# Biometric Attendance System using WebAuthn & Firebase

Secure Fingerprint-Based Authentication with Cryptographic Keys

## 🔍 Overview

This document outlines the design and implementation of a secure biometric attendance system using WebAuthn, cryptographic keys, and Firebase. The solution respects biometric privacy by never storing raw fingerprint data. Instead, it uses device-based authentication to generate secure keys for identity verification.

## 🧭 System Flow

### 1. Registration Phase

- Learner scans their fingerprint via device biometric (WebAuthn).  
- A cryptographic key pair is generated.  
- The public key is stored in Firebase associated with the learner.  
- The private key stays securely on the device.

### 2. Authentication / Attendance Check-In

- Learner selects their name from a list.  
- The device prompts for fingerprint authentication.  
- A signed challenge is created if the fingerprint matches.  
- The public key in Firebase is used to verify the signature.  
- If valid, attendance is marked.

## 🔐 Cryptographic Foundation

Biometric data is never stored or transmitted. Devices like phones or browsers use fingerprints to access a secure enclave storing private keys. During registration, only a public key is sent to Firebase. During authentication, the fingerprint unlocks the private key to sign a message (challenge), proving identity.

## 🌍 Real-World Use Cases

- Google Passkeys  
- Apple Face ID/Touch ID Logins  
- Microsoft Hello Authentication

## 🧰 Tools & Technologies

- WebAuthn API (Browser-side Biometric Integration)  
- Firebase Firestore (Cloud Data Storage)  
- GitHub Pages (Optional Frontend Hosting)  
- JavaScript, HTML, CSS (Frontend)

## 📌 Important Notes

- The cryptographic credential is tied to a device.  
- Re-registration is required if users switch devices.  
- Works best on shared kiosks or school devices for attendance systems.

## ✅ Summary

This system is secure, scalable, and respects user privacy. It leverages the power of modern browser APIs and Firebase to deliver a lightweight and efficient biometric attendance platform without compromising fingerprint data.