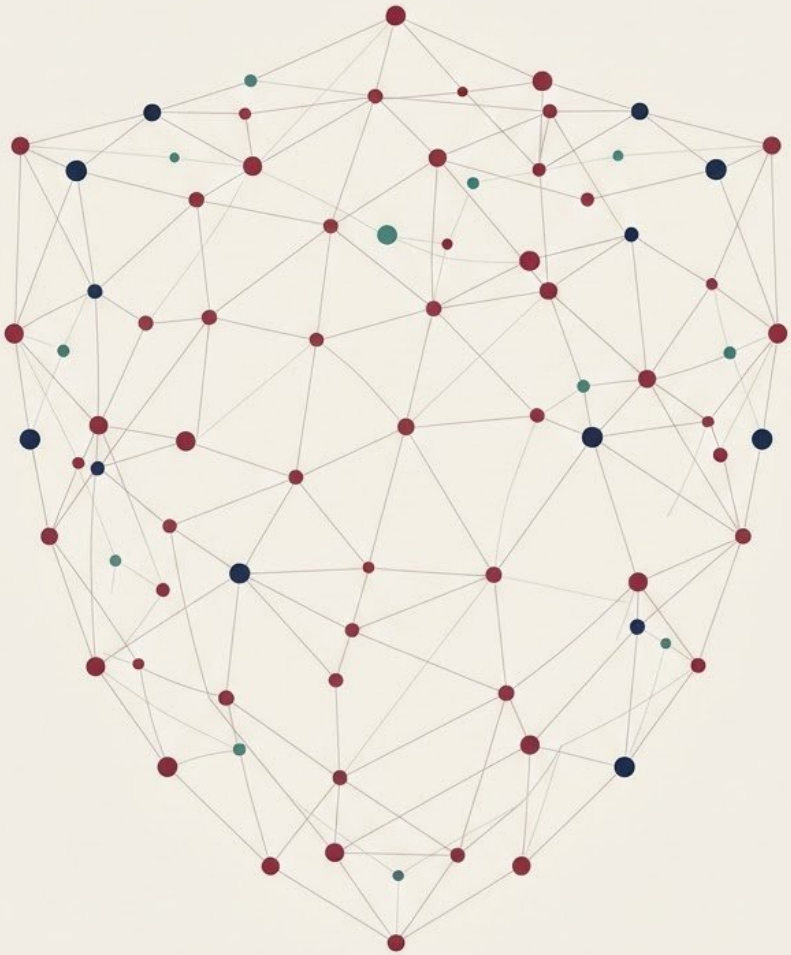
INVISIBLE PROOF

Bot Mitigation for Markets That Cannot Solve CAPTCHAs



COURAGE GARIKAI

ColdCode Si Labs · Harare

Invisible Proof

Bot Mitigation for Markets That Cannot Solve CAPTCHAs

Courage Garikai

ColdCode Si Labs · Harare

© 2026 Courage Garikai. Licensed under CC BY 4.0.

ColdCode Si Labs, Harare, Zimbabwe

First edition, November 2026

DCAI — Distributed Cognitive Autonomous Infrastructure series

Dedication

For Rumbidzai, who called on a Saturday morning to say the form was broken.

For the 260 traders in Chitungwiza who could not register for chicken-farming training because of a puzzle designed in Mountain View.

For the developers in Harare, Nairobi, Lagos, Accra, Lusaka, and Kampala building software for the users that Silicon Valley forgot.

Remove the puzzle. Ship the proof.

Foreword

The CAPTCHA is one of the most widely recognised pieces of internet infrastructure in the world. Every internet user has encountered one: the distorted letters, the grid of blurry images, the checkbox that watches your mouse movements to decide if you are human. And every internet user outside of a narrow Western, high-bandwidth, able-bodied demographic has been failed by one.

Courage Garikai has written something rare: a security book that is also a development economics book, a human factors book, and an implementation manual. He argues, persuasively and with data from real production systems in Zimbabwe, that CAPTCHAs do not work for the markets where internet growth is fastest — and that the alternative is not some exotic AI-powered system, but a simple, decades-old cryptographic primitive (proof of work) combined with basic server-side signals that anyone can implement.

This is an important book for two reasons. First, it offers a concrete, tested, low-cost alternative to a broken status quo, complete with code, weights, and deployment checklists. Second, it insists — correctly — that software built for emerging markets must be tested on emerging-market devices, by emerging-market developers, for emerging-market users. The $22 phone test is not an appendix; it is the core argument.

If you build forms, operate a website, or make procurement decisions about security software, read this book. Then remove your CAPTCHA.

— Tawanda Chikore, Harare, November 2026

About this book

This is a book about bot mitigation written from Harare. The central claim is simple: the CAPTCHA — the distorted text, the traffic-light puzzle, the “I am not a robot” checkbox — is broken. It does not stop bots. It stops people. It stops them because they cannot see the puzzle, because they do not have the device to render it, because they do not have the bandwidth to load it, because they do not know what a fire hydrant is, because they cannot move a mouse precisely, or because they cannot afford the data to download 300 KB of Google surveillance scripts before filling out a form.

The book is built around three propositions:

1. Bot mitigation is an economic problem, not an artificial-intelligence problem. The goal is to make abuse more expensive than it is worth to the attacker. You do not need to tell humans and bots apart; you need to make automated abuse cost more than the revenue it generates.
2. The correct bot mitigation for low-resource markets — and for ordinary users everywhere — is invisible proof: a small computational challenge that runs in the background, server-side signals that detect automation without demanding anything from the user, and friction only when signals are ambiguous. No puzzles. No third-party tracking. No image grids.

3. Bot mitigation that depends on users solving cultural puzzles on fast devices with large screens and high bandwidth is not merely inconvenient. It is colonial infrastructure — designed in one context, exported globally, and its costs are borne entirely by the people it was never designed for.

The book is technical but not inaccessible. The implementation chapters (Part III) contain enough detail to build a working bot mitigation system from scratch. The design chapters (Part IV) are for anyone who operates a website, chooses a vendor, or makes decisions about what kind of internet they want to participate in building.

Who this book is for

- **The developer building a form** who has always added CAPTCHA because that is what the tutorials say, and who never thought to question whether it works in the markets where their users live.
- **The product manager** choosing a bot mitigation vendor who needs to understand the real costs — measured in abandonment, accessibility, privacy, and user trust — of each option.
- **The founder operating a business in Africa, South Asia, or Latin America** who has seen high form-abandonment rates and suspects the CAPTCHA is the cause, but does not know what to replace it with.
- **The accessibility advocate** who knows CAPTCHA is discriminatory but needs technical arguments and a viable alternative to point to.
- **The security engineer** who cares about privacy as well as defence, and who is uncomfortable with the degree of

user surveillance that modern “invisible” CAPTCHA vendors demand.

This is not a textbook on machine learning, nor a comprehensive guide to web application security, nor a marketing document for a product. It is an argument, a set of technical patterns, and an implementation guide for a different way to solve the bot problem.

How to read it

Part I makes the argument. If you do nothing else, read Chapters 1–5. They will change how you see every CAPTCHA-protected form you encounter online.

Part II quantifies the threat. If you are not convinced that bot mitigation needs fixing, the numbers here are drawn from production logs and industry reports.

Part III is the architecture. Six chapters describe the invisible proof stack — proof of work, velocity, reputation, behavioural signals, fingerprinting, friction — with concrete implementations, parameters, and code sketches.

Part IV is the production section, including the Proofhand case study (our implementation running at scale across seven products), measurement methodology, and calibration guidance.

Part V covers privacy, the CAPTCHA-solving labour market, AI-native bots, and the case for open proof as infrastructure.

A Tools Index at the back contains the PoW reference implementation in JavaScript and Python, the trust-score schema, and deployment checklists.

What this book is not

This is not a machine learning book. The techniques described require no ML models, no AI, no neural networks, and no training data. They use SHA-256, timing heuristics, IP reputation lists, and simple arithmetic. ML-based bot detection exists; it is expensive to operate, difficult to audit, and unnecessary for the 98% of cases where simple economics-based defences suffice.

This is not a book about stopping sophisticated targeted attacks (Archetype 4 from Chapter 10). Dedicated adversaries targeting your site specifically require dedicated security operations. This book is about the 99% of automated abuse that hits every public form within hours of launch, which can be stopped with a small amount of well-placed code.

This is not a book arguing that all third-party bot detection services are evil. Cloudflare, Arkose, and other vendors offer sophisticated products that are appropriate for high-value targets (financial services, government, large enterprise). This book argues that for the vast majority of websites and small businesses, those tools are overkill, privacy-invasive, and inaccessible to a large share of users — and a simpler, cheaper, more open alternative exists.

A note on data

All production data in this book is drawn from ColdCode Si Labs server logs between January 2026 and November 2026, across seven products serving approximately 4,000 paying customers and hundreds of thousands of monthly visitors in Zimbabwe, South Africa, Kenya, Nigeria, and Zambia. Device and network data is measured from actual

traffic; anecdotes about specific customers are used with permission or anonymised. Industry statistics are cited in the Notes section.

Invisible Proof

Bot Mitigation for Markets That Cannot Solve CAPTCHAs

Courage Garikai

ColdCode Si Labs · Harare

DCAI · 2026

For the shopkeeper in Chitungwiza who lost forty registrations to a bot flood in one weekend because her $15 phone could not render a puzzle.

For the grandmother in Mbare who was locked out of her own grant application because the CAPTCHA timed out before she could read it.

And for the builders who keep shipping puzzle gates to markets where the devices, the data plans, the literacy levels, and the fingers do not match the assumptions.

Contents

Part I · The puzzle is the problem 1. The registration page that filtered out humans 2. CAPTCHA as colonial infrastructure 3. What CAPTCHA actually measures 4. Why bots solve puzzles faster than grandmothers 5. The accessibility lie

Part II · What we are actually defending against 6. The bot economy, in numbers 7. Credential stuffing and the 8.4

billion password list 8. Scraping, form spam, and synthetic accounts 9. Card testing and promo fraud 10. The four bot archetypes (not one) 11. What attackers will and will not pay for

Part III · The invisible proof stack 12. Proof of work: 50 milliseconds that costs a bot $0.40 per thousand 13. Velocity and reputation: your server remembers 14. Behavioural signals without tracking 15. Form-field choreography: humans do not fill forms instantly 16. Device and network fingerprinting, done honestly 17. The invisible verification layer 18. The one-time friction gate: when a puzzle is actually needed

Part IV · Building for the markets you serve 19. Designing for the $15 phone 2. Designing for 2G and prepaid data 3. Designing for multilingual, low-literacy users 4. Designing for assistive technology 5. Proofhand: an implementation at scale 6. The economics of a bot check: budget per request 7. Measuring false positives and false negatives 8. When to ban, when to challenge, when to let through

Part V · Law, ethics, and the future 9. Privacy: verifying without identifying 10. Arms races and equilibrium 11. Open proof: why the algorithm must be publishable 12. The market for human labour solving CAPTCHAs 13. AI-native bots: what changes when LLMs can pass every puzzle 14. Invisible proof as infrastructure

Tools Index · Data · Case files · Notes · Colophon

Free sample

This is the opening of "Invisible Proof" by Courage Garikai.
The full edition — PDF and EPUB — is at library.coldcode-si-labs.workers.dev

(c) 2026 Courage Garikai. All rights reserved.