IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Framework for Cognitive CAPTCHA Designing

S.S. Kulkarni[1*], H.S. Fadewar[2]

[1,2]School of Computational Sciences, S. R. T. M. University, Nanded, India

[*]*Corresponding Author sushama.s.kulkarni@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i3.502505 | Available online at: www.ijcseonline.org

Accepted: 09/Mar/2019, Published: 31/Mar/2019

***Abstract*—** Designing a CAPTCHA requires choosing a challenge which is difficult for bots and easy for human being. Cognitive CAPTCHA provide much needed human advantage as compared to bots. Various available cognitive CAPTCHAs attempt to explore the potential AI hard problems in number of possible ways. In this paper we provide a framework to design cognitive CAPTCHAs. It will serve as a guideline to design the cognitive challenge in an efficient way. This will give baseline features to be considered while designing any cognitive CAPTCHA.

***Keywords*—** Cognitive CAPTCHA, HCI, Web security, Accessibility, Human Interactive Proof (HIP), Bots

I. INTRODUCTION

CAPTCHA (Completely Automatic Public Turing Test to Tell Computer and Human Apart) is a test to categorize users as human or bot. Most of the current CAPTCHAs present a visual challenge in the form of text, image, audio, video, game or a puzzle. Few other CAPTCHAs present a test purely based on cognitive aspects. All of the CAPTCHAs strive to use best possible AI hard problem. Hence every broken CAPTCHA indicates advancement in AI capabilities.

Existing cognitive CAPTCHAs utilize human capabilities like perception, natural language processing, mathematical and analytical skills for designing cognitive challenge for bots. But while designing a new cognitive CAPTCHA, certain factors like complexity of cognitive challenge, simplicity of interface and usage of obfuscation techniques has to be considered. It yields a user friendly and universally accessible cognitive CAPTCHA.

In this paper we have reviewed existing cognitive CAPTCHA techniques in order to understand their limitations. We have also compared current cognitive CAPTCHAs with respect to complexity level, simplicity of interface and usage of obfuscation techniques. Based on the inferences we have suggested a framework for cognitive CAPTCHA designing. It will provide guideline to design better and efficient cognitive CAPTCHA.

Rest of the paper is organized as follows, Section I contains the introduction of CAPTCHA concept, Section II contain the related work on cognitive CAPTCHA by several researchers. Section III contains comparison of existing cognitive CAPTCHAs, Section IV describes the proposed framework for cognitive CAPTCHA designing, and section V explains the conclusion of this research paper.

II. RELATED WORK

Human-Cognition based CAPTCHA was proposed which required user to solve mathematical, inference or logical questions. Majority of survey participants found Human-Cognition based CAPTCHAs acceptable [1]. Move & Select CAPTCHA based on human cognitive psychology, required user to move and correctly rearrange the randomly placed pieces of an image and then select events associated with image from a drop down list [2]. Usability and security study for the Move & Select CAPTCHA exhibited better results as compared to ESP PIX and EZ-GIMPY CAPTCHA. A CAPTCHA based on human cognitive factor asked user to choose the desired types of challenge from 5 types of challenges [3]. 5 types of questions were namely analytical, mathematical, general, text based and image based. A tree-based handwritten CAPTCHA utilized superior perception and spatial recognition abilities of human being [4]. Tree-based handwritten CAPTCHA depicted extremely low machine recognition rate and very low difficulty level for human users. A CAPTCHA utilizing cognitive ability of human through PHP presented user alphanumeric characters hidden within innovative designs and asked the user to recognize the presented alphanumeric string [5]. It utilized the better visual perception abilities of human being as compared to machines. A four panel cartoon CAPTCHA required user to rearrange the stages of a funny story in proper order. It utilized the superior humour understanding abilities of human being. [6]. C-CAPTCHA introduced 7 new models of cognitive CAPTCHA. It focused on weaker bot abilities like perception, common sense reasoning,

abstraction and natural language processing [7]. Dynamic Cognitive Game CAPTCHAs utilized superior dynamic gaming capabilities of human being by presenting a simple moving object matching game as a challenge [8]. It depicted better usability and robustness against relay attacks. A knowledge based cognitive CAPTCHA was designed to utilize very specific knowledge (oriented for particular area or discipline) [9]. But it cannot be used for general users since it requires specialized knowledge. A cognitive CAPTCHA was proposed with combination of honeypot [10]. It used simple mathematical CAPTCHA in image format and used honeypot to further deviate bots. But author did not provide more details about this mathematical cognitive CAPTCHA. An authentication protocol was proposed using multi-level cognitive CAPTCHA [11]. It used Attention moving verification, Multi questions verification code and Fuzzy perception thresholds for designing cognitive CAPTCHAs. It expected user to exhibit expert knowledge or high cognitive and perceptual skills. Thus they are not useful for common people having varying level of cognitive abilities. A Basic Survey of CAPTCHA considered application and challenges in CAPTCHA techniques [12]. It suggested 2 step CAPTCHA generation by randomizing alphanumeric characters and attaching different queries with it. It attempted to achieve usability and simplicity of CAPTCHA interface. Researchers highlighted the risk of attacks in cloud environment [13]. This illustrates continuous efforts of researchers for strong security measures to provide online security.

III. COMPARISON OF EXISTING COGNITIVE CAPTCHAS

We have compared existing CAPTCHAs to highlight the necessity of uniform norms for designing any cognitive CAPTCHA. Table I shows the comparison of existing cognitive CAPTCHAs.

Comparison of existing cognitive CAPTCHAs indicates that the majority of cognitive CAPTCHAs have Medium or High complexity level and Moderately Difficult or Difficult to handle interface. It depicts the high viscosity is required to solve these CAPTCHAs. Thus user has to invest more efforts and skills for solving these CAPTCHAs. Some of the Cognitive CAPTCHAs also implement certain obfuscation techniques. Thus they are not accessible for people with partial or total blindness. Complexity of cognitive question, a difficult to handle user interface and obfuscation techniques together increase error proneness of a cognitive CAPTCHA.

Table 1 Comparison of existing cognitive CAPTCHAs

CAPTCHA Name	Complexity level	Interface	Obfuscation (Yes/No)
Human-Cognition based CAPTCHA	Medium	Simple	No
Move & Select CAPTCHA	High	Moderately Difficult	No
CAPTCHA based on human cognitive factor	Medium	Simple	Yes
Tree-based handwritten CAPTCHA	High	Difficult	Yes
CAPTCHA utilizing cognitive ability of human through PHP	Medium	Moderately Difficult	Yes
Four panel cartoon CAPTCHA	High	Difficult	No
C-CAPTCHA	High	Difficult	Yes
Dynamic Cognitive Game CAPTCHAs	Low	Simple	No
Knowledge based cognitive CAPTCHA	High	Moderately Difficult	No
Multi-level cognitive CAPTCHA	High	Moderately Difficult	Yes

This illustrates the requirement of certain guidelines for designing the cognitive CAPTCHAs. Thus in section IV we propose a framework for cognitive CAPTCHA designing.

IV. PROPOSED FRAMEWORK FOR COGNITIVE CAPTCHA DESIGNING

Every type of CAPTCHA including text, audio, and video CAPTCHA should mandatorily have following properties [14]:

- **Automation**: Computer programs should be able to generate and grade the tests.
- **Openness**: The underlying databases and algorithms used to generate and grade the tests should be public.
- **Usability**: Humans should easily solve these tests in a reasonable amount of time.
- **Security**: The program generated tests should be difficult for machines to solve by using any existing algorithm.

But there are no particular extensive features focused on designing cognitive CAPTCHAs. Every CAPTCHA design has to be human friendly and AI hard as well. Cognitive CAPTCHA should utilize following aspects of human cognition process:

- Attention
- Perception and recognition
- Memory
- Learning
- Reading, speaking, and listening

- Problem-solving, planning, reasoning, decision-making

Existing cognitive CAPTCHA often have a difficult to handle interface for end user. Some of the above mentioned cognitive CAPTCHAs like Move & Select CAPTCHA and four panel cartoon CAPTCHA have high viscosity. Thus user has to perform number of activities to solve the CAPTCHA tests. Such CAPTCHAs are time consuming and require more efforts from a user. A CAPTCHA utilizing cognitive ability of human through PHP have less visual clarity which makes it difficult for visually challenged people. Four panel cartoon CAPTCHA required humor understanding that is a culture sensitive task. Some of the humors may not have relevance in different cultures and societies. Hence it has high error proneness. Multi-level cognitive CAPTCHA required complex cognitive skills or expert knowledge level to solve the cognitive challenge. This shows the lack of uniform norms for designing cognitive CAPTCHAs. Thus we propose a framework to design Cognitive CAPTCHA. It will serve as a pointer to essential features for any cognitive CAPTCHA. Figure 1 depicts the proposed framework for cognitive CAPTCHA designing.

Proposed framework for cognitive CAPTCHA designing consists of following features:

- **Low viscosity**: Amount of efforts a human user has to put, to solve a cognitive CAPTCHA must be less. Cognitive CAPTCHA challenge should not be cumbersome for human user.
- **Audio-Visual clarity**: Cognitive challenge presented in audio or visual format must be clear and should not contain any noise or blurring. Strength of cognitive CAPTCHA should rely on superior cognitive capabilities of human being and not on the technically added noise. Audio-Visual clarity of a cognitive CAPTCHA would make it universally accessible for all users including the people with various disabilities.
- **Greater AI-Hardness**: In the arena of ever improving AI capabilities, a cognitive CAPTCHA must be armed with the problems having high degree of AI-Hardness.
- **Less error-proneness:** The terms and symbols used to present a cognitive CAPTCHA challenge must be helpful for a user to avoid making unintentional mistakes. Language and pictures used should be culturally neutral and unambiguous.

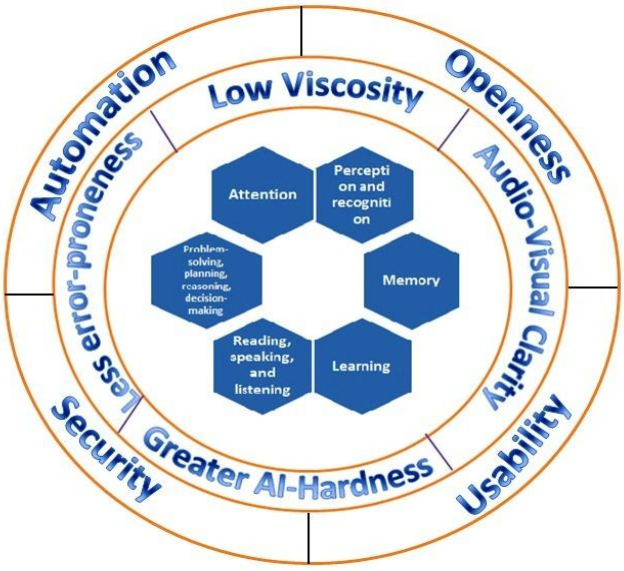

Figure 1. Proposed Framework for cognitive CAPTCHA Designing

V. CONCLUSION

The proposed framework depicts the thumb rules for designing any cognitive CAPTCHA. Features like low viscosity, audio-visual clarity and less error-proneness will together increase human friendliness of a cognitive CAPTCHA. AI-Hardness will increase the robustness against bot attacks. Low viscosity, audio-visual clarity will make the cognitive CAPTCHAs universally accessible for people with disabilities and thus compliant to Web Content Accessibility Guidelines (WCAG) 2.0. Less error-proneness will make a cognitive CAPTCHA neutral for culturally and linguistically diverse people. Implementation of proposed framework for cognitive CAPTCHA will yield more efficient, robust, usable and accessible cognitive CAPTCHAs for all human users.

REFERENCES

[1] S. K. Saha, A. K. Nag, D. Dasgupta, "*Human-Cognition-Based CAPTCHAs*", IT Professional, Vol. **17**, No. **5**, pp. **42-48, 2015**.

[2] M. M. Tanvee, M. T. Nayeem, M. M. Rafee, "*Move & Select: 2-Layer CAPTCHA Based on Cognitive Psychology for Securing Web Services*", International Journal of Video & Image Processing and Network Security, IJVIPNS/IJENS, Vol. **11**, Issue. **5**, pp. **9-17**, **2011**.

[3] M. J. M. Chowdhury, N. R. Chakraborty, "*CAPTCHA Based on Human Cognitive Factor*", International Journal of Advanced Computer Science and Applications, Vol. **4**, No. **11**, pp. **144-149**, **2013**.

[4] A. Rusu, R. Docimo, "*Leveraging Cognitive Factors in Securing WWW with CAPTCHA",* In the Proceedings of USENIX Conference on Web Applications, **2010**.

[5] V. Dhaka, G. Gandhi, "*Developing a CAPTCHA Utilizing Cognitive Ability of Human through PHP*", International Journal of Advanced Networking Applications, Special Issue, pp. **50–54, 2015**.

[6] T. Yamamoto, T. Suzuki, M. Nishigaki, "*A Proposal of Four-panel cartoon CAPTCHA*", In the Proceedings of IEEE

International Conference on Advanced Information Networking and Applications 2011, pp. **159–166**, **2011**.

[7] D. G. S. Edgar, G. C. Salvador, M. F. R. Edgardo, "*Designing New CAPTCHA Models Based on the Cognitive Abilities of Artificial Agents*", Research in Computing Science, Vol. **138**, pp. **127-136, 2017**.

[8] M. Mohamed, S. Gao, N. Saxena, C. Zhang, "*Dynamic Cognitive Game CAPTCHA Usability and Detection of Streaming-Based Farming*", In Workshop on Usable Security (USEC), co-located with NDSS, **2014**.

[9] M. R. Ogiela, N. Krzyworzeka, L. Ogiela, "*Application of knowledge-based cognitive CAPTCHA in Cloud of Things security*", Concurrency and Computation: Practice and Experience, Vol. **30**, No. **21**, pp. **1-11**, **2018.**

[10] N. Divyashree, "*Secured Conversion and Generation of Cognitive Catch Implementing Honeypot Technique*", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. **20**, No. **3**, pp. **24-26**, May-June **2018.**

[11] M. R Ogiela, L. Ogiela, "*Authentication Protocols Using Multi-level Cognitive CAPTCHA, Advances in Internet, Data and Web Technologies"*, EIDWT 2019, Lecture Notes on Data Engineering and Communications Technologies, Vol. **29**, pp. **114–119**, Springer, Cham, February **2019**.

[12] A. Bhalerao, L. Rade, "*A Basic Survey of CAPTCHA :Application and Challenges",* International Journal of Scientific Research in Computer Science and Engineering, Vol.**06**, No. **01**, pp.**1-5**, **2018.**

[13] P. Devi, "*Attacks on Cloud Data: A Big Security Issue*", International Journal of Scientific Research in Network Security and Communication, Vol.**6**, No.**2**, pp.**15-18**, **2018.**

[14] K. A. Kluever, R. Zanibbi, "*Balancing Usability and Security in a Video CAPTCHA*", In 5th Symposium on Usable Privacy and Security, SOUPS, ACM, p.p. **1–11, 2009.**

Authors Profile

Mrs. S. S. Kulkarni pursued Bachelor of Science from S. R. T M. University, India in 2005 and Master of Science from S. R. T M. University, India in year 2007. She has aquired Post Graduate Diploma in Advanced Computing from CDAC, Pune, India in year 2008. She is currently pursuing Ph.D. in School of Computational Sciences, S. R. T M. University, India. She has published several research papers in reputed international journals and conferences including IEEE & Springer and it's also available online. Her main research work focuses on Web Security Algorithms, Accessibilty on web, Human Computer Interaction and CAPTCHA based security. She has 3 years of industrial experience and 1 years of teaching experience.

Dr. H. S. Fadewar pursued Bachelor of Science from Dr. B. A. M. University, India and Master of Science from S. R. T M. University. He has obtained M. Phil. from Y. C. M.O. University and pursued Ph.D. from S. R. T M. University, India. He is currently working as Assistant Professor in School of Computational Sciences, S. R. T M. University, India since 2011. He a life member of The Indian Science Congress Association, Kolkata and International Association of Engineering. He has published more than 40 research papers in reputed international journals and conferences including IEEE, Springer and it's also available online. His main research work focuses on Human Computer Interaction, Data Mining and Biometrics. He has more than 15 years of teaching experience and 10 years of Research Experience.

