AI Based Technologies for Authentication

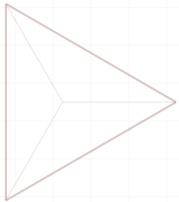
Moving from static body parts to the rhythm of interaction

Vijay Anantharamaiah

2026 Edition

Section 1

The State of Play



Why are we still talking about login?

- I’ve spent 20 years looking at login screens.
- We keep adding layers, but we haven’t solved the core problem.
- **The fundamental issue:** We are still asking for a "Key" rather than recognizing the "Person."
- Security today is often just a tax on the user’s time.

Passwords: The bad idea we can’t quit

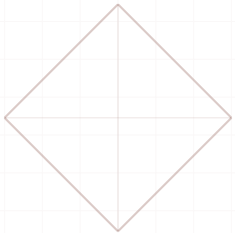
- Passwords rely on "secrets." But humans are terrible at keeping secrets.
- 80% of us reuse them. Attackers know this.
- It’s a binary check: if the secret matches, you’re in.
- It doesn’t matter if you’re a human or a script in a basement in another country.

MFA: 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.
- **The new threats:** 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:

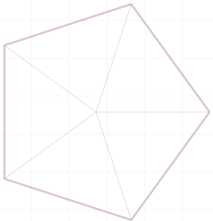
- Your face is public data.
- Biometrics are identifiers, not secrets.
- You can’t "reset" your face if the database leaks.

The ‘Point-in-Time’ Fallacy

- Static auth happens once at the start of a session.
- What happens after you log in?
- If you walk away from your desk, the session stays alive.
- **The Gap:** We have no way of knowing if the person still sitting there is the same person who logged in.

Section 3

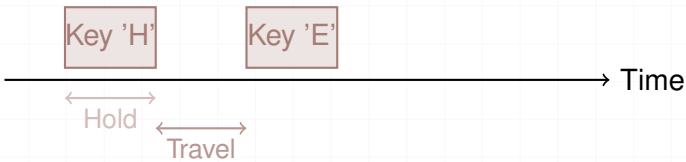
The Behavioral Shift



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.
- **The Goal:** Continuous, invisible trust that doesn’t need a prompt.

Keystroke Dynamics: The brain-hand loop



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:** We measure the natural "noise" in your typing.
- Humans are consistently inconsistent. Bots move with too much precision.

Mouse Dynamics: Human Jitter

The indicators:

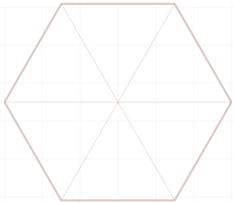
- **Arcs:** Humans move in curves, not lines.
- **Tremors:** Tiny nervous system jitters (8-12Hz).
- **Velocity:** How we slow down before we click.

Mobile Interaction: Swipes and Sensors

- **Touch Area:** How much of your thumb actually touches the screen.
- **Swipe Curves:** The specific velocity and pressure of your scroll.
- **Sensor Fusion:** Correlating a swipe with the phone's physical movement (the Gyroscope).

Section 4

How it works (The Pipeline)



Collecting Telemetry: What we listen for

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

The Engine: Why Time-Series Models?

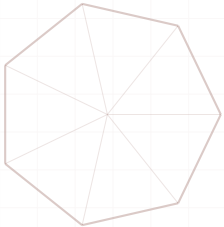
- Individual actions mean nothing. The **Sequence** is everything.
- **RNN and LSTM:** These models have a memory. They understand that action *B* depends on action *A*.
- **The Profile:** The output is a mathematical digest of your interaction style.

The Score: Trust as a Probability

- We move away from "Yes/No."
- The AI gives us a confidence score from 0.0 to 1.0.
- **The Question:** "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.

The Cold Start Problem: Day 1 Challenge

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

Behavioral Drift: Life happens

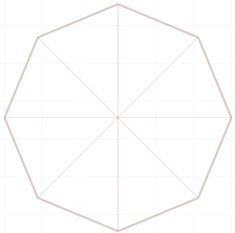
- **Human interaction isn’t fixed:**
- You get older. You get tired. You drink too much coffee.
- You buy a new mechanical keyboard.
- **Online Learning:** The model has to update its weights slowly with every verified session to "age" with you.

Handling Trauma: The ‘Broken Arm’

- **Failure Mode:** You break your hand. Your score drops to 0.0 instantly.
- **Architectural Recovery:**
- Identify the sudden, persistent anomaly.
- Trigger a "Step-up" challenge (FaceID or Video call).
- If verified, we start a "New Baseline" training phase.

Section 6

The Arms Race



AI vs. AI: Generative Malware

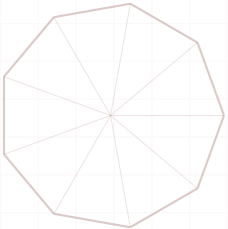
- **The Threat:** Malware that "watches" you, learns your rhythm, and then replays it.
- **GANs:** Attackers use AI to generate "human-like" noise to bypass anomaly detection.
- It’s no longer a human vs. a machine; it’s AI defending against AI.

The Physical World: Our best defense

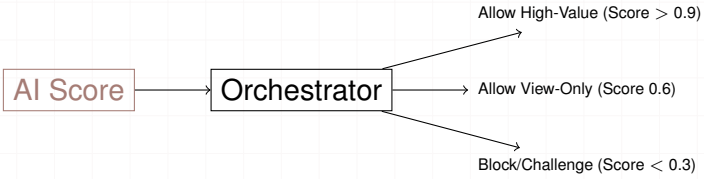
- Purely digital signals can be synthesized. Physical correlations are harder.
- **Sensor Fusion:** Correlating the phone's Accelerometer with the keyboard.
- **The Test:** Does the device physically vibrate when you hit "Enter"?
- **Result:** Malware can fake the keypress, but it can't move the physical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

Section 7

Zero Trust Architecture



Trust as a Spectrum



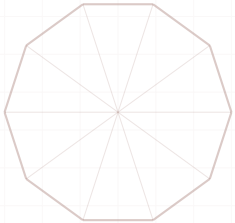
Trust is earned continuously, not granted once.

Session Revocation: Killing the connection

- In Zero Trust, identity expires every minute.
- 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: What we don’t see

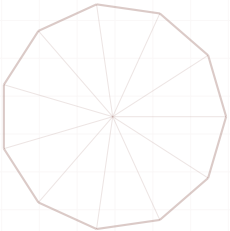
- **The Rule:** Never collect what you don’t need.
- **The Fix:** Discard character values (*ASCII*) at the source.
- We only extract the **Inter-arrival Time** ($\blacksquare T$).
- We know *how* you type, but we have no idea *what* you are saying.

The Accessibility Paradox

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

Section 9

Summary



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.

Session Summary

- Moving from binary checks to probability scores.
- Edge inference: Why local processing matters.
- Zero Trust: Treating identity as a decaying state.
- Privacy: Extracting behavior without keylogging.

Questions?

Thank You!

vijayanant.com>

<hello@vijayanant.com>