Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Intrinsic Situation Reaction CAPTCHA for Better Web Security

Pooja Shende
Dept. of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India

Rajeev Pandey
Dept. of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India

Shikha Agrawal
Dept. of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India

Abstract - These days, web security is widespread. It is important to be wary of dishonest behavior. Numerous hackers try to develop interactive software or websites that automatically attempt to compromise data. Web servers become busy or unavailable as a result of the numerous junk entries it generates. CAPTCHA is a method to prevent spam entries. It is capable of identifying and rejecting bots. The acronym for Completely Automated Public Turing test to tell Computers and Humans Apart is CAPTCHA. The development of CAPTCHA offers a variety of methods, such as distorted text, image recognition, mathematical problem solving, gaming-based, and many more. Game-based testing is very popular these days, but since games are not intellectual, there are many ways to get past them. Thus, the Intellectual CAPTCHA is essential in this day and age. The Situation Reaction Challenge with Intrinsic Decisions serves as the foundation for the suggested study. The suggested study can more precisely differentiate between humans and bots according to their intrinsic problems. It is believed that humans are better suited to deal with real-world problems, whereas machines are somewhat less able to understand the situation or come up with a solution. Therefore, simple scenarios that is easier for humans but practically impossible for bots present challenges for the proposed research. To solve the issue in the allotted time, humans must use common sense. It is based on a challenging AI (Artificial Intelligence) problem that uses game theory to solve.

Keywords - ***CAPTCHA, Web Security, Game Theory, OCR, Image Processing, Decisive Attacks, Bots.***

I. INTRODUCTION

This is CAPTCHA or the Completely Automated Public Turing Test to Tell Computers and Humans Apart. This security tool is designed to distinguish between real users and fake bots. CAPTCHAs present challenges that are easy for humans to solve but difficult for computers like identifying distorted characters or numbers or identifying specific areas in an image. These checks aid in preventing automated abuse of websites [1]. In order to prevent automated abuse of internet services CAPTCHA technology has been crucial since its initial introduction in 2000 [2]. Traditional text-based CAPTCHAs used alphanumeric character distortion to differentiate between humans and bots. However because AI has advanced many of the older CAPTCHA methods are no longer functional. With a focus on enhanced security and user experience this study investigates recent advancements and trends in CAPTCHA [3].

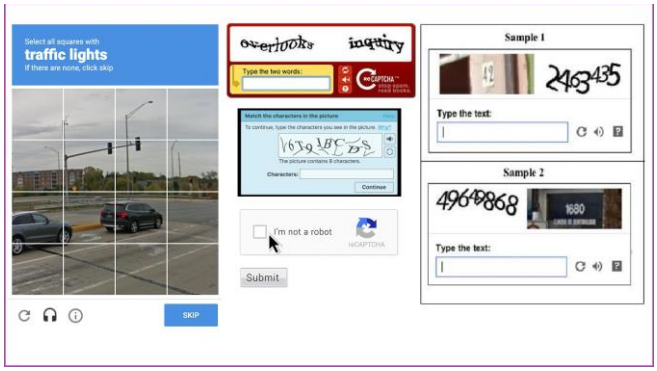


Fig. 1. Types of CAPTCHA [4]

The evolution of CAPTCHA reflects the ongoing struggle between security and evolving technology. Since their initial introduction in 2000 as text-based tasks to distinguish humans from machines CAPTCHAs have evolved into image-based tasks such as item identification and audio CAPTCHAs for users with disabilities. While behavioral CAPTCHAs like Google's reCAPTCHA v3 analyze user behavior to detect bots without upsetting users invisible CAPTCHAs speed up the process even more [5]. As AI technologies such as machine learning and neural networks develop bots have become more adept at solving traditional CAPTCHAs leading to the development of biometric and other methods [6]. The arms race continues as CAPTCHAs are integrated into broader security models in an attempt to balance robust protection with user convenience. Gaming CAPTCHAs (Completely Automated Public Turing Tests to Tell Computers and Humans Apart) are a novel alternative to traditional text and image-based human verification systems. They offer engaging interactive and potentially safer methods of differentiating humans from automated bots. In order to provide a comprehensive performance analysis of gaming CAPTCHAs this study looks at usability security robustness and computational efficiency across a number of prototype designs. The study's objectives include identifying problems categorizing gaming CAPTCHAs according to their types performing an experimental evaluation with both human

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

participants and automated attack simulations and reviewing relevant literature. The findings demonstrate that a well-designed gaming CAPTCHA can sustain high usability scores withstand basic automated solvers and perform well under high server load even when graphical complexity and system responsiveness are traded off. With the aid of the results security system scalability and user experience can be balanced. Gaming CAPTCHAs a new class of human verification tools differentiate between automated bots and actual users by using interactive game-like elements. With the help of short intuitive tasks that are simple for people but challenging for computers to perform gaming CAPTCHAs aim to improve user engagement accessibility and resilience. This contrasts with conventional text- or image-based CAPTCHAs which often have low user satisfaction and are susceptible to solvers that use machine learning. Through the use of load analysis empirical user testing and automated attack simulations this study offers a comprehensive performance analysis of gaming CAPTCHAs in three crucial areas: computational efficiency security and usability. For desktop and mobile environments three prototype designs with responsive layouts and adjustable difficulty were put into practice. These designs featured drag-and-drop sequencing object-matching and physics-based balancing tasks.

II. RELATED WORKS

Zhang, Tao et al. [33] presents the convolution neural network-based CAPTCHA recognition algorithm and examines the features of simple segmentation CAPTCHA and indivisible verification code. It creates the training network structure for various CAPTCHAs and fully utilizes the convolution neural network's self-learning capabilities. It also streamlines the conventional CAPTCHA recognition process in character segmentation, eliminates the need for additional human intervention, and gives the training network model itself excellent anti-noise and anti-rotation features. Haipeng Wang et al. [34] suggested a CAPTCHA in which users must find specific objects in an image based on a text query. The author uses 3D-shaped synthetic images (e.g. English letters, numbers, geometric shapes, etc.) to create images. Numerous facets of visual reasoning, including object identification, comparison, spatial relationships, etc., are included in the text queries. To make sure this design is usable; the author conducted both online and controlled experiments. To confirm the CAPTCHA security, an attack simulation was also carried out. Additionally, we attempted neural style transfer to create new images, and the experiment verified its efficacy. Jesudoss A. et al. [35] proposed a hard independent authentication scheme where user is required to input secret OTP (One Time Password). However, the author does not assert that the suggested work is better than the widely used SSL or Kerberos protocols. These widely used protocols are unquestionably better and unmatched. Although this work can be used as a pre-authentication module to yield useful results, it is not a replacement for these protocols. This work could be expanded by adding single-sign-on functionality and defense against SQL Injection attacks. Hu Yu, et al. [36] presented a convolutional neural network-based CAPTCHA. Character adhesion and distortion can be identified without segmentation, according to the CAPTCHA of images. The network structure is modularized to recognize the various character lengths of the CAPTCHA image with minor modifications, and a multitask joint training model is introduced to increase the network learning rate and model generalization ability. According to experimental results, the suggested approach has a good recognition effect, with recognition accuracy reaching 96. 5%. Chinese character recognition CAPTCHAs will be added in subsequent work. S.Ezhilarasi et al. [37] implemented an image recognition and annotation model which is based on user's decision. Image pre-processing techniques like color quantization, luminosity, image dithering, rescaling, morphological operations, and image transparency are applied to the randomly tiled images of nature, animals, flowers, everyday objects, fruits, vegetables, vehicles, etc. After processing the image; system added some noise over an image for turning it more complicated that cannot easily recognized. In order to test an image process operator's ability to withstand noise and evaluate the effectiveness of various noise filters, authors purposefully corrupt an image with noise. Either this kind of CAPTCHA might be complicated even for human also or it can be detected by using Tensorflow.



Fig. 2. Noise generation and Annotation based Decision-Making [37]

Shotaro Usuzaki et al. [38] suggested a CAPTCHA method to fend off automated and relay attacks. In this CAPTCHA, the user uses their mouse cursor to follow a target object from randomly appearing decoy objects. This technique focuses on the delay time that happens between the bot and the distant human-solvers during a relay attack, which makes breaking the CAPTCHA challenging. Finding the right parameters is essential to obfuscating our CAPTCHA without compromising usability. Muhammad A. Shah et al. [39] introduced vCAPTCHA, a voice recognition-based CAPTCHA scheme. According to the author's analysis, a speech-based vCAPTCHA system would minimize the annoyance of legitimate human users while more successfully protecting online resources from bots. Author uses Pocketsphinx for speech recognition that is pre-built model where training is not performed manually. But Google voice recognizer is not getting more powerful and able to recognize various voice commands and voice based system is always considered as weak authentication protocol and not a trustworthy approach.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

III. PROBLEM IDENTIFICATION

T, Ayushi et al. [40] proposed an intrinsic situation reaction based CAPTCHA where human is required to solve it by understanding the real life situations. As fig 3 where; there is a situation that "You have an important meeting, at the same time you have to drop your wife at railway station; who is new in the city. You have a friend with his bike. What you should do? Drag & Drop husband and wife." The situation is bit complex to understand and its time taking because of so long caption to read. So, as per the complexity level and time taken; the CAPTCHA is not much effective for real world application. Situation must be easier for human and caption should be short but it should not be easier for bot to solve.



Fig. 3. Situation Reaction Test CAPTCHA [38]

The dynamic interactive scenarios that comprise situations such as understanding the requirements of situation and take ideal decision accordingly. This contrasts with conventional CAPTCHAs which depend on the interpretation of static images or text recognition. Gaming CAPTCHAs pave the way for a new era of human-computer verification that emphasizes semantic behavior analysis embodied intelligence and real-time interaction as automation advances and concerns about AI-generated traffic increase. This approach enables CAPTCHAs to be integrated into multi-modal environments such as AR/VR smart devices and gesture-controlled interfaces providing dependable security measures even as AI systems advance. Here the situations are based on textual as well as visual information and in the era of AI; it is easier to understand the situations. So, the security came into risk and it is required to rectify and solve it by intellectual situations that cannot be understand by reading the captions or visual information. It should only be understand by human and no hassle should be faced.

IV. PROPOSED METHODOLOGY

The highly sophisticated and secure Situation Reaction based CAPTCHA technique which is intended to effectively differentiate between humans and bots is introduced in the proposed work. In contrast to traditional CAPTCHAs SR-CAPTCHA uses a situation-reaction test to ask users to make logical decisions based on real-world scenarios. Machines cannot react appropriately to these scenarios because they are designed to take advantage of human cognitive abilities. After a certain number of unsuccessful attempts the system blocks the user. It records each unsuccessful attempt and processes them automatically. The user is presented with a fresh and distinct scenario with every subsequent access. This dynamic method lowers predictability while enhancing security. Game theory which examines human decision-making under challenging conditions is the foundation of SR-CAPTCHA. It differs from traditional CAPTCHA systems in that it concentrates on real-world problems that call for critical thinking a skill unique to humans. For Turing testing and advanced bot identification the system works well because it simulates real-world everyday decision-making situations and offers an example of a challenging AI problem. A CAPTCHA ought to be as easy as possible for humans and almost impossible for bots. AI problems shouldn't be a source of annoyance for the user rather they should be enjoyable. The proposed system is capable of handling difficult AI problems that are easy for humans to solve but nearly impossible for bots. This system is based on common situations that people face in their lifetimes. For instance a couple in a restaurant has food on the table but they are not eating because they are both using their phones. The query that facilitates their eating will now be asked. It can be viewed as a mini-game but it has a difficult AI problem that only humans can solve because it requires understanding and common sense based on real-world scenarios. The answer would be that people generally began using their phones in restaurants rather than properly eating their food. They will drag their phones across the table before they start eating. In this instance the user must click or drag and drop there is no simple yes/no response allowed. Determining whether the intervening user is a human or a bot is the models goal.

So, the human strategy is considered as:

$$s_a \in S_a \tag{1}$$

CAPTCHA strategy is considered as:

$$s_b \in S_b \tag{2}$$

G is considered as the game rule:

$$G = (S_a, S_b, \mu_a, \mu_b) \tag{3}$$

$$\mu_a(S_a, S_b) \in (Success = 1, Failure = 0) \in (Human/Bot) \tag{4}$$

$$\mu_b(S_a, S_b) \in (Correct = 1, Failure = 0) \in (CAPTCHA) \tag{5}$$

Let the bot played σ_a and CAPTCHA played σ_b:

$$E[\mu_a] = \sum_{s_a \in S_a, s_b \in S_b} \sigma_a(s_a)\,\sigma_b(s_b)\mu_a(S_a, S_b) \tag{6}$$

$$E[\mu_b] = \sum_{s_a \in S_a, s_b \in S_b} \sigma_a(s_a)\,\sigma_b(s_b)\mu_b(S_a, S_b) \tag{7}$$

Let structuring the CAPTCHA as:

$$\max_{\mu_a \in s_1^{bot}} E[\mu_a] \ll \max_{\mu_a \in s_1^{human}} E[\mu_a] \tag{8}$$

Where $E[\mu_a]$ is considered as expected success rate for human/bot, $E[\mu_b]$ is considered as expected success rate for CAPTCHA. s_1^{bot} is considered as the set of strategy for bot and s_1^{human} is considered as the set of strategy for human. max is the best possible success. $\ll$ is defined as much less than.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

A person is looking for his mobile phone when he wake-up, he is confused and unable to find. User is required to help him to find his mobile.

Question: Help him to find his mobile?

Expected Answer: Move (drag and drop) pillow because it is just under the pillow. Generally when people wake-up in the morning; usually they find their mobile phones under that.

"E" is considered as the level of the finding the mobile phone

"M" is considered as the confusion level or finding the mobile phone on wrong places. So, $(1 = Mobile\ Not\ Found, 0 = Mobile\ Found)$

"I" is considered as an interactions with stuffs presented in the room.

$$E = f(I, M) \quad (9)$$

$E = f(I, M)$ is considered as the function of interaction with the stuffs. If $M = 1$ then

$$I \to 0$$

If $M = 0$ then

$$I + + \to Mobile\ Found$$

Now the linear relationship can be defined as:

$$E = j_1.I - j_2.M \quad (10)$$

Where $j_1, j_2 > 0$ represent the interactions and distractions. If mobile not found $(M = 1)$ then it is penalized. If mobile found $(M = 0)$ then distraction has been removed.

Situation 1: Mobile not found, then

Let $M = 1$ that means mobile not found, let $I = 0$

$$E = j_1.0 - j_2.1 = -j_2 \ \to Negative\ Efforts \quad (11)$$

Situation 2: Mobile found, then

Let $M = 0$ that means he found his mobile, let $I = 0$

$$E = j_1.1 - j_2.0 = j_1 \ \to Positive\ Efforts \quad (12)$$

Now, the modelling strategy can be defined as:

$$A(t) + M(t) = 1 \quad (13)$$

Where $A(t)$ is considered as the attention function to the person at time t, $M(t)$ is considered as the attention function to mobile at time t.

Let the effort made at time t:

$$I(t) = \alpha\ A(t)^2 \quad (14)$$

Now the effort function can be defined as:

$$E(t) = \beta.I(t) - \gamma.M \quad (15)$$

$$E(t) = \beta.\alpha.A(t)^2 - \gamma.\big(1 - A(t)\big)^2 \quad (16)$$

$$\text{If } \theta = \alpha\beta \quad (25)$$

$$;E(t) = \theta\ A(t)^2 - \gamma.\big(1 - A(t)\big)^2 \quad (17)$$



Fig. 4. Proposed Situation Challenge I

In Fig.4, the user must assist the person who has misplaced and is searching for his cell phone. In his bedroom, the user can assist him in locating his phone. The phone could be in the almirah, underneath the bed, near the trash can, or somewhere else in the room. However; in essence or by applying the common sense that a person employs in his day-to-day activities. He starts by looking under the pillow for his cell phone, which is the first thing he checks, and it is there. A human is able to consider this issue and come up with a solution with ease, but bots are unable to do so. There is a time limit for players to figure out the game's solution. Everything can be dropped and dragged to any location. When a user locates the phone, they must drag and drop it to that person. In this case, they have successfully completed the CAPTCHA and are able to fill out the required form. This is a recently introduced CAPTCHA in which humans, not bots, are the only ones who can intervene. If you are unable to resolve the issue within the allotted time, CAPTCHA will expire, and new strategies will be needed. A form that can only be submitted once will appear after the user has completed the CAPTCHA. Prior to filling out and submitting the form, you must always find the best solution to the given situation. The game will expire and a different scenario will be presented if the user makes a mistake.



Fig. 5. Proposed Situation Reaction I

A game's answer shows the players' ideal decisions, whether they have similar, opposing, or mixed interests, as well as the potential outcomes of these decisions. The game hypothesis has been used in a number of scenarios where player decisions affect the result. By focusing on the important elements of navigation or perspectives constrained by the players rather than by pure possibility, the hypothesis goes beyond the conventional hypothesis of likelihood. For instance, it has been used to ascertain which combinations are most likely to affect a coalition of citizens or an elector's selection of jurors. The initial step involves setting a timer to encourage the user to assess the situation and take the necessary action. If the user selects the correct option the input fields are enabled allowing them to continue as long as the timer hasn't reached zero. If the task is finished in the allotted time the credentials will be accepted by the server. If the required steps are not followed a

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

timeout occurs and the validation fails. Errors are also observed. The user is given a new scenario to finish when the CAPTCHA expires and they make the same mistake once more. Game designers need to be able to create an experience that includes a lot of difficult original choices with engaging feedback in addition to understanding how choices affect a computer gaming experience. The three skills required to create successful decision-based games are the ability to recognize a decision point evaluate it and design fun decision-making play without compromising other game elements. There is only one difference: optimization involves a single decision maker who makes decisions all the time whereas game theory looks at how the decisions made by several players interact. That is by forecasting the last player's actions in each scenario one can predict the actions of the next-to-last player and so forth.

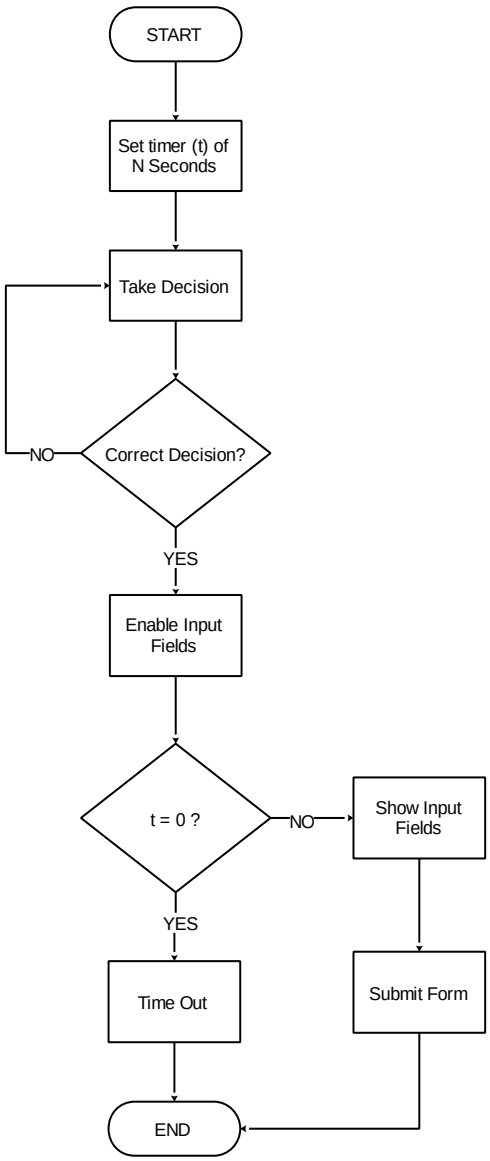


Fig. 6. Flow Chart of Proposed Model

In the related fields of automated scheduling and planning and automated theorem proving the method is referred to as backward search or backward chaining. In chess it's known as retrograde analysis. Backward induction has been used to solve games for as long as game theory has existed.

Cognitive Game Theory Algorithm

Initialization of Game Environment

Input: Set of Object Location X=(a_1, b_1), (a_2, b_2) ,…… (a_n, b_n)

Output: $D = \{Correct\ Decision, Incorrect\ Decision\}$

Step 1: Initialize game

Step 2: Set time $t_{max} \leftarrow$ 60 seconds

Step 3: Define target area:

$$T_a = \{(a,b) \parallel (a,b) - (a_{target}, b_{target}) \parallel < \varepsilon\} \quad (18)$$

Where ε is defined as the tolerance radius of the game.

Step 4: Set Coordinates (left, right, bottom, top) //drag & drop

Step 5: Coordinate Transformation

$$a_{new} = a_{left}^{(n)} + \left(\left(\frac{a_{old} - a_{left}^{(0)}}{a_{right}^{(0)} - a_{left}^{(0)}}\right) \cdot \left(a_{right}^{(n)} - a_{left}^{(n)}\right)\right) \quad (19)$$

$$b_{new} = b_{top}^{(n)} + \left(\left(\frac{b_{old} - b_{top}^{(0)}}{b_{bottom}^{(0)} - b_{top}^{(0)}}\right) \cdot \left(b_{bottom}^{(n)} - b_{top}^{(n)}\right)\right) \quad (20)$$

Where a_{new} and b_{new} are the new location of the object after drag & drop.

Step 6: if T (a_{new}, b_{new}) collide T_a // Target Area

So the decision can be defined as-

$$Decision(a_{new}, b_{new}) = \begin{cases} Correct & if\ (a_{new}, b_{new}) \in T_a \\ Incorrect & Otherwise \end{cases} \quad (21)$$

Step 7: while (t > 0) do

Repeat Step 5 & 6;

end while

Step 8: For each iteration *i;*

$$t_i = t_0 - i.\Delta t \quad (22)$$

Δt is considered as the time taken per interaction. But if;

$$t_i \leq 0 \leftarrow Verification\ Failed \quad (23)$$

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Step 9: End

For the Game Theory Algorithm the situation reaction-based approach is the basis. The game must first be configured with time t. The user can change the coordinates of each drag-able object when they are moved to a different location. Therefore each movement requires a calculation of the new location. The system constantly updates the location of the target object which is present among all the other objects. Until t is not equal to zero the user must find the target object and drag it to the desired location. The user will have made the correct decision once they have located the target object and struck the target location. If the designated time has elapsed and a reload button appears the CAPTCHA verification is unsuccessful. The reload button causes a new scenario to appear when the user clicks it.

V. RESULT AND ANALYSIS

The experimental outcome depends on a few parameters such as average time recorded, min & max time, number of successful and unsuccessful users, standard deviation, variance, complexity and limitation.

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \quad (24)$$

$$S = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2 \quad (25)$$

Where N is the total number of participants, x_i is the individual participant, and μ is the system mean value.

$$variance\ (S) = \sigma^2 \quad (26)$$

Program complexity is slightly higher for bots but frequently lower for humans. Human trails and attacks carried out to grant unauthorized bots access to the base system and the proposed system will be used to analyze the results. Thirty of the participants in table I use the CAPTCHA and their time is consistently recorded as such.

Table 1 Experimental Results

Parameters	Proposed
Total No. of Users	30.0
Total No. of Accomplished Users	29.0
Total No. of Failed Users	1.00
Mean Time (μ) in seconds	8.37
Minimum Time Recorded in seconds	5.00
Maximum Time Recorded in seconds	15.0
Precision of Success	0.97
Precision of Failure	0.03
Standard Deviation (σ)	2.91
Variance (S)	8.50

Table 2 Frequency Table

Value in (seconds)	Frequency
0	1 (3.3333333333333%)
5	3 (10%)
6	3 (10%)
7	5 (16.666666666667%)
8	4 (13.333333333333%)
9	3 (10%)
10	5 (16.666666666667%)
11	3 (10%)
12	1 (3.3333333333333%)
14	1 (3.3333333333333%)
15	1 (3.3333333333333%)

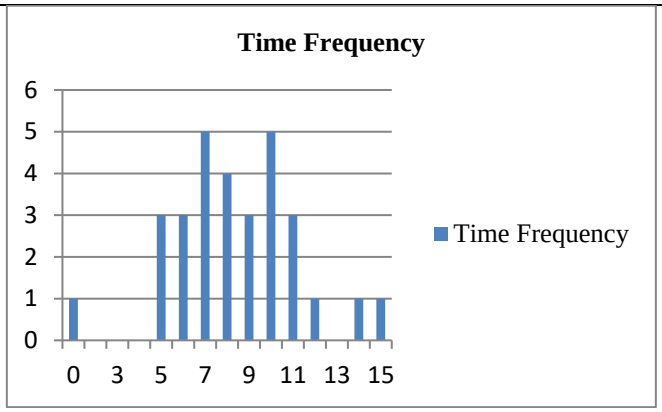


Fig. 7. Frequency of Users w.r.t Time

Table 3 Result Comparison

Authors	Game Type	ASR	BS	MTS	Complexity
Conti, M [41]	Object Matching	96.2	8.50	12.8	High
Mohamed, M [42]	Mouse gesture	93.5	12.0	10.0	Medium
Clarke, N [43]	Point-collecting	90.0	<2.0	9.00	Very High
PlayThru-CAPTCHA [44]	Drag and drop	87.5	18.6	8.00	Medium
Line-CAPTCHA [45]	Draw on path	91.8	11.2	13.3	High
IDSR [40]	Drag and drop	90.0	10.0	5.0	Very High
Proposed	**Drag and drop**	**96.67**	**0.033**	**5.00**	**High**

*ASR – Average Success Rate in %
*BS - Bot Solvability in %
*MTS – Minimum Time to Solve in Seconds

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

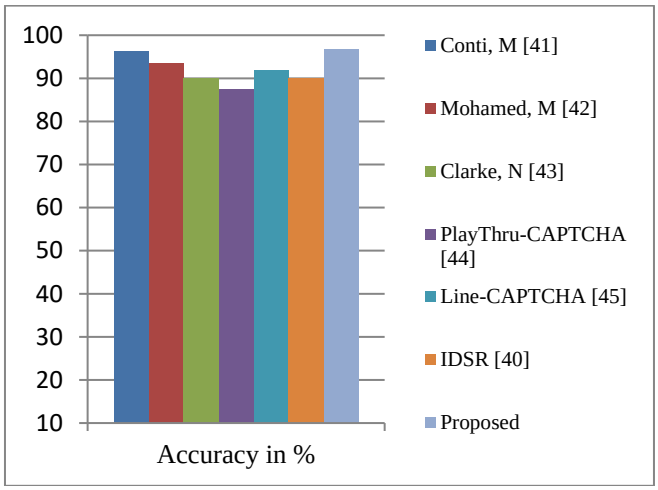


Fig. 8. Graphical analysis of accuracy for different techniques

VI. CONCLUSION

Intrinsic Situation Reaction based CAPTCHA is a contemporary problem that bots must solve intellectually. The suggested task can classify either humans among bots or bots among humans. Since the user must apply common sense to solve the CAPTCHA, the suggested challenge is based on a challenging AI problem. The user can solve the situation-based challenge in a matter of seconds by using common sense or making the fundamentally correct decision. Therefore the most successful CAPTCHA to date that is better able to distinguish between humans and robots is provided by the New Technique for Generation of CAPTCHA based on Gaming Methodology. This is the next generation of CAPTCHA which offers the best security benefits and is enjoyable for users. The system is adequate for suggesting an increased degree of protection in the gaming CAPTCHA domain since no attacks can compromise its security premises. As per the user inference earlier gaming CAPTCHA is bit difficult to understand due to inclusion of high complexity. But the experience regarding the proposed CAPTCHA that directly relate to the humans common sense; it is bit easier to understand and solve within given time and the average to time to solve the CAPTCHA is 8.37 seconds. The minimum time recorded is 5 seconds, maximum time recorded is 15 seconds, and precision of success is 0.967, precision of failure is 0.033. So, as per the result analysis the Standard Deviation and Variance are 2.91 and 8.50 respectively. The proposed CAPTCHA is useful in many areas including big data optimization and digital transactions where human latency is frequently significant. In the future the intrinsic situations-based gaming CAPTCHA concept that is currently being proposed could be improved with more intellectual efforts that are nearly impossible for bots to solve but easily solved by humans. While machines are incapable of solving many intellectual problems, humans are able to do so in a specific amount of time. The system performed better than the base paper and earlier recommended systems. As artificial intelligence are rapidly growing to solve the human related problems; so it is required to propose an hard AI based problems where human can understand it easily but almost impossible for bots. The real time situations can be visually represented with hidden task can helps to improve the scope of the future works.

REFERENCES

[1] “Imperva: CAPTCHA”, 06 July 2025. Accessed on: Nov. 27, 2024. [Online]. Available: https://www.imperva.com/

[2] Von Ahn, L., Blum, M., & Langford, J. (2003). "Telling humans and computers apart automatically." *Communications of the ACM*, 46(5), 56-60.

[3] Goodfellow, I., et al. (2014). "Generative Adversarial Nets." *Advances in Neural Information Processing Systems.*

[4] “Geeksforgeeks: what-is-captcha-attack”, 22 July. 2022. Accessed on: Nov. 27, 2024. [Online]. Available: https://www.geeksforgeeks.org/what-is-captcha-attack/

[5] Akhawe, D., & Felt, A. P. (2013). Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. *USENIX Security Symposium.*

[6] Bursztein, E., Martin, M., & Mitchell, J. (2011). Text-based CAPTCHA Strengths and Weaknesses. *Proceedings of the 18th ACM Conference on Computer and Communications Security.*

[7] Mori, G., & Malik, J. (2003). Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. *IEEE Computer Vision and Pattern Recognition (CVPR).*

[8] J.J. (06 July 2025). 3 things to consider before you implement CAPTCHA for accessibility. Medium. https://uxdesign.cc/3-things-to-consider-before-you-implement-captcha-for-accessibility-7b4fe01cd747

[9] Noury, Zahra & Rezaei, Mahdi. (2020). Deep-CAPTCHA: a deep learning based CAPTCHA solver for vulnerability assessment. 10.31219/osf.io/km35b.

[10] Tam, H., Florencio, D., & Herley, C. (2008). Secure CAPTCHAs Using Audio and Images. Proceedings of the 17th International Conference on World Wide Web (WWW).

[11] Bigham, J. P., & Cavender, A. C. (2009). Evaluating Existing Audio CAPTCHAs and an Interface Optimized for Non-Visual Use. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

[12] Ahmed, Tanvir & Tushar, Kaiser & Islam, Sunjida & Rahman, Md.Mahbubur. (2016). Siimple, Robust & User Friiendlly CAPTCHA 'InstaCap' for Web Securiity. International Journal of Hybrid Information Technology. 9. 163-182. 10.14257/ijhit.2016.9.1.15.

[13] Chew, M., & Baird, H. S. (2003). BaffleText: A Human Interactive Proof. International Journal on Document Analysis and Recognition (IJDAR).

[14] Ahn, L. V., & Blum, M. (2004). Peekaboom: A Game for Locating Objects in Images. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

[15] Gossweiler, R., Kamvar, M., & Baluja, S. (2009). What's Up CAPTCHA? A CAPTCHA Based on Image Orientation. Proceedings of the 18th International Conference on World Wide Web (WWW).

[16] Ong, J. (2013, October 9). Future Ad Labs signs Heinz and Reckitt Benckiser as launch partners for its gamified CAPTCHA. *TNW | Insider*. https://thenextweb.com/news/future-ad-labs-signs-heinz-and-reckitt-benckiser-as-launch-partners-for-its-gamified-captcha.

[17] Bursztein, E., Martin, M., & Mitchell, J. (2014). The End is Nigh: Exploring the Collapse of HTTPS Visual Indicators. Proceedings of the USENIX Security Symposium.

[18] Ridloghfry. (2024, November 18). Integrating Google reCAPTCHA into Your Next.js Application: A Step-by-Step Guide. *Medium*. https://blog.devgenius.io/integrating-google-recaptcha-into-your-next-js-application-a-step-by-step-guide-f7df3f7c57e0.

[19] Zhu, B. B., Yan, J., Li, Q., Yang, M., & Xu, N. (2010). "Attacks and design of image recognition CAPTCHAs." *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*, pp. 187–200. https://doi.org/10.1145/1866307.1866329

[20] Nguyen, Hoang & Subramani, Karthika & Acharya, Bhupendra & Perdisci, Roberto & Vadrevu, Phani. (2024). C-Frame: Characterizing

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

and measuring in-the-wild CAPTCHA attacks. 277-295. 10.1109/SP54263.2024.00200.

[21] L. Von Ahn and L. Dabbish. Labeling images with a computer game. In Proceedings of the SIGCHI conference on Human factors in computing systems, pages 319–326. ACM, 2004.

[22] Clark Pope and Khushpreet Kaur. Is it human or computer? defending e-commerce with captchas. IT professional, 7(2):43–49, 2005.

[23] Noshina Tariq and Farrukh Aslam Khan. Match-the-sound captcha. In Information Technology-New Generations, pages 803–808. Springer, 2018.

[24] Yan, J., & Ahmad, A. S. (2008). *A low-cost attack on a Microsoft CAPTCHA.* In *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08)*, 543–554. https://doi.org/10.1145/1455770.1455841

[25] *GitHub - 013231/3D-CAPTCHA: A python module for generate 3D CPATCHA.* (n.d.). GitHub. https://github.com/013231/3D-CAPTCHA

[26] "Jquery script: Minimal Math Captcha Plugin For jQuery - Captcha Basic", 25 May 2017. Accessed on: Sep. 25, 2024. [Online]. Available: https://www.jqueryscript.net/form/Basic-Math-Captcha-Plugin.html

[27] Rusu, A., Rusu, D., & Corlatean, A. (2014). *CAPTCHA — A Friendly Access Gate to Web Resources.* Journal of Mobile, Embedded and Distributed Systems, 6(2), 91–100. Available at: https://www.jmeds.eu/index.php/jmeds/article/view/CAPTCHA

[28] Miyamoto, D., Eto, M., Yagi, T., & Kadobayashi, Y. (2008). *Human Interactive Proof with a Logic Puzzle.* In *International Conference on Security and Management (SAM)*, pp. 1–7.

[29] Samariya, Durgesh. (2015). Computer Science and Management Studies Designing CAPTCHA for Web Security Using Rotating and Spiliting Image against OCR Software. International Journal of Advance Research in Computer Science and Management Studies.

[30] Sundararajan, V., & Woodard, D. L. (2011). *Biometric Score Fusion: A Multi-Classifier Approach for CAPTCHA Security.* In *IEEE Transactions on Information Forensics and Security*, 6(4), 1111–1120. https://doi.org/10.1109/TIFS.2011.2156812

[31] Das, Resul & Baykara, Muhammet & Tuna, Gürkan. (2015). Novel CAPTCHA Approaches to Protect Web Forms against Bots.

[32] Rusu, A., Rusu, D., & Corlatean, A. (2014). *CAPTCHA — A Friendly Access Gate to Web Resources.* Journal of Mobile, Embedded and Distributed Systems, 6(2), 91–100.

[33] T. Zhang, H. Zheng and L. Zhang, "Verification CAPTCHA Based on Deep Learning," 2018 37th Chinese Control Conference (CCC), Wuhan, 2018, pp. 9056-9060, doi: 10.23919/ChiCC.2018.8482847.

[34] H. Wang, F. Zheng, Z. Chen, Y. Lu, J. Gao and R. Wei, "A Captcha Design Based on Visual Reasoning," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, 2018, pp. 1967-1971, doi: 10.1109/ICASSP.2018.8461764.

[35] J. A. and M. T. M., "Hardware-Independent Authentication Scheme Using Intelligent Captcha Technique," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-7, doi: 10.1109/ICECCT.2019.8869353.

[36] Y. Hu, L. Chen and J. Cheng, "A CAPTCHA recognition technology based on deep learning," 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), Wuhan, 2018, pp. 617-620, doi: 10.1109/ICIEA.2018.8397789.

[37] S. Ezhilarasi and P. U. Maheswari, "Image Recognition and Annotation based Decision Making of CAPTCHAs for Human Interpretation," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2020, pp. 1-6, doi: 10.1109/ICITIIT49094.2020.9071558.

[38] S. Usuzaki et al., "Interactive Video CAPTCHA for Better Resistance to Automated Attack," 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU), Auckland, New Zealand, 2018, pp. 1-2, doi: 10.23919/ICMU.2018.8653624.

[39] M. Shah and K. Harras, "Hitting Three Birds with One System: A Voice-Based CAPTCHA for the Modern User," 2018 IEEE International Conference on Web Services (ICWS), San Francisco, CA, 2018, pp. 257-264, doi: 10.1109/ICWS.2018.00040.

[40] Thakur, A., Agrawal, S., & Pandey, R. (2019). An enhanced intellectual captcha based on intrinsic situation reaction turing test. International Journal of Recent Technology and Engineering, 8(2), 3726–3731. https://doi.org/10.35940/ijrte.B3215.078219

[41] Conti, M., Guarisco, C., & Spolaor, R. (2015). CAPTCHaStar! A novel CAPTCHA based on interactive shape discovery. Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks.

[42] Mohamed, M., Clarke, N., Li, F., & Papadaki, M. (2014). Dynamic cognitive game CAPTCHA usability and detection of streaming-based farming. In Proceedings of the International Conference on Cybercrime, Security and Digital Forensics. https://www.researchgate.net/publication/260944463

[43] Mohamed, M., Clarke, N., Papadaki, M., & Li, F. (2017). On the security and usability of dynamic cognitive game CAPTCHAs. Journal of Information Security and Applications, 35, 71–84. https://doi.org/10.1016/j.jisa.2017.05.007

[44] [Are You a Human?] (2013). PlayThru CAPTCHA system. Commercial system reviewed in cognitive CAPTCHA literature and deployment documentation. (Archived at: https://www.researchgate.net/publication/260944463)

[45] [LineCAPTCHA System]. (2018). Draw-on-path CAPTCHA using behavioral biometrics. Discussed in Springer's lecture notes and referenced in game CAPTCHA surveys (e.g., Mohamed et al., 2017).

(This work is licensed under a Creative Commons Attribution 4.0 International License.)