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

DOI: https://doi.org/10.22214/ijraset.2023.50794

Returing Image-The Captcha Initiator

Ruchitha Sathe[1], Sangamithra Nalam[2], Bhoomika Dharavath[3], Mrs. S. Divya[4]
Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology

Abstract: The CAPTCHA is used to provide the security against the malicious software by generating a test which only a human can complete. The CAPTCHA stands for Completely Automated Public Turing test to tell computer and human apart. Currently, we are using CAPTCHA are image and text-based data. The reusable CAPTCHA security engine will provide a better way to generating the data for CAPTCHA and will increase the difficulty in bypassing the system by use of improved algorithm. CAPTCHAs are designed to prevent bots – programs that pose as humans on the Internet – from abusing internet services. Bots, driven not to dominate but to sell, sign up for thousands of free email accounts every minute, sending millions of spam messages from them. Such reading-based CAPTCHAs exploit the large gap between humans and machines in their ability to read images of text.

Keywords: Captcha, Images, Security, Authentication, Java Servlets, Turing test.

I. INTRODUCTION

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a security measure used to differentiate between humans and computer programs attempting to access a website or application. CAPTCHAs are commonly used to prevent spam and abuse, as well as protect user information from bots and automated attacks. The generation of CAPTCHAs involves the creation of image or audio-based challenges that humans can solve easily, but machines find difficult. The aim of this CAPTCHA generation project is to develop a highly secure and reliable system that generates CAPTCHAs using advanced algorithms and techniques.

The project will focus on creating CAPTCHAs that are difficult for automated programs to solve, while at the same time being easy for humans to decipher. The project will involve designing and implementing a system that generates different types of CAPTCHAs, including image-based CAPTCHAs, audio-based CAPTCHAs, and other novel forms of challenges. Basically, Turing image is also known as CAPTCHA.

A CAPTCHA a contrived acronym for "Completely Automated Public Turing Test to tell Computers and Humans Apart" ^{is} a type of challenge response test used in computing to determine whether the user is human. The captcha is in the form entering a sequence of letters or numbers in a distorted image.

CAPTCHA helps protect you from spam and password decryption by using you to complete a simple test that proves you are human and not a computer trying to break into a password protected account.

The project will also involve testing the effectiveness of the generated CAPTCHAs against various types of attacks, including machine learning attacks, to ensure their security. The successful completion of this project will result in the development of a highly effective CAPTCHA generation system that can be used by various organizations and websites to enhance their security measures and protect user information. To ensure the security of the generated CAPTCHAs, the project will also involve testing their effectiveness against various types of attacks, including machine learning attacks. This will involve using machine learning algorithms to try and solve the generated CAPTCHAs and identifying the weaknesses in the system. The results of these tests will be used to refine the CAPTCHA generation algorithms and improve their security. The project will also consider the user experience of the generated CAPTCHAs.

The CAPTCHAs should be easy for humans to solve, with clear instructions and minimal confusion. The generated CAPTCHAs should not be overly frustrating or time-consuming, as this can lead to user frustration and potentially drive them away from the website or application.

In summary, the CAPTCHA generation project aims to develop a highly secure and reliable system for generating CAPTCHAs that are difficult for automated programs to solve, while at the same time being easy for humans to decipher. The project will involve a combination of machine learning algorithms, image processing techniques, and audio processing techniques to create various types of CAPTCHAs, as well as testing their effectiveness against various types of attacks. The success of the project will result in the development of a highly effective CAPTCHA generation system that can be used by various organizations and websites to enhance their security measures and protect user information.

II. LITERATURE SURVEY

A literature survey for a CAPTCHA project is a review of existing research and publications related to CAPTCHA technology and its use in various applications. The survey involves collecting and analyzing relevant literature from academic journals, conference proceedings, and other sources to gain a better understanding of the current state of CAPTCHA technology, its limitations, and potential areas for improvement. The purpose of the literature survey is to identify the gaps and challenges in the existing CAPTCHA technology, explore innovative solutions, and evaluate the effectiveness of different CAPTCHA techniques against various types of attacks. This information is then used to develop new CAPTCHA generation techniques that are more secure, user-friendly, and difficult for automated programs to solve. The literature survey for a CAPTCHA project can cover a wide range of topics, including CAPTCHA security, design, implementation, evaluation, and optimization. Some of the key areas that may be covered in the literature survey include the types of CAPTCHAs currently in use, their vulnerabilities, the attacks used to break them, the effectiveness of various countermeasures, and the new approaches and technologies that are being developed to enhance CAPTCHA security. Overall, a literature survey for a CAPTCHA project is an essential step in the research and development of CAPTCHA technology. It provides a foundation of knowledge and insights that can guide the development of new and innovative CAPTCHA techniques that are more effective, secure, and user-friendly.

A way to tell apart a human from a computer by a test is known as a Turing Test. When a computer program is able to generate such tests and evaluate the result, it is known as a CAPTCHA (Completely Automated Public test to Tell Computers and Humans Apart). In the past, Websites have often been attacked by malicious programs that register for service on massive scale. Programs can be written to automatically consume large amount of Web resources or bias results in on-line voting. This has driven researchers to the idea of CAPTCHA-based security, to ensure that such attacks are not possible without human intervention, which in turn makes them ineffective. CAPTCHA-based security protocols have also been proposed for related issues, e.g., countering Distributed Denial-of-Service (DDoS) attacks on Web servers. A CAPTCHA acts as a security mechanism by requiring a correct answer to a question which only a human can answer any better than a random guess. Humans have speed limitation and hence cannot replicate the impact of an automated program. Thus, the basic requirement of a CAPTCHA is that computer programs must be slower than humans in responding correctly. To that purpose, the semantic gap between human understanding and the current level of machine intelligence can be exploited. Most current CAPTCHAs are text-based.

Commercial text-based CAPTCHAs have been broken using object-recognition techniques, with accuracies of up to 99% on EZ-Gimpy. This reduces the reliability of security protocols based on text-based CAPTCHAs. There have been attempts to make these systems harder to break by systematically adding noise and distortion, but that often makes them hard for humans to decipher as well. Image-based CAPTCHAs have been proposed as alternatives to the text media. More robust and user-friendly systems can be developed. State-of-theart content-based image retrieval (CBIR) and annotation techniques have shown great promise at automatically finding semantically similar images or naming them, both of which allow means of attacking image-based CAPTCHAs.

A new technology is built over the CAPTCHA called graphical CAPTCHA which is resilient to dictionary attack and hence more secure with the hybrid use of CAPTCHA and graphical password one can address a number of security problems such as relay attacks, CARP does not act as a cure all technique but it stipulates security and usability to legitimate use in real time.

A. Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key considerations involved in the feasibility analysis is:

1) *Technological Side:* This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system
2) *Economical Side:* This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

3) *Legal Side:* The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.
4) *Operational Side:* This assessment involves conducting a study for the purpose of analyzing and determining whether the needs of the organization can be met after the completion of the project. Added to that, it also analyzes how the project plan will cater to the requirements as stated in the requirements analysis phase of the system development.

III. EXISTING SYSTEM

In the existing system we use mainly text based CAPTCHA which we are using from the begging of time, so the today there is some software which can bypass this test. The hacker hacks the data from the system and then they make software according to that and the CAPTCHA is bypassed. While a human need to enter a long sentence in the box before the access to the website. While solving the CAPTCHA is a boring and sometimes even though it is right, it shows error and we can say that at first CAPTCHA use to protect from spam bot, but today bots are defeating the CAPTCHA while sometimes humans can’t solve it.

IV. PROPOSED SYSTEM

In the proposed system will generate the CAPTCHA by using a new improved algorithm which will be interesting to solve at the same time it will be tougher than previous to solved by the bots while will feel easy. The humans have limitations on the speed of response then compared to any computer and hence the computer must be slower than the human and so we will make full benefit of this and use it in the proposed system. The system will contain colored graphical interface with the font is limited to two while the border line thickness and color will be fixed .The system will generate random text which will be shorter than the present system but will be difficult to hack as it will randomly generate.

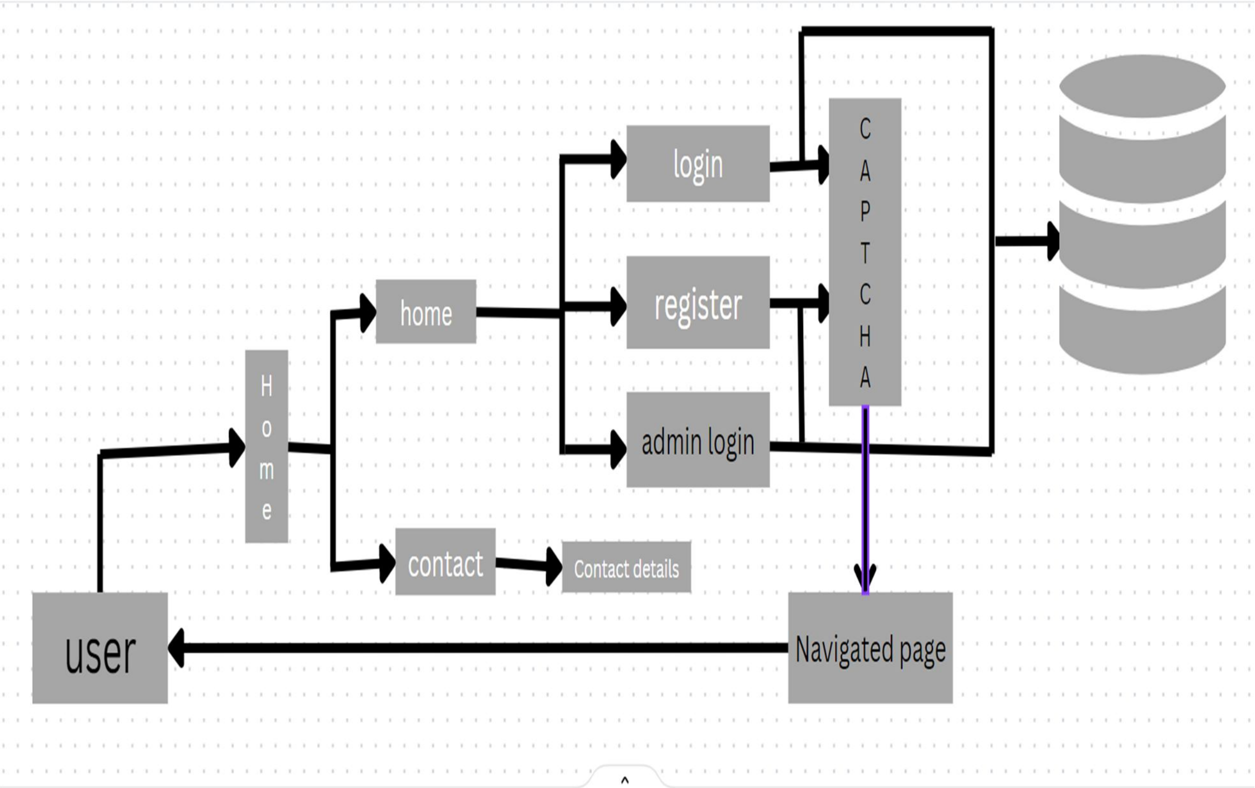

Fig 1: Captcha Architecture

V. RESULTS

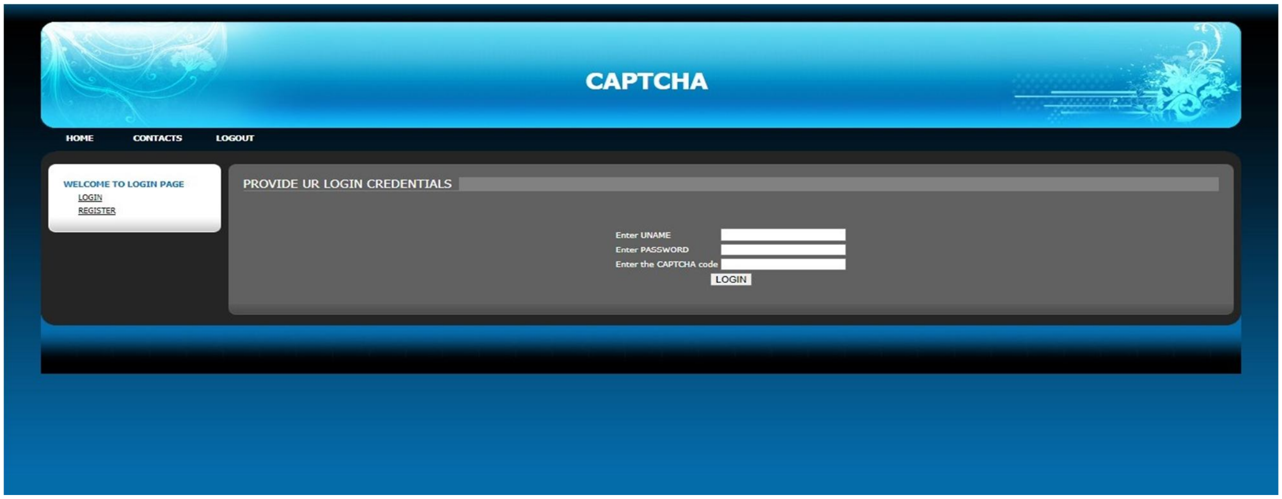

Figure 2: Login Page

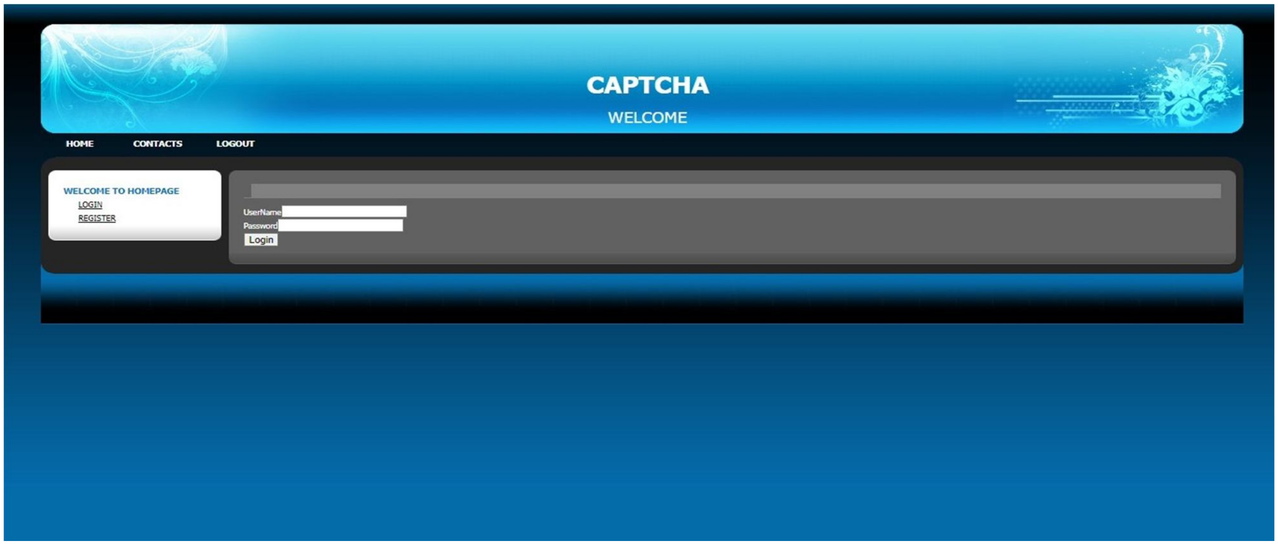

Figure 3: Admin login

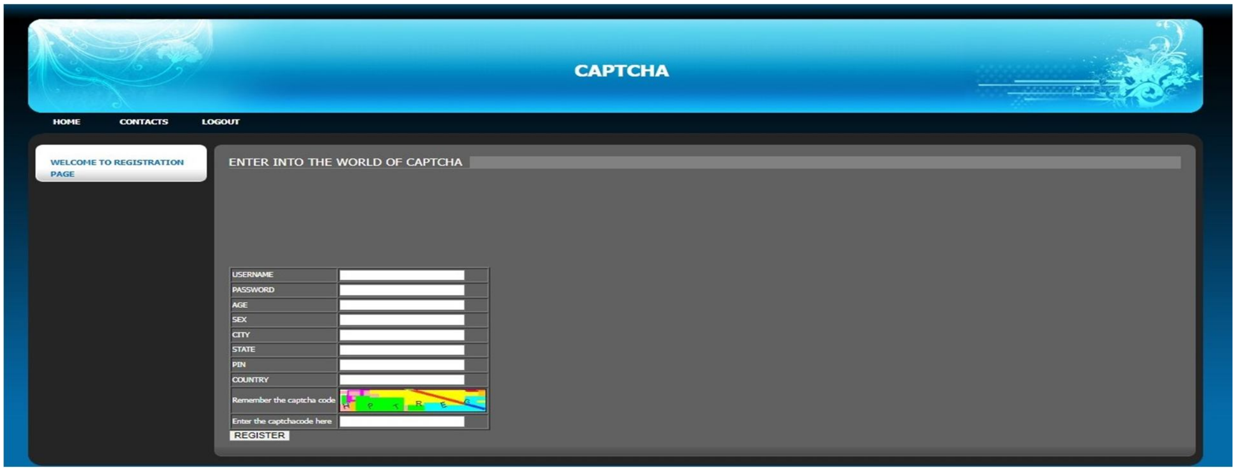
CAPTCHA
HOME
CONTACTS
LOGOUT
WELCOME TO REGISTRATION PAGE
ENTER INTO THE WORLD OF CAPTCHA
USERNAME
PASSWORD
AGE
SEX
CITY
STATE
PIN
COUNTRY
Remember the captcha code
Enter the captchacode here
REGISTER

Figure 4: Registration page

VI. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, CAPTCHA generation is an essential aspect of modern web security, as it helps prevent automated attacks and ensures the security of user data. The process of CAPTCHA generation involves designing a challenge-response mechanism that can distinguish between human users and automated bots. Different types of CAPTCHAS, such as image-based, audio-based, or interactive CAPTCHA, can be generated based on the requirements of the website or application. System testing is essential to ensure that the CAPTCHA is effective, secure, and user-friendly. Various software development life cycle models, such as the Waterfall model, Spiral model, and Agile model, can be used to develop and test CAPTCHA systems. The future scope of CAPTCHA generation lies in the development of more advanced and secure mechanisms to protect websites and applications from automated attacks. Research is ongoing to develop new types of CAPTCHAS that are more resistant to automated attacks and easier to use for humans. Additionally, advancements in machine learning and artificial intelligence may enable the development of more intelligent CAPTCHA systems that can adapt to changing attack strategies. Overall, CAPTCHA generation will continue to be an essential aspect of web security, and advancements in technology will lead to the development of more secure and user-friendly CAPTCHA systems in the future.

REFERENCES

[1] Bursztein, E., Martin, M., & Mitchell, J. C. (2014). Text-based CAPTCHA strengths and weaknesses proceedings of the 23rd USENIX Security Symposium, 303-318.

[2] Elson, J., Douceur, J., Howell, J., & Saul, J. (2007). Asirra: A CAPTCHA that exploits interest-aligned manual image categorization. Proceedings of the 14th ACM Conference on Computer and Communications Security, 366-374.

[3] Golle, P. (2008). Machine learning attacks against the Asirra CAPTCHA. Proceedings of the 15th ACM Conference on Computer and Communications Security, 535-542.

[4] Mondal, A. K., & Saini, S. (2020). Security Analysis of Different Types of CAPTCHAS. Proceedings of the 10th International Conference on Computational Intelligence and Communication Networks, 148-151.

[5] Von Ahn, L., & Dabbish, L. (2008). Designing games with a purpose. Communications of the ACM, 51(8), 58-67.

[6] Yan, J., & El Ahmad, A. S. (2008). A low-cost attack on a Microsoft CAPTCHA. Proceedings of the 15th ACM Conference on Computer and Communications Security, 543-554.

[7] Zhou, X., & Ye, J. (2014). Audio CAPTCHA recognition based on deep neural networks. Proceedings of the 2014 IEEE International Conference on Acoustics, Speech, and Signal Processing, 8123-8127.

[8] L. Von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," Communications of the ACM, vol. 47, pp. 56-60, 2004.

[9] A. L. Coates, H. S. Baird, and R. J. Fateman, "PessimalPrint: a reverse Turing test," International Journal on Document Analysis and Recognition, vol. 5, pp. 158-163, 2003.

[10] J. Yan, "Bot, cyborg and automated turing test," in Security Protocols Workshop, 2006, pp. 190-197

[11] H. Baird and K. Popat, "Human interactive proofs and document image analysis," presented at the The 5th IAPR