TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Behind Every CAPTCHA — How Your Imperfection Trained the Perfect Bot

Every day, millions of people click on fire hydrants and buses to show they're human, but what if that was never meant to prevent bots and actually be a concealed method of training bots?

By **Khadija Ejaz** | University of Agriculture Faisalabad | Published: May, 2026
chija.mikan31@gmail.com | Position: e.g., Student Researcher

Introduction

The time I have tried to prove that I'm a human. I do not remember the number of times that I have pressed the squares on a CAPTCHA trying to show that I am human; I have to press the buttons to find the traffic light and I click my way through and feel mildly annoyed about it as I click the boxes.

What you did not know, for the past two decades, your clicks have not only accessed a website, but they have also been used to help build one of the most advanced AIs of all time. You are the data and you are the labor force, and you received zero dollars to do so.

In this article, I will discuss the evolution of CAPTCHA from a security tool to an AI judge and how our own weaknesses, which often embarrass us, have become the last line of defence against the machines we have been developing.

> ***" In a world of perfect algorithms, your human messiness is the only thing a machine can't easily replicate."***

Technology Overview

CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart, was developed in the early 2000's for a simple purpose of preventing access to technology by using an easy security measure of difficult-to-read text. With that invention accomplished, the in 2004 a computer scientist named Luis von Ahn, developed the reCAPTCHA v1 where users would decipher distorted words that were scanned pages from old books and historical documents. These pages were what computers could not digitize on their own and so each time users deciphered them, they contributed to preserving some part of our past. Users were unaware of that.

In 2009 Google acquired the reCAPTCHA project and exploded its impact. The reCAPTCHA v2 project, created by Google, now includes image puzzles from Google Maps that have the users identify images of streets, street intersections and street signs. Every time a user clicks on an image of a bus or pedestrian crossing, he/she is helping to build the image recognition software for Google's self-driving cars! Millions of people are providing billions of clicks that are building the computer vision models for

today's autonomous vehicles and AI image recognition. What's poetic is that as users completed puzzles to prove they were human, with every correct answer they also made these machines smarter, more intelligent and human-like in their abilities to understand our visual world.

Figure 1: ***reCAPTCHA V2***

Credit: https://2captcha.com/ // https://2captcha.com/api-docs/recaptcha-v2

Key Findings & Impact

The Puzzle is Gone - The Judge is Here:

Today's artificial intelligence has surpassed traditional image captchas by an unbelievable margin. Modern AIs can now solve image captchas quicker and more accurately than any human. The teacher has been outdone by the student. Because of this, the tests that were once performed openly are now done in secret.

The security measures of today have switched from the use of puzzles to use only a behavioral analysis system for collecting signals. For every second that passes since you land on the page, information is captured from your browser and used to track your actions. Various Signals Collected to Perform Behavioral Analysis:

1) Movements with the mouse: How natural does your mouse move compared to how you historically used it.

2) Typing rhythm: How similar is the timing of your keystrokes compared to how a machine types.

3) Scrolling behavior: Do you scroll down a page like a human or like a machine. A human would pause, go back up, and go back down.

4) Time spent on page: Did you read or did you hurriedly execute.

When this information is sent to the server, an algorithm will generate a trust score based on your behavioral data and assign you a trust score of between 0.0 and 1.0. The closer you are to 1.0, the more likely you are a human. If you're closer to 0.0, they will think you're a robot. You will never see your score, only the website owner will see it. In the blink of an eye, decisions will be made whether to allow you access, challenge you, or block you.

This change is extremely significant to Pakistan's quickly growing e-commerce, fintech, and digital services square. There are ongoing bot attacks against all of these types of platforms from Daraz, JazzCash, and various SaaS start-ups, so fake account creation, credential stuffing, and automated fraud are all considered bot attacks and are something that all online operations are continually combating. The invisible security for users looking to use a legitimate service from these platforms greatly reduces the amount of time or friction required for legitimate users in Pakistan when using their services, thus increasing conversion rates as well as building trust with their customer base.

The Power of Being Imperfect:

And this is where the fun begins.

Bots are too perfect. They travel in straight lines without deviation. They click at the same amount of time each time they work—always the same amount of time between clicks. It's the very precision of the bot's execution that makes it easy to see how the bot is executing tasks incorrectly.

Humans, on the other hand, have beautiful inconsistencies in how they get things done. One hand may shake a little while holding a mouse, or a mouse may go slightly off track when trying to click on a link, etc. Typists speed up and slow down while typing; there are pockets of time that are completely unpredictable. Scientists refer to this biological noise as "noise." Ultimately this noise represents a valuable piece of information for modern day digital security.

Your cursor moving around and around while you type is an excellent example of this noise. Your key strokes are extremely inconsistent because they cannot be copied. Your "distraction" is an example of another piece of noise. These signals from your activity on the Internet help to create your own digital fingerprint. They are your digital fingerprint—distinct, undeniable, and impossible to replicate—and if they are the only things that can prove that you exist, then imperfection has become the measure of life in a world where an algorithm is perfect.

What's Next?

Engineers working on the next generation of security systems are looking to eliminate the use of puzzles as much as possible. The vision is for a totally seamless internet that will use your device history, behavioural patterns, and biological noise to authenticate you before you click anything.

While there will continue to be an evolving CAPCHA, In this future, the CAPCHA will also become the Internet; hence, at some point along the way, the question must be asked: If proving your humanity is done by constantly monitoring your behaviour (monitoring your movements, timing, and habits each session), then at what point does security no longer exist; rather, it is being surveilled?

For Pakistan, where data privacy laws are still being developed, this issue should be given serious public and policy attention.

The ideal bot exists today; it can see streets, recognize signs, solve puzzles, and move about through a computer's interface very fluently. All of us built this bot; every time we have clicked on a fire hydrant, we have been building this bot.

All that exists between the humans who created this bot and this bot is the chaotic and beautiful messiness of being a human.

Your mistakes are what give you your identity. Your inconsistencies prove that you are you. In a world of perfectly functioning machines, it is our imperfectness that makes us unique and irreplaceable

About the Author

I am Khadija Ejaz currently pursuing the degree of Bachelor of Information Technology at University of Agriculture Faisalabad. I can be reached at chija.mikan31@gmail.com

Keywords: *CAPTCHA; Artificial Intelligence; Cybersecurity; Behavioral Analysis; reCAPTCHA; Pakistan Tech.*

References

[1] Von Ahn, L., Maurer, B., McMillen, C., Abraham, D. and Blum, M. (2008) 'reCAPTCHA: Human-Based Character Recognition via Web Security Measures', Science, 321(5895), pp. 1465–1468. DOI: 10.1126/science.1160379.

[2] Bursztein, E., Martin, M. and Mitchell, J. (2011) 'Text-based CAPTCHA Strengths and Weaknesses', Proceedings of the ACM Conference on Computer and Communications Security, pp. 125–138. DOI: 10.1145/2046707.2046724.

[3] Google Security Blog (2018) 'Introducing reCAPTCHA v3: The New Way to Stop Bots'. Available at: https://security.googleblog.com/2018/10/introducing-recaptcha-v3-new-way-to.html (Accessed: July 2025). (Google Online Security Blog)

[4] Motoyama, M., Levchenko, K., Kanich, C., McCoy, D., Voelker, G.M. and Savage, S. (2010) 'Re: CAPTCHAs — Understanding CAPTCHA-Solving Services in an Economic Context', USENIX Security Symposium, pp. 435–452.

[5] Shet, V. (2014) 'Are you a robot? Introducing "No CAPTCHA reCAPTCHA"', Google Developers Blog. Available at: https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html (Accessed: July 2025). (Google Online Security Blog)

[6] 'The truth about those annoying CAPTCHA tests', Scienceline. Available at: https://scienceline.org/2024/02/the-truth-about-those-annoying-captcha-tests/ (scienceline.org)