Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II (Gpo 501)

Privacidad y Seguridad de los Datos

Francisco Mestizo Hernández - A01731549

Octubre 27, 2023

Introducción

El reto consiste en desarrollar una herramienta con la cual se pasará lista automáticamente a los alumnos. Además, se llevará un registro de las participaciones de los estudiantes. Estas dos funcionalidades se lograrán utilizando inteligencia artificial y visión computacional. Para pasar lista a los estudiantes se utilizará reconocimiento facial y para las participaciones se utilizarán algoritmos para detección de pose.

Este sistema permitirá que los profesores lleven un seguimiento más sencillo de los estudiantes que asisten a la clase y que tan frecuentemente participan o no.

Privacidad y seguridad de los datos

Dentro del proyecto hay varias áreas en donde se utilizan diferentes datos y se debe garantizar la privacidad de los usuarios. A continuación se describen los mecanismos que se seguirán para asegurar la seguridad de los datos.

Leyes y privacidad

En México, el artículo 16 de la Constitución Mexicana establece que todos los ciudadanos tienen derecho a que se protejan sus datos personales, así como a el acceso, la rectificación, cancelación y a manifestar su oposición. Esto es mejor conocido como los derechos ARCO. El proyecto está enfocado hacia el sector privado, por lo que se debe seguir la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). De acuerdo con el INAI, en esta legislación se marcan 8 puntos importantes:

La licitud indica que los datos personales otorgados solamente pueden ser utilizados para actividades lícitas y para lo que se acordó con los usuarios que dieron sus datos personales.

El consentimiento se refiere a que los responsables del proyecto deben obtener el consentimiento de las personas a las que pertenecen los datos personales antes de usarlos. Además, se tiene que ser específico con la finalidad que tendrá el uso de esos datos personales. Este consentimiento se puede dar al aceptar un aviso de privacidad o al recibir la aceptación por algún medio escrito o digital.

Con el principio de información se establece que los responsables del proyecto deben informar claramente a los usuarios por medio de un aviso de privacidad las características principales del tratamiento que se le dará a sus datos personales.

La calidad indica que los datos pertenecen a las personas correctas, no contienen errores, están actualizados y se tratan de forma que no sean perjudiciales para el titular.

Con la finalidad se estipula que los datos solamente se utilizan para lo establecido en el aviso de privacidad que recibió el usuario. Todas las finalidades deben ser explicadas sin dar lugar a confusión o interpretaciones.

La lealtad marca que los datos no deben perjudicar al titular y deben ser obtenidos de forma correcta, no por medio de fraudes o negligencia.

La proporcionalidad dice que se debe tratar de recabar la menor cantidad de datos y debe tratarse de datos que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que se indica.

Y la responsabilidad indica que los responsables del proyecto deben velar por el cumplimiento de todos los requisitos y demostrar ante los titulares y las autoridades que se está cumpliendo con todo.

Todas las medidas de privacidad que se mencionan en las siguientes secciones están basadas en la legislación mencionada en este apartado.

Reconocimiento facial y detección de pose

Los algoritmos que se utilizarán para la detección de la pose y el reconocimiento facial son pre entrenados. En caso de que se desarrollaran modelos de IA para la pose y el reconocimiento facial para este proyecto, sería importante tomar en cuenta de dónde vienen los datos (imágenes) con los que se está haciendo el entrenamiento. Y al tratarse de imágenes donde aparecen personas, especialmente para el reconocimiento facial, se debe tener el consentimiento de todos los involucrados y ellos tienen que estar enterados del uso que se le dará a sus imágenes.

Aún así, aunque el modelo de reconocimiento facial esté pre entrenado, solamente reconoce caras, sin asignarlas a una persona. Para que este mismo modelo reconozca una cara y al mismo tiempo la relacione con un nombre, se le debe dar imágenes de esa persona para

que conozca sus características. Es por esto, que los estudiantes y su padres o tutores tienen que estar conscientes y dar su consentimiento para que se entrene el modelo con sus caras.

Para proteger la privacidad de los estudiantes, el modelo no reconoce las caras por un nombre, si no que lo hace por medio de un ID generado aleatoriamente y que no se puede relacionar directamente con la persona a la que pertenece la cara. Esto quiere decir que el modelo reconocerá al estudiante Jorge Martínez por su id aleatorio (15efggh45) y todas las operaciones que el modelo haga, como guardar su asistencia o las participaciones serán con ese id y no con el nombre real de la persona.

Almacenamiento y seguridad de los datos

Las imágenes y videos se almacenan en servicios de AWS como S3 y los datos de los usuarios se almacenan en una base de datos hosteada en MongoDB. Debido a que se encuentran en la nube, es probable que pueda recibir ataques de terceros para acceder a la información. La ventaja que se tiene es que los proveedores cuentan con bastantes capas de protección para que los datos no sean accedidos.

Por ejemplo, se puede hacer que toda la información de la base de datos esté encriptada y si es accedida por alguien que no debería, aún así no pueda ver la información. También se debe realizar la configuración adecuada para que la base de datos solo pueda ser accedida desde la IP del servidor donde está nuestra página web.

Gestión de accesos

Dentro del sistema, existen cuatro roles principales: los desarrolladores, los administradores, los docentes y los estudiantes. A continuación se lista cada rol y la información a la que tienen acceso.

- Estudiantes: Los estudiantes solamente tienen acceso a ver la información relacionada con sus asistencias, participaciones y cursos.
- Docentes: Los docentes pueden ver la información de los cursos que imparten, como los alumnos que están en ese curso, sus participaciones, asistencias y estadísticas generadas a partir de estos datos.

- Administradores: Los administradores tienen acceso, pueden gestionar y editar la información de los cursos y de los perfiles de los usuarios mencionados anteriormente.

- Desarrolladores: Los desarrolladores tienen acceso a las credenciales necesarias para acceder a todos los servicios de almacenamiento, tanto la base de datos, como las imágenes y videos. De todas formas, solamente tienen acceso a estos datos durante el desarrollo para hacer que el sistema funcione. Por lo tanto, deben firmar un acuerdo para mantener la confidencialidad de los datos y asegurar que sólo los utilizarán para el objetivo del proyecto.

Información para el usuario final

Para que todos los usuarios conozcan estas medidas y para cumplir con las normativas de la ley, se les hará firmar una carta. En esta se les listarán todos los mecanismos que se siguen para mantener la privacidad de sus datos, así como informarles del uso que se le dará a estos datos.

Las cartas de consentimiento deberán ser firmadas por los estudiantes, sus padres o tutores y los docentes, ya que son los usuarios de los que se almacenará información.

Bibliografía

INAI, (2021). *Normativa y legislación en PDP.* México: INAI. https://micrositios.inai.org.mx/marcocompetencias/?page_id=370