AI Based Technologies for Authentication

Moving from static body parts to the rhythm of interaction

Vijay Anantharamaiah

2026 Edition

Section 1

The State of Play

Why are we still talking about login?

- We all have seen and built login screens.
- We keep adding layers, but we haven’t solved the core problem.
- We are still asking for a "Key" rather than recognizing the "Person."
- We are unable simplify security without making bad UX

A bad idea we can’t quit

- Passwords rely on "secrets." But humans are terrible at keeping secrets.
- 80% of us reuse them. Attackers know this.
- It’s a binary check: if the secret matches, you’re in.
- It doesn’t matter if you’re a human or a script in a basement in another country.

Adding friction to hide the flaws

- We added SMS codes and hardware keys to slow down attackers.
- It worked, but it made using software a chore.
- SIM swapping and proxy phishing have made even "Strong MFA" bypassable.
- We’re verifying the *device*, not the *human* holding it.

Section 2

Biometrics (The First Wave)

Faces and Fingers as Identifiers

What we have now:

- TouchID and FaceID are fast.
- They made the "Front Door" much easier to open.

The reality check:

- Your face is public data.
- Biometrics are identifiers, not secrets.
- You can’t "reset" your face if the database leaks.

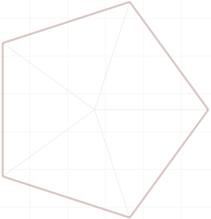
The Session

- If you walk away from your desk, the session stays alive.

The ’Point-in-Time’ is a lie.

Section 3

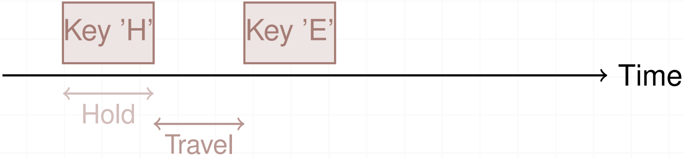
A Shift in Behavior



Recognizing ‘Who’ through ‘How’

- We’re moving from physical traits to behavioral ones.
- It’s about neuromuscular habits
- Things you don’t even think about.
- Continuous and invisible

Keystroke Dynamics



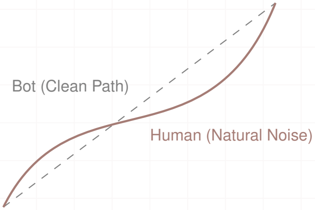
What we measure:

- **Hold (Dwell):** How long your finger stays on the key.
- **Travel (Flight):** The time between pairs of keys.

Typing Patterns: More than just speed

- Everyone has a unique neuromuscular "rhythm" for letter pairs like "TH" or "ING."
- **Entropy:** Measure the natural "noise" in your typing.
- Humans are inconsistent. Bots move with too much precision.

Human Jitter



The indicators:

- Humans move in curves, not lines.
- Tiny nervous system jitters (8-12Hz).
- How we slow down before we click.

Mobile Interaction

- How much of your thumb actually touches the screen.
- The specific velocity and pressure of your scroll.
- Correlating a swipe with the phone’s physical movement (Gyroscope).

Section 4

How it works

What we listen for

- We’re looking at a stream of events: 60 to 100 times per second.
- Mouse coordinates, key timings, touch surface area.
- Converting "pixels" to "ratios." 100 pixels on a 4K monitor is not the same as 100 pixels on a laptop.

Why Time-Series Models?

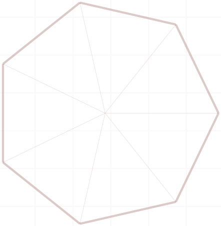
- Individual actions mean nothing. The **sequence** is everything.
- Models have a memory. They understand that action *B* depends on action *A*.
- The output is a mathematical digest of your interaction style.

Trust as a Probability

- We move away from "Yes/No."
- The AI gives us a confidence score from 0.0 to 1.0.
- What is the probability that the person typing right now is the true owner of this account?

Section 5

Architectural Reality



Why Cloud round-trips don’t work

The Latency Problem:

- Sending every mouse move to the cloud is a bandwidth nightmare.
- Round-trip lag (200ms) makes "Invisible Auth" feel janky and slow.

The Edge Solution:

- Ship the model weights to the device.
- Perform inference locally (WASM or CoreML).
- Only risk scores leave the device.

Day 1 Challenge

- AI needs data to learn your "Normal."
- **1:** Rely on legacy auth (Passwords/FaceID).
- **2:** The AI watches in the background but doesn’t block anything yet.
- **3:** Only promote the AI to "Primary" once the baseline is stable.

Life happens

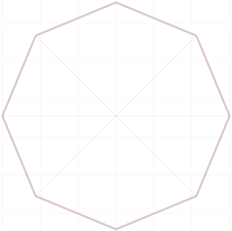
- Human interaction isn’t fixed
- Ageing.
- Fatigue.
- Caffeine intake.
- Fancy new mechanical keyboard.
- Injury.
- The model has to update its weights slowly with every verified session to "age" with you.

The ‘Broken Arm’

- You break your hand. Your score drops to 0.0 instantly.
- Identify the sudden, persistent anomaly.
- Trigger a "Step-up" challenge (TouchId/FaceId or other).
- If verified, we start a "New Baseline" training phase.

Section 6

The Arms Race



AI vs. AI

- Malware that "watches" you, learns your rhythm, and then replays it.
- **GANs:** Attackers use AI to generate "human-like" noise to bypass anomaly detection.
- It’s no longer a human vs. a machine; it’s AI defending against AI.

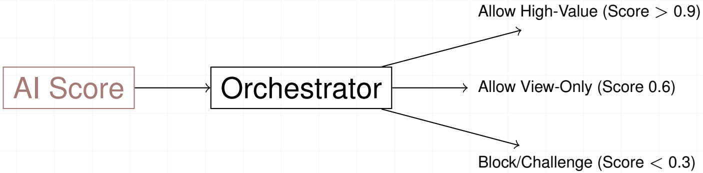
Our best defense

- Purely digital signals can be synthesized. Physical correlations are harder.
- Correlating the phone’s Accelerometer with the keyboard.
- Does the device physically vibrate when you hit "Enter"?
- Malware can fake the keypress, but it can’t move the physical phone.

Section 7

Zero Trust Architecture

Trust as a Spectrum



AI Score

Orchestrator

Allow High-Value (Score $>$ 0.9)

Allow View-Only (Score 0.6)

Block/Challenge (Score $<$ 0.3)

We are moving from ’Authenticated’ to ’Continuously Verifying’.

Session Revocation

- If someone else sit downs at your computer mid-session, the behavioral score drops.
- The connection is terminated immediately.
- We move from "Login events" to "Ambient state."

Section 8

Privacy and Accessibility

Privacy by Design

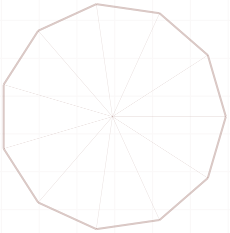
- Never collect what you don’t need.
- Discard character values (*ASCII*) at the source.
- We only extract the Inter-arrival Time (■*T*).
- We know *how* you type, but we have no idea *what* you are saying.

The Accessibility Paradox

- Assistive tech (screen readers) looks like "Bot behavior" to AI.
- We must detect accessibility flags and switch to specialized baseline models.
- Security should never be a tax on disability.

Section 9

Recap



The Long Arc of Identity

- Passwords were about secrets.
- Biometrics were about bodies.
- Behavioral intelligence is about **Context**.
- The goal is security that stays out of the user's way until it's actually needed.

Summary

- We're trading 'Yes/No' for a sliding scale of trust.
- Edge inference: Why local processing matters.
- Zero Trust: Treating identity as a decaying state.
- Privacy: Extracting behavior without keylogging.

Questions?

?

Thank You

Thank You!

vijayanant.com

<hello@vijayanant.com>