WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Captcha

Praveen Kumar[1], Ramegowda M[2]

[1]S J C Institute of Technology Dept of ECE, Chikkaballapur Praveenkumarpmd7@gmail.com
[2]S J C Institute of Technology Dept of ECE, Chikkaballapur Rgm7885@gmail.com

ABSTRACT-

CAPTCHA, or Completely Automated Public Turing Test to Tell Computers and Humans Apart, is a security mechanism used to distinguish between human and automated computer programs. It presents users with a challenge that requires human-like reasoning to solve, such as identifying distorted text, selecting certain images, or answering simple math problems. CAPTCHA has become an essential tool for protecting websites and online services from malicious bots and automated attacks, while still allowing legitimate human users to access the resources they need. This abstract provides a brief overview of CAPTCHA and its importance in online security.

I. INTRODUCTION

CAPTCHA, or Completely Automated Public Turing Test to Tell Computers and Humans Apart, is a security mechanism used to prevent automated programs from accessing online resources that are intended for human users. CAPTCHA challenges are designed to be easy for humans to solve but difficult for computers to complete accurately, requiring human-like reasoning to pass the test. CAPTCHAs typically involve presenting the user with distorted text, images, or audio that must be identified and entered correctly to gain access to the resource. CAPTCHAs have become an essential tool for protecting websites and online services from spam, fraud, and other malicious attacks that rely on automated bots. This introduction provides an overview of CAPTCHA and its importance in online security.

II. METHODOLOGY

There are several methods used to create and implement CAPTCHA challenges, each with its strengths an CAPTCHA, or Completely Automated Public Turing Test to Tell Computers and Humans Apart, is a security mechanism used to prevent automated programs from accessing online resources that are intended for human users. CAPTCHA challenges are designed to be easy for humans to solve but difficult for computers to complete accurately, requiring human-like reasoning to pass the test. CAPTCHAs typically involve presenting the user with distorted text, images, or audio that must be identified and entered correctly to gain access to the resource. CAPTCHAs have become an essential tool for protecting websites and online services from spam, fraud, and other malicious attacks that rely on automated bots. This introduction provides an overview of CAPTCHA and its importance in online security. weaknesses. Some of the most common methodologies used for CAPTCHA include:

1. Image-based CAPTCHA: This method involves presenting the user with an image that contains distorted text, numbers, or symbols. The user is then required to enter the characters they see into a text box to prove they are human. Image-based CAPTCHA is effective against automated bots that cannot recognize distorted text.

2. Audio-based CAPTCHA: This method presents the user with a series of audio recordings that contain spoken letters or numbers. The user is then required to enter the characters.They hear into a text box to prove they are human. Audio-based CAPTCHA is effective against automated bots that cannot recognize spoken language.

3. Math-based CAPTCHA: This method presents the user with a simple math problem that they must solve to gain access to the resource. Math-based CAPTCHA is effective against automated bots that cannot perform mathematical operations.

4. Behavior-based CAPTCHA: This method involves analyzing user behavior to determine if they are human. For example, a website may track how quickly a user completes a form or how long they spend on a page to determine if they are a bot or a human.

Overall, CAPTCHA methodologies aim to create challenges that require human-like reasoning to solve while remaining difficult for automated bots to complete accurately. By using a combination of different methodologies, websites can create CAPTCHA challenges that are both effective and user-friendly.

III. BLOCK DIAGRAM

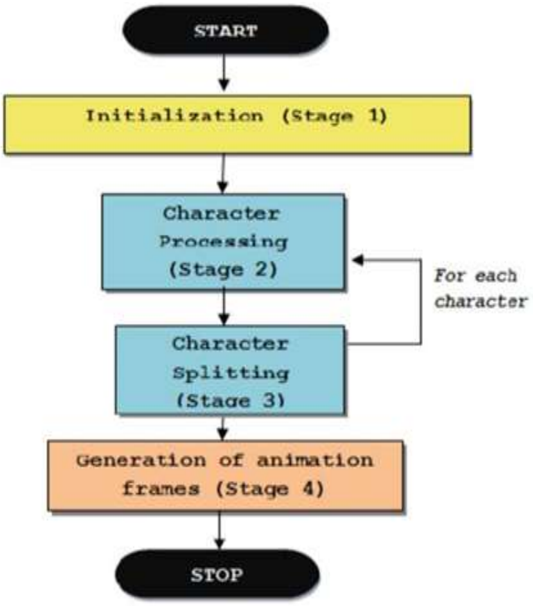
START
Initialization (Stage 1)
Character Processing (Stage 2)
For each character
Character Splitting (Stage 3)
Generation of animation frames (Stage 4)
STOP

Fig 1: Block diagram of the System Functionality

Fig1 describes the block diagram of the system funtionality. A typical CAPTCHA system consists of the following components:

User Interface: This is the component that presents the CAPTCHA challenge to the user, usually in the form of an image, audio recording, or simple math problem.

Captcha Generator: This component is responsible for generating the CAPTCHA challenge. It uses algorithms to create images or audio recordings that are difficult for automated bots to recognize.

Response Validation: This component is responsible for validating the user's response to the CAPTCHA challenge. It checks if the user's response matches the correct solution generated by the Captcha Generator.

Access Control: This component is responsible for granting or denying access to the resource based on the user's response to the CAPTCHA challenge. If the user's response is correct, they are granted access to the resource. If their response is incorrect, they are denied access

IV. EXPECTED OUTCOMES

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge-response test used to determine whether a user is human or not. The outcomes of CAPTCHA can vary depending on its purpose and implementation.

Here are some of the common outcomes of CAPTCHA:

Authentication: CAPTCHA is used to authenticate human users and prevent automated bots from accessing a website or application. By completing a CAPTCHA test, a user can prove that they are a real human and gain access to the content or service.

Security: CAPTCHA is used to prevent various types of attacks, such as spamming, phishing, and brute force attacks. By requiring users to complete a CAPTCHA test, it becomes more difficult for automated bots to carry out these types of attacks.

User Experience: CAPTCHA can also impact the user experience of a website or application. If the CAPTCHA test is too difficult or frustrating to complete, it can turn users away or discourage them from using the service.

Accessibility: CAPTCHA can also pose challenges for users with disabilities, such as visual impairments or hearing loss, who may have difficulty completing the test. It is important to ensure that CAPTCHA is implemented in a way that is accessible to all users.

V. ADVANTAGES

Preventing automated attacks: CAPTCHA prevents automated bots from carrying out malicious activities such as spamming, hacking, and distributed denial of service (DDoS) attacks.

Protecting user accounts: CAPTCHA helps to prevent brute- force attacks on user accounts by ensuring that only humans can enter the correct username and password combinations.

Improving website security: CAPTCHA helps to improve the overall security of websites and online services by reducing the risk of automated attacks and unauthorized access.

Enhancing user experience: CAPTCHA is a user- friendly way to verify that a user is human. It can be implemented in a variety of ways, such as image recognition, audio challenges, or simple math problems, making it accessible to a wide range of users.

Preventing spam: CAPTCHA is an effective way to prevent spam by requiring users to prove that they are human before submitting a form or creating an account. This reduces the amount of spam that businesses receive and helps to keep their email servers and websites running smoothly.

VI. APPLICATIONS

Preventing spam: CAPTCHA can be used to prevent spam bots from filling out forms, posting comments, or sending messages. This helps to keep the website clean and free of unwanted content.

Protecting user accounts: CAPTCHA can be used as an additional layer of security to protect user accounts from unauthorized access. For example, a CAPTCHA can be used to prevent brute force attacks where bots try to guess the user's password by trying multiple combinations.

Preventing automated attacks: CAPTCHA can be used to prevent automated attacks such as Denial of Service (DoS) attacks, where bots try to overwhelm a website by sending a large number of requests.

Validating online polls: CAPTCHA can be used to validate online polls and surveys, ensuring that only human votes are counted.

Digitizing books: CAPTCHA can be used to digitize books and other documents by using humans to transcribe the text from scanned images. This helps to improve the accuracy of optical character recognition (OCR) software.

Enhancing AI: CAPTCHA can be used to improve machine learning algorithms by training them to recognize images and text. For example, CAPTCHA can be used to train self-driving cars to recognize traffic signs and signals.

VII. CONCLUSION

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is a security feature that is widely used to distinguish between humans and machines on the internet. It is an effective method to prevent automated bots from accessing and exploiting online services, as it requires users to perform a task that is easy for humans but difficult for machines.

There are various types of CAPTCHA, including text- based, image-based, audio-based, and behavioral-based. Each type has its own strengths and weaknesses, and the choice of which type to use depends on the specific needs and requirements of the application.

While CAPTCHA is an effective tool to prevent automated bots from accessing online services, it is not foolproof. Advanced bots and artificial intelligence algorithms can bypass some CAPTCHA tests, and some users with disabilities may find it difficult or impossible to complete certain types of CAPTCHA tests.

Overall, CAPTCHA remains an important tool in online security, but it should be used in conjunction with other security measures, such as two-factor authentication, to provide a comprehensive defense against online threats.

VIII. REFERENCES

[1] Carnegie Mellon University, CAPTCHA: Telling Humans and Computers Apart Automatically. Available from: http://www.captcha.net/ [Accessed: April 22, 2015].

[2] Pope, C. & Kaur, K. (2005), "Is it human or computer? Defending e-commerce with Captchas", IT Professional, vol. 7, no. 2, pp. 43-49.

[3] Raj, S.B., Devassy, D. & Jagannivas, J. (2010), "A new architecture for the generation of picture based CAPTCHA", Electronics Computer Technology (ICECT), 2011 3rd International Conference on, Kanyakumari, 2011, vol. 6, no. pp. 67-71.

[4] Shirali-shahreza, M. (2008), "Dynamic CAPTCHA ", Communications and Information Technologies, 2008. ISCIT 2008. International Symposium on. Lao.2008, vol., no. pp. 436- 440.

[5] Parc's Captchas, Parc's Captchas the new trend of technology and security, Available from: http://www2.parc.com/istl/projects/captcha/index.htm [Accessed: April 2, 2014,].

[6] Almazyad, A.S., Ahmad, Y. & Kouchay, S.A. (2011), "Multi-Modal CAPTCHA: A User Verification Scheme", Information Science and Applications (ICISA), 2011 International Conference on,Jeju Island,2011., vol., no. pp. 1-7.

[7] Cui, J.S., Zhang, W.Z.,Y .,Liang. Y., Xiao ,B., Mei., J.T., Zhang .,D. & Peng , W. (2010), "A 3- layer Dynamic CAPTCHA Implementation", Education Technology and Computer Science (ETCS), 2010 Second International Workshop on. Wuhan, vol. 1, no. pp. 23-26.

[8] Singh Ved. & Pal preet. (2014), "Survey of different Types of CAPTCHA", international Journal of computer science and information technologies, 2014 vol.5, no. 2 pp. 2242-2245.

[9] Chen Li, W.A., Wang, J. & Liu (2010), "Protection Through Multimedia CAPTCHAS",, vol., no. pp.

[10] Chow, R., Golle, P. Jakobsson, M., Wang .L.& Wang , X.(2208), "Making CAPTCHAs clickable ", Conference HotMobile '08 Proceedings of the 9th workshop on Mobile computing systems and applications on. New York.2008, vol., no. pp.