iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41167

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

A Review on Various Implemented CAPTCHA in the Field of Web Security

Apoorva Dubey[1], Meenakshi Patel[2]
[1, 2]*Computer Science & Engineering, Oriental Institute of Science & Technology, Bhopal, Madhya Pradesh, India*

Abstract: ***CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a process of identifying whether user is human or robot. It is very important to know the user end because security can be breach. There are different CAPTCHA problems accessible like twisted string, image recognition, math and gaming CAPTCHA. Game based problem is intuitive and profoundly got as contrast with the other CAPTCHA. In this sort of CAPTCHA client needs to tackle an AI problem either by drag and drop technique or click based, contingent upon the game. The paper is expected to audit different carried out CAPTCHA and analyze their shortcoming and security boundaries. A large number of the CAPTCHAs are based on click based strategies where client needs to recognize the photos according to its appearance and snap in like manner. However, this sort of CAPTCHA can be mediated by image processing like object classifier. Dragging an item to the objective region is a successful way however it must be performed or tackled by a scholarly problem. On the off chance that dragging an item to the objective region by object acknowledgment, framework might get broken by relay attacks.***
Keywords: CAPTCHA, Gaming CAPTCHA, Picture Recognition, Web Security, Image Processing, Relay Attacks.

I. INTRODUCTION

Essentially, the CAPTCHA was invented during the 2000s as a way to deal with exploring whether user was a human or robot - a sort of Turing Test. The test wasn't completely mechanized - people expected to attempt to decipher some mutilated text - confused to robots. Additionally with so many web clients completing these tests reliably, Google saw an opportunity for something different. Directly following purchasing CAPTCHA in 2009 it became reCAPTCHA and we were given something to do interpreting old pieces of composing, whether or not we got it. Unfortunately, the free record organization wasn't to persevere. A new report by Google saw that AI robots had the choice to interpret the CAPTCHAs with 99.8% accuracy, and numbers in pictures with 90%. One more method for isolating should be found. Though this case could look direct, there is a very refined cycle behind it. Google's examination works away in the background running its own Turing Test considering how the client is acting all through their associations on the site. Notwithstanding making it significantly more clear for us to complete affirmation processes, planners are ceaselessly looking for ways to deal with making it smoother. Adventure forward "The Honeypot" system. The Honeypot procedure simplifies everything for clients, while giving a fruitful strategy for getting those problematic spambots. It has been furthermore understood that people will wrap up any problem, as lengthy according to their viewpoint. So envision a situation where we made a couple of vague fields that should be filled in by spambots [1].

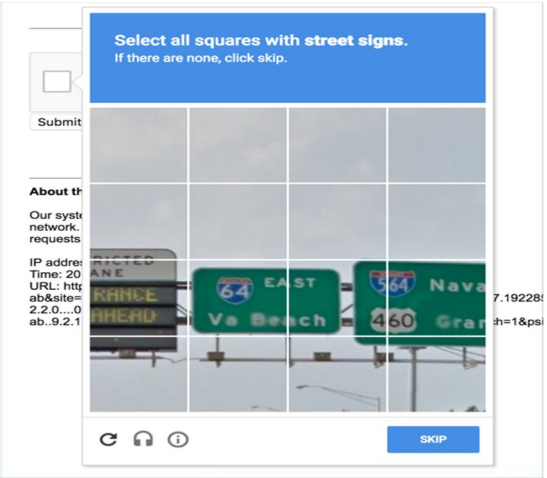


Fig. 1.Google's Risk Analysis [1]

By making the check cycle imperceptible, people aren't bothered by it using any and all means, and you can feel reassured that those spambots are willing giving up themselves - especially when gotten together with Google's important assessment. With a more present day spam catcher comes more complex development. There are a couple of unprecedented educational activities web based counting how to set it up, so it justifies placing assets into. The imperative thing to look out for is ensuring your clients can regardless use autocomplete, without being hailed as a robot [1]. There are different situation where hazard investigation can be estimated by confronting specific hard AI based problems however problem ought to be more straightforward for human and harder for robot and can be addressed soon.

II. RELATED WORKS

A. Related Works

Philip Kirkbride et al. [2] proposed a CAPTCHA for interruption discovery. In this paper, makers considered the cunning use of game-like CAPTCHA as a methodology for data collection to be used in making a direct biometric for perceiving underhanded record use. Given the prerequisite for changing security without compromising client experience, it is acknowledged that game-like CAPTCHA for the time of biometric social data can offer a response. Makers recommend that a model game-like CAPTCHA be made and done as a component of an interference ID structures (IDS) for extra audit on the sufficiency of game-like CAPTCHA for account affirmation. If such a game is made using front-end web advancement like JavaScript and HTML, it will be for the most part easy to discover the data using a past library like rrweb.io. After each game-play the data assembled will be delivered off a server side informational collection. To reproduce authentic use, various guineas pigs will be free to use the CAPTCHA on different days, rather than a couple of times in progression. The fundamental 5-10 game plays will be used as the selection time span and gatherings after that will be used with a SVM computation to conclude whether it can unequivocally isolate the primary player from others. Tolerating precise results from this one-class SVM computation, makers could attempt to moreover chip away at the speed of ID by joining other client credits like IP, client subject matter expert, time-district, and login-time. Monther Aldwairi et al. [3] proposed a framework that surveyed one more kind of CAPTCHA: Flash-based CAPTCHA. According to the outline results, this CAPTCHA was the most favorable to use since it was casted a voting form the least difficult to settle, with the most un-number of dissatisfactions. Likewise, it was considered the fastest, the most wonderful to handle, and the most un-demanding to remember after not including it for a huge time allotment. Also, Flash-based CAPTCHA needs less resources appeared differently in relation to the current CAPTCHAs, making it more capable for use. Streak based CAPTCHA is impenetrable to OCR attacks since this assault targets text-based CAPTCHAs, and the way that this CAPTCHA needs intellectual abilities to address, which makes it more impenetrable to electronic attacks. Additionally, clients from different age social events, levels of preparing, Internet capacities and shockingly those with vision shortcomings had the choice to address it with practically no problem.

Fig. 2.Flash based Game [3]

Ahmet Faruk Çakmak et al. [5] proposed a sound CAPTCHA which is based on RastaPLP Features by SVM. The Naïve Bayes procedure precisely recognizes around 42% of the test digits. This system moreover failed considering the way that each class part in the train set isn't changed considering the way that the train set has a colossal number of upheaval class (11th class) parts, while the parts from 0 to 9 are genuinely less. None of the 100 sound reports in the test set were totally seen by Naïve Bayes procedure. Since the amount of parts isn't changed, regardless of the way that the classes from 0 to 9 somewhat seen even in the train set, the disturbance class has a by and large low accomplishment speed of 71%. To this end all test sound archives are not seen without bumble, yet whether or not a section is wrongly given out to the fuss class, it suggests that the test part is misclassified. Nitisha

Payal et al. [6] proposed a CAPTCHA which is based on mixture pictures. AJigJax is a drag-drop based Captcha in a sort of straight jigsaw puzzle. The proposed work presents two levels in Captcha, one is CL1: AJigJax; for those locales that are rarely gotten to or need less security or no approval and other one is CL2: AJigJax; for those destinations that have essential information and need affirmation to be done and are consistently gotten to. Based on the display evaluation of Captcha, we can decidedly say that AJigJax Captcha is actually tended to, connecting with, less monotonous, straightforward. AJigJax is more secure as rearranged are gotten than making text to breeze through the assessment. CL2: AJigJax should be tended to by legitimated client as the possibility of graphical mystery key is added to it.

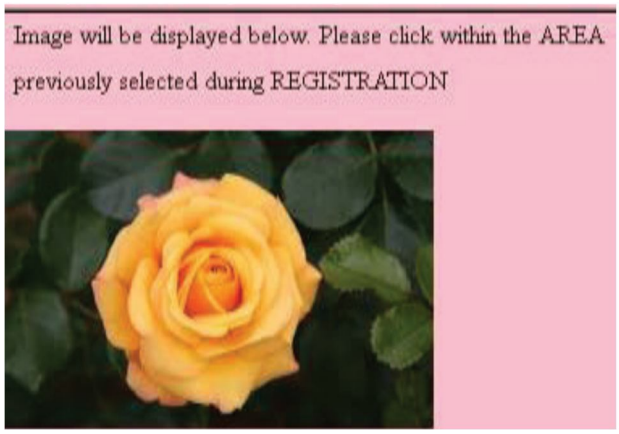


Fig. 3. Pass Point Challenge [6]

Cao Lei et al. [7] proposed a CAPTCHA which is based on finger speculating game makes machines to make a second rationale judgment on the reason for the ID, worked on the trouble for machines to pass. The finger-speculating game has the wide underpinning of the populace, so the CAPTCHA clearly diminishes the trouble of human acknowledgment. It is an advancement of the current picture confirmation code innovation field. Yet, finger speculating game is definitely not a scholarly methodology through which is server can be gotten all the more definitively. Now and again finger speculating game can turn out to be more befuddling a direct result of different signals inciting in the screen for acknowledgment that debased the presentation of the CAPTCHA and may aggravate clients to communicate with it.

Fig. 4. Finger Gessing CAPTCHA [7]

Hong Yu et al. [8] proposed an Automatic Generation of Game-based CAPTCHA. In the crucial execution, the game based CAPTCHA uses text based thought marks. Thusly a bot outfitted with PC vision capacities can without a doubt see the text in the game. However, to break the CAPTCHA, the bot moreover needs to reason about the association between the thoughts, either through glancing through on the web or breaking into the data informational index. Notwithstanding the way that we remove the fundamental data informational index from ConceptNet which is uninhibitedly accessible, the AGCG structure can be handily passed on with a private data informational index which is more secure for business use. Ideally, private data informational index has relations that don't cover through and through with public normal data informational collections due to the deficiency of data informational collection and the colossal proportion of possible ordinary relations. It could take a piece longer for players to finish proposed game based CAPTCHA than a regular visual set up CAPTCHA as for a PC.

Regardless, the games could convey more enjoyment to a client than an OCR task, not totally settled. Proposed game-based CAPTCHA could be more appropriate for compact circumstances where it is more clear for the clients to swipe and take than to type in words. The CAPTCHA is a huge propaganda to hold bots back from getting to web access. Proposed game-based CAPTCHAs join the security of the traditional visual based CAPTCHAs, the human appropriateness of the reasoning based CAPTCHAs, and the fun of computer games. It can normally make huge enough number of game based CAPTCHAs to prevent direct savage power attacks. Subsequently we acknowledge that proposed game-based CAPTCHAs are prepared for laying out a more secure environment on Internet and giving a better web organization than clients.

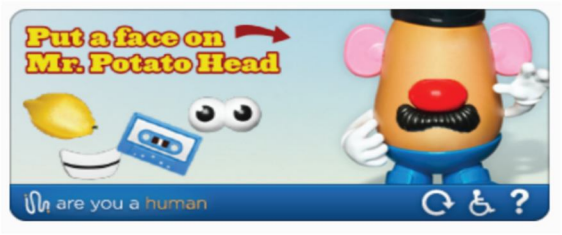


Fig. 5.Game-based CAPTCHA [8]

Shardul Vikram et al. [9] proposed non-nosy moving-target safeguard framework named as NOMAD. Wanderer holds web bots back from automating web resource access by randomizing HTML parts while not affecting normal clients. Specifically, to thwart web bots strikingly recognizing HTML parts for later motorization, NOMAD randomizes name/id limit potential gains of HTML parts in each HTTP structure page. According to the evaluation, NOMAD can hinder this huge number of web bots with a for the most part low vertical. Migrant can be typically completed at the server-side by changing the source code of the web applications. Furthermore, NOMAD could be executed as middleware between the server and client, to do whatever it takes not to add the multifaceted design to the server side reasoning of the web applications. Doing NOMAD as a middleware grants it to be free and all around appli-connection to different web applications (without directly changing the source code) and client side innovations (e.g., different projects and modules). Thusly, the middleware game plan will be clear to the two servers and end clients. Zhen Li et al. [10] proposed a CAPTCHA which is based on game hypothesis. In this paper, we officially displayed the relationship of the decision-production by the protector and the assailant in a Stackelberg game hypothetical system. Through best reaction and technique examination, the make back the initial investment points of whether taking on machine solver or human solver not set in stone. In spite of customary thinking to make CAPTCHA harder, we proposed two models that highlight simple CAPTCHA with time dormancy imperatives as well as fuse of cryptographic money mining into existing CAPTCHA system. The outcomes deter assailants from utilizing human solvers and create a government assistance improving CAPTCHA plan of action. Ibrahim et al. [11] proposed a framework in which client should turn the 3D square and distinguish the particular tones though set apart with question marks. When the client can turn and recognized the person referenced over 3D block, framework permit client to get gotten to any other way another problem will be served and shading model will get changed and another test proposes. Text box and 3D square both have indistinguishable tones and client expects to match both the shadings and perceive the right letter and type around there for effective turing test.

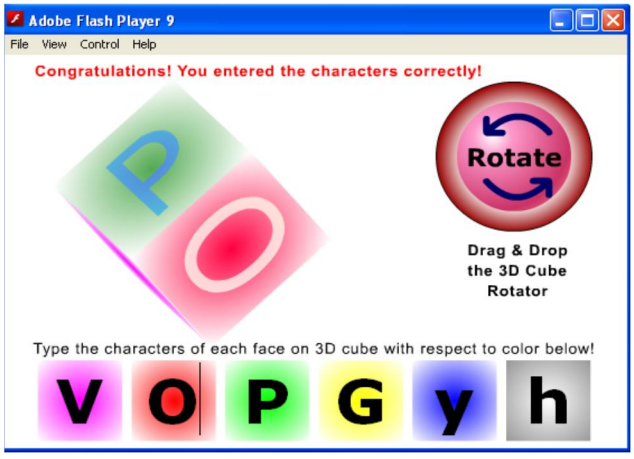


Fig. 6.3D Cubic CAPTCHA [11]

Aadhirai et al. [12] proposed a framework which is based on vision where client should distinguish the item based on distance. Proposed framework serves a picture of certifiable where different sort of items depends. Framework raises a fake problem where client should perceive a specific article which is farthest from a predetermined item. It might challenging to perceive for those individual who has unfortunate vision since there is a foggy appearance which is hard for ordinary human too. On the off chance that it is feasible to notice, it very well may be just finished by human not by bots. It is exceptionally gotten CAPTCHA which having troublesome fake problem which is difficult to tackle by bots.

Fig. 7.Distance based CAPTCHA [12]

III. PROBLEM IDENTIFICATION

S. Ezhilarasi et al. [4] proposed a framework which is based on picture recognition named as IRA (Image Recognition Annotation). In this framework, creators misshaped the picture by resizing, morphology and straightforwardness. Framework added a few commotion in the pictures and makes it muddled for bots to be handled. Be that as it may, some time adding clamor in the picture makes it muddled for human too. CAPTCHA ought to be just about as simple as feasible for human and ought not take an excessive amount of time. It implies that CAPTCAH should be simple, less tedious, less space intricacy and high got. Presently gaming CAPTCHA is in pattern and requires specific consideration from client by making it intriguing. In any case, not picture handling based approaches like google focal point that works with tensorflow and just go for it based methods are significantly more proficient to perceive and arrange the items from pictures that can break the security premises of the picture acknowledgment based CAPTCHA. Author present the IRA CAPTCHA where picture has been contorted and client is expected to recognize the image and snap on radio button likewise. However, at some point twisting level turns it more muddled for human too that might bother clients.

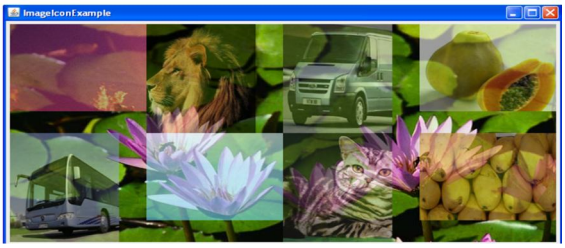


Fig. 8.IRA CAPTCHA for Overlapped Picture [4]

Fig. 8 shows the IRA CAPTCHA where pictures have been overlapped with other pictures and user is required to identify the picture and click accordingly. It may confuses the users to get the actual one.

Table No. I Performance Comparison

Author's Name and Performance Comparison of their Research Paper				
Features	Ibrahim et al. [11]	Aadhirai et al. [12]	Cao Lei et al. [7]	S.Ezhilarasi et al. [4]
Security	Medium	High	High	High
Time complexity	High	Medium	Medium	High
Space Complexity	High	Medium	Medium	Medium
Difficulty Level	Medium	High	High	High
Speed	Low	Medium	Medium	Low
Attacks May Affect	Image Processing-Color Detection	-	Image Processing-Gesture Recognition	Image Processing-Object Classification

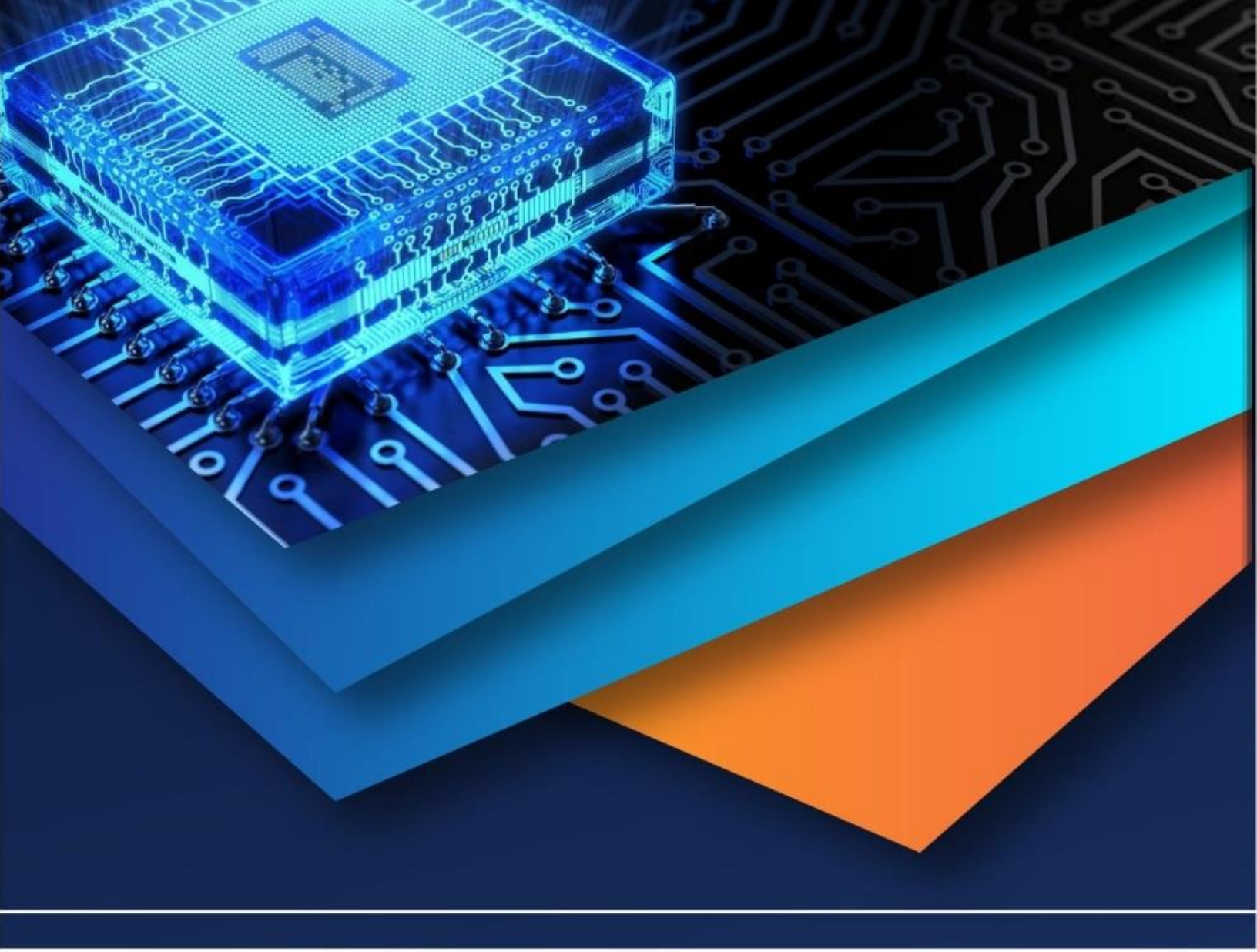
IV. CONCLUSION & FUTURE SCOPE

The intension of the paper is to survey different carried out frameworks in the field of CAPTCHA. The majority of the frameworks have been involved picture recognition CAPTCHA where pictures might be in unique appearance or contorted structure. Typical picture can be perceived utilizing AI draws near and misshaped one get confounds human as well. Certain frameworks are based on streak gaming however game level is bit lower and regularly simple for bot as well. Dragging an item to the objective position is definitely not a scholarly methodology. A gaming CAPTCHA currently can be improved and become more intelligent to get the web premises all the more precisely. Game might be choice based or it very well may be expressed as definitive games. Definitive game can be frequently simple for human however remarkably difficult for robots.

REFERENCES

[1] WebNots, Fix I'm Not A Robot reCAPTCHA Issue in Google Search, 2018. [Online]. Available: https://www.webnots.com/fix-im-not-a-robot-captcha-issue-in-google-search/, [Accessed: 25-Feb-2022]
[2] P. Kirkbride, M. A. Akber Dewan and F. Lin, "Game-Like Captchas for Intrusion Detection," IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, 2020, pp. 312-315.
[3] Aldwairi, Monther & Mohammed, Suaad & Padmanabhan, Megana. (2020). Efficient and Secure Flash-based Gaming CAPTCH.
[4] 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), 2020, pp. 1-6, doi: 10.1109/ICITIIT49094.2020.9071558.
[5] Cakmak, Ahmet & Balcilar, Muhammet. (2019). Audio Captcha Recognition Using RastaPLP Features by SVM.
[6] N. Payal and R. K. Challa, "AJIGJAX: A hybrid image based model for Captcha/CaRP," 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON), 2016, pp. 38-43, doi: 10.1109/UPCON.2016.7894621.
[7] Cao Lei, "Image CAPTCHA technology research based on the mechanism of finger-guessing game," Third International Conference on Cyberspace Technology (CCT 2015), 2015, pp. 1-4, doi: 10.1049/cp.2015.0843.
[8] Yu, Hong and Mark O. Riedl. "Automatic Generation of Game-based CAPTCHAs." (2015).
[9] S. Vikram, Chao Yang and Guofei Gu, "NOMAD: Towards non-intrusive moving-target defense against web bots," 2013 IEEE Conference on Communications and Network Security (CNS), 2013, pp. 55-63, doi: 10.1109/CNS.2013.6682692.
[10] Z. Li and Q. Liao, "CAPTCHA: Machine or Human Solvers? A Game-Theoretical Analysis," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018, pp. 18-23, doi: 10.1109/CSCloud/EdgeCom.2018.00013.
[11] Ibrahim FurkanInce, YucelBatu Salman, Mustafa ErenYildirim and Tae-Cheon Yang, "Execution Time Prediction For 3D Interactive CAPTCHA By Keystroke Level Model" in Fourth International Conference on Computer Sciences and Convergence Information Technology of IEEE 2009.
[12] Aadhirai R, Sathish Kumar P J and Vishnupriya S, "Image CAPTCHA: Based on Human Understanding of Real World Distances" Proceedings of 4th International Conference on Intelligent Human Computer Interaction, IEEE 2012.
[13] JingSong Cui, LiJing Wang, JingTing Mei, Da Zhang, Xia Wang, Yang Peng, WuZhou Zhang, "CAPTCHA Design Based on Moving Object Recognition Problem" in IEEE 2009.
[14] Jing-Song Cui, Jing-Ting Mei, Xia Wang, Da Zhang, Wu-Zhou Zhang , "A CAPTCHA Implementation Based on 3D Animation" in International Conference on Multimedia Information Networking and Security of IEEE 2009.
[15] [20] D. Rajpal and A. Tiwari, "Non-Intrusive Intellectual Gaming CAPTCHA for Optimal Web Security," 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), 2018, pp. 1-7, doi: 10.1109/ICACAT.2018.8933614.
[16] S. Wang, "A comprehensive survey of data mining-based fraud detection research," in International Conference on Intelligent Computation Technology and Automation, Changsha, China, 2010.
[17] J. Zhang, X. Hei and Z. Wang, "Typer vs Captcha: private information based captcha to defend against crowdsourcing human cheating," ArXiv, vol. abs/1904.12542, 2019.

[18] R. Gafni and I. Nagar, "Captcha security affecting user experience," Informing Science and Information Technology, vol. 13, pp. 63-77, 2016.
[19] R. Gafni and I. Nagar , "Captcha: impact on user experience of users with learning disabilities," Interdisciplinary Journal of e-Skills and Lifelong Learning, vol. 12, pp. 207-223, 2016.
[20] M. Okada and S. Matsuyama, "New captcha for smartphones and tablet PC," in IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2012.
[21] S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics," in European Convention on Security and Detection, Brighton, UK , 1995.
[22] B. Sayed, I. Traore, W. Isaac and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," IEEE Systems Journal, vol. 7, no. 2, pp. 262-274, 2013.
[23] J. Ramon and N. Jacobs, "Opponent modeling by analyzing play," in Computers and Games workshop on Agents in Computer Games, Edmonton, Canada, 2000.
[24] G. E. Farr, A. R. Jansen, D. L. Dowe and G. E. Farr, "Inductive inference of chess player strategy," in International Conference on Artificial Intelligence, Melbourne, Australia, 2000.
[25] R. Kenneth, Behavioral biometrics: a remote access approach, Wiley, 2008.
[26] J. Liu, F. Yu, C.-H. Lung and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," IEEE Transactions on Wireless Communications, vol. 8, no. 2, pp. 806-815, 2009.
[27] T. Eude and C. Chang, "Oneclass SVM for biometric authentication by keystroke dynamics for remote evaluation," International Journal on Computational Intelligence, vol. 34, no. 1, pp. 145-160, 2017.
[28] C. Shen, Z. Cai, X. Guan, Y. Du and R. A. Maxion, "User authentication through mouse dynamics," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 16-30, 2013.
[29] R. V. Yampolskiy, "Human computer interaction based intrusion detection," in International Conference on Information Technology, Las Vegas, USA, 2007.
[30] S. Cho, C. Han, D. Hee and H. Kim, "Web-based keystroke dynamics identity verification using neural network," Journal of Organizational Computing and Electronic Commerce, vol. 10, no. 4, pp. 295-307, 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY