RECONOCIMIENTO FACIAL PARA EL INGRESO A INSTITUCIONES EDUCATIVAS

Jonnathan Guamán
Wilson Pinos
Sebastián Once

DIVISIÓN DE TAREAS

ROLES

Scrum master

Wilson Pinos

Equipo de desarrollo

Jonnathan Guamán
Sebastián Once

OBJETIVOS

Implementar un flujo de acceso que identifique al usuario en menos de 1 s, eliminando cuellos de botella en la entrada y minimizando filas

Sustituir o complementar credenciales físicas (carnés) por biometría facial, dificultando la suplantación de identidad.

Ofrecer al personal de seguridad y al administrador un panel que muestre quién entra y sale al instante, con registros timestamp.

ARQUITECTURA TECNOLÓGICA

Captura de imagen
Cámaras IP HD (con visión infrarroja opcional) montadas en los accesos, que envían el stream al servidor para análisis.

Preprocesamiento con OpenCV
Detección de rostros en el frame, corrección de iluminación y alineamiento de cara (rotación/recorte) para estandarizar la entrada al modelo.

Embeddings faciales con FaceNet/TensorFlow
Conversión de cada rostro en un vector numérico (embedding) que encapsula sus rasgos únicos; comparación contra la base de datos.

Back-end (Java Spring Boot + MongoDB/MySQL)
Servicio REST que recibe embeddings, consulta coincidencias y devuelve el veredicto de “acceso permitido” o “rechazado”.

Front-end (React/Angular)
Dashboard para administradores: panel de control, historial de accesos, gestión de usuarios y alertas en tiempo real.

VENTAJAS

Automatización

El sistema opera sin intervención humana, ahorrando tiempo y recursos de seguridad.

Rapidez

Gracias a modelos optimizados y hardware adecuado, la validación facial es casi instantánea.

Seguridad

Con técnicas anti-spoofing (detección de máscara o pantalla), se impide el ingreso con fotos o videos.

DESVENTAJAS Y DESAFÍOS

Falsos positivos/negativos en condiciones de luz extremas
Escenarios con contraluz o poca iluminación pueden degradar la fiabilidad del reconocimiento.

Costo inicial de hardware y licencias
Inversión en cámaras especializadas, servidores con GPU y posibles licencias de software.

Mantenimiento (actualizar modelos, calibrar cámaras)
Reentrenar el modelo ante cambios demográficos, recalibrar sensores y gestionar parches de seguridad.

CONSIDERACIONES ÉTICAS Y DE PRIVACIDAD

Consentimiento informado de estudiantes y apoderados
Protocolos de comunicación claros: qué datos se recogen, con qué fin y por cuánto tiempo.

Retención mínima de datos biométricos
Sólo almacenar embeddings cifrados (AES-256), no imágenes crudas, y borrarlos al cumplirse el plazo legal.

Acceso restringido a la base de datos
Implementar control de accesos por roles, logs de auditoría y autenticación multifactor en el panel de administración.

Cumplimiento de la LOPD-Ecuador y estándares internacionales
Asegurar la conformidad con la normativa local (Ley Orgánica de Protección de Datos) y buenas prácticas de GDPR.

PLAN DE IMPLEMENTACIÓN

Fase 1

Prueba piloto en un aula (1 mes)
Validar hardware y modelo con un grupo reducido, ajustar umbrales de similitud y resolver incidencias.

Fase 2

Escalado a todo el plantel (3 meses)
Ampliar cobertura de cámaras, desplegar más instancias de servidor y formar al personal de TI.

Fase 3

Con técnicas anti-spoofing (detección de máscara o pantalla), se impide el ingreso con fotos o videos.

CONCLUSIÓN

Este sistema tiene que ofrecer un control de acceso rápido y fiable que refuerza la seguridad en instituciones educativas, minimizando suplantaciones mediante técnicas anti-spoofing. Almacena únicamente embeddings cifrados y aplica protocolos de consentimiento y retención mínima, garantizando cumplimiento normativo (LOPD-Ecuador/GDPR) y respeto por la privacidad de los estudiantes.