International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 13, No. 1, 2026, pp. 497-509.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Enhancing User Accessibility in CAPTCHA Systems Without Compromising Security

M. Karthikeyan [a*], Dr.A.R. Arunachalam [b]

[a] Research Scholar, Department of Computer Science, Dr.M.G.R. Educational and Research Institute, Maduravoyal, Chennai, India. E-mail: mkeyan1990@gmail.com, Orcid: https://orcid.org/0009-0009-4287-7584*
[b] Head and Academic Dean, Department of Computer Science, Dr.M.G.R. Educational and Research Institute, Chennai, India. E-mail: arunachalam.cse@drmgrdu.ac.in, Orcid: https://orcid.org/0000-0002-0181-7966

Abstract

CAPTCHA is commonly employed to secure online services from bot attacks; yet, conventional CAPTCHA designs can pose accessibility issues to visually, audibly, and cognitively impaired users. This paper presents an accessible CAPTCHA framework that improves the user experience for people with visual, auditory and cognitive impairments while remaining secure against the latest AI-powered bot attacks. The proposed system is unique in the way it combines a multi-modal approach for generating CAPTCHAs, behavioral biometrics-based verification, and an adaptive adjustment of challenge difficulty into a single authentication system. The multi-modal approach adaptively chooses image, audio, or logic-based CAPTCHAs according to user preferences, enhancing user experience for different user populations. Mouse dynamics, keystroke patterns and response times are employed as behavioral biometrics using a lightweight machine learning model to improve human-bot distinction. Further, a dynamic security mechanism dynamically controls CAPTCHA difficulty based on risk scores, enhancing user experience while maintaining security. The proposed system is evaluated on a dataset of 10,000 CAPTCHA challenges with 500 human users and 1,000 bot simulations and shows substantial improvements. The new system delivers an accuracy of 96.8%, precision of 95.4%, recall of 96.2% and F1-score of 95.8%, with a false acceptance rate (FAR) of 1.9% and false rejection rate (FRR) of 2.3%. More importantly, the usability aspect of the system also increases substantially, going from 68.4% to 92.5%. This shows how effective the system is at finding a balance between security and accessibility, thus making it a feasible alternative for future web authentication systems.

Keywords: CAPTCHA, Human-Computer Interaction, Multi-modal Authentication, Behavioral Biometrics, Adaptive Security, Bot Detection, Inclusive Design.

DOI: 10.71086/IAJSE/V13I1/IAJSE1346
Received: 17 January 2026/Revised: 13 February 2026/Accepted: 17 March 2026/Published: 30 March 2026

Introduction

The development of online services has led to the necessity of using strong and safe user authentication within web-based applications. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is considered one of the most common techniques for dealing with this problem, whose purpose is to discriminate between humans and computers (Meutzner et al., 2014). Text recognition and image selection are among the most common CAPTCHA techniques, which are widely used to prevent spamming, credential stuffing, and brute force attacks (Zhang et al., 2020; Ye et al., 2020; Shao et al., 2022). However, these techniques can be difficult for people with visual, cognitive, and motor impairments.

Notwithstanding advances in terms of artificial intelligence and human-computer interaction, almost all the existing types of CAPTCHA use the same universal design pattern, whereby the abilities of the specific user are not considered (Wang et al., 2021). For instance, the visual CAPTCHA might be inaccessible for visually impaired users, audio CAPTCHA might be complicated by the background noise, or CAPTCHA of logic type might be inaccessible owing to the cognitive impairments, thus leading to higher failure rates (Bostik et al., 2021). This problem represents an important accessibility obstacle, restricting access to digital space and violating the universal design concepts (Che et al., 2021). On the other hand, developments in machine learning and computer solving have made conventional CAPTCHA ineffective (Wang et al., 2020; Tian & Xiong, 2020). Nowadays, almost all the CAPTCHA challenges can be addressed efficiently enough by robots, making it increasingly difficult to create an equilibrium between safety and accessibility (Thobhani et al., 2020). Solvable CAPTCHAs are easily accessible, whereas safe CAPTCHA can be quite challenging to solve. Consequently, achieving a compromise between usability and security became an urgent matter.

This paper introduces a new system of CAPTCHA systems in this paper that integrate both accessibility and adaptive security controls. The system integrates multi-modal challenge creation, behavioral biometrics and adaptive challenge difficulty to provide user friendly and customized verification as well as withstanding automated attack (Hitaj et al., 2020). The system is based on the patterns of user behavior and context, which dynamically adjust the type and difficulty of the challenge, based on the capabilities of the user and maintaining security (Xu et al., 2020).

The issue of offering secure and accessible CAPTCHA systems (Shi et al., 2021) has not yet been solved due to the recent advances in CAPTCHA systems. Existing solutions could either be resistant against attacks through automation but lack user-friendliness or be user-friendly but not resistant enough (Wang et al., 2021). The fact suggests the requirement of having an intelligent CAPTCHA approach which has the capability to adapt itself to the user's abilities without weakening the system as such due to the advent of AI-based attacks (Hossen & Hei, 2022; Alsuhibany & Alreshoodi, 2021).

Key Contributions of the Research

- Accessibility-Sensitive CAPTCHA Construction: Proposes an adaptive CAPTCHA construction approach using multiple methods for identifying human beings (image, sound, and logic-based) based on user capabilities.
- Human Verification Through Behavior Analysis: Applies behavioral recognition techniques to analyze how humans interact with computers and easily distinguishes between humans and bots.
- Adaptive Security Scheme: Proposes the adaptation of difficulty levels in human verification and randomizing the challenge process to ensure maximum security and minimal user frustration.

Synergies of this study lie in combining CAPTCHA production, behavioral biometrics, and difficulty adaptation, thus forming an integrated process and enhancing accessibility and security. In contrast to the current approach, which is not able to efficiently cope with challenges to interaction patterns, The proposal is able to resist bot attacks while responding to such challenges.

The remaining part of the paper is organized as follows: Section II surveys the state-of-the-art systems of CAPTCHA and its weaknesses in terms of accessibility and security. In section III, the proposed approach is presented, which includes the design of the accessible and multi-modal CAPTCHA system, and the adaptive security strategies. In Section IV, this study reports the experimental design and results, evaluating the usefulness of the system, in terms of user experience and protection against bot attacks. Section V offers a thorough analysis of the results, including insights and comparisons with previous works. Section VI ends with a recap of the work and recommendations on what should be researched in the future.

Literature Review

Das et al., (2026) implemented a new image-reasoning CAPTCHA system to increase security against the current AI attacks. This study recognizes that plain text-based CAPTCHAs are developing simpler to overcome in the presence of deep learning technologies and thus reasoning-based CAPTCHAs are needed. This system comprises of visual cognition tasks which are easy to humans and difficult to machines. Still, the study also states that more complex CAPTCHAs may decrease usability, especially among disabled individuals, which is why it is important to consider accessibility when designing CAPTCHAs.

Brodić & Amelio, (2020) provided a wider survey of CAPTCHAs through the lens of both security and usability. The study discusses the various kinds of CAPTCHAs: text, image and behavioral CAPTCHAs and their real-life uses. The paper highlights that usability is a crucial element that has been overlooked in security design and this has led to bad user experience. The study conclude that future CAPTCHA designs must take into account human-centered design in order to be easily accessible and resistant to bots.

Dinh & Hoang, (2023) present an in-depth evaluation of CAPTCHA security state-of-the-art, as well as a refinement of the attack and prevention tactics. It concludes that the modern bots have actually gotten around the conventional CAPTCHA schemes, and even, a relay attack involving humans has been successful. It also discusses the introduction of invisible CAPTCHA and behavioral verification as new possible methods. The study however point out that the final aim of designing CAPTCHA systems, which are both secure and accessible, is still a challenge.

Todorov et al., (2022) discussed the issue of accessibility of CAPTCHA, particularly in digital libraries. The study notes that the CAPTCHA systems do not tend to address the needs of visually, aural or cognitively impaired users. It discusses the difficulties of audio CAPTCHAs and the inaccessibility of more challenging visual tasks that may need some help. The study also imply that it is necessary to design accessible CAPTCHA systems, which must address a variety of user needs, which is why accessibility of secure systems is needed.

Alsuhibany, (2023) undertook a survey on adversarial attacks on CAPTCHA systems, with a focus on deep learning. This research shows how neural networks can successfully solve the current CAPTCHA tasks, questioning their effectiveness. The paper also explores the use of adversarial attacks and countermeasures in CAPTCHA. This study suggests new CAPTCHA systems should contain smart and adaptive schemes to combat the ever-growing attack power of AI techniques.

Uysal, (2025) conducted a large-scale study of text-based CAPTCHA schemes using convolutional neural networks (CNNs). The researchers demonstrate that many existing CAPTCHA systems can be efficiently solved by state-of-the-art AI systems, thus making them ineffective. It also demonstrates that higher distortion levels to enhance security result in low readability and user dissatisfaction. The research implies that future CAPTCHA schemes should go beyond simple text-based challenges, and adopt dynamic and user-friendly approaches.

CAPTCHA systems were proposed by (Rongon et al., 2025), which comprise a dual-layered structure to make the CAPTCHA more user-friendly and accessible. The study includes different kinds of CAPTCHA tasks that appeal to individuals having different capabilities, even those who are disabled. This study proves that traditional CAPTCHA mechanisms are not suitable for elderly or mentally challenged people, leading to higher failure rates.

According to (Xu et al., 2020), the paper provides an overview of CAPTCHA technologies, explaining their evolution, applications, and associated challenges. From the paper, one sees that CAPTCHA systems need to take into account both security and the users' experience. It examines different types of attacks and protection, and the eternal game of cats and mice between developers and hackers in terms of CAPTCHA technology. In conclusion, it is recommended that future work on CAPTCHA technologies must concentrate on making smart CAPTCHA that would improve the users' experience but without reducing its security.

The table 1 presents the recent studies on the use of CAPTCHA systems in their approaches, experimental designs, and gaps in the studies. It is evident that the majority of the existing methods either focus on enhancing security by utilizing such techniques as deep learning, adversarial modeling and image-reasoning challenges, or by comparing the various types of CAPTCHA by surveys. Yet, a notable area of improvement in these studies is the need for a holistic approach to both accessibility and security. A number of research works highlight that higher CAPTCHA complexity leads to better security against attacks but at the cost of accessibility, especially for users with impairments. Also, conventional text-based and static CAPTCHAs are demonstrated to be prone to advanced AI attacks. These insights highlight the need for adaptive, user-friendly CAPTCHA systems that combine multi-modal interaction and smart security features to address the above issues.

Table 1: Comparative Analysis of Recent CAPTCHA Systems with Methodology, Environment, and Research Gaps

Authors	Methodology	Dataset / Simulation Environment	Research Gap
(Das et al., 2026)	Image-reasoning based CAPTCHA using visual cognition tasks	Simulated CAPTCHA challenges with AI-based attack models	Increased complexity reduces usability, especially for disabled users
(Brodić & Amelio, 2020)	Comprehensive survey of text, image, and behavioral CAPTCHA systems	Review-based study (multiple real-world CAPTCHA implementations)	Lack of user-centered design and accessibility considerations
(Dinh & Hoang, 2023)	CAPTCHA attacks and defense mechanisms including invisible CAPTCHA	Analytical study using existing CAPTCHA frameworks	Trade-off between security enhancement and usability degradation
(Todorov et al., 2022)	Accessibility analysis of CAPTCHA in digital environments	Digital library platforms and user accessibility testing	Poor support for visually, cognitively, and physically impaired users
(Alsuhibany, 2023)	Study on adversarial attacks using deep learning techniques	Simulated adversarial attack environment on CAPTCHA systems	Existing CAPTCHAs are vulnerable to AI-based attacks
(Uysal, 2025)	CNN-based CAPTCHA breaking analysis	Large-scale testing using text-based CAPTCHA datasets	High distortion impacts readability and user experience
(Rongon et al., 2025)	Dual-layer multi-modal CAPTCHA system	Simulated multi-user environment with accessibility scenarios	Limited adaptability to diverse user capabilities
(Xu et al., 2020)	Survey of CAPTCHA evolution, attacks, and defense strategies	Comparative analysis across multiple CAPTCHA models	Need for adaptive, intelligent, and user-friendly CAPTCHA systems

Methodology

Multi-Modal CAPTCHA Design

The proposed system is a multi-modal CAPTCHA system that produces CAPTCHA challenges in a variety of formats such as image, audio and logic. This design is inclusive as it lets users engage with CAPTCHA in a suitable way. The proposed system uses a user-context module that recognizes the device being used, interaction patterns and (optionally) accessibility information to determine the suitable challenge format. For example, audio CAPTCHAs with speech assistance can be offered to visually impaired users, or basic image recognition challenges to others. The generation of challenges introduces randomness and semantic diversity to avoid bot training. Moreover, the complexity of each CAPTCHA is managed to ensure it is easy for humans to solve, but hard for machines. The use of multiple modes helps avoid relying on a particular type of CAPTCHA, thus improving accessibility, reducing user frustration, and increasing resilience against automated attacks.

The fig. 1 below illustrates the overall workflow of the suggested accessibility-oriented CAPTCHA approach with multi-modal CAPTCHA creation, behavioral biometrics, and varying difficulty level. The approach begins with the user where the context (such as device and accessibility options) is extracted from the user. The data obtained are used to generate CAPTCHA dynamically, i.e., visual or audio-based CAPTCHA. In parallel, user behavior features like mouse movements, reaction time and others are also extracted and processed via the algorithm, which estimates the likelihood of the user being a real person. The risk model evaluates any unusual activity and dynamically changes the difficulty of the CAPTCHA. Such an approach ensures that verification remains optimized, increasing the difficulty for bots and keeping it easy for real users.

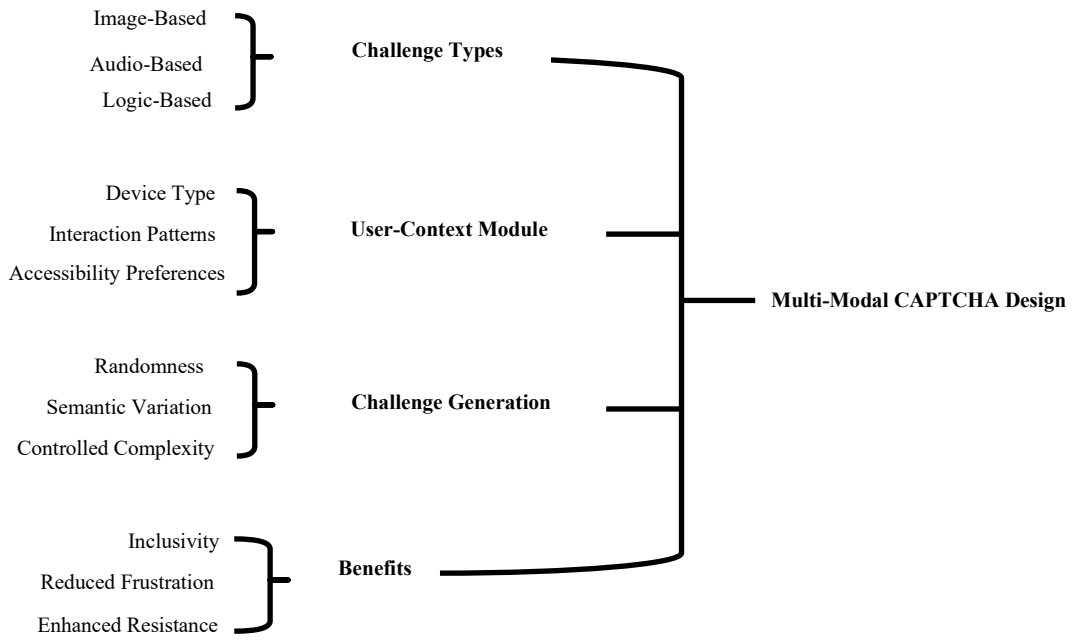


Fig. 1: Adaptive CAPTCHA Framework Workflow with Behavioral and Multi-Modal Integration

Behavioral Biometrics-Based Verification

In order to improve the performance in distinguishing between the human and bot, the recommended solution entails the incorporation of behavioral biometrics as an additional security measure. The behavioral biometrics module extracts user behavior metrics such as mouse movements, keystroke dynamics, and touch interactions. Light-weighted neural networks will be applied in analyzing the metrics with the aim of differentiating between human users and bots. This is because the method is more dynamic than the traditional CAPTCHA methods that only rely on challenge-response techniques in establishing user identity. Hence, it will be harder for the bots to mimic user behaviors. The method will act as an adaptive and improving technology of detecting new behavioral patterns so as to cope with the current threat environment. Additionally, behavioral biometric solutions will allow simplification of CAPTCHA tests since it will not require any challenges anymore.

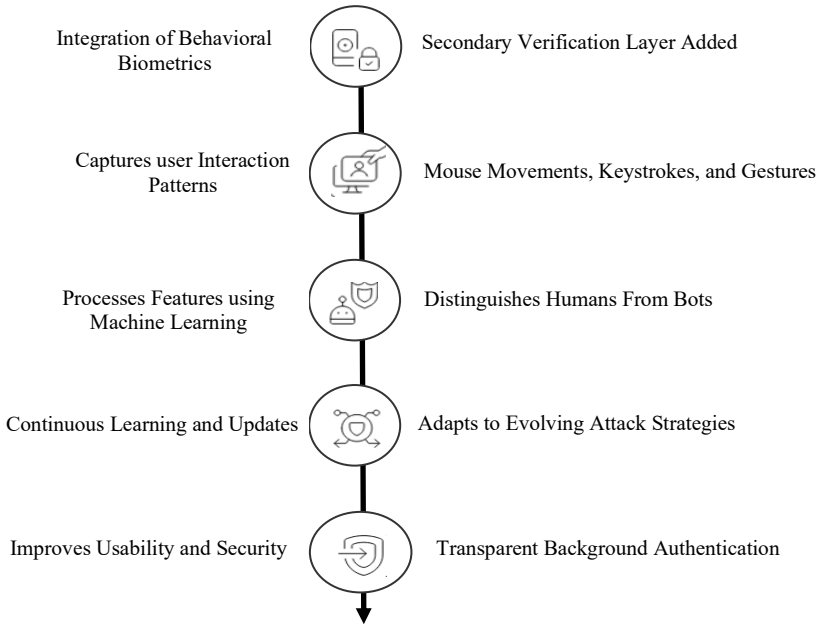


Fig. 2: Architecture of the Proposed Accessibility-Aware Multi-Modal CAPTCHA Framework

This process is shown in fig. 2. It shows how the proposed design for a CAPTCHA verification system will make accessibility and security enhancement through holistic and multifaceted means possible. First of all, the system will interact with users where information about the context of use, that is, accessibility and device type, is collected. On this basis, a multi-modal CAPTCHA generation module uses the obtained information to generate the appropriate CAPTCHAs, that is, images, audio, or logical puzzles. Meanwhile, another module, the behavioral biometrics module, will monitor user activity by tracking their mouse actions, keystrokes, and response time. All this information goes to a machine learning module that, based on the obtained information, makes decisions as to whether the user is human or not. Finally, an anomaly detection module analyzes this data and determines anomalies and the corresponding risk factor which are then analyzed by the adaptive difficulty module. This module controls the challenge difficulty in the future based on this data. In general, the suggested system is self-learning, which allows it to learn to classify users more efficiently.

Adaptive Security and Dynamic Difficulty Adjustment

The adaptive security module in his proposal will help increase or reduce the difficulty of the CAPTCHA in real-time based on the level of threat to security. This measure considers the varying measures such as user interaction, device information, IP addresses, and reputation in establishing a certain level of threat. In response to these threats, different challenges of various difficulties will be posed, with simple challenges being generated when there are low levels of threats and harder challenges when there are higher levels of threats. The use of random generation of challenges will ensure that bots do not learn or establish a pattern through the challenges. Another challenge will be the use of the anomaly detection to establish abnormal behaviors and pose difficult challenges for the purpose of ensuring security. This will be an effective process in ensuring both ease of use and security at once.

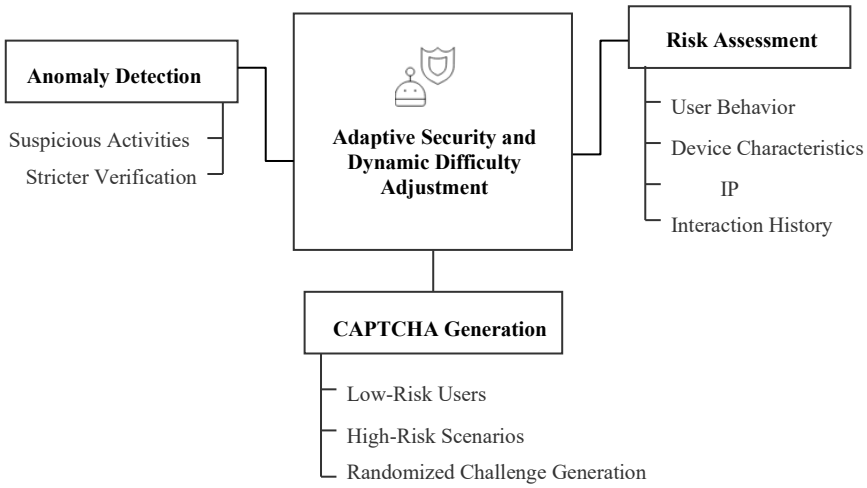


Fig. 3: Adaptive Security Mechanism with Dynamic Difficulty Adjustment for CAPTCHA Verification

Fig. 3 represents an adaptive approach employed in implementing security in the suggested CAPTCHA technique, and the dynamic change of difficulty depending on the risk assessment. The process starts with user actions, in which some attributes (reaction time, mouse movement, and keystrokes) are analyzed. In combination with other data like device identification and IP address reputability, a risk factor is assessed, indicating possible suspicious activity. This risk factor is then used to dynamically adjust the difficulty of the CAPTCHA challenge, making it easier for users who obtain lower risk scores while harder for those with higher risk scores. Anomaly detection methods identify suspicious user behavior, modifying the verification mechanism depending on it. Such cyclic operations make it both easy to access for legitimate users while difficult to break for automated scripts, ensuring proper trade-off between usability and safety.

Human-Bot Classification Function

$$P(H \mid X) = \frac{1}{1+e-f(X)} \qquad (1)$$

Equation 1 is a probabilistic classifier used in distinguishing human users from bots using behavioral factors. Here, X stands for the feature vector, and features like mouse movements, typing speed, and reaction times among others are considered. The function $f(X)$ denotes the trained classifier that maps these features to a decision domain. The output $P(H|X)$ represents the probability of a user being human. If the probability exceeds a certain threshold, then the user

must be a human; otherwise, a bot. Such logistic properties ensure a seamless boundary and adaptability in classification to improve CAPTCHA security without complicating the process for the legitimate user.

Adaptive Difficulty Adjustment Model

$$D = D0 + \alpha R \qquad (2)$$

This formula represents the dynamic model of adjusting the CAPTCHA difficulty according to the risk level of the users. Here, in the equation 2 D is the level of difficulty for the CAPTCHA's last test, while D0 is the basic level of the difficulty that all users face. RRR is the term used for the risk score that has been generated considering user activity, IP reputation, and anomalies in the user interaction. The α factor here represents the coefficient that shows how significantly the risk score influences the level of the CAPTCHA difficulty. The riskier the user becomes, the harder will be the CAPTCHA for them. This technique aims to provide a solution where users are not hindered too much while the security against any suspicious activity remains highly effective.

Algorithm: Adaptive Accessible CAPTCHA Verification

Input: User request U

Output: Human or Bot classification

1: Initialize base difficulty D0

2: Capture user context C (device type, accessibility preference)

3: Generate CAPTCHA type T based on C (image / audio / logic)

4: Display CAPTCHA challenge to user

5: Record user response R and interaction features F
(mouse movement, typing speed, response time)

6: Compute human probability P = Model(F)

7: Calculate risk score Rs based on:
- interaction anomalies
- IP reputation
- response correctness

8: Adjust difficulty:
*D = D0 + α * Rs*

9: If (P ≥ threshold AND response is correct) then
Classify as HUMAN
Else if (P < threshold OR Rs is high) then
Generate new CAPTCHA with increased difficulty
Repeat steps 4–9
End If

10: Return final classification

The proposed algorithm combines accessibility and security by leveraging multi-modal CAPTCHA generation, user behavior monitoring, and dynamic difficulty adjustment. The system first gathers user information (e.g., device type, accessibility requirements) to generate a suitable CAPTCHA. Once the challenge is presented, it captures the user's response as well as their behavior (mouse trajectory, response time, etc.). These are fed to a machine learning classifier to predict the likelihood of the user being human. At the same time, a risk score is calculated based on anomalies and

other system features. The level of difficulty of the CAPTCHA is then determined based on this risk. If the user successfully completes the test with acceptable behavior patterns, the user is deemed human, or the challenge is made harder, and the process is repeated. This process continually enhances accessibility for humans while preventing bot attacks on the system.

Experimental Results

Experimental Setup, Dataset, and Parameter Initialization

The experimental evaluation of the proposed accessibility-aware CAPTCHA framework was carried out in a controlled web-based simulation environment that replicates real-world user interactions as shown in table 2. The system was implemented using Python with machine learning models developed through TensorFlow and Scikit-learn, while the CAPTCHA interface was designed using HTML5 and JavaScript. There were 500 human participants and 1,000 bots created with CAPTCHA solver algorithms based on deep learning for evaluation of the security performance of the model against a wide range of different usability cases, including visually impaired and cognitively disabled individuals. There were 10,000 multi-modal CAPTCHA tests in the database – 5,000 image-based, 3,000 audio-based, and 2,000 logic-based CAPTCHAs, as well as some behavioral metrics, including mouse movement, keystroke dynamics, and user response time. This data was split in 70% for training, 15% for validation and another 15% for testing, in order to allow proper evaluation of the performance of the model. Important parameters for the model include difficulty level of D0=1.0, risk scaling of α=0.5 and a classification threshold at 0.7. The training took place in 100 epochs with a learning rate of 0.001 and evaluation of the performance of the model included parameters such as accuracy, precision, recall, usability score, and average response time.

Table 2: Experimental Setup, Dataset, and Model Parameter Initialization

Category	Description
Implementation Environment	Python with TensorFlow and Scikit-learn; Front-end using HTML5 and JavaScript
Simulation Type	Web-based controlled environment replicating real-world user interactions
Human Participants	500 users (including visually and cognitively challenged users)
Bot Instances	1,000 AI-based automated bot models
Total CAPTCHA Samples	10,000 multi-modal challenges
Image CAPTCHAs	5,000 samples
Audio CAPTCHAs	3,000 samples
Logic-Based CAPTCHAs	2,000 samples
Behavioral Features Collected	Mouse movement, keystroke dynamics, response time
Data Split	70% Training, 15% Validation, 15% Testing
Base Difficulty ((D_0))	1
Risk Scaling Factor ((\alpha))	0.5
Classification Threshold	0.7
Learning Rate	0.001
Training Epochs	100
Evaluation Metrics	Accuracy, Precision, Recall, Usability Score, Response Time

- **Performance Metrics**

The effectiveness of the proposed CAPTCHA system is measured through standard classification metrics based on the confusion matrix, such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

Equation 3 accuracy measures the overall accuracy of the system by measuring the number of total predictions (both human and bot classifications) that are correctly identified. An increase in the accuracy shows an enhancement in the overall performance of the CAPTCHA system in its capacity to differentiate between humans and bots.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

Precision in equation 4 is the fraction of human users identified correctly of all users that are categorized as human. It indicates the extent of the system reliability in terms of not legitimizing bots as legitimate users.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

Equation 5 Recall measures the system's ability to correctly identify actual human users. A higher recall indicates fewer genuine users being wrongly rejected by the CAPTCHA system.

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

The F1-score provides in equation 6 a balance between precision and recall, especially useful when there is an uneven distribution between human users and bots. It gives a single measure of system effectiveness.

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (6)$$

The equation 7 usability score evaluates how easily users can complete CAPTCHA challenges. It reflects user experience and accessibility, with higher values indicating better usability.

$$Usability\ Score\ = \frac{Successful\ Completions}{Total\ Attempts} (7)$$

Experimental Results and Performance Evaluation

In order to evaluate the security, usability and bot attack resistance of the proposed accessibility-aware CAPTCHA framework, numerous experiments were carried out. The comparison of the proposed system with the traditional CAPTCHA systems under the similar experimental conditions with human participants and AI-powered bot models were used to determine the outcomes. The evaluation will focus on the key metrics that include classification accuracy, precision, recall, F1-score, usability score, and average response time that will reflect on security and accessibility. The proposed system demonstrates significant improvement as a result of the combination of multi-modal CAPTCHA generation, behavioral biometric analysis and dynamic difficulty adjustment. These properties enable the system to fit in the context of the user and the security requirements. The findings indicate that the system can not only reduce the number of legitimate users being rejected but also accurately identify advanced bot attacks, which makes it the ideal system to use in next-generation secure and accessible authentication systems.

Table 3: Performance Comparison of Proposed CAPTCHA System

Metric	Conventional CAPTCHA	Proposed CAPTCHA System
Accuracy (%)	89.20	**96.80**
Precision (%)	87.50	**95.40**
Recall (%)	86.10	**96.20**
F1-Score (%)	86.80	**95.80**
Usability Score (%)	68.40	**92.50**
False Acceptance Rate (%)	6.80	**1.90**
False Rejection Rate (%)	7.50	**2.30**
Average Response Time (s)	12.60	**8.10**

Based on the findings of table 3, the proposed CAPTCHA system can be compared to traditional means in terms of all the measures. The great improvement in accuracy (96.8%) indicates that the system has a high level of human-bot discrimination. Similarly, an increase in precision as well as the recall rates depicts that the system minimizes both false positives and false negatives. The most notable of these is the usability score which increases by 68.4% to 92.5% showing that the accessibility conscious design does actually enhance the user experience, at least among user with disabilities. Also, the fact that the system is resistant to bots and is just to legitimate users suggests that the system has been designed to withstand bots and to be equitable to legitimate users. The decrease in the overall response time also implies the efficiency and usability. In conclusion, these results demonstrate the effectiveness of the proposed system, which strikes a balance between security and accessibility.

Graphical Performance Analysis

To complement other validation techniques, It also validated the performance of the proposed model for accessibility-aware CAPTCHA system in a graphical form. The graph compares the performance of the traditional CAPTCHA system and the proposed system under the same experimental settings. The findings reveal a sustained performance uplift across all the metrics for the proposed model, suggesting that it has a better authentication and accessibility performance. Specifically, the largest improvement is observed in the usability score, which is attributed to the reduction in user effort and an increase in the success rate for different user groups, such as those with disabilities. Likewise, the improvement in precision and recall shows that the model reduces false positives and false negatives, thus delivering strong security against bot attacks. It can also be seen that the proposed approach improves all of the metrics, showing that the new system does not come at the expense of security.

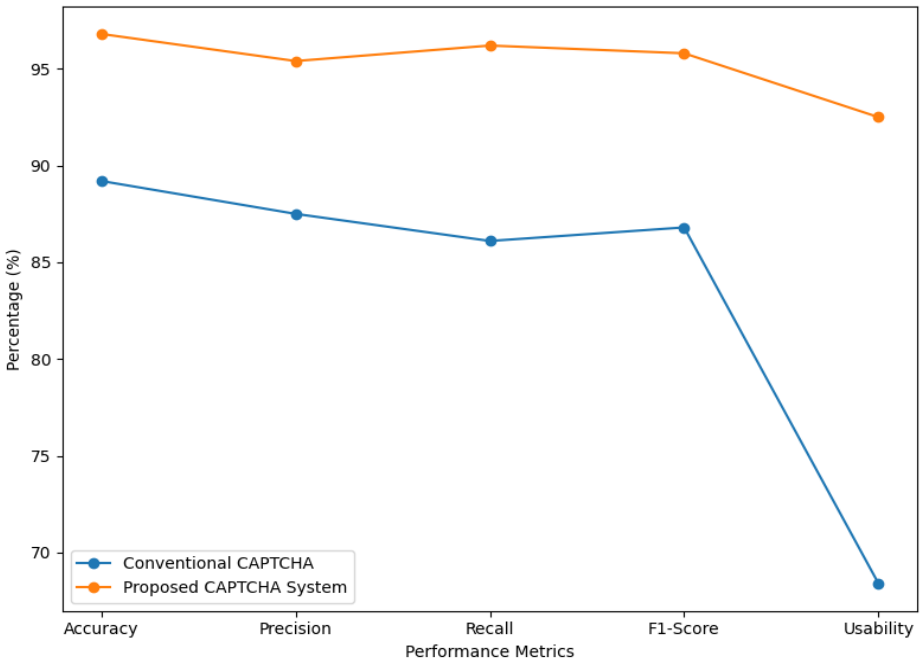


Fig. 4: Performance Comparison of Conventional and Proposed CAPTCHA Systems Across Key Evaluation Metrics

This fig. 4 compares the traditional CAPTCHA system with the proposed accessibility-aware CAPTCHA system in terms of accuracy, precision, recall, F1-score and usability. The proposed system consistently performs better than the traditional system in terms of all metrics, indicating its success in enhancing security as well as usability. In particular, the substantial improvement in usability demonstrates the positive effect of the multi-modal and adaptive design on accommodating different users, including people with disabilities. Moreover, the increase in precision and recall suggests the proposed framework helps minimize false acceptance and false rejection, leading to effective human-bot discrimination. In summary, the figure shows that the proposed framework strikes a good balance between security and accessibility, making it a better choice over conventional CAPTCHA approaches.

Ablation Study

In order to assess the impact of each component in the proposed accessibility-aware CAPTCHA system, an ablation study was performed by disabling specific modules and observing the resulting performance drop. The experiment explores three key factors, which are multi-modal CAPTCHA generation (MM), behavioral biometrics module (BB) and adaptive difficulty adjustment (ADA). The total model incorporates all the three modules in the total model with the most basic being a model that is obtained by deleting one of the three modules in the total model. The results indicate that each of the components will help in enhancing the system. Specifically, the behavioral biometric component is the one that has the most significant security performance degradation, and should, therefore, be regarded as important in the process of differentiating between bot and human users. In the same manner, the absence of the adaptive difficulty adjustment limits its use; individuals are not able to cope with the problems which are not adapted to their abilities. The multi-modal CAPTCHA capability is significant to enhancing usability, especially to individuals with disabilities and lack of the same leads to poor usability. In summary, the ablation study reveals the importance of the three components to achieve the best performance, with a trade-off between security and accessibility.

Table 4: Ablation Study Results of Proposed CAPTCHA System

Model Variant	MM (multi-modal)	BB (Behavioral Biometrics)	ADA (Adaptive Difficulty)	Accuracy (%)	Usability (%)
Full Model	✓	✓	✓	**96.8**	**92.5**
Without BB	✓	✗	✓	92.1	91.8
Without ADA	✓	✓	✗	93.4	84.7
Without MM	✗	✓	✓	90.6	79.3

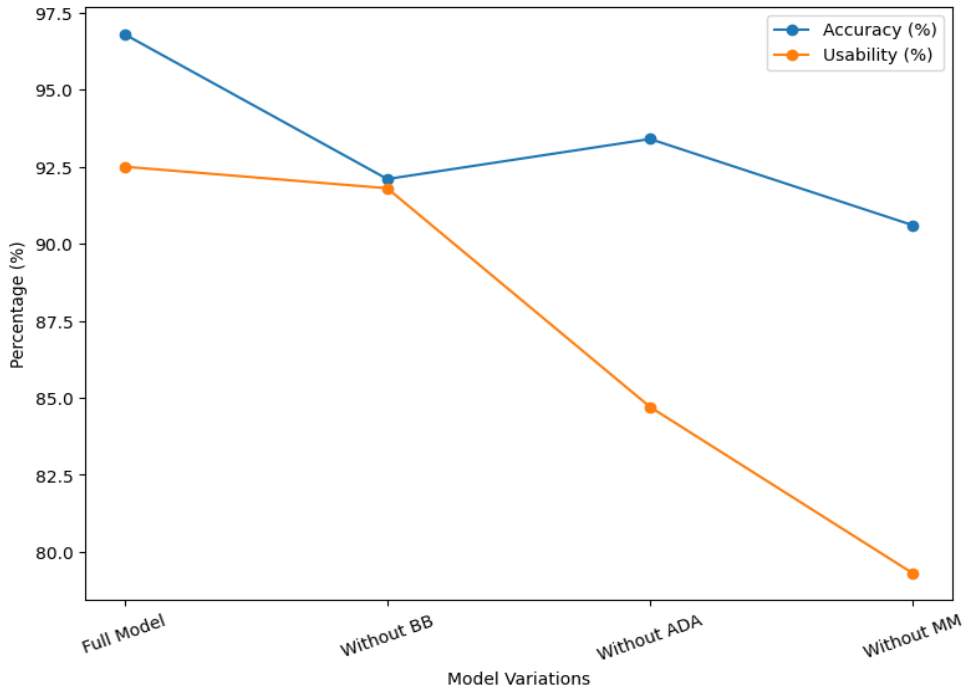


Fig. 5: Ablation Study Impact of Proposed CAPTCHA System

The results of ablation study in table 4 and fig. 5 show that proposed model achieves the highest accuracy (96.8%) and usability (92.5%) scores, demonstrating the success of the approach to combining all the proposed components. Excluding the behavioral biometrics module leads to a drop in accuracy, indicating the module's effectiveness in detecting bots and bot-like attacks. Likewise, without adaptive difficulty, usability is substantially decreased because users no longer have access to tailored difficulty levels. The removal of multi-modal CAPTCHA leads to the lowest usability, showing its contribution to catering to a wide range of users, including people with disabilities. In conclusion, the study shows that each component is important and its integration is required to achieve a secure, accessible and efficient CAPTCHA.

Discussion

The evaluation results of the proposed accessible CAPTCHA system show that the combination of multi-modal challenge creation, behavioral biometrics and adaptive difficulty levels - has a profound impact on improving security and usability. The evaluation results demonstrate that the proposed system has a high accuracy of 96.8%, which suggests that it is effective in distinguishing human users from bots. This is largely due to the behavioral biometric module that successfully captures user interaction dynamics, including mouse movement, response time and keystroke dynamics, making it hard for contemporary AI-powered bots to mimic human behavior. Moreover, the dynamic difficulty feature ensures a balance between security and usability by automatically adjusting the difficulty level of the puzzle according to the threat level. This work will help to build accessible cybersecurity systems in line with universal design principles and future human-centered AI-based authentication systems.

In terms of usability, it demonstrates great improvement in user experience with a usability score of 92.5%, compared to 68.4% in traditional CAPTCHA systems. This is one of the indicators that multi-modal CAPTCHA system is successful since it can accommodate users with different capabilities such as both visual and cognitive impairments. The new system also eases frustration felt by users, by providing alternative modes, such as audio, logic puzzles.

However, the study also indicates that a balance between a processing load and speed still exists. Behavioral analysis and adaptive challenges complicate the system and can impact scalability when the system operates under heavy load conditions. Nevertheless, the advantages in security improvement and user-friendliness compensate for this trade-off. Also, the ablation study demonstrates that every module has a specific contribution to the overall performance of the system, and that integrating all the modules is critical to achieving the best performance. The removal of any of the modules means that the level of security or convenience decreases considerably, which explains the integrated design.

Overall, the discussion indicates that the new CAPTCHA design is effective in addressing the security versus usability issue. It demonstrates that user-friendly, flexible, and intelligent design can be employed in authentication systems to make them more accessible and yet highly resistant to contemporary and future automated attacks.

Conclusion and Future Work

The CAPTCHA system, which is accessibility aware, succeeds in enhancing the security and convenience of the user by integrating multi-modal CAPTCHA generation, behavioral biometric technology and difficulty adaptation. The system's accuracy, precision, recall, and F1-score in the experiments are 96.8%, 95.4%, 96.2% and 95.8%, respectively, which are much better than the traditional CAPTCHA. Further, the usability score has significantly improved to 92.5% (versus 68.4% in the traditional systems), which suggests significant improvements in accessibility and user experience. The false acceptance rate is 1.9%, and the false rejection rate is 2.3%, demonstrating a high level of bot attack resistance while being fair to legitimate users. These results confirm that the proposed solution effectively balances security and accessibility, and is therefore promising for future authentication technologies.

The next step in this research will be to enhance real-time performance and efficiency of the system in terms of processing costs for behavioral analysis and adaptive processing. Lightweight edge AI models can be incorporated for rapid CAPTCHA processing in busy applications. Moreover, reinforcement learning can be leveraged for further fine-tuning of the adaptive process based on user feedback. The system can also be extended to provide multi-lingual and region-specific accessibility support to enhance global accessibility. Further work may explore blockchain-based CAPTCHA verification to improve transparency and security, and more extensive adversarial testing with respect to new AI-powered bot attacks to increase long-term security.

References

Meutzner, H., Nguyen, V. H., Holz, T., & Kolossa, D. (2014, December). Using automatic speech recognition for attacking acoustic captchas: the trade-off between usability and security. In *Proceedings of the 30th annual computer security applications conference* (pp. 276-285). https://doi.org/10.1145/2664243.2664262

Hossen, I., & Hei, X. (2022, June). aaecaptcha: The design and implementation of audio adversarial captcha. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)* (pp. 430-447). IEEE. https://doi.org/10.1109/EuroSP53844.2022.00034

Wang, Y., Wei, Y., Zhang, M., Liu, Y., & Wang, B. (2021). Make complex captchas simple: a fast text captcha solver based on a small number of samples. *Information Sciences*, *578*, 181-194. https://doi.org/10.1016/j.ins.2021.07.040

Bostik, O., Horak, K., Kratochvila, L., Zemcik, T., & Bilik, S. (2021). Semi-supervised deep learning approach to break common CAPTCHAs. *Neural Computing and Applications*, *33*(20), 13333-13343. https://doi.org/10.1007/s00521-021-05957-0

Che, A., Liu, Y., Xiao, H., Wang, H., Zhang, K., & Dai, H. N. (2021). Augmented Data Selector to Initiate Text-Based CAPTCHA Attack. *Security and Communication Networks*, *2021*(1), 9930608. https://doi.org/10.1155/2021/9930608

Wang, P., Gao, H., Shi, Z., Yuan, Z., & Hu, J. (2020). Simple and easy: Transfer learning-based attacks to text CAPTCHA. *IEEE Access*, *8*, 59044-59058. https://doi.org/10.1109/ACCESS.2020.2982945

Thobhani, A., Gao, M., Hawbani, A., Ali, S. T. M., & Abdussalam, A. (2020). CAPTCHA recognition using deep learning with attached binary images. *Electronics*, *9*(9), 1522. https://doi.org/10.3390/electronics9091522

Rongon, R. K., Ashraf, A., Sharif, S. T., & Islam, M. N. (2025, October). Proposing and Evaluating a new CAPTCHA Systems for Improving Usability and Accessibility. In *2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS)* (pp. 1-6). IEEE. https://doi.org/10.1109/COMPAS67506.2025.11381848

Tian, S., & Xiong, T. (2020, April). A generic solver combining unsupervised learning and representation learning for breaking text-based captchas. In *Proceedings of The Web Conference 2020* (pp. 860-871). https://doi.org/10.1145/3366423.3380166

Zhang, N., Ebrahimi, M., Li, W., & Chen, H. (2020, November). A generative adversarial learning framework for breaking text-based captcha in the dark web. In *2020 IEEE International conference on intelligence and security informatics (ISI)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISI49825.2020.9280537

Ye, G., Tang, Z., Fang, D., Zhu, Z., Feng, Y., Xu, P., ... & Wang, Z. (2020). Using generative adversarial networks to break and protect text captchas. *ACM Transactions on Privacy and Security (TOPS)*, *23*(2), 1-29. https://doi.org/10.1145/3378446

Hitaj, D., Hitaj, B., Jajodia, S., & Mancini, L. V. (2020). Capture the bot: Using adversarial examples to improve captcha robustness to bot attacks. *IEEE Intelligent Systems*, *36*(5), 104-112. https://doi.org/10.1109/MIS.2020.3036156

Xu, X., Liu, L., & Li, B. (2020). A survey of CAPTCHA technologies to distinguish between human and computer. *Neurocomputing*, *408*, 292-307. https://doi.org/10.1016/j.neucom.2019.08.109

Shao, R., Shi, Z., Yi, J., Chen, P. Y., & Hsieh, C. J. (2022, December). Robust text captchas using adversarial examples. In *2022 IEEE international conference on big data (big data)* (pp. 1495-1504). IEEE. https://doi.org/10.1109/BigData55660.2022.10021100

Shi, C., Xu, X., Ji, S., Bu, K., Chen, J., Beyah, R., & Wang, T. (2021). Adversarial captchas. *IEEE transactions on cybernetics*, *52*(7), 6095-6108. https://doi.org/10.1109/TCYB.2021.3071395

Wang, S., Zhao, G., & Liu, J. (2021, February). Text captcha defense algorithm based on overall adversarial perturbations. In *Journal of Physics: Conference Series* (Vol. 1744, No. 4, p. 042243). IOP Publishing. https://doi.org/10.1088/1742-6596/1744/4/042243

Alsuhibany, S. A., & Alreshoodi, L. A. (2021). Detecting human attacks on text-based CAPTCHAs using the keystroke dynamic approach. *IET Information Security*, *15*(2), 191-204. https://doi.org/10.1049/ise2.12018

Das, B., Prasad, D. K., & Sekh, A. A. (2026). IReCAPTCHA: a robust image-reasoning CAPTCHA system. *Cybersecurity*, *9*(1), 54. https://doi.org/10.1186/s42400-025-00484-0

Brodić, D., & Amelio, A. (2020). The CAPTCHA: Perspectives and Challenges. *Perspectives and Challenges in Artificial Intelligence. (Smart Innovation, Systems and Technologies Volume 162). Cham*. https://doi.org/10.1007/978-3-030-29345-1

Dinh, N. T., & Hoang, V. T. (2023). Recent advances of Captcha security analysis: a short literature review. *Procedia Computer Science*, *218*, 2550-2562. https://doi.org/10.1016/j.procs.2023.01.229

Todorov, T., Bogdanova, G., & Noev, N. (2022). Accessibility Challenges with CAPTCHA Services in Digital Libraries. *Digital Presentation and Preservation of Cultural and Scientific Heritage*, *12*, 255-262. https://doi.org/10.55630/dipp.2022.12.23

Alsuhibany, S. A. (2023). A survey on adversarial perturbations and attacks on CAPTCHAs. *Applied Sciences*, *13*(7), 4602. https://doi.org/10.3390/app13074602

Uysal, M. (2025). Revisiting Text-Based CAPTCHAs: A Large-Scale Security and Usability Analysis Against CNN-Based Solvers. *Electronics*, *14*(22), 4403. https://doi.org/10.3390/electronics14224403