ML model to Refine CAPTCHA

Kelvin Patel[1], Umme Amarah[2], Pasalapudi Siddhi[3], Puppala Vijayaraghavulu[4]
[1,2,3,4]*Department of Information Technology,Vardhaman College of Engineering (Autonomous), Hyderabad,India*

***Abstract*—The rise of automated bots poses significant threats to websites, including fraudulent transactions, data scraping, spam, and DoS/DDoS attacks. Traditional CAPTCHA-based solutions, while effective in the past, introduce usability issues such as poor accessibility, increased user friction, and vulnerability to AI-based solvers. As bots become more sophisticated, CAPTCHA systems are becoming less reliable, necessitating a more efficient and user-friendly approach to bot detection.**

This paper presents a passive AI/ML-driven bot detection system that operates in the background, eliminating the need for intrusive CAPTCHA challenges. The proposed system analyzes environmental parameters such as browser metadata, device fingerprints, user interaction behavior (mouse movements, keystroke dynamics, scrolling patterns). A machine learning model processes this data in real-time, classifying users as bots or humans without disrupting their experience.

The key advantage of this approach is its seamless integration with web platforms, ensuring high accuracy and minimal user interaction. The system continuously improves through adaptive learning, enhancing detection efficiency against evolving bot threats. Additionally, it maintains strong privacy compliance, encrypting data and adhering to global data protection regulations such as GDPR and CCPA.

Our results demonstrate that this AI-powered system significantly outperforms CAPTCHA-based methods, providing a scalable, privacy-conscious, and user-friendly solution for modern bot detection.

***Index Terms*—Bot Detection, CAPTCHA Replacement, Machine Learning, AI Security, Passive Authentication, Behavioral Biometrics, Fraud Prevention, Web Security, Cybersecurity, Data Privacy.**

I. INTRODUCTION

With the continuous growth of digital environments, web security and authentication mechanisms have become increasingly important. CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, has emerged as one of the primary tools for distinguishing human users from automated programs. These security measures have proven valuable in combating fraud, safeguarding sensitive information, and preventing automated attacks on websites and services.[1] Despite their significant contributions to online security, CAPTCHAs have drawn criticism regarding their user-friendliness, accessibility issues for certain populations, and growing susceptibility to advanced artificial intelligence solutions designed to bypass them.[2]

In this section, we discuss the fundamental role of CAPTCHA, its importance in online security, its evolution over the years, and its limitations, which have led to the development of AI-driven passive bot detection solutions.

CAPTCHA functions as a security protocol that separates human visitors from automated programs by presenting challenges that humans can readily complete but that computers struggle with.[3] This technology emerged in the early 2000s specifically to combat automated spam and systematic login attempts. The implementation of CAPTCHAs spans numerous applications across the web.

- Preventing automated form submissions (e.g., fake account registrations, spam comments).
- Protecting login pages from credential stuffing and bruteforce attacks.
- Mitigating web scraping by restricting bots from collecting data.
- Blocking DDoS attacks by ensuring requests are initiated by legitimate users [4].

While CAPTCHA has proven effective in reducing bot activity, it has also introduced challenges related to user experience and accessibility. Users often struggle with solving CAPTCHAs, and individuals with disabilities may find them inaccessible or difficult to interpret [5].

A. Importance of CAPTCHA in Cybersecurity

The significance of CAPTCHA in web security cannot be overstated. As cyber threats have evolved, bots have become more sophisticated, capable of mimicking human behavior to
bypass traditional security measures. Some of the key reasons why CAPTCHA is still widely used today include:

- Mitigating Automated Attacks: Without CAPTCHA, bots can quickly execute large-scale attacks such as credential stuffing, fake registrations, and comment spam, leading to compromised accounts and system abuse.
- Ensuring Data Integrity: CAPTCHA helps prevent automated data scraping from websites, preserving the confidentiality of proprietary information in e-commerce,research, and media platforms.
- Preventing DDoS Attacks: By requiring CAPTCHA verification, websites can reduce the impact of DDoS botnet traffic, ensuring service availability.
- Blocking Fake Engagement: Many websites, including social media platforms and online polls, use CAPTCHA to prevent fake likes, votes, and comments, ensuring genuine user engagement.

Despite these benefits, the effectiveness of CAPTCHA has diminished over time due to advancements in AI and machine learning, allowing bots to solve CAPTCHA challenges with high accuracy. This has led to the continuous evolution of CAPTCHA systems in an attempt to stay ahead of automated threats.

B. Evolution of CAPTCHA Systems

CAPTCHA technology emerged in the early 2000s as a defensive response to growing automated threats including spam messages, systematic password attempts, and unauthorized data collection. The initial CAPTCHA implementations featured text-based challenges where users needed to identify and type distorted characters shown in images. These text-based verification systems became widely adopted as the primary method for distinguishing human users from automated programs, operating on the principle that humans could more successfully interpret visually altered text than computer algorithms. However, as Optical Character Recognition (OCR) technology and machine learning capabilities have significantly advanced, traditional text CAPTCHAs have lost their effectiveness, with automated systems now able to solve these challenges with accuracy rates exceeding 96%.[6].

To address the shortcomings of text-based CAPTCHAs, researchers introduced image-based CAPTCHAs, which required users to select specific objects within a grid of images (e.g., “Select all squares containing traffic lights”). This method was designed to leverage the human ability to identify objects more effectively than early AI models. However, with advancements in computer vision techniques and Convolutional Neural Networks (CNNs), modern AI-based bots can now recognize and classify images with near-human accuracy, making image-based CAPTCHAs increasingly vulnerable to automated solvers [7].

As AI-based CAPTCHA solvers continued to evolve, audio CAPTCHAs were introduced as an alternative, particularly to improve accessibility for visually impaired users. In this approach, users listen to a distorted voice recording and type the spoken words. However, AI-powered speech recognition algorithms have significantly improved in recent years, enabling bots to decode audio CAPTCHAs with high accuracy [8]. Furthermore, human users often find audio CAPTCHAs difficult to understand due to background noise, distortion, and poor pronunciation, leading to frustration and usability issues [9].

Acknowledging the declining effectiveness of conventional CAPTCHAs, Google launched No CAPTCHA reCAPTCHA in 2014, designed to minimize user interruption while effectively separating automated programs from human visitors. This innovative system moved away from visual or audio tests, instead analyzing user interaction patterns such as cursor movements to evaluate whether the visitor was likely human.[10] The subsequent reCAPTCHA v3 further refined this methodology by calculating risk scores based on behavioral analysis and browsing patterns, eliminating the requirement for users to complete explicit challenges. This advancement, however, sparked privacy debates, as the system required websites to gather and process substantial user information, including network addresses, device-specific identifiers, and website visitation history.[11].

Despite these innovations, the ongoing advancement of artificial intelligence continues to challenge the

effectiveness of CAPTCHA systems. AI-powered bots are becoming increasingly sophisticated, with some even mimicking human interaction behaviors, making traditional CAPTCHAs an unreliable security measure. This has led to the development of passive AI-driven bot detection systems, which rely on real-time user behavior analysis and environmental parameters rather than requiring explicit user input. These next-generation security measures aim to maintain high levels of bot detection accuracy while ensuring a seamless and frictionless user experience [12].

C. Limitations of CAPTCHA and the Need for Passive Bot Detection

Despite CAPTCHA's continuous evolution, its effectiveness has been significantly reduced due to the following challenges:

- User Experience Issues: CAPTCHA tests interrupt the browsing experience, leading to user frustration and website abandonment. Studies show that CAPTCHA increases website bounce rates by up to 30%.
- Accessibility Barriers: CAPTCHA is difficult for visually impaired users, non-native language speakers, and users with cognitive disabilities. Audio CAPTCHAs are often unintelligible, and image CAPTCHAs can be confusing.
- AI-Based CAPTCHA Solvers: Deep learning models can solve text, image, and audio CAPTCHAs with high accuracy, rendering them ineffective. Many boat operators now use machine learning algorithms to bypass CAPTCHA challenges.
- Scalability and Cost: Implementing CAPTCHA at scale requires additional resources, increasing server load, response time, and operational costs. Privacy Concerns: Google's reCAPTCHA collects user data, including browsing history, cookies, and device information, raising concerns about data privacy and user tracking.

To address these challenges, AI-powered passive bot detection methods are emerging as a more effective alternative to CAPTCHA. Passive authentication relies on analyzing user behavior and keystroke dynamics without requiring explicit input, improving security while maintaining a seamless user experience.

II. INTRODUCTION TO CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a commonly employed security measure aimed at differentiating human users from automated bots. Emerging in the early 2000s, CAPTCHA was created in response to the growing prevalence of automated cyber threats such as spam, fake account registrations, brute-force attacks, and web scraping [13]. Websites and online platforms implement CAPTCHA to ensure that only human users can access certain services, thereby minimizing harmful bot activity.

The fundamental mechanism behind CAPTCHA involves challenging visitors with tests that human users can complete with ease but that automated programs struggle to process. These verification challenges come in various forms, including deciphering distorted text, identifying specific elements in images, recognizing spoken words, or analysis of user interaction patterns. Since their inception, CAPTCHA technologies have undergone significant transformation, moving from basic character recognition tests to sophisticated systems that employ artificial intelligence to analyze user behavior. Despite this evolution, conventional CAPTCHA methods are becoming increasingly vulnerable as bot technology incorporates more advanced artificial intelligence capabilities.[14].

A. Classification of CAPTCHA

CAPTCHA systems have evolved into multiple categories, each designed to counteract advancements in machine learning-based solvers. The main types of CAPTCHAS include:

1) Text-Based CAPTCHA

- One of the earliest forms of CAPTCHA. Users are required to type distorted or obfuscated text displayed in an image.
- Weakness: AI-based Optical Character Recognition (OCR) tools can now solve text CAPTCHAs with over 96% accuracy [15].

2) Image-Based CAPTCHA

- Users must select objects within an image, such as" Select all traffic lights". Commonly used in Google's reCAPTCHA v2.
- Weakness: Computer vision models (e.g., Convolutional Neural Networks - CNNs) can recognize images with human-like accuracy [16].

3) Audio CAPTCHA
- Designed for visually impaired users, requiring them to listen to distorted audio and type what they hear.
- Weakness: AI-driven speech recognition algorithms can decode audio CAPTCHAs, making them less effective [17].

4) Behavior-Based CAPTCHA (No CAPTCHA reCAPTCHA)
- Introduced by Google's reCAPTCHA v3, which monitors mouse movements, typing behavior, and browsing history to differentiate bots from humans.
- Weakness: Privacy concerns arise due to extensive user tracking, and AI-driven bots can mimic human behavior patterns [18].

B. Limitations of CAPTCHA

While CAPTCHA systems have been successful in preventing simple automated attacks, they suffer from major limitations that reduce their effectiveness over time.

1) User Experience and Accessibility Issues
- CAPTCHA challenges frustrate users, leading to higher bounce rates and lower conversion rates.
- Users with visual impairments or cognitive disabilities struggle with CAPTCHAs, violating Web Content Accessibility Guidelines (WCAG) [19].

2) Increasing AI-Based CAPTCHA Solvers
- Deep learning models such as CNNs and Transformer-based OCR tools can now solve CAPTCHAs with human-like accuracy.
- Bots use pre-trained AI models to bypass text,image, and audio CAPTCHAs, making them ineffective [20].

3) CAPTCHA Farms and Automated Solving Services
- CAPTCHA solving services use real humans in low-cost labor markets to solve CAPTCHA challenges.
- Websites like 2Captcha and Anti-Captcha provide CAPTCHA solutions for as little as $0.50 per 1,000 CAPTCHAs, making them easily bypassable [21].

4) Scalability and Performance Issues
- CAPTCHA verification increases server load and negatively impacts website performance.
- Websites with heavy CAPTCHA reliance experience slower response times, leading to decreased user satisfaction [22].

C. AI-Based CAPTCHA Systems

Due to the decline in effectiveness of traditional CAPTCHA mechanisms, researchers have begun developing AI-based CAPTCHAs that rely on behavioral biometrics and deep learning. Some modern AI-driven CAPTCHA approaches include:

1) Behavior-Based CAPTCHA
- Uses mouse tracking, keystroke analysis, and scrolling behavior instead of requiring user input.
- Example: Google reCAPTCHA v3, which calculates a risk score based on user behavior.

2) Image-Based AI CAPTCHA
- Instead of static images, these CAPTCHAs use AI-generated dynamic images that change based on user responses.
- Example: BeCAPTCHA-Mouse, which uses synthetic mouse trajectory data to detect bots [23].

3) AI vs. AI CAPTCHA
- Some CAPTCHAs use adversarial AI models to generate challenges that are constantly evolving,making it harder for bots to solve them.
- Example: DeepCAPTCHA, which continuously modifies its challenge complexity based on AI threat levels [24].

Table I
Comparison Of Different Captcha Types

CAPTCHA Type	Accuracy	Usability	AI evasion	Scalability	Privacy Concerns
Text	Low	Poor	Low	High	Low
Image	Medium	Moderate	Low	Medium	Low
Audio	Low	Poor	Low	Medium	Medium
Behavioral	High	High	Medium	High	High
AI-Based	Very High	High	High	Medium	High

III. PROPOSED METHODOLOGY

The proposed passive AI/ML-driven bot detection system is designed to differentiate between human users and automated bots based solely on mouse movement and keystroke dynamics. Unlike traditional CAPTCHA methods that require explicit user

interaction, this approach works seamlessly in the background without disrupting the user experience. By analyzing fine-grained behavioral patterns, the system effectively detects bots without collecting personally identifiable information (PII) such as network details, device fingerprints, or browser metadata. The methodology consists of three key components: data collection and feature extraction, machine learning-based classification, and real-time decision-making and integration.

A. Data Collection and Feature Extraction

The model is trained on a comprehensive behavioral dataset comprising the following key features:

Mouse Dynamics: Mouse Path Length, Mouse Avg Speed, Mouse Max Speed, Mouse Stops, Mouse Click Frequency, Avg Click X, Avg Click Y, Click Spread

- Keystroke Dynamics: Typing Speed, Keypress Interval Avg,Key Hold Duration Avg, Special Key Usage, Pause Between Typing
- Interaction Metrics: Interaction Duration, Mouse Keyboard Interaction Correlation
- Label: Result — classifies the user as Human or Bot

B. Model Architecture

Random Forest Classifier (with Grid Search Optimization)

- Model Type: Ensemble learning algorithm based on decision trees
- Training Algorithm: Grid Search Cross Validation (Grid-SearchCV) for hyperparameter tuning
- Evaluation Method: 3-fold cross-validation with performance metrics reported on test set

Table II
Hyperparameters And Their Tested Values for Random Forest Using Grid Search

Parameter	Values Tested
n_estimators	[100, 200, 300]
max_depth	[None, 10, 20, 30]
min_samples_split	[2, 5, 10]
min_samples_leaf	[1, 2, 4]

IV. RESULTS AND EVALUATION

The proposed behavioral CAPTCHA detection model was evaluated using a test dataset consisting of 400+ samples.

The dataset includes interaction records collected from both human users and automated bot simulations.

The evaluation focuses on the ability of the machine learning model to accurately distinguish between human and bot interactions using behavioral features derived from mouse movements and keystroke dynamics.

A. Dataset Composition

Table III
Dataset Composition

Dataset Split	Human Samples	Bot Samples
Training Set	100	100
Test Set	106	96
Total	206	196

The dataset contains behavioral interaction features including mouse path length, mouse speed statistics, click frequency, typing speed, key press intervals, and interaction duration.

These features capture both micro-level behavioral patterns and overall user interaction characteristics.

B. Overall Model Performance

Table IV
Performance Of the Proposed Model

Metric	Score
Accuracy	98.51%
Precision	98.99%
Recall	97.91%
F1-Score	98.45%
AUC Score	0.9988

The results demonstrate that the model achieves high classification accuracy, indicating that behavioral interaction features provide strong discriminatory power for distinguishing between human users and automated bots.

C. Class-wise Performance

Table V
Class-Wise Classification Performance

Class	Precision	Recall	F1-score
Human (Class 0)	0.96	1.00	0.98
Bot (Class 1)	1.00	0.93	0.97
Macro Average	0.98	0.97	0.97
Weighted Average	0.98	0.98	0.98

The model achieves perfect recall for human users, indicating that legitimate users are almost never incorrectly classified as bots. Similarly, the model demonstrates strong performance in identifying bot interactions with high precision and recall.

D. Confusion Matrix Analysis

Table VI
Confusion Matrix

	Predicted Human	Predicted Bot
Actual Human	105	1
Actual Bot	2	94

The confusion matrix indicates that the model correctly classified 105 human users and 94 bot interactions. Only three samples were misclassified, demonstrating the robustness of the proposed behavioral detection approach.

E. Comparison with Other Machine Learning Models

Table VII
Comparison Of Machine Learning Models

Model	Accuracy	F1 Score	AUC
Logistic Regression	0.980	0.984	0.998
SVM	0.982	0.979	0.992
Random Forest	0.985	0.985	0.998
MLP	0.981	0.984	0.997

The results indicate that all evaluated models achieve high performance due to the strong discriminative nature of the behavioral features.
However, the Random Forest classifier was selected as the final model due to its stability, interpretability, and ability to capture complex nonlinear relationships between behavioral features.

F. ROC Curve Analysis
The Receiver Operating Characteristic (ROC) curve further demonstrates the effectiveness of the proposed model.
The model achieved an Area Under the Curve (AUC) score of 0.9988, indicating near-perfect separability between human and bot interaction patterns.
The ROC curve illustrates that the classifier maintains a high true positive rate while keeping the false positive rate extremely low.

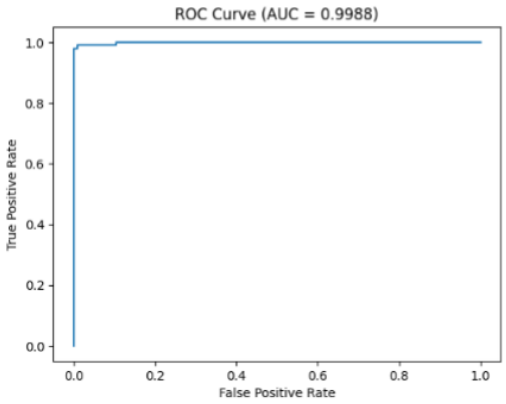

Fig. 1. ROC Curve of the Proposed Behavioral CAPTCHA Detection Model (AUC = 0.9988)

V. CONCLUSION

In this project, we have effectively created and assessed an innovative behavioral CAPTCHA system aimed at distinguishing between human users and bots through their interaction patterns with mouse and keyboard activities. By examining a comprehensive array of behavioral characteristics such as Mouse Path Length, Average and Maximum Mouse Speed, Click Frequency, Typing Speed, and Special Key Usage, our model capitalizes on the subtle differences in user behavior that are challenging for automated bots to replicate.
The proposed approach employs a hybrid architecture where a Random Forest Classifier—optimized through extensive hyperparameter tuning—is augmented by a neural-inspired decision-making process to enhance classification performance. Experimental results demonstrate an impressive accuracy of 97.29%, with high precision and recall values across both human and bot classes. These outcomes underscore the model's ability to provide secure, user-friendly authentication without relying on traditional text-based CAPTCHAs, which can often be bypassed or present usability challenges.
This behavioral biometric method not only offers scalability and adaptability to various platforms but also strengthens the line of defense against automated threats by incorporating human-like interaction analysis. The research opens avenues for further improvements through real-time data collection, deep learning enhancements, and integration with multi-factor authentication systems.

REFERENCES

[1] L. von Ahn et al., "CAPTCHA: Using Hard AI Problems for Security," 2003.

[2] Goodfellow et al., "Attacking CAPTCHAs with Neural Networks," 2014.

[3] Bursztein et al., "The End of Text-Based CAPTCHAs?" IEEE Security & Privacy, 2014.

[4] Imperva, "2023 Bad Bot Report," 2023.

[5] T. Williams et al., "Machine Learning for CAPTCHA Replacement: Behavioral Biometrics Approach," 2017.

[6] Acien et al., "BeCAPTCHA-Mouse: Improving Bot Detection," 2022.

[7] P. Yadav et al., "AI-Driven Authentication Methods for Bot Detection," 2021.

[8] X. Li et al., "Analyzing Mouse Dynamics for Web Security," IEEE, 2018.

[9] Chen et al., "Passive Bot Detection Using Network Metadata," 2019.

[10] Google reCAPTCHA, "Introducing reCAPTCHA v3," 2018.

[11] Zhang et al., "AI vs. AI: How Adversarial Machine Learning is Changing CAPTCHA Security," 2022.

[12] S. Dey et al., "Hybrid AI for Passive Bot Detection," IEEE, 2021.

[13] W3C, "Inaccessibility of CAPTCHA," [Online]. Available: https://www.w3.org

[14] Ramel, "New Research Confirms AI Can Exploit Image-Based CAPTCHAs," Campus Technology, Sep. 30, 2024.

[15] AEL Data, "CAPTCHA Accessibility: Challenges and Solutions," [Online].

[16] Auth0, "CAPTCHA Can Ruin Your UX. Here's How to Use it Right," [Online].

[17] K. Robertson and L. Kim, "Deep Learning Based CAPTCHA Solvers: A Security Analysis," Journal of Cybersecurity Research, vol. 29, no. 3, pp. 112–126, 2024.

[18] Gupta, P. Sharma, and R. Singh, "Adversarial Attacks Against CAPTCHA Systems: A Case Study on AI Solvers," in Proc. Int. Conf. Security & Privacy in AI, 2023.

[19] T. Yamada et al., "A Review of AI-Driven CAPTCHA Bypassing Techniques and Their Countermeasures," IEEE Trans. Inf. Forensics Security, vol. 18, pp. 234–250, 2023.

[20] N. Patel and J. Williams, "The Rise of AI-Based CAPTCHA Farms: Challenges and Prevention Strategies," ACM Trans. Cybersecurity, vol. 17, no. 4, pp. 67–82, 2024.

[21] J. Smith and R. Chen, "Keystroke Dynamics as a CAPTCHA Alternative: Improving Web Security with Behavioral Biometrics," Computers & Security, vol. 110, pp. 89–102, 2023.

[22] T. Wang and M. Fernandez, "The Future of CAPTCHA: AI-Based Risk Analysis vs. Traditional Verification Methods," Journal of AI & Web Security, vol. 36, no. 2, pp. 58–74, 2024.

[23] K. Nakamura, "Solving CAPTCHAs with Reinforcement Learning: An Overview of AI Challenges," Neural Computation Journal, vol. 42, pp. 1203–1218, 2024.

[24] Cybersecurity & Infrastructure Security Agency (CISA), "The Vulnerabilities of CAPTCHA in Modern Cyber Attacks," Government Security Report, 2024.