# Gesture Based Security Touchpoint

## The current scenario

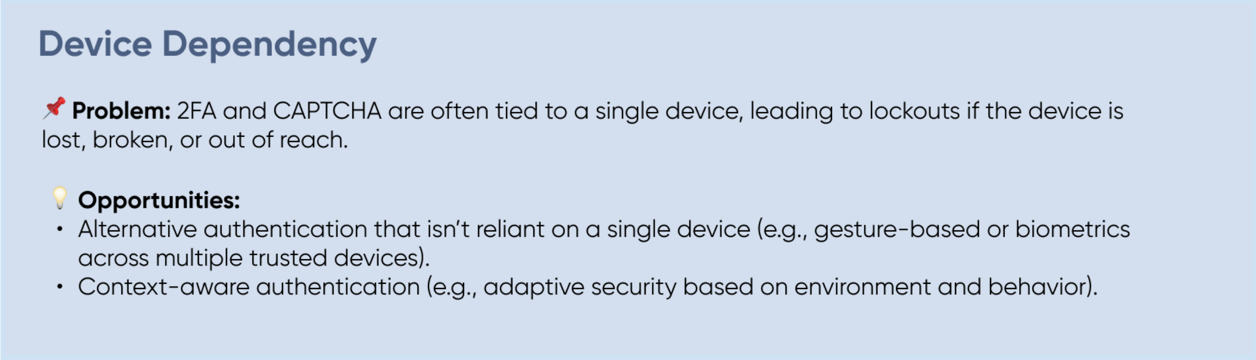
The project addresses the frustrations and accessibility issues associated with current security touchpoints like CAPTCHAs and 2FA. In today's digital landscape, these security measures, while crucial for protecting user data, often disrupt the user experience by being cumbersome, time-consuming, and inaccessible for users with disabilities.

## Research Question

The key research question revolves around how to create more user-friendly and inclusive security authentication systems, potentially leveraging AI. The project aims to find solutions that balance robust security with a seamless and intuitive user experience.

## Key Pain Points

To gain a deeper understanding of the challenges users face with current security touchpoints, I employed a user-centered research approach that included direct engagement with individuals. I conducted interviews and held conversations with a diverse group of people to gather firsthand accounts of their experiences with systems like CAPTCHAs and two-factor authentication. These interactions revealed recurring pain points, such as the frustration of device dependency, the annoyance of frequent re-authentication, and the difficulties faced by users with disabilities. This qualitative data, combined with sentiment analysis from other sources, provided valuable insights into the emotional and functional needs that current security measures often fail to meet, directly informing the development of more user-friendly and inclusive authentication solutions for my project.

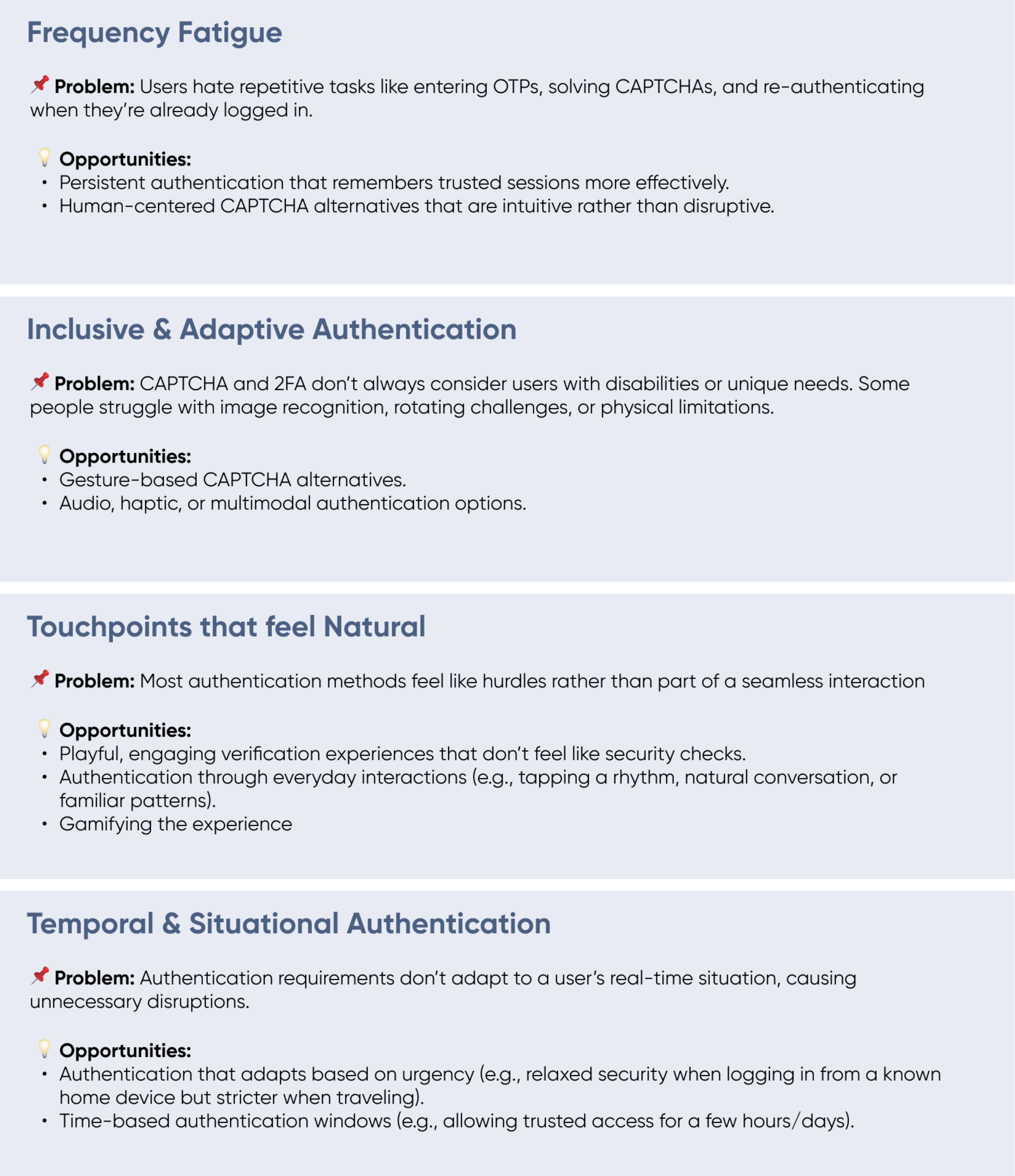


### Device Dependency

📌 **Problem:** 2FA and CAPTCHA are often tied to a single device, leading to lockouts if the device is lost, broken, or out of reach.

💡 **Opportunities:**

- Alternative authentication that isn't reliant on a single device (e.g., gesture-based or biometrics across multiple trusted devices).
- Context-aware authentication (e.g., adaptive security based on environment and behavior).



## Frequency Fatigue

📌 **Problem:** Users hate repetitive tasks like entering OTPs, solving CAPTCHAs, and re-authenticating when they're already logged in.

💡 **Opportunities:**

- Persistent authentication that remembers trusted sessions more effectively.
- Human-centered CAPTCHA alternatives that are intuitive rather than disruptive.

## Inclusive & Adaptive Authentication

📌 **Problem:** CAPTCHA and 2FA don't always consider users with disabilities or unique needs. Some people struggle with image recognition, rotating challenges, or physical limitations.

💡 **Opportunities:**

- Gesture-based CAPTCHA alternatives.
- Audio, haptic, or multimodal authentication options.

## Touchpoints that feel Natural

📌 **Problem:** Most authentication methods feel like hurdles rather than part of a seamless interaction

💡 **Opportunities:**

- Playful, engaging verification experiences that don't feel like security checks.
- Authentication through everyday interactions (e.g., tapping a rhythm, natural conversation, or familiar patterns).
- Gamifying the experience

## Temporal & Situational Authentication

📌 **Problem:** Authentication requirements don't adapt to a user's real-time situation, causing unnecessary disruptions.

💡 **Opportunities:**

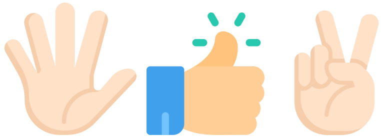
- Authentication that adapts based on urgency (e.g., relaxed security when logging in from a known home device but stricter when traveling).
- Time-based authentication windows (e.g., allowing trusted access for a few hours/days).

## Ideation

- **Gesture-Based Security Authentication System:** This solution is for any user with a device equipped with a camera. When a user needs to authenticate, instead of entering a password or code, they use predefined gestures recognized by the system's computer vision. This offers a more intuitive and potentially faster authentication method, reducing reliance on traditional passwords and 2FA using motion detection and gesture recognition.

- **Haptics-Based Security Authentication System:** This solution is for users with devices that support advanced haptic feedback. When authentication is required, the device generates a personalized vibration sequence. The user then replicates this sequence through touch gestures to log in. This provides an alternative authentication method for devices without cameras, offering a secure and engaging tactile experience, and involves haptic rendering models to create unique vibration patterns.
- **AI-Based Adaptive Authentication System:** This solution is for all users seeking a more seamless login experience. The system uses AI to contextually authenticate users based on factors like trusted locations, network patterns, and behavioral biometrics. This aims to eliminate the need for traditional 2FA by automatically logging in users in trusted situations.

## My Solution: Gesture-Based Security Authentication System



I chose to work on the Gesture based Authentication System because of the ease of use, accessibility and pre existing models on gesture recognition which made it easier for me to build my AI.

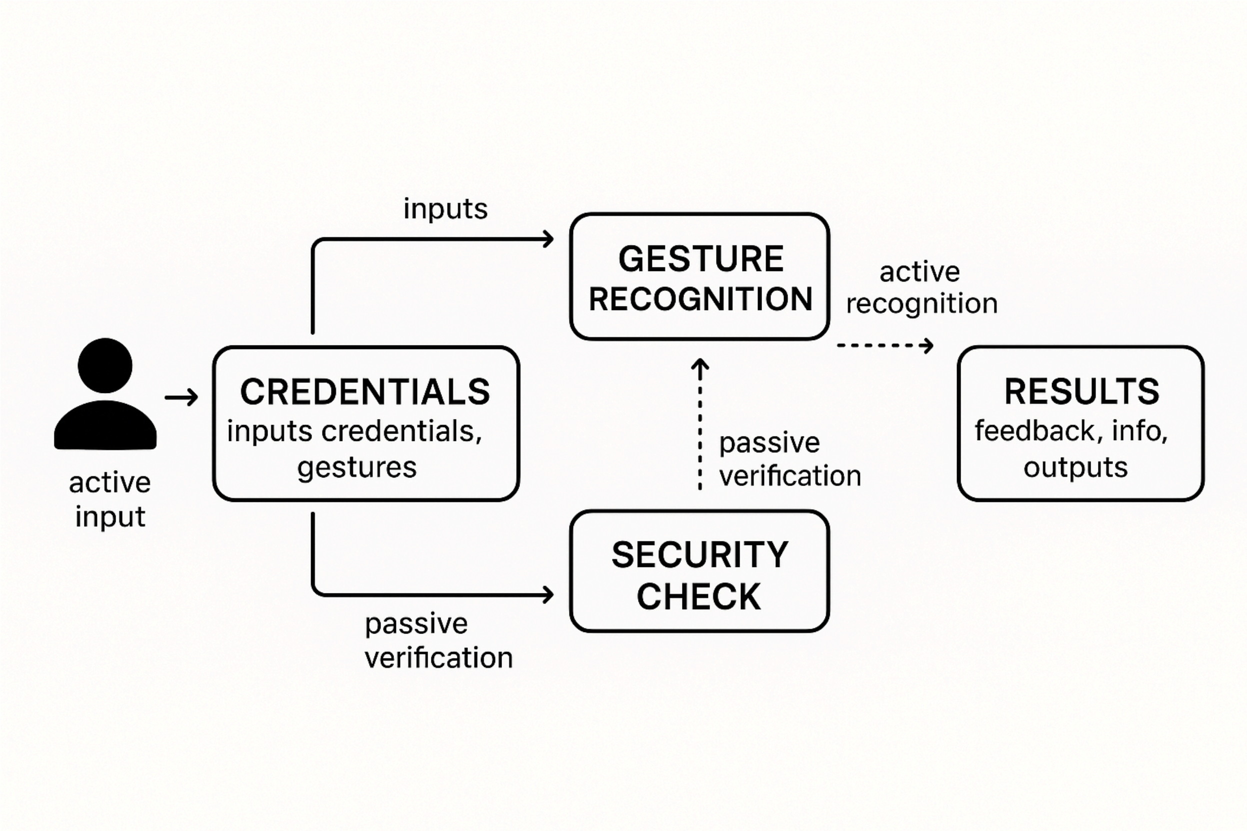
### About my project

The gesture-based authentication system aims to replace or augment traditional password and two-factor authentication methods with a more intuitive and user-friendly approach. It leverages computer vision and machine learning to recognize and validate user-defined gestures for secure access.

Step 1: User open a website
Step2: Adds credentials and passwords
Step3: Clicks on Gesture Check
Step4: A security check to enable gesture recognition
Step 5: A splash screen explaining users about the next steps
Step6: A gesture appears on the screen that the user has to perform for 3 seconds
Step7: Another gesture to perform
Step8: User verified, gets logged in the webpage

### Key Features and Considerations:

- **Real-time Processing:** The system processes gestures in real-time, ensuring a fast and responsive authentication experience.
- **Security:** The use of dynamic gesture sequences and feature extraction makes it difficult for bots to log in such sites
- **Accessibility:** Gesture-based authentication can offer an alternative for users who may have difficulty with traditional text-based passwords or CAPTCHAs.
- **Feedback:** The system provides clear visual feedback to the user during the authentication process, indicating whether the gestures are being recognized correctly.



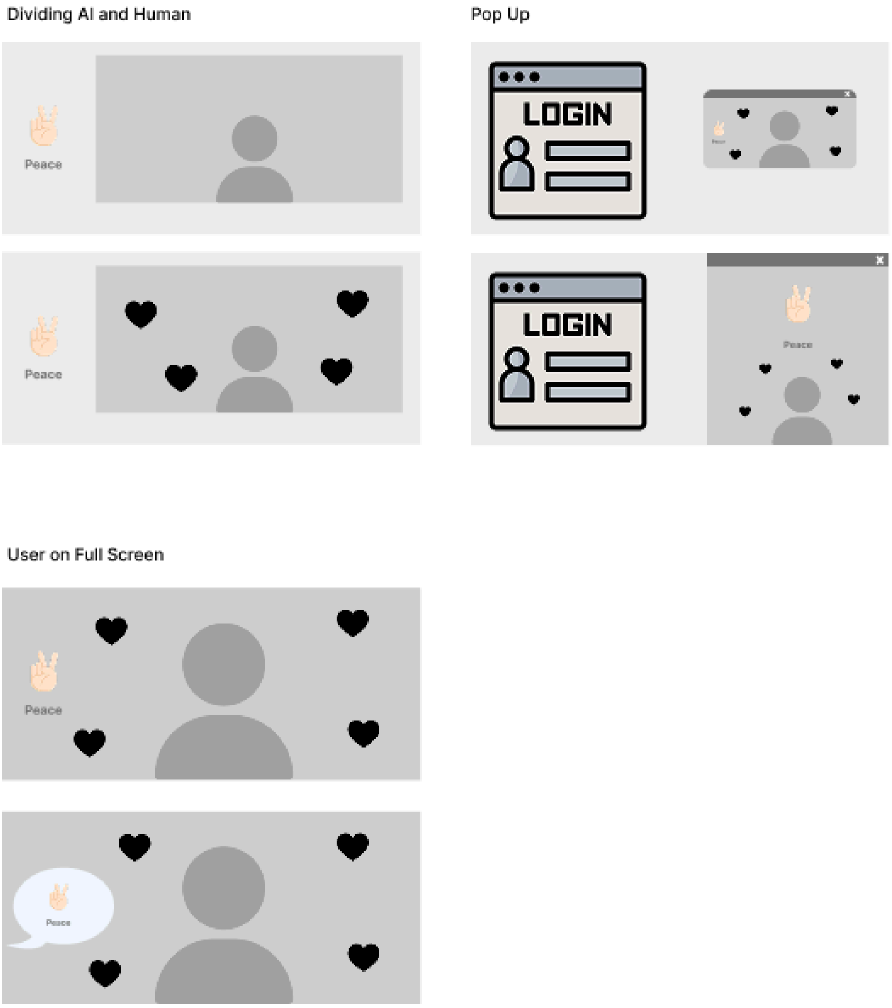
## Base Model - Google Media Pipeline

For my project, I explored using MediaPipe, an open-source framework by Google, for real-time gesture recognition. Initially, I encountered challenges as the model I found wasn't functioning due to outdated libraries. Through debugging, specifically patching the library paths, I was able to resolve this and get the model working. The model operates by first detecting hands in an image, then identifying 21 3D keypoints. These keypoints are converted into features, which are then fed into a trained model to classify the gesture present, outputting a label and a probability score. I experimented with both images highlighting hand gestures and real-world images containing both gestures and users, and the model performed well in both scenarios. While the model is image-based I integrated this model with a real-time video gesture recognition tool for the final solution. My solution is a system that identifies gestures in live video streams, and enhances user engagement by incorporating gamification elements like visual effects (emojis) upon successful gesture recognition.

## The Interface

For my interface, I wanted to keep it simple and efficient. Since the user would only interact with the security touchpoints for a few minutes, the UI should be clean and less cluttered to convey the main idea and information clearly.
For this I explored some concepts:

UI Sketches

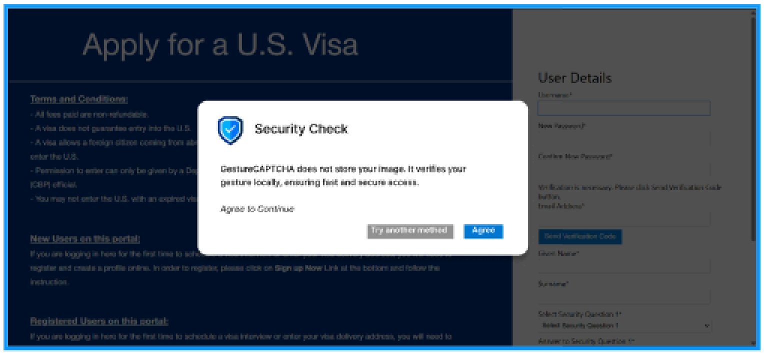


Dividing AI and Human

Pop Up

User on Full Screen

While designing the user interface, I talked to users and **identified some key mental models** they have about security touchpoints. These models, or their expectations about how security should work, were really important and made me include certain elements in the final design. User feedback like this was crucial in confirming that my design and UI choices were the right ones.



# Apply for a U.S. Visa

**Terms and Conditions:**

- All fees paid are non-refundable.
- A visa does not guarantee entry into the U.S.
- A visa allows a foreign citizen coming from ab
enter the U.S.
- Permission to enter can only be given by a De
(CBP) official.
- You may not enter the U.S. with an expired vis

**New Users on this portal:**

If you are logging in here for the first time to sch
register and create a profile online. In order to register, please click on **Sign up Now** Link at the bottom and follow the instruction.

**Registered Users on this portal:**

If you are logging in here for the first time to schedule a visa interview or enter your visa delivery address, you will need to

## User Details

Username*

New Password*

Confirm New Password*

Verification is necessary. Please click Send Verification Code button.
Email Address*

Send Verification Code

Given Name*

Surname*

Select Security Question 1*
Select Security Question 1

Answer to Security Question 1*

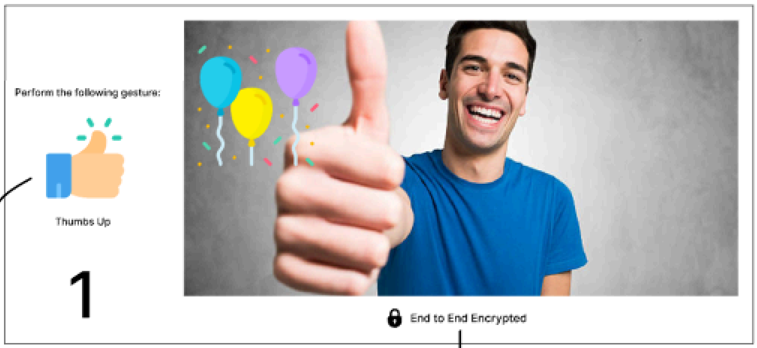
### Security Check

**GestureCAPTCHA does not store your image. It verifies your gesture locally, ensuring fast and secure access.**

*Agree to Continue*

**Mental Model:** *"I want to be the one to start the interaction — not have the system surprise me."*

**Mental Model:** *"I need to know what's about to happen before I'm asked to do something."*



Perform the following gesture:

Thumbs Up

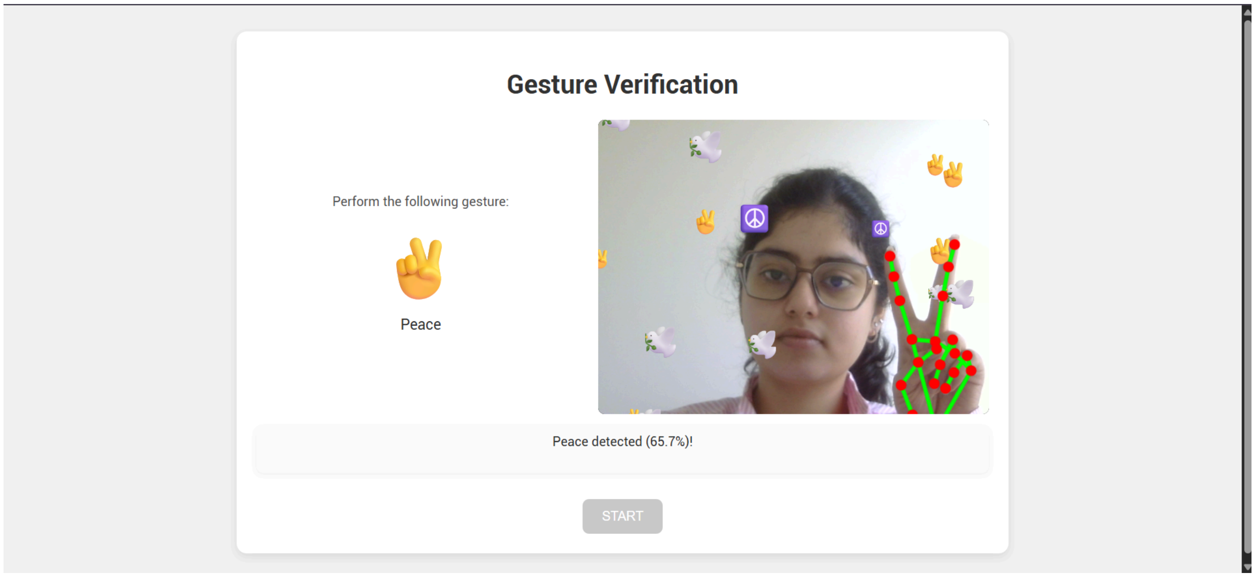
1

End to End Encrypted

**Mental Model:** *"If I don't know the name of a gesture, I can't be expected to perform it correctly."*

**Mental Model:** *"If I'm using my camera for a security check, it could be recording me — and that feels risky."*

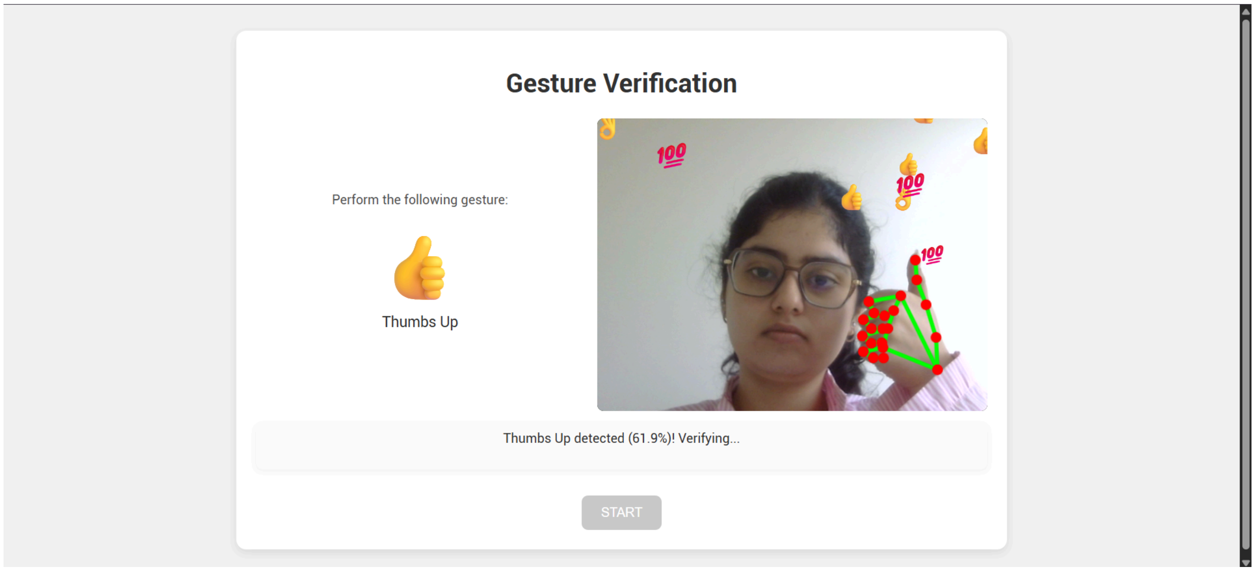
## Final UI:



Gesture Verification

Perform the following gesture:

Peace detected (65.7%)!



Gesture Verification

Perform the following gesture:

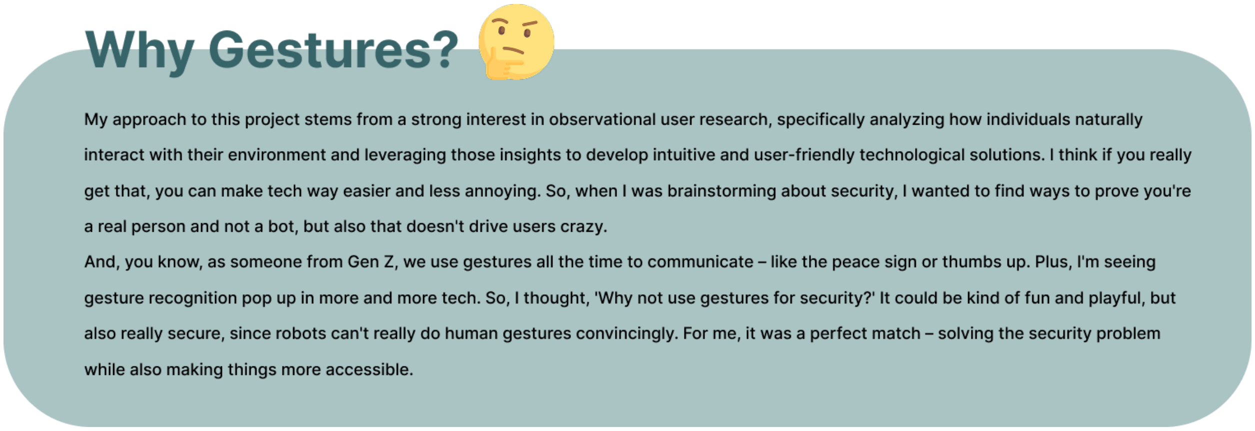
Thumbs Up detected (61.9%)! Verifying...

## Conclusion

Putting the model into action had some tough parts. I've updated the model's interface since the last demo, and now it guides users through a series of gestures and confirms them. My next steps involve refining the interface's design and adding accessibility features like voice control. I also want to make the interactive parts more fun and engaging.

**Next Challenge**

When I had people test the model, they could use the interface itself, but they had trouble grasping the whole concept because the gesture process took a relatively short time (a min). Users didn't have enough time to understand that the gestures were actually logging them in. I need to address this feedback by finding a way to make the process quicker or provide better real-time feedback to improve user comprehension.



## Why Gestures? 🤔

My approach to this project stems from a strong interest in observational user research, specifically analyzing how individuals naturally interact with their environment and leveraging those insights to develop intuitive and user-friendly technological solutions. I think if you really get that, you can make tech way easier and less annoying. So, when I was brainstorming about security, I wanted to find ways to prove you're a real person and not a bot, but also that doesn't drive users crazy.

And, you know, as someone from Gen Z, we use gestures all the time to communicate – like the peace sign or thumbs up. Plus, I'm seeing gesture recognition pop up in more and more tech. So, I thought, 'Why not use gestures for security?' It could be kind of fun and playful, but also really secure, since robots can't really do human gestures convincingly. For me, it was a perfect match – solving the security problem while also making things more accessible.