A Deep Dive into Captcha Mechanisms and Their Evolution

Prof. Madhavi Kulkarni [1], Riddhi D. Waghmode[2], Pratiksha S. Hodade[3], Krushna B. Dhadge[4], Gaurav A. Chaudhari[5]
[1,2.3,4,5]*Computer Engineering, JSPM's BSIOTR, Pune, IND*

***Abstract*—This paper is a review on current text based, image-based, audio-base methods of CAPTCHA to make them easier for humans and harder for machines. It highlights the vulnerabilitie s of such systems to sophisticated machine learning attacks. Furthermore, the paper explores new ways to improve CAPTCHA security using adversarial machine learning techniques. It also discusses some changes like the game mechanism for fingerguessing, which is one of gamification techniques to improve user interaction and experience as well. This review provides an analysis of these developments to reveal the advantages and limitations different CAPTCHA methodologies as well potential for future advancements, underpinning the need for ongoing innovation in code design that is secure.**

***Index Terms*—CAPTCHA,Adversarial Machine Learning, User Experience, Image Recognition, Security Mechanisms.**

I. INTRODUCTION

A. Overview of CAPTCHA Technologies

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is an important tool for preventing online platforms from being abused by automated bots [1]. And this system works as a security gate which makes simple things for the human and harder to detected by bots. So, ultimately CAPTCHAs became a solution for problems such as spamming and preventing access to the data by web scrapers that don't have permission. However, some popular implementations of CAPTCHA include computer generated text distortions; image recognition challenges and audio prompts to verify a user [2].

Traditional CAPTCHA techniques are also experiencing major difficulties, partly due to the rapid expansion of artificial intelligence and machine learning especially in computer vision [3]. Our findings warn that even the best textual CAPTCHA's can be broken with a sophisticated deep learning algorithm, and calls for future work to address them in depth appropriately.

B. Challenges in Traditional CAPTCHA Systems

Traditional CAPTCHA systems have a number of inherent limitations that prevent their widespread use [4]. For example, even the scriptbased CAPTCHA's security barrier tend to fail because of arms race against revolutionary new OCR
s. Likewise, image-based CAPTCHA's can be solved by machine learning algorithms with strong pa tern recognition and the capability to interpret visual distortions [2]. Additionally, the user experience that comes with all of these traditional methods is often very poor overextended or unclear CAPTCHA can frustrate legitimate parties and drive higher rates of abandonment on websites
[5].

A type of CAPTCHA's is also difficult for people with disabilities because they rely on visual and auditory information [6]. Available CAPTCHA systems emphasize enhancing security only where This situation highlights the more urgent demand of Crisp, A. C for system which should not only protect attack and also be usable from digital accessibility point of view in general user experience [5].

C. Innovations in CAPTCHA Design

Such remaining challenges have driven researchers to explore novel designs for CAPTCHA, taking advantage of recent technological [7]. The primary development in this space is the growth of adversarial machine learning methods capable of manipulating weaknesses present in ML models to produce CAPTCHA's (that are both hard for automated solvers and easy enough for humans to interpret) [6]. It uses

perturbations and adversarial examples to design challenges that are difficult for bots.

CAPTCHA systems also increasingly incorporate game-like elements, including mechanics inspired by common games like rock-paper-scissors [6]. These novel CAPTCHAs engage users with recognizable game formats, increasing user satisfaction while simultaneously significantly raising the difficulty for automated systems to defeat [5].

D. Objectives of the Review

This paper elaborates an extensive study of the enhancements in CAPTCHA technology, covering traditional systems as well as it advances till date. Summary of the contributions by this review are presented as following;

Assess limitations of the existing state-of-theart traditional CAPTCHA systems and challenges they face against modern threats; [8]. • Extensive discussion of the various exciting approaches adversarial machine learning practiced for making CAPTCHA safer [9].

Understanding the incorporation of gamification tactics for increased user engagement and accessibility Patel et al. [10]. • Future research directions and emerging trends with regard to CAPTCHA design are as follows in order to guide the ongoing developments for this vital part of cybersecurity.

II. OVERVIEW OF TRADITIONAL CAPTCHA SYSTEMS

By efficiently distinguishing between automated bots and human users, the conventional CAPTCHA system serves as a safeguard for online sites. There are tasks in this system that are easy for humans to finish but challenging for machines [2]. Common examples of these issues include audio signals intended to verify the user's identity, image recognition tasks, and distorted text [3].

A. Issues with Ordinary CAPTCHA Procedures

Ordinary CAPTCHA frameworks have a number of genuine issues: • Expanded helplessness to Robotization: Numerous text-based CAPTCHAs are getting simpler for bots to induce around as optical character acknowledgment (OCR) innovation creates. In a comparative vein, image-based CAPTCHAs are getting to be less compelling in general since progressively advanced machine learning models can presently illuminate them with relative ease [5].

- Issues with the client encounter: Numerous individuals discover CAPTCHAs irritating, particularly when they are hazy or difficult to get a handle on. Higher rates of site departure may result from this [6]. Since a few CAPTCHA sorts may be blocked off or troublesome to utilize, the issue is impressively more extreme for individuals with inabilities [3].
- Inconsistency and Confusion: The require of standardization over distinctive CAPTCHA implementations can make perplexity for clients and oppositely impact their experiences, ultimately undermining the anticipating security purpose of CAPTCHAs [3].

III. INNOVATIONS IN CAPTCHA TECHNOLOGY

CAPTCHA technology has become an essential mechanism for combating automated attacks on digital platforms [4]. By employing innovative strategies, CAPTCHA systems can effectively tackle enduring security challenges.A CAPTCHA works as a decentralized affirmation device, requiring clients to add up to assignments that are basic for individuals but strikingly troublesome for bots.

A. CAPTCHA Technology Solutions to Key Problems in Online Security

Improved Security: Progressed CAPTCHA strategies can reinforce the adequacy of security measures [5]. By utilizing procedures such as picture acknowledgment and design location, these frameworks guarantee that get to to touchy information and administrations is allowed as it were to authentic clients [6].

Improved User Experience: Contemporary CAPTCHA solutions aim to reduce user frustration by incorporating gamification elements [3]. This strategy engages users through familiar gaming mechanics, rendering the verification process more enjoyable while still presenting a challenge to automated systems [4].

Adaptive Complexity: Not at all like customary CAPTCHA frameworks, which tend to be inactive, adaptive CAPTCHAs adjust their complexity based on

the evaluated danger level [7]. By leveraging machine learning calculations, these CAPTCHA's can analyze client behavior in genuine time and alter the trouble of errands in like manner, enhancing their adequacy against dynamically sophisticated bots [5].

Data Integrity: By integrating blockchainlike principles, innovative CAPTCHA systems can guarantee the integrity of user interactions [2]. These frameworks are competent of safely following and logging client reactions, minimizing the dangers of extortion and unauthorized get to, in this way increasing by and large believe in online stages [1].

Cost Efficiency: With decreased asset requirements for observing and less occasions of mishandle, the usage of progressed CAPTCHA technology can lead to significant taken a toll reserve funds for habit suppliers [4]. Progressed security measures moreover offer assistance reduce the money related strain associated with breaches and unauthorized get to.

IV. A BRIEF INTRODUCTION TO CAPTCHA TECHNOLOGY

As a defence against automated assaults, CAPTCHA technology has emerged as a significant advancement in online security. Captcha methods were first developed to distinguish between human users and bots, but they have since developed to address new issues in digital interactions. An outline of the core components of the CAPTCHA system is given in this section.

A. Fundamentals of CAPTCHA Technology

Completely Automated Public Turing test to Tell Computers and Humans Apart or CAPTCHA is a challenge-response tool used to confirm whether a user is human. The secret to CAPTCHA's success is its capacity to display tasks that are simple for people to perform but difficult for automated systems to do [5]. The following are the essential elements of CAPTCHA technology:

Challenge Mechanism: he difficulties that users face is at the heart of CAPTCHA systems. These could involve picking out particular photos, recognising altered language, or resolving simple puzzles. Unlike traditional verification techniques, CAPTCHAs are made to keep consumers interested while maintaining a high level of security [5].

Human Verification: CAPTCHA tests are made to take use of cognitive abilities that humans have that are difficult for robots to imitate. For instance, Thakker et al. found that tasks involving visual recognition or pattern identification are typically easy for people to understand but challenging for automated computers [8].

B. Types of CAPTCHA Challenges

CAPTCHA systems use a variety of challenges to authenticate users:

Text-based CAPTCHAs: Users must decipher distorted letters and numbers in these tasks. But improvements in optical character recognition (OCR) technology have made them less effective, leading to a move towards more sophisticated substitutes [1].

Image-based CAPTCHAs: In these challenges, users are required to choose particular items or images from a grid. Because humans can quickly identify visual patterns, image-based CAPTCHAs are a useful tool for differentiating between humans and bots [2].

Audio CAPTCHAs: The purpose of audio CAPTCHAs is to increase accessibility by asking users to listen to a series of spoken characters and type them appropriately. Even while they are helpful, those with hearing loss may find them challenging, and they are also vulnerable to changes in voice recognition technology. [4].

C. Validation Mechanisms

A central authority is not necessary for CAPTCHA systems to validate challenges. Rather, the challenge-response procedure that users must go through to verify their identity determines how effective they are. Frequently employed strategies include:

Dynamic CAPTCHAs: These systems change the degree of difficulty according to a user's activities or past interactions, making it harder for suspected automated bots to use while maintaining usability for real users [6].

ReCAPTCHA: Google created ReCAPTCHA, a security-enhancing tool that blends behavioural analysis and conventional CAPTCHA challenges [7]. It can more precisely ascertain whether the user is human by employing sophisticated risk evaluation techniques.

D. The Role of Machine Learning

Both the development of CAPTCHA systems and the strategies for getting around them depend more and more on machine learning [3]. Adversaries are using machine learning techniques to get beyond CAPTCHA security measures, which are designed to outsmart bots [5]. The constant rivalry between CAPTCHA systems and bot technologies emphasises how important it is to keep coming up with new ideas in order to keep CAPTCHA work-
ing [4]

V. ALGORITHMS USED IN CAPTCHA SYSTEMS

A. Randomized Challenge Generation

In order to guarantee that every user encounters a different difficulty throughout interactions, CAPTCHA systems employ randomised challenge generation [5]. This unpredictability is essential because it keeps automated bots from using problems that have already been resolved, enhancing the security and reliability of CAPTCHA systems.

B. Image Distortion Techniques

Picture-based CAPTCHAs use specific algorithms to alter text or visual content. Methods like adding visual noise, reshaping things, and changing colour schemes provide intricate puzzles that are easy for humans to solve but far more difficult for automated systems.

C. Resistance to Optical Character Recognition (OCR)

CAPTCHA systems use algorithms created to fight OCR technology as they advance [4]. These include changing font sizes and types, rotating characters, and randomly allocating text spacing to prevent automated systems from reading and interpreting the message.

D. Behavioral Analysis Algorithms

CAPTCHA systems have started including algorithms that evaluate user behaviour, including typing speed and mouse movement patterns. The system can differentiate between real users and bots thanks to this dynamic analysis, adding an additional degree of security [5].

E. Adaptive CAPTCHA Systems

Machine learning-powered adaptive systems are one of the latest developments in CAPTCHA design. While automated systems face increasing complexity, these CAPTCHAs ensure that legitimate users encounter little friction by adjusting the difficulty of tests based on user habits [7]

F. Monitoring User Interactions

The CAPTCHA's capacity to weed out nonhuman interactions is further enhanced by these technologies, which spot odd behaviour that might point to bot activity.

VI. METHODOLOGY

A. Search Strategy

A systematic approach was adopted for researching CAPTCHA technology, focusing on welldefined objectives. A thorough peer-review process was conducted to ensure that only high-quality studies were considered. The following databases and repositories were used for the review:

- IEEE Access
- ResearchGate
- International Journal of Computer Applications
- IEEE Xplore
- scholar.archive.org
- arXiv.org
- SpringerLink
- ScienceDirect

These sources were chosen for their reliability in publishing significant research articles on CAPTCHA and its various applications [3]. The goal of the review is to provide a detailed survey of the literature, covering topics like "CAPTCHA Mechanisms," "User Interaction in CAPTCHAs," and "Security Challenges in CAPTCHAs."

B. Inclusion Criteria

To ensure the relevance of the selected studies, the following criteria were established:

- Time Frame (2018-2024): Only studies published within this timeframe were included to capture the latest innovations in CAPTCHA systems [4].
- Research Focus: The studies had to focus on key aspects such as CAPTCHA design, algorithms, and the effectiveness of these systems in preventing automated attacks [5].

C. Exclusion Criteria

To ensure clarity and focus in the analysis, the following exclusion criteria were applied:

- Non-CAPTCHA Research: Studies that were not directly related to CAPTCHA or focused only on broader security technologies without impact on CAPTCHA effectiveness were excluded [7].
- Purely Theoretical Research: Studies that focused solely on theoretical CAPTCHA aspects without practical evaluation or applications were excluded [6].

D. Study Selection and Assessment

A systematic method was employed for study selection and evaluation to ensure the inclusion of the most relevant research:

- Initial Screening: Titles and abstracts were reviewed to exclude studies that did not meet the inclusion criteria.
- In-Depth Review: Selected studies were then analyzed in detail, focusing on their methodologies, results, and conclusions, particularly in terms of CAPTCHA effectiveness and resistance to automation.

E. Research Classification

To structure the analysis, the research was divided into three main perspectives:

- Technical Perspective: Research in this category focused on CAPTCHA algorithms, design approaches, and their effectiveness in differentiating human users from bots.
- User Experience: This category explored how CAPTCHAs influence user experience, balancing security with ease of use.
- Security Analysis: Research that examined vulnerabilities in CAPTCHA systems and provided solutions for enhancing resistance to sophisticated automated attacks was categorized here.

F. Quality Assessment

Each selected study was evaluated for credibility and relevance. The criteria used for assessment included:

- Impact on CAPTCHA Design: Studies that contributed directly to improving CAPTCHA security were given priority.
- Methodological Rigor: Preference was given to studies that posed clear research questions and applied robust methodologies, such as empirical research or validated models.
- Research Contributions: Studies with significant results and contributions to the advancement of CAPTCHA technology were prioritized to maintain a high standard in the review.

VII. ISSUES IN CAPTCHA TECHNOLOGY

A. Scalability Challenges

Problem: The increasing complexity of jobs in response to growing user numbers is a significant scaling difficulty for CAPTCHA systems requests. CAPTCHA systems have to handle more queries as the user base grows, which could cause delays and detract from the user experience as a whole [6]. Additionally, creating unique tasks for every user might put a load on server resources, particularly for websites with a lot of traffic.

Solution: Cloud-based solutions that improve processing power and ease load distribution can be used by CAPTCHA systems to address scalability concerns. Furthermore, adaptive challenge generation—where the CAPTCHA difficulty changes in real-time based on user interaction data—can be made possible by employing machine learning techniques, which will improve server performance [5].

B. User Experience Challenges

Problem: Because of their intricacy or difficulty, many CAPTCHA systems can frustrate users, increasing website desertion rates [1]. Specifically, conventional text-based CAPTCHAs might not be user-friendly and provide accessibility issues for those with disabilities [4].

Solution: In order to improve user experience, developers should concentrate on making CAPTCHA designs that are more engaging and intuitive, including image or audio CAPTCHAs, which better suit human cognitive processes [7]. Additionally, implementing adaptable designs that adapt to different devices helps guarantee a flawless user experience [6]

C. Accessibility Challenges
Problem: Some CAPTCHA forms primarily rely on visual or auditory cues, which may disadvantage people with disabilities and give rise to moral questions around accessibility and inclusivity in online settings [3].
Solution: Including alternative CAPTCHA techniques that address a variety of user requirements is essential. For example, offering people with visual impairments options can be achieved by combining visual challenges with audio CAPTCHAs. Furthermore, improving inclusion requires strict adherence to accessibility guidelines such as WCAG (Web Content Accessibility Guidelines).

D. Security Vulnerabilities
Problem: The efficacy of CAPTCHA systems is constantly threatened by automated solvers and sophisticated machine learning techniques that can get beyond traditional obstacles [4].
Solution: It's critical that CAPTCHA design continues to innovate. Resistance against automated attacks can be increased by utilising sophisticated techniques, such as dynamic CAPTCHAs that adapt to user behaviour and algorithms that examine interaction patterns. Investigating adversarial machine learning can potentially yield important information for developing CAPTCHA systems that are safer.

E. Resistance to Adoption
Problem: Because of worries about cost, complexity, or possible disruption to current procedures, some organisations may be reluctant to adopt new CAPTCHA technologies.
Solution: Case studies that highlight the efficiency and return on investment (ROI) of contemporary CAPTCHA systems can help organisations encourage implementation. Additionally, providing technical personnel with training sessions and tools helps allay worries about switching to new systems and promote an innovative culture within businesses.

VIII. LATEST RESEARCH PROGRESS IN CAPTCHA TECHNOLOGY

Current Advancements in Captcha Technology Research Numerous insights and new patterns that impact CAPTCHA technology's effectiveness and uptake for safe online interactions have been uncovered by recent studies:

A. Benefits and Challenges
The significant benefits of modern CAPTCHA systems, including increased security, user engagement, accessibility, and resistance to automated attacks, are highlighted in a 2024 literature analysis. Li and associates [3]. According to research, using sophisticated CAPTCHA designs can guarantee a seamless user experience while drastically reducing the success rates of bot attacks [4]. There are still issues, though, such as the requirement for better accessibility and user experience. According to studies, excessively complicated CAPTCHAs may cause legitimate users to become frustrated and increase the rate of desertion [5].

B. AI and CAPTCHA Integration
Combining artificial intelligence (AI) and CAPTCHA systems is another emerging topic [2]. This tactic uses machine learning algorithms that adapt to user behaviour in order to increase CAPTCHA effectiveness. For example, one study showed that by constantly changing the difficulty levels, adaptive CAPTCHAs which learn from user interactions can significantly improve efficacy against bots. The combination of AI and CAPTCHA systems also makes it easier to spot trends linked to automated attempts to get around security measures [7].

C. User Experience and Accessibility Enhancements
According to research from the evaluated publications, accessibility and user experience are becoming more and more important in contemporary CAPTCHA systems. It has been demonstrated that innovations like audio CAPTCHAs enhance usability for users who are blind or visually impaired.
thus, increasing the range of applications for CAPTCHA technology. Furthermore, a number of studies support interesting and approachable challenge forms, such gamified CAPTCHAs which improve user pleasure while guaranteeing robust security [3].

D. Data Security and Privacy Concerns
As CAPTCHA systems get more complex, worries about user privacy and data security have gained attention. Research shows that even while CAPTCHA systems improve security, protecting user data during

the verification process is crucial [2]. These issues can be lessened by implementing encryption techniques and adhering to data protection laws like the GDPR, which will boost user confidence [4].

E. Ongoing Research and Future Directions

Current CAPTCHA technology research emphasises the need for ongoing innovation to counteract changing security threats [6]. Future research will probably look at how well different CAPTCHA types work in different situations and assess how well they can be adjusted to new bot technologies. Furthermore, state that researchers are working to develop standardised five metrics to thoroughly evaluate the security and efficacy of CAPTCHA systems.

IX. DIFFERENT RESEARCH TRENDS AND OPEN ISSUES IN CAPTCHA TECHNOLOGY

This section outlines the current trends and challenges in CAPTCHA technology from various viewpoints:

A. Technological Perspective

Advancements in CAPTCHA Design: The require for imaginative CAPTCHA plans that upgrade security and client involvement is highlighted by later improvements. For occurrence, CAPTCHA's can alter to client intelligent much obliged to the utilize of machine learning calculations, which increments their adequacy against mechanized bots. Maintained progressions are vital to remain up with the quickly changing field of bot innovation.

Evolutionary Algorithms: One curiously approaches to CAPTCHA plan is the utilize of developmental calculations. Over time, these calculations can modify CAPTCHA challenges, making more troublesome errands for robotized frameworks whereas keeping up their ease of use for human clients. This adaptability fortifies security by making expectations more troublesome for bots.

Adversarial Patches: Utilizing ill-disposed patches in image-based CAPTCHAs is another imaginative strategy. Whereas still being promptly unmistakable to human clients, these patches can veil specific viewpoints of pictures, making it more troublesome for machine learning models to get it them accurately. This methodology abuses robotized systems imperfections to supply a novel challenge that creates in pair with machine learning breakthroughs.

Accessibility Improvements: Guaranteeing that CAPTCHA frameworks are usable by all people, counting those with incapacities, is basic. Inquire about highlights the need for sound and elective text-based CAPTCHAs to cater to a assorted client base. This inclusivity not as it were improving client fulfillment but moreover grows the pertinence of CAPTCHA over diverse stages.

B. User Experience Overview

Balancing Security and Usability: Compelling CAPTCHA frameworks must strike a adjust between exacting security measures and client comfort. CAPTCHA's that are excessively complicated can dishearten authentic clients, driving to higher rates of deserting. Client encounter considers propose that gamified CAPTCHA's, which lock in clients through pleasant intuitive, can improve both security and by and large fulfillment.

C. Regulatory Perspective

Compliance with Data Protection Regulations: As CAPTCHA advances development, it is significant to guarantee compliance with information security controls, such as GDPR. Analysts are exploring ways to actualize CAPTCHA's that regard client security whereas keeping up vigorous security conventions. Setting up a clear system for these controls will help in directing the application of CAPTCHA over different segments.

D. Consumer Perspectives

Trust and Transparency: Building up buyer believe in CAPTCHA frameworks is crucial. Clear communication with respect to how CAPTCHA's work, their part in upgrading security, and their effect on client involvement can essentially impact client acknowledgment. Understanding both the preferences and confinements of CAPTCHA's will empower clients to lock in more readily with these frameworks.

E. Implementation Challenges

Integration with Existing Systems: One of the diligent challenges in CAPTCHA innovation is the integration of these frameworks with current web stages without disturbing client involvement. Investigate proposes that consistent integration techniques are fundamental

to guarantee CAPTCHA's work successfully nearby other security measures.

Last-Mile Deployment Issues: Successfully sending CAPTCHAs over all client touchpoints is basic. Specialized challenges amid execution can ruin execution and client engagement, requiring focused on endeavors from designers to optimize CAPTCHA arrangements for different situations.

X. CONCLUSION

By thwarting automated attacks and confirming user identity, CAPTCHA technology is essential to bolstering internet security. Adversarial tactics and adaptive algorithms are two recent developments that have improved CAPTCHA's resistance to complex bots while preserving its usability for authorised users. This review promotes engaging designs that improve user experience and highlights the importance of striking a balance between security and usability. Consumer trust will be further increased by following data protection regulations and communicating openly about CAPTCHA features. Research is still essential for improving CAPTCHA technology, even in the face of integration issues with current systems. CAPTCHA will be crucial to online security as it develops further.

REFERENCES

[1] R. K. Gupta and T. S. Reddy," Robustness ofCAPTCHA Mechanisms Against Automated Attacks: A Comprehensive Review," International Journal of Computer Applications, vol. 178, no. 7, pp. 1-9, 2023. doi:10.5120/ijca2023912123

[2] L. M. Pereira, K. R. McKinney, and A. R.Thakur," An Examination of Image-Based CAPTCHA: Security vs. Usability," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1115-1124, 2020. doi:10.1109/TIFS.2020.2991425

[3] Y. Z. Li, R. P. Kim, and F. W. Zhang," Advancements in CAPTCHA Technology: Addressing Emerging Security Challenges," Journal of Cybersecurity and Privacy, vol. 3, no. 4, pp. 567-582, 2021. doi:10.3390/jcp3040034

[4] D. A. Johnson and M. F. Davis, "InnovativeApproaches to Enhancing CAPTCHA Effectiveness," International Journal of Advanced Computer Science and Applications, vol. 12, no. 5, pp. 55-64, 2021. doi:10.14569/IJACSA.2021.0120508

[5] S. V. Thakker, J. Parab, and S. Kaisare," Advances in AI-Based CAPTCHA: A Review of Techniques and Security," Emerald Open Research, vol. 7, pp. 1-15, 2023.doi:10.24151/em2023.106

[6] P. M. Kuznetsov, G. A. Tsyrkov, and Y. A.Yermokhin, "A Study of CAPTCHA Adaptation to Machine Learning Attacks," Journal of Information Security and Applications, vol.45, pp. 15-23, 2022. doi: 10.1016/j.jisa.2022.102598

[7] J. H. Moedjahedy, S. I. Adam, and J. Maramis," Improved CAPTCHA Techniques for Web Security," IEEE Access, vol. 8, pp. 49764-49772, 2022. doi:10.1109/ACCESS.2022.3021456

[8] C. S. Dsouza and A. K. Singh," Enhancing User Experience in CAPTCHA Systems Through Gamification," Journal of HumanComputer Interaction, vol. 13, no. 2, pp. 201214, 2020. doi:10.1080/10447318.2020.187054

[9] B. N. Smith and E. O. Watson," Evaluatingthe Impact of Adversarial Machine Learning on CAPTCHA Security," IEEE Computer Society Press, vol. 17, no. 1, pp. 35-45, 2021. doi:10.1109/CS2021.506

[10] N. Patel and S. Agarwal," A ComparativeStudy of Image and Audio-Based CAPTCHA Mechanisms," International Journal of Information Security Science, vol. 11, no. 4, pp.231-239, 2020.doi:10.46511/ijiss.2020.304712