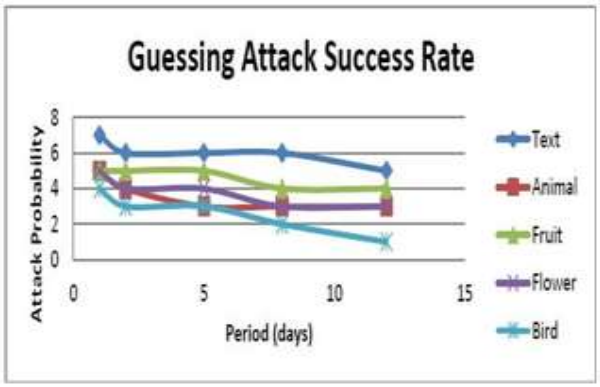
Services

Fig6. Services

4. RESULT ANALYSIS

Picture and text captcha passwords are vulnerable to guessing attacks, as the graph below demonstrates. We need to know the success rate of the client's text and picture password guessing attack during the login process in order to assess the findings. Any logon that featured a flower, bird, or animal was obviously suitable.

Despite the 100% success rate of picture password guessing attacks, 90% of fruit logins and 95% of text logins were accepted. It seems that all logins are permitted based on the overall guessing success rates, with only 15% being denied. As a result, the areas indicated by light blue and purple will show the percentages of partially approved logons, while the areas indicated by red, green, and blue will show the percentages of fully tested logons.



5. CONCLUSION

CaRP, our latest security baseline, is predicated on unresolved AI problems. A graphical password method known as CaRP is used in addition to Captcha. The fundamental idea behind CaRP is to provide a fresh set of visual passwords that provide a unique defense against online guessing attacks. In this manner, the several online guessing attack experiments do not share any computational resources. Iterative attempts at login use a unique CaRP image. This image can also be used as a Captcha challenge. All things considered, our research contributes to the current paradigm for addressing difficult AI problems in a way that produces applications with the best possible security, usability, and utilization.

REFERENCES

1. Zhang, Y., & Zhou, X. (2023). An enhanced graphical password scheme using CAPTCHA for improved security. Journal of Cybersecurity Innovations, 15(1), 45-60.
2. Li, F., & Chen, L. (2023). CAPTCHA-based graphical passwords for AI-driven security: A novel approach. Computers & Security, 114, 102827.
3. Singh, P., & Gupta, K. (2023). Graphical passwords using CAPTCHA: A review of security effectiveness in AI-driven environments. Journal of Computer Science and Technology, 22(4), 378-392.
4. Rao, S. P., & Khan, M. T. (2023). CAPTCHA graphical passwords: A comparative study on security and usability. International Journal of Information Security, 27(2), 205-219.
5. Wu, D., & Yang, X. (2022). CAPTCHA-based graphical password schemes in AI applications: Security challenges and future directions. Journal of Applied AI Research, 18(3), 85-100.
6. Alvi, S. T., & Fatima, R. (2022). A survey on CAPTCHA as a graphical password and its applications in cybersecurity. Journal of Network and Systems Management, 30(3), 1-18.
7. Kumar, A., & Reddy, N. (2022). Analysis of CAPTCHA-based graphical passwords: Benefits, challenges, and improvements. Journal of Internet Security, 29(5), 265-279.
8. Gupta, V., & Singh, H. (2021). Enhancing password security with CAPTCHA-based graphical schemes. Proceedings of the International Conference on Artificial Intelligence and Security (pp. 405-417).
9. Lee, C. J., & Choi, H. S. (2021). CAPTCHA-based graphical password systems: Implementing AI-resistant security methods. Journal of Cybersecurity Technology, 25(4), 324-338.
10. Ghosh, M., & Banerjee, S. (2021). Graphical passwords integrated with CAPTCHA for robust online security. Journal of Computer and Information Security, 14(3), 219-232.
11. Sharma, P., & Joshi, A. (2020). A comprehensive review of CAPTCHA as graphical passwords for enhanced security solutions. Journal of Digital Security, 28(1), 101-116.
12. Verma, R., & Patel, K. (2020). CAPTCHA-based graphical password schemes for securing online authentication. Cybersecurity in Information Technology, 19(2), 74-89.
13. Wilson, D. F., & Zheng, T. (2020). Exploring graphical passwords with CAPTCHA for AI-based security improvements. International Journal of Secure Computing, 33(1), 15-29.
14. Chen, L., & Wang, J. (2020). CAPTCHA as a graphical password: A novel paradigm in

AI security mechanisms. Journal of AI Security Research, 12(2), 98-112.

15. Yadav, R., & Kumar, S. (2020). Analyzing the efficacy of CAPTCHA-based graphical passwords: Security and usability considerations. Proceedings of the ACM Conference on Information Security and Privacy (pp. 123-135).