Deusto
Facultad de Ingeniería
Ingeniaritza Fakultatea

Grado en Ingeniería Informática

Informatikako Ingeniaritzako gradua

Proyecto fin de grado

Gradu amaierako proiektua

Estudio sobre la privacidad en el aprendizaje federado mediante el desarrollo de un sistema de recomendación online

Ibai Guilén Pacho

Director: Diego Casado Mansilla

Bilbao, mayo de 2021

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Objetivos y Alcance

1.1. Obejetivos

Los objetivos de este proyecto pueden clasificarse en varios grupos. Por un lado están los objetivos generales, objetivos que a simple vista no tienen hitos específicos para en qué estado se encuentran y si se han cumplido o no.

Por otro lado se encuentran los objetivos específicos, estos, al contrario que los generales, son hitos específicos fácilmente identificables que permiten saber si la tarea se ha completado, y en caso contrario saber en qué estado se encuentra la tarea. Dentro de este grupo se encuentran los objetivos específicos de desarrollo, apartado donde se agrupan los objetivos que permiten saber en qué estado de desarrollo se encuentra el proyecto y que funcionalidades incorpora. Pero además, también se encuentran los objetivos de estudio, donde se incluyen los objetivos que tienen que ver con el estudio de los diferentes experimentos que se realizarán.

1.1.1. Generales

El objetivo general de este proyecto es el de desarrollar un sistema de recomendaciones online basado en federated learning. Este sistema se desarrollará sobre un sistema de recomendaciones ya existente basado en Machine Learning y deberá adaptarlo para su correcto funcionamiento con información descentralizada.

Para respetar la privacidad y derechos de los usuarios el proyecto deberá incluir la privacidad como patrón de diseño, cumpliendo tanto con las normativas vigentes en Europa y España,como con las posibles nuevas medidas que entren en vigor en un futuro.

Por último, el sistema deberá asegurar que la información se quede en el dispositivo y no se comparta ninguna información que no sea la del propio modelo desarrollado por el participante de la red.

1.1.2. Específicos

Los objetivos específicos son fácilmente reconocibles y concretos, lo que permite saber con exactitud cuando se han cumplido los objetivos y cuando no.

1.1.2.1. De desarrollo

Los objetivos de desarrollo tienen que ver con el correcto desarrollo del sistema de recomendación basado en federated learning.

Parametrización y configuración: Se tendrán que configurar las plataformas de desarrollo para poder ejecutar el sistema de recomendación centralizado con mayor rapidez y agilizar el desarrollo del proyecto. También se tendrán que configurar las Raspberries y la Jetson Nano, aprovisionarlas del software necesario para ejecutar en ellas el sistema de recomendación y ejecutarlo sin problemas.

Desarrollo: Se desarrollarán todas las características de los sistemas de recomendación derivadas de la fase de investigación.

1.1.2.2. De investigación

Los objetivos de investigación, al contrario que los de desarrollo, tienen que ver con la búsqueda de soluciones a las incógnitas del proyecto. Es decir, suplir las limitaciones derivadas del federated learning, además de la formación del propio alumno en esta tecnología.

Formación: El alumno deberá formarse en conocimientos sobre Inteligencia Artificial para poder comprender los conceptos. También deberá familiarizarse con el código del sistema de recomendación para poder realizar las modificaciones pertinentes en él. Además, el alumno deberá leer artículos científicos sobre federated learning para comenzar a investigar las soluciones a los problemas derivados del proyecto.

Sistema de recomendación: Se deberá investigar la forma de combinar modelos de IA de cada Raspberry. Además, se investigarán y realizarán las modificaciones pertinentes en el sistema de recomendación para cumplir los siguientes puntos:

- Que sea capaz de obtener las recomendaciones para un único usuario en concreto.
- Que sea capaz de guardar y cargar los modelos entrenados de LightFM.
- Que el modelo de LightFM sea capaz de admitir aprendizaje incremental.

1.1.2.3. De estudio

Los objetivos de estudio tienen que ver con el análisis de los resultados del sistema de recomendación basado desarrollado sobre federated learning.

Análisis: El estudio del sistema deberá analizar la diferencia de rendimiento entre el sistema de recomendación con información centralizada y distribuida. Y analizar cómo afectan los distintos modelos y su combinación al rendimiento del sistema de recomendación.

Privacidad: Hay que valorar y analizar la privacidad y seguridad de los datos personales de los usuarios tanto en el modelo central, como en el distribuido. Se deberán evitar los problemas de seguridad y privacidad implícitos de la implementación de un sistema de recomendación basado en federated learning

1.2. Alcance

En el alcance se centra en concretar qué objetivos entran en el desarrollo del proyecto y cuáles no. Para ello se ha dividido este apartado en dos grupos, los objetivos y tareas que entran en el alcance del proyecto y los que no. La segregación en estos grupos nos permite concretar con más precisión los límites del proyecto, evitando que el proyecto se amplíe más allá de sus límites.

1.2.1. Dentro del alcance

Entran dentro del alcance los objetivos y tareas derivadas del desarrollo de un sistema de recomendación basado en federated learning, tanto las tareas de parametrización y configuración del hardware como el desarrollo de software. Esto incluye todos los objetivos específicos de desarrollo mencionados en el apartado anterior.

Del mismo modo quedan dentro del alcance los objetivos de investigación del apartado anterior, ya que son indispensables para el correcto desarrollo del sistema de recomendación

También se incluye el estudio y análisis de los resultados del sistema de recomendación, así como su precisión y sus inconvenientes, es decir, todo lo comentado en los objetivos específicos de estudio.

Para finalizar se incluirá un estudio de la estabilidad legal del sistema en el tiempo. Esto incluye la corroboración del cumplimiento de las actuales medidas de protección de datos y el estudio de las posibles futuras medidas, legislaciones y derechos que limiten el uso de información en Europa.

Todo esto quedará recogido en la memoria técnica del proyecto que será entregada como proyecto fin de grado.

1.2.2. Fuera del alcance

Fuera del alcance queda cualquier estudio de mercado sobre si la solución sería viable económicamente además de cualquier estudio de alternativas a federated learning.

No se incluirá ni se recogerá ninguna legislación fuera del marco jurídico Español y del Ordenamiento jurídico de la Unión Europea. Lo que deja fuera del alcance cualquier derecho, legislación o restricción de cualquier estado u organización ajeno a los comentados.

Queda fuera del alcance también la encriptación de las comunicaciones entre los diferentes dispositivos.

Capítulo 2

Metodología

2.1. Metodología