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

Antecedentes y justificación

1.1. Antecedentes

Este proyecto parte del proyecto de R.Sánchez[1] donde se desarrolló un sistema de recomendación de estrategias de persuasión basado en aprendizaje activo. Para comprender los antecedentes que han incurrido en el desarrollo de este proyecto primeró hay que conocer y comprender qué son los sistemas de recomendación y después entender los problemas de seguridad y privacidad que van ligados a estos.

1.1.1. Sistemas de recomendación

Los sistemas de recomendación fueron mencionados por primera vez en los años 90 y han ido evolucionando hasta estar implantados en gran parte de las empresas actuales. Estos sistemas son sistemas de filtrado de información, que partiendo de una gran cantidad de datos, tanto del usuario como de los elementos a recomendar, pueden predecir cuál será el elemento más apropiado para el usuario. Estos sistemas están estrechamente relacionados con el marketing, ya que el objetivo es conseguir recomendar un elemento que sea del agrado e interés de los usuarios suele ir ligado a fines económicos.

Hoy en día se usan en multitud de ámbitos, desde las redes sociales hasta las distribuidoras de contenido como Netflix, pasando por compañías de comercio electrónico como Amazon.

A la hora de realizar la recomendación se realizan filtrados de diferente tipo, estos no son más que la forma en la que el sistema busca correlacionar los usuarios con los elementos que estos consumen, compran o ven. Entre los métodos más comunes

para relacionar esta información y obtener resultados eficientes se encuentran:

- Filtros demográficos, que recomiendan en función del sexo, edad, país, oficio,...
- Filtros basados en contenidos, como Youtube, que recomiendan contenidos similares a los valorados por los usuarios.
- Filtrado colaborativo, que consiste en recomendar al usuario elementos valorados positivamente por usuarios similares a él.

Sin embargo, existen sistemas híbridos que utilizan varias de las estrategias de filtrado anteriores combinadas. Un ejemplo de ello es el mencionado Amazon, que tiene uno de los algoritmos de recomendación más potentes y eficientes actualmente.

Sin embargo, existen sistemas híbridos que utilizan varias de las estrategias de filtrado anteriores combinadas. Un ejemplo de ello es el mencionado Amazon, que tiene uno de los algoritmos de recomendación más potentes y eficientes actualmente.

Esto se debe a dos cosas, en primer lugar que cuenta con una gran cantidad de información de los usuarios, tanto su edad, género, país, dirección, rutinas (si tienen Alexa), ... como los artículos que miran, compran, añaden a la lista, etc. Con todo esto el algoritmo es capaz de ofrecer recomendaciones muy precisas a los usuarios, lo que le da una gran calidad de servicio a la empresa gracias a esto.

De hecho, en Amazon, si queremos revisar las recomendaciones tenemos un apartado propio para ellas al que se puede acceder fácilmente (Fig1.1).

Fig. 1.1: Recomendaciones de Amazon (Fuente: Amazon[2])

1.1.2. Privacidad digital

Queda claro que un sistema de recomendación depende plenamente de la información de la que dispone, de forma que, de cuanta más información disponga de los usuarios, más precisión tendrá en sus predicciones. Para obtener esta información muchos anunciantes se han valido de diversas herramientas y utilidades, pero si se ha de destacar alguna son las cookies de terceros. Estas, son definidas por Google[**ComoBorrarHabilitar**] cómo:

> *"... son archivos que crean los sitios web que visitas para guardar información de la navegación y facilitar tu experiencia en línea. Gracias a las cookies, los sitios pueden mantener abierta tu sesión, recordar tus preferencias del sitio y proporcionarte contenido relevante en función del lugar donde te encuentres. Hay dos tipos de cookies:*
>
> - *Las cookies de origen, que las crea el sitio que visitas. El sitio se muestra en la barra de direcciones.*
> - *Las cookies de terceros, que las crean otros sitios. Parte del contenido que ves en la página web que visitas, como anuncios o imágenes, pertenece a estos sitios."*

A simple vista estas cookies parecen inofensivas, pero el problema radica en su utilización. Aunque suelen ser usadas con fines analíticos por compañías de marketing online, estas se usan para registrar el comportamiento de un usuario y crear un perfil para generar publicidad personalizada. Mediante estas se puede registrar el comportamiento de un usuario en internet, saber sus movimientos, hábitos, páginas que visita, edad, sexo, etc.

En España y en la Unión Europea existe una legislación sobre la privacidad y la protección de datos que restringe y limita los datos que estas empresas pueden registrar de nuestra navegación, el Reglamento General De Protección de Datos (RGPD). En el documento adjunto Anexo A, sección A.2 se puede consultar un breve resumen de la legislación en vigor. En lo referente a las cookies este reglamento presenta varios elementos importantes. En primer lugar, debe haber un consentimiento explicito por el usuario en el consentimiento de la política de cookies. En segundo lugar, la aceptación de las cookies de terceros no ha de ser un impedimento para el uso del servicio. En último lugar, todas las cookies y rastreadores que operen en la web del propietario deberán ser mostradas al usuario en un lenguaje sencillo.

De todos modos esta legislación no impide que se realice un perfilado del usua-

rio, que se haga un seguimiento de este por la red o que se analice el tiempo que pasa el usuario en la página. Pero con la maduración de la tecnología cada vez más gente se preocupa por el uso que le dan estas empresas a los datos y son más críticos con estas prácticas. Esto ha llegado incluso a la política, donde España esta desarrollando una carta pionera de derechos digitales, donde, entre otras cosas, recoge el derecho de los usuarios a no ser perfilados (Anexo A, sección A.3).

Hoy en día existen muchos navegadores y complementos que permiten bloquear este tipo de rastreadores, lo que ha llevado al sector y a Google a tener que explorar nuevas vías para obtener esta información. La solución propuesta por Google ha sido su nuevo sistema Federated Learning of Cohorts, aprendizaje federado de cortes, con el que se compromete a dejar las cookies de terceros.

Lo que a priori puede significar una buena noticia no es para nada la realidad. Este sistema permite a Google y a su navegador agrupar usuarios en base a sus intereses y perfiles geográficos gracias al historial de navegación y a los datos recogidos durante la navegación. Aunque permite que los usuarios no puedan ser distinguidos dentro de un grupo este perfilado supone una persecución y rastreo más grave que la acaecida por las cookies de terceros. En primer lugar, sitúa a Google como principal proveedor de marketing digital, lo que afectaría tanto a las funciones que podrían desempeñar las empresas de marketing digital como al precio que tendrían que pagar por la información.

Ante esta imposición de Google varias empresas se han pronunciado y han expresado su total desacuerdo con la política, navegadores como DuckDuckGo o Brave la han calificado de anticompetitiva, invasiva y abusiva. Esto se debe a que el navegador de Google, Google Chrome, acapara el 64.19 %[1] de la red y podría obligar a utilizar su sistema a muchos anunciantes y sitios web.

Cabe destacar que este sistema aun no ha sido aprobado por la Unión Europea, para ello se debe comprobar que cumpla el RGPD y no vulnere ningún derecho de los ciudadanos.

[1]Fuente: https://gs.statcounter.com/, 27/04/2021

1.2. Justificación

Este proyecto es una respuesta a todo lo anterior,al estado de la industria del marketing digital, donde se exprimen al máximo las leyes y normas sobre protección de datos y privacidad digital, y a la actitud de las grandes empresas por perfilar a los usuarios y recoger tanta información de estos como les sea posible. Se quiere demostrar que se puede utilizar el aprendizaje federado preservando la privacidad de los usuarios en un sistema de recomendación, permitiéndoles tener el control total sobre su información en su propio dispositivo.

Además, para ello se utilizarán dispositivos como las Raspberry Pis, las cuales servirán para demostrar que no se necesitan dispositivos especialmente potentes para participar en una red de aprendizaje federado. Evidenciando que es posible implementar un sistema de recomendación respetuoso con el usuario, acorde al RGPD y salvaguardando los derechos digitales.

Capítulo 2

Objetivos y Alcance

2.1. Objetivos

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 de los que no se puede saber su estado o si se han cumplido o no.

Por otro lado se encuentran los objetivos específicos. Estos, al contrario que los generales, son fácilmente identificables, ya que permiten saber si la tarea se ha completado, y en caso contrario, saber en qué estado se encuentra dicha 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 qué 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.

2.1.1. 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 otro sistema de recomendaciones ya existente basado en Machine Learning, y se deberá adaptar 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.

Una vez desarrollado implementado el aprendizaje federado se estudiará la diferencia con el sistema de recomendación centralizado, privacidad, seguridad, eficiencia, etc.

2.1.2. Específicos

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

2.1.2.1. 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.

2.1.2.2. 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 tendrá que 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.

2.1.2.3. De estudio

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

Análisis: El estudio del sistema tendrá que analizar la diferencia de rendimiento entre el sistema de recomendación con información centralizada y distribuida. También tendrá que 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

2.2. Alcance

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 se amplíe más allá de sus límites.

2.2.1. 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.

Se recogera el desarrollo de todo el proyecto en la memoria técnica que será entregada como proyecto fin de grado.

2.2.2. 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 3

Metodología

La metodología es un factor muy importante de este proyecto, es la hoja de ruta a seguir, y por ello hay que definirla con precisión y saber cuál es la más apropiada.

3.1. Consideraciones

Debido a los objetivos mencionados en el apartado correspondiente anterior, queda claro que existen varios tipos de objetivos en el proyecto. La metodología deberá ayudar a cumplir todos los objetivos específicos para cumplir los objetivos generales. Sin embargo, dentro de los específicos se puede observar que coexisten tres tipos diferentes: de desarrollo, de investigación y de estudio.

Es difícil utilizar una misma metodología para el correcto desarrollo de los tres objetivos, ya que pertenecen a distintas disciplinas, así pues, se ha optado por combinar distintas metodologías para ello. De esta forma se consigue conducir todos los objetivos en una misma dirección. Las metodologías que se combinarán serán:

- Metodología Cuantitativa, metodología de investigación.
- Modelo espiral, metodología de desarrollo de software.

3.2. Metodología de Investigación

La metodología cuantitativa es una metodología de investigación que se centra en la recopilación y el análisis de los datos, lo que nos servirá como guía para los objetivos de estudio y el análisis de los resultados de los experimentos.

Esta metodología dice que se deben llevar a cabo varias fases de las que solo se realizarán las siguientes tres:

1. Definir claramente el problema y lo que se quiere hacer.
2. Delimitar el problema, concretar el alcance de la investigación.
3. Revisión de la literatura, buscar los conocimientos necesarios para realizar el estudio.

Después de haber realizado las tres fases de la metodología de la investigación se aplicará la investigación empírica al estudio, ya que encaja perfectamente con el planteamiento de este proyecto. Esta forma de investigación es una forma de obtener conocimiento a través de la observación o experiencia. Además, mediante este método se nos incita a probar distintos experimentos y modificaciones de estos con el objetivo de encontrar resultados diferentes.

Para aplicar esta metodología se usará Ciclo empírico de A.D. de Groot (Fig.3.1). Este ciclo nos ayuda a ordenar y entender las fases del proyecto, a conocer los siguientes pasos y a no perdernos.

En el primer paso se encuentra la observación. Como el alumno ya ha adquirido la formación en el apartado tres de la metodología cuantitativa podrá empezar observando cómo funciona el sistema de recomendación. A medida que se den más vueltas al modelo, esta observación se realizará sobre los resultados de los experimentos a la hora de aplicar federated learning.

En el segundo paso, el de inducción, se plantean las ideas o hipótesis acerca del paso de observación. En la primera vuelta, estas hipótesis e ideas serán sobre lo que ha aprendido el alumno y sobre cómo se aplicará el federated learning al proyecto. En las demás vueltas serán sobre los resultados observados y cómo estos afectan al proyecto y al estudio y qué mejoras podrían realizarse.

Tanto la fase de deducción, donde se formulan los experimentos y pruebas a realizar, como la de pruebas, donde se realizan los experimentos para probar las hipótesis y recopilar datos, se sustituirán por la metodología de desarrollo de software en espiral. De esta forma, el modelo del ciclo empírico quedaría combinado con el de espiral para que la investigación y los experimentos que se están realizando mediante software sean concretos y tengan una correcta gestión (véase fig.3.3).

En el paso de evaluación, se interpretan los resultados de los experimentos de los anteriores dos pasos. En este apartado se hará un gran uso de la estadística para mostrar la información, tanto gráfica como analiticamente.

Se pueden realizar tantas vueltas al ciclo empírico como sean necesarias.

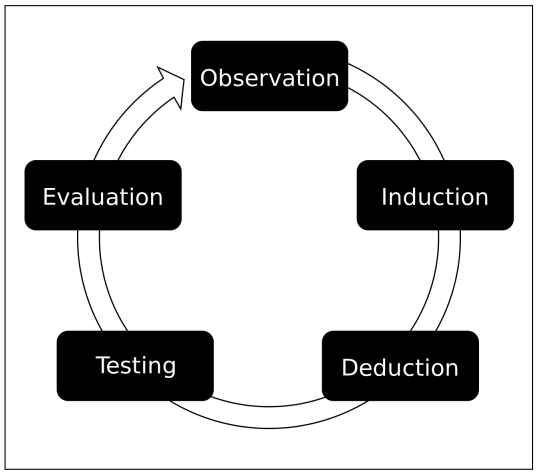

Fig. 3.1: Ciclo empírico de A.D. de Groot (Fuente: Wikipedia[3])

3.3. Metodología de desarrollo

El modelo en espiral (Fig.3.2) formará parte del ya mencionado Ciclo empírico y agrupará los pasos de formulación de los experimentos y su ejecución. Se ha optado por incluir esta metodología dentro de otra para detallar más profundamente cómo será el proceso de desarrollo de software derivado de la investigación realizada.

Se ha elegido este modelo entre otros por varias razones importantes:

- Define claramente lo que es un ciclo completo, los pasos a dar y las tareas a realizar. También fija los objetivos al inicio de cada ciclo de la espiral, lo que unido al paso de inducción del ciclo empírico implica que se definen objetivos claros y concisos sobre las hipótesis planteadas.
- Al ser un modelo continuo, se pueden realizar tantas iteraciones sobre la espiral como se necesiten, permitiendo desarrollar tantos experimentos como hipótesis se plantean en el apartado de inducción del ciclo empírico. Además, cada vuelta de la espiral incluye el desarrollo de prototipos (lo que en este caso sería un experimento), que al contar con una fase de integración consigue que puedan coexistir todos en el mismo entorno de desarrollo.

- Cumple con las fases de Deducción y Testeo del ciclo empírico ya que incluye los pasos de estas en la fase de desarrollo de la espiral.

- Por último y más importante, se ha elegido esta metodología porque tiene en cuenta la gestión y análisis de riesgos. Esto tiene gran importancia al tratarse de un proyecto complejo con múltiples dispositivos y tanta cantidad de pruebas a realizar.

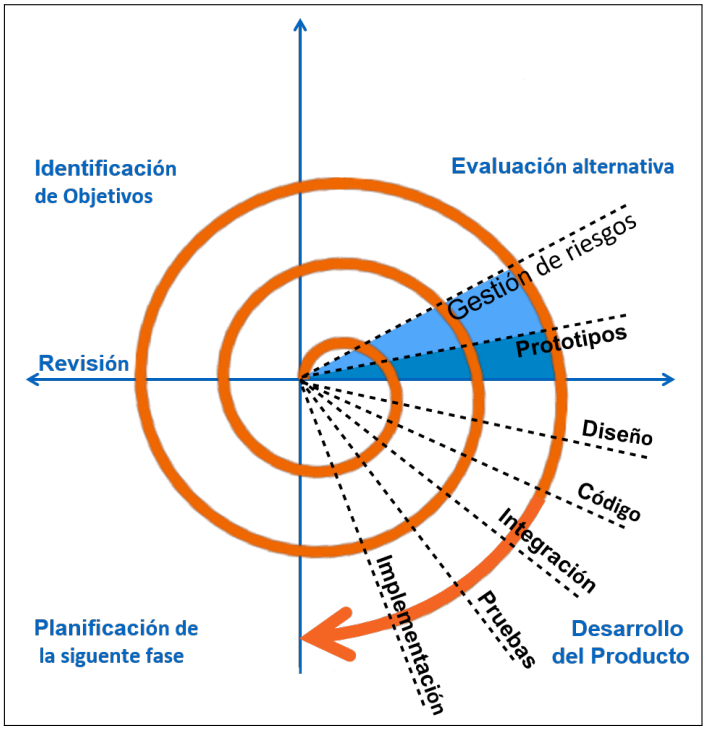

Fig. 3.2: Modelo en el Espiral, Autor Desconocido (Fuente: Blog[4])

3.4. Conclusión

Partiendo del ciclo empírico, escisión de la metodología de investigación cuantitativa, se hará especial incapié en la continua reflexión y teorización sobre el modelo de fededrated learning implantado.

Para el correcto desarrollo del software, las anteriormente mencionadas fases de deducción y testeo serán incluidas en el modelo de la espiral, consiguiendo así, una gestión eficiente y precisa sobre los pasos a dar tanto en investigación como en el desarrollo de software.

Como se ha comentado anteriormente, la agrupación de estas dos metodologías permitirá combinar la investigación con el desarrollo de software, descubriendo a base de prueba y error y a base de analizar los resultados las mejores soluciones para el sistema de recomendación basado en federated learning.

Por lo cual, una vez el alumno haya definido claramente el problema, su alcance y se haya formado en la tecnología, podrá comenzar a utilizar el ciclo presente en la figura 3.3.

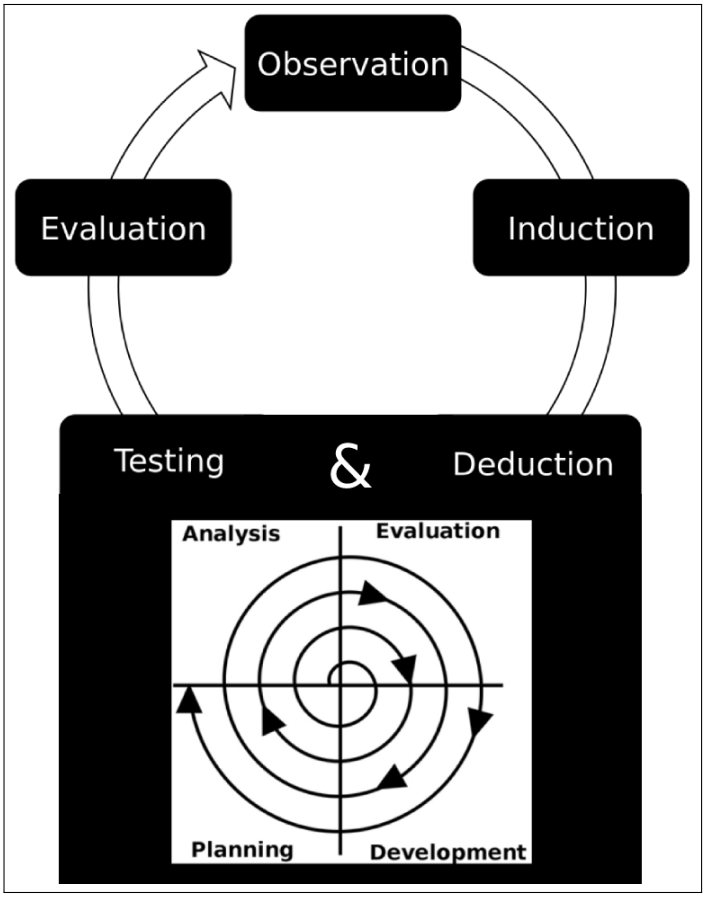

Fig. 3.3: Metodología de trabajo del proyecto final de grado (Autor: Ibai Guillén)

Capítulo 4

Planificación

La planificación de este proyecto se ha realizado con un diagrama GANTT. Este esta presente en la tabla 4.1, en caso de querer observar la tabla a una escala mayor esta se encuentra en el anexo B sección B.1.

La planificación de este proyecto es un proceso complejo que ha de contener todos los pasos necesarios para conseguir el objetivo del estudio. Para ello se ha dividido en 4 fases de 3 semanas, empezando la primera el 22 de Febrero de 2021 y terminando la ultima fase el 16 de mayo de 2021.

Las tareas de este proyecto se han agrupado en varios grupos:

- El registro del proyecto.
- La formación.
- Configuración del hardware.
- Adaptación del sistema de recomendación online a aprendizaje federado.
- Desarrollo de la memoria.
- Estudio del rendimiento

A su vez, estos grupos cuentan con subtareas más concretas que permiten programar adecuadamente la duración del proyecto.

- El registro del proyecto.
    - ◇ Definición de título y descripción.
    - ◇ Registro del proyecto a través del formulario.

- La formación.
  - ◇ Formación sobre conceptos de Machine Learning.
  - ◇ Formación sobre conceptos de los sistemas de recomendación.
  - ◇ Formación sobre conceptos de Federated Learning.
  - ◇ Formación sobre LightFM.
  - ◇ Familiarización con el sistema de recomendación de R.Sánchez.
- Configuración del hardware.
  - ◇ Configuración de las RaspBerrys.
  - ◇ Configuración de la JetsonNano.
  - ◇ Aprovisionamiento de los Sistemas Operativos.
  - ◇ Instalar y ejecutar sistema de recomendaciones.
- Adaptación del sistema de recomendación online a aprendizaje federado.
  - ◇ Guardado , cargado y envío de modelos de inteligencia artificial.
  - ◇ Agregación de los modelos de inteligencia artificial.
  - ◇ Recomendación para un único usuario.
  - ◇ Combinar recomendaciones para un único usuario.
  - ◇ Combinar recomendaciones para varios usuario.
  - ◇ Reentrenar modelos.
  - ◇ Visualización de los resultados de rendimiento por gráficas.
- Desarrollo de la memoria.
  - ◇ Resumen.
  - ◇ Introducción.
  - ◇ Antecedentes y Justificación.
  - ◇ Objetivos y Alcance.
  - ◇ Consideraciones éticas.
  - ◇ Metodología.
  - ◇ Planificación.
  - ◇ Introducción al Federated Learning.

    - ◇ Desarrollo.
    - ◇ Presupuesto.
    - ◇ Conclusiones y Trabajo futuro.
    - ◇ Bibliografía.
    - ◇ Definiciones y Acrónimos.
    - ◇ Anexos.
- Estudio del rendimiento.
    - ◇ Estudio del rendimiento de un sistema de recomendaciones centralizado.
    - ◇ Estudio del rendimiento de un sistema de recomendaciones de modelos agregados.
    - ◇ Estudio de rendimiento del sistemas de recomendaciones final.

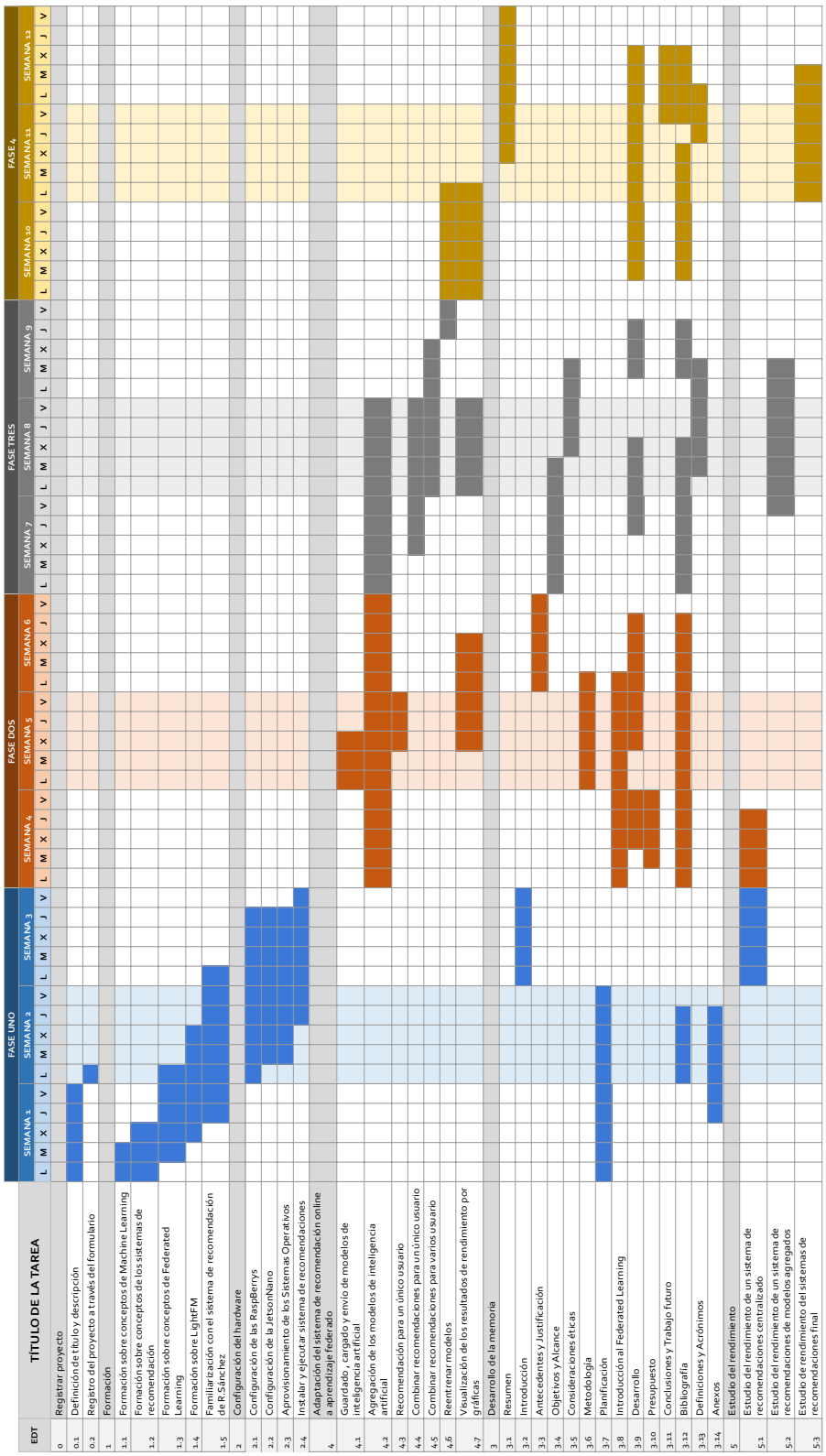

Tabla 4.1: Planificación del proyecto

Capítulo 5

Introducción al Federated Learning

Es de gran importancia comprender y conocer lo que es el Federated Learning para entender tanto el desarrollo, como la resolución de los problemas y retos que supone su implementación, por eso, en el presente apartado se explicará a conciencia de que se trata esta tecnología.

5.1. Información general

El aprendizaje federado, es una técnica de aprendizaje automático que entrena un algoritmo a través de diversos dispositivos descentralizados, manteniendo siempre la información en cada uno de ellos (Fig5.1). El algoritmo que se busca entrenar en los dispositivos puede ser de cualquier tipo dentro del campo del aprendizaje automático, redes neuronales artificiales, aprendizaje profundo, árbol de decisión, etc. Por lo cual, se puede decir que el aprendizaje federado es una tecnología habilitadora para el entrenamiento de modelos de aprendizaje automático en redes de dispositivos.

Al contrario del aprendizaje automático convencional que reúne toda la información en un mismo computador, el aprendizaje federado busca entrenar un algoritmo en cada uno de los dispositivos que participen en la red, para luego combinarlos y conseguir un modelo de aprendizaje robusto. Los dispositivos que forman parte de esta red son denominados participantes y todos ellos forman la denominada como red de aprendizaje colaborativo. En esta red, todos aprenden de todos sin necesidad de compartir su información, consiguiendo mejorar la precisión y eficacia del algoritmo.

Esta red permite repartir la carga de trabajo entre todos los participantes, pues-

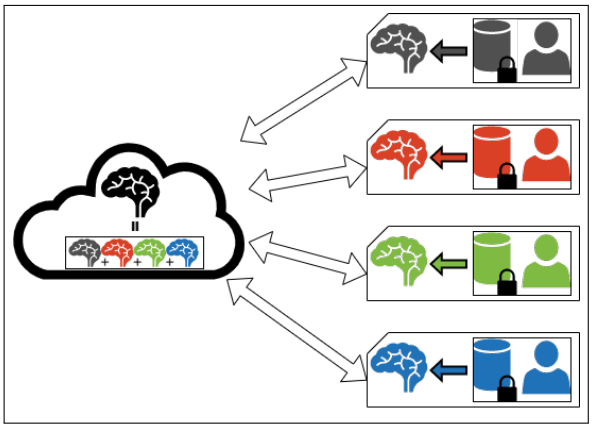

Fig. 5.1: Diagrama de una red de Federated Learning

to que cada uno se encarga de entrenar su propio modelo. Esto es posible gracias a que cada vez los dispositivos móviles tienen procesadores más rápidos y más potentes, lo que permite que sean capaces de realizar tareas más complejas y pesadas. De esta forma, se consigue que cada dispositivo sea propietario exclusivo de su información y no tenga que compartirla con ningún otro. Además, hoy en día los costes de comunicación son superiores a los de computación, por lo que cuanto más acciones se puedan computar en los dispositivos de los participantes menor será el consumo del entrenamiento del algoritmo.

Sin embargo, debido a estas características propias del aprendizaje federado también sufre de grandes inconvenientes. El hecho de que la red está formada por diferentes participantes la hace heterogénea, con diferentes capacidades de cómputo y diferentes velocidades de conexión entre los distintos participantes, lo que puede incurrir en desconexiones o pérdidas de paquetes durante el proceso de aprendizaje.

5.2. Fundamentos y Protocolo

En general existen dos tipos de entidades en los sistemas de Federated Learning, los propietarios de la información (participantes de la red) y el propietario del modelo (servidor de Federated Learning). Los propietarios de la información entrenan localmente el modelo con la información de la que disponen, mientras que el propietario del modelo agrega los diferentes modelos recibidos de los participantes para mejorar el algoritmo.

La comunicación puede ser llevada a cabo de diferentes maneras, de hecho, hay diseños de protocolos de aprendizaje federado como el desarrollado por los autores

del trabajo [5], que lo dividen en 3 fases:

- Selección de los participantes: El servidor elige un grupo de dispositivos conectados para participar en la red.
- Configuración: El servidor se configura en base al mecanismo de agregación definido y envía a los participantes el modelo global.
- Reporte: El servidor recibe la actualización de cada modelo de su respectivo participante. Más tarde los agrega usando el algoritmo elegido.

Además, estos autores definen un parámetro de población con el objetivo de limitar el acceso en caso de que haya muchos participantes, evitando que se conecten a la vez y saturen la red.

5.3. Problemas presentes

Como se ha mencionado antes, implementar el aprendizaje federado implica problemas y costes que hay que asumir y tratar con el objetivo de crear un sistema eficiente y estable.

Cada actualización del modelo conlleva millones de parámetros, además se llevan tantas actualizaciones a cabo como precisión se quiera en el modelo. La gran dimensión de las actualizaciones puede incurrir en un aumento de los costes de conexión y generar un cuello de botella que puede verse agravado por los participantes, ya sea por la asimetría en las velocidades de internet o por la asimetría en la capacidad de cómputo. Es por eso, que para mejorar el rendimiento y reducir el coste de comunicación se deben considerar varias cosas.

- En primer lugar, todos los dispositivos deben contar con una conexión estable, preferiblemente conexión por cable, o en su defecto conexión inalámbrica por Wi-Fi, descartando por completo todas aquellas conexiones por telefonía móvil.
- En segundo lugar, para minimizar el número de rondas de comunicación se puede realizar computación adicional en los dispositivos para que la agregación global se realice antes.
- También se puede reducir el tamaño de las comunicaciones, ya sea por compresión del modelo, compresión de los datos, o por el uso de una pequeña muestra representativa de estos en vez de enviarlos por completo.

- Por último, se pueden minimizar las actualizaciones de los modelos en base a la importancia de estas. Evitando enviar el modelo global hasta que este no suponga una clara mejora para los participantes.

Capítulo 6

Desarrollo

6.1. Requisitos del sistema

Como bien se ha mencionado previamente, este proyecto trata de adaptar el sistema de recomendación realizado por R.Sánchez [1] a un sistema de recomendación basado en Federated Learning que permita el aprendizaje colaborativo de los participantes. Es por ello que para conocer los requisitos iniciales de diseño del sistema de recomendación se remite al trabajo del autor.

En este apartado se presentarán únicamente los requisitos de la adaptación del sistema y se partirá del trabajo realizado por R.Sánchez. Se presentarán dos tipos de requisitos. En primer lugar los requisitos no funcionales de diseño, las condiciones que debe cumplir la especificación del diseño para cumplir los objetivos del proyecto. En segundo lugar, los requisitos funcionales, las condiciones que ha de cumplir el sistema para ser capaz de funcionar sobre el hardware del que se dispone.

6.1.1. No Funcionales

En cuanto a los requisitos no funcionales se encuentran todos aquellos que se han tenido en cuenta a la hora de plantear el diseño del sistema, es decir, todos los inherentes de la privacidad como patrón de diseño. Por ello el sistema :

RNF1 Mantendrá toda información de los usuarios en sus dispositivos.

RNF2 No expondrá la información de los modelos de inteligencia de los usuarios a otros usuarios.

RNF3 No discriminará entre los modelos de inteligencia artificial a la hora de tomar decisiones.

RNF4 No perjudicará deliberadamente al modelo de un participante.

RNF5 No compartirá información que no sea sintética.

RNF6 No extraerá información de los modelos de los participantes.

RNF7 Combinará los diferentes modelos de los participantes sin acceder a su información.

RNF8 Cumplirá tanto con la LOPD-GDD como con el RGPD (véase ApéndiceA, sección A.2).

RNF9 Respetar los derechos digitales de los usuarios y cumplir con la carta de derechos digitales de España (véase ApéndiceA, sección A.3).

6.1.2. Funcionales

Los requisitos funcionales son básicos en este proyecto para que el sistema sea compatible y ejecutable en el hardware. Por ello, para que el sistema sea compatible con el harware se han definido los siguientes requisitos:

RF1 El sistema ha de ser ejecutable bajo la arquitectura ARMv8.

RF2 El sistema ha de ser ejecutable bajo la arquitectura x86 y x64.

RF3 El sistema ha de ser ejecutable bajo la arquitectura AArch64.

RF4 El sistema ha de ser ejecutable en Linux.

RF5 El sistema ha de ser ejecutable en Windows.

Además, al margen de los requisitos de compatibilidad también se encuentran los requisitos de recursos, y es que teniendo un hardware poco potente es imprescindible que el software sea lo más óptimo posible para aprovecharlo al máximo. Es por eso que también se definen los siguientes requisitos:

RF6 El sistema ha de ser capaz de entrenar los modelos en un espacio de tiempo razonable, siendo este siempre inferior a los 100 segundos por cada 10 epochs.

RF7 El sistema de recomendación no puede colapsar el dispositivo que lo ejecute,

RF8 El sistema de recomendación debe permitir que el dispositivo pueda funcionar con normalidad durante su ejecución.

6.2. Gestión de riesgos

El motivo de esta sección viene de la definición del modelo en espiral como metodología clave para el desarrollo de este proyecto. Este modelo recoge la identificación y gestión de riesgos como pieza fundamental del ciclo de vida, y en un proyecto con tal complejidad técnica y con tantos dispositivos involucrados, es indispensable tener un plan de acción ante cualquier incidente.

Con tantos dispositivos que gestionar, el proceso de configuración de estos puede llegar a ser algo pesado, y más si alguno de estos falla o se rompe. Si se rompiese o se corrompiese una tarjeta SD de una Raspberry Pi habría que reinstalar y configurar todos los paquetes a mano, proceso que puede ser bastante largo puesto que requiere de interacción humana. Para evitar esto se ha tomado la dedcisión de crear un script de aprovisionamiento tanto para la Nvidia Jetson Nano como para las Raspberry Pis, de esta manera, en caso de que una tarjeta SD se averiase, bastaría con cambiarla, configurar el protocolo SSH para acceder remotamente a ella y ejecutar el script. Cuando el proceso terminase el dispositivo estaría listo para poder ejecutar el proyecto sin ningún problema.

Las tareas de inteligencia Artificial no son especialmente livianas para un dispositivo, lo que durante un entrenamiento prolongado en el tiempo podría incurrir en un aumento de temperatura de este. Para evitar que los dispositivos alcancen temperaturas elevadas o que sufran cualquier tipo de cortocircuito por su manipulación inadecuada se ha optado por instalarlos en un rack (Fig 6.1). Esta carcasa aparte de proteger los dispositivos viene equipada con ventiladores que ayudaran a que la temperatura de estos sea siempre la adecuada.

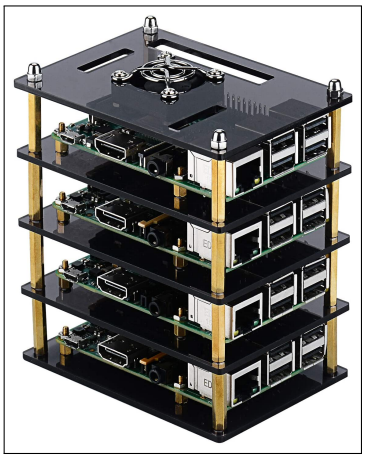

Fig. 6.1: Rack para Raspberry Pi (Fuente: Amazon[6])

Durante el desarrollo se tiene que acceder a estos dispositivos en multitud de ocasiones, para ello se utiliza el protocolo SSH. Sin embargo, al realizarse este proyecto en un ámbito doméstico, existe la probabilidad de que el router sea reiniciado o apagado por cualquier causa externa al proyecto. En tal caso puede que las direcciones IP sean sustituidas y haya que realizar un análisis de la red o acceder fisicamente a estos dispositivos para averiguar la IP. Para evitar este proceso se ha instalado el paquete *AVAHI*[1] que permite acceder mediante SSH a las raspberrys sustituyendo la dirección IP por el nombre de servidor de los dispositivos.

Para gestionar los cambios que se irán haciendo sobre el software sin problemas es indispensable contar con herramientas de control de versiones. Estas herramientas permiten gestionar cuándo se han realizado qué cambios y en caso de necesitarse se podrían revertir con facilidad. En este caso, tanto para el desarrollo del proyecto como para el desarrollo de la memoria se utilizará Git como controlador de versiones. Además, se utilizará Github como repositorio de código en la nube, para así poder clonar el repositorio a los dispositivos facilmente.

6.3. Especificación del diseño

Teniendo en cuenta los anteriores requisitos y los objetivos del proyecto la especificación del diseño concretará como se han diseñado las diferentes funcionalidades y como se ha implementado el Federated Learning en el proyecto.

6.3.1. Instalación de los requisitos en el hardware

6.4. Tecnologías utilizadas

6.4.1. Sistema de recomendación

El sistema de recomendación de R.Sánchez utiliza LightFM[2] para crear los modelos de inteligencia artificial. Para implementar el aprendizaje federado se ha tenido que modificar gran parte del sistema de recomendación previo y se ha tenido que hacer uso de las utilidades que proporciona LightFM que se van a explicar en los siguientes apartados.

[1] AVAHI es un servicio que facilita el descubrimiento de dispositivos en la red local a través de mDNS/DNS-SD.

[2] LightFM es una implementación en python de varios algoritmos populares de recomendación.

6.4.1.1. Creación del modelo

El paso de creación del modelo es un paso complejo puesto que conlleva la correcta gestión de muchos datos e información. Asimismo, estos datos han de estar correctamente estructurados y construidos, puesto que LightFM requiere que la información este convertida a matrices dispersas y no tolera elementos vacíos en ellas. Para ello LightFM proveé de herramientas de creación de datasets que facilitan la creación de las matrices, de forma que sea más fácil incluirlas en el modelo.

Entre estas herramientas se encuentran:

- *build_user_features(...)* Permite crear la matriz CSR de usuarios y atributos de usuarios.
- *build_item_features(...)* Permite crear la matriz CSR de items y atributos de items.
- *build_interactions(...)* Permite crear las matriz COO de interacciones y las matriz COO de sus correspondientes pesos.

Hay que tener en cuenta que las matrices CSR (Compressed Sparse Row) hacen referencia a las matrices que admiten operaciones matriciales y acceso eficientemente; y que las matrices COO (Coordinate list) hacen referencia a las matrices que soportan modificaciones eficientemente, son generalmente utilizadas para construir matrices.

6.4.1.1.1. Atributos de los usuario Para crear el modelo es necesario, entre otras cosas, disponer de las características de los usuarios. En este caso contamos con multitud de atributos sobre cada usuario: edad, género, nivel educativo, país, cultura de trabajo, perfil PST (Pinball, Shortcut, Thought-ful), barreras, intenciones y confianza.

Para convertir toda esa información del usuario a la matriz CSR que exige LightFM habrá que llamar a *build_user_features(...)* con los IDs de usuario y y sus atributos, formando una lista que tenga listas de los IDs de los usuarios con sus listas de atributos, es decir:

$$\Big[\Big[userId_1 \quad \Big[feature_{11} \quad \cdots \quad feature_{1w}\Big]_1\Big] \quad \ldots \quad \Big[userId_v \quad \Big[feature_{v1} \quad \cdots \quad feature_{vw}\Big]_v\Big]\Big]$$

Teniendo en cuenta que:

$$\begin{aligned} v &\leftarrow \textit{Cantidad de IDs de usuario} \\ w &\leftarrow \textit{Contidad de atributos por usuario} \\ userId_v &\leftarrow \textit{ID del usuario } v \\ feature_{vw} &\leftarrow \textit{Atributo } w \textit{ del usuario } v \end{aligned}$$

Una vez creada la lista y pasado como parámetro al método, obtendremos la matriz CSR de atributos de usuario.

6.4.1.1.2. Atributos de los elementos Además de los usuarios y de sus atributos, también se ha de disponer de los elementos a ordenar en el ranking, llamados items, y de sus características. En este caso estos items representan las estrategias de persuasión por las que se preguntó a los usuarios en el cuestionario. Sin embargo, al contrario que en el punto anterior, no contamos con tantos atributos sobre estos items, sino que cada estrategia de persuasión cuenta con dos atributos llamados dimensiones. Estos atributos no se encuentran presente en todas las estrategias, lo que da como resultado que haya algunas que tengan dos, una o ninguna dimension.

Para convertir toda esa información de los items a la matriz CSR que exige LightFM habrá que llamar a *build_item_features(...)* con los IDs de las estrategias y y sus atributos, formando una lista que tenga listas de los IDs de las estrategias con sus listas de atributos, es decir:

$$\Big[\Big[itemId_1 \quad \Big[feature_{11} \quad \cdots \quad feature_{1w}\Big]_1\Big] \quad \ldots \quad \Big[itemId_v \quad \Big[feature_{v1} \quad \cdots \quad feature_{vw}\Big]_v\Big]\Big]$$

Teniendo en cuenta que:

$$\begin{aligned} v &\leftarrow \textit{Cantidad de IDs de estrategias} \\ w &\leftarrow \textit{Contidad de dimensiones por estrategia} \\ itemId_v &\leftarrow \textit{ID de la estrategia } v \\ feature_{vw} &\leftarrow \textit{Atributo } w \textit{ de la estrategia } v \end{aligned}$$

Una vez creada la lista y pasado como parámetro al método, obtendremos la matriz CSR de atributos de usuario.

6.4.1.1.3. Interacciones Para crear un modelo de LightFM se necesita user_features, item_features

model = LightFM()

6.4.1.2. Ajuste

6.4.1.3. Predicción

6.4.1.4. Evaluación

La evaluación de los resultados obtenidos de las predicciones de los modelos es un apartado fundamental que permite analizar la eficacia de estas predicciones. Además, la utilización de métricas y técnicas permitirá poder comparar los resultados entre sí para poder demostrar si la predicción es correcta, aceptable o errónea.

6.4.1.4.1. Métricas

6.5. Consideraciones sobre la implementación

En este capitulo se describirán tanto las causas que han llevado a adoptar la previa especificación del diseño del sistema como las razones detrás de ellas. Con el objetivo de ayudar a entender el porqué de las decisiones tomadas se hablará sobre la privacidad, seguridad, la combinación de los modelos y las limitaciones técnicas presentes en este proyecto.

6.5.1. Privacidad

Con el objetivo de no vulnerar la privacidad de los datos, la agregación de los modelos será realiza por consenso sobre usuarios sintéticos. De esta forma, se evitan problemas derivados del robo de datos y las consecuencias tanto legales como personales de este.

Partiendo del principio de que si no circula ningún dato de ningún usuario por la red no se corren tantos riesgos se plantea este sistema de agregación como una alternativa viable a los sistemas tradicionales de ensamblado.

6.5.2. Seguridad

Este sistema está expuesto a los ataques de seguridad derivados de la implementación del Federated Learning. Sin embargo, debido a la naturaleza del algoritmo de consenso, algunos ataques podrían ser minimizados o incluso erradicados.

Un ejemplo de ello es el ataque por envenenamiento. Existen dos tipos de envenenamiento, por datos y por modelo, pero ambos consisten en que un participante de la red, con el objetivo de dañar tanto al sistema como a los participantes, envía modelos de inteligencia artificial (o los datos si es por envenenamiento de datos) debidamente manipulados. En los sistemas de agregación de modelos de inteligencia artificial por ensamblado este tipo de ataque suele ser bastante dañino, ya que es capaz de distorsionar por completo los resultados del modelo final con lo enviado por el atacante.

Sin embargo, debido a la condición del sistema de agregación por consenso, este tipo de ataques no son tan efectivos, ya que el modelo con datos envenenados podría ser ignorado si el método por el que se realiza el consenso es la moda. Con la moda se elegiría el ranking en función de los valores más frecuentes, es decir, el modelo del atacante sería ignorado por presentar predicciones que no se ajustan a ninguno de los demás participantes.

Cabe destacar que con el objetivo de detectar ataques y encontrar posibles modelos maliciosos se podrían descartar del proceso todos aquellos modelos que presenten unas predicciones totalmente diferentes. Se podría analizar la varianza de las predicciones de cada modelo para descartar del proceso a presuntos modelos envenenados.

6.5.3. Combinación de modelos

Debido a que el principal objetivo de este proyecto es el desarrollo de un sistema de recomendación con aprendizaje federado con la privacidad como patron de diseño, la combinación de los diferentes modelos de los participantes ha sido un factor muy importante a tener en cuenta. En el Machine Learning tradicional esta agregación de modelos se producía mediante el ensamblado de modelos. Sin embargo, este proceso no es compatible con este proyecto puesto que para poder ensamblar los modelos habría que compartir información de los participantes de la red.

Para evitar compartir ningún tipo de información que comprometiese la seguridad y privacidad de los participantes de la red de aprendizaje federado pero conseguir que los participantes aprendiesen entre ellos, se optó por compartir los modelos de inteligencia artificial exclusivamente.

6.5.4. Limitaciones técnicas

Debido a que los dispositivos que iban a formar la red iban a ser 4 Rasberry Pis modelo 3b+, el procesado de los datos era un proceso de especial importancio por la *escasa* capacidad de computo de estos dispositivos. Estos dispositivos, como se puede ver en el capítulo de especificación del diseño, son dispositivos que tienen cuatro núcleos y 1.4GHz de frecuencia, lo que comparado con un ordenador de sobremesa actual supone una gran diferencia de potencia de cálculo.

Además, esa no es la unica diferencia que tienen respecto a los ordenadores de escritorio, las Raspberry Pis funcionan sobre arquitectura ARMv8 y no sobre las tan usadas x64 y x86 . Esto implica un gran problema a la hora de instalar los paquetes necesarios para que el proyecto sea ejecutable en estos dispositivos, ya que la mayoría de los paquetes necesarios están pensados para las arquitecturas más comunes (x64 y x86). Sin embargo, se han podido encontrar las versiones funcionales de todos los paquetes para estos dispositivos.

El dispositivo que iba a agregar los datos, la Nvidia Jetson Nano, ha sido más sencilla de configurar puesto que esta funciona sobre arquitectura AArch64, extensión de 64bits de la arquitectura ARM.

Bibliografía

[1] R. Sánchez-Corcuera, D. Casado-Mansilla, C. E. Borges y D. López-de-Ipiña, "Persuasion-based recommender system ensambling matrix factorisation and active learning models," en, *Pers Ubiquit Comput*, mar. de 2020, ISSN: 1617-4909, 1617-4917. dirección: http://link.springer.com/10.1007/s00779-020-01382-7 (visitado 24-04-2021).

[2] *Amazon.es: compra online de electrónica, libros, deporte, hogar, moda y mucho más.* es-es. dirección: https://www.amazon.es/ (visitado 25-04-2021).

[3] *Investigación empírica*, es, Page Version ID: 127477170, jul. de 2020. dirección: https://es.wikipedia.org/w/index.php?title=Investigaci%C3%B3n_emp%C3%ADrica&oldid=127477170 (visitado 20-04-2021).

[4] *El Ciclo de Vida del Software — Proceso Básico en Metodologías*, es, oct. de 2016. dirección: https://okhosting.com/blog/el-ciclo-de-vida-del-software/ (visitado 20-04-2021).

[5] K. Bonawitz y col., "Towards Federated Learning at Scale: System Design," *arXiv:1902.01046 [cs, stat]*, mar. de 2019, arXiv: 1902.01046. dirección: http://arxiv.org/abs/1902.01046 (visitado 26-04-2021).

[6] *para Raspberry Pi 4 Model B,Raspberry Pi 3 B + Caja con Ventilador de refrigeración y disipador de Calor, Caja de acrílico de 4 Capas Caja apilable Cluster Caja para Raspberry Pi 3/2 Modelo B: Amazon.es: Grandes electrodomésticos.* dirección: https://www.amazon.es/Raspberry-Ventilador-refrigeraci%C3%B3n-disipador-acr%C3%ADlico/dp/B07J9VMNBL/ref=sr_1_2?__mk_es_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&dchild=1&keywords=raspberry+rack&qid=1619378660&sr=8-2 (visitado 25-04-2021).

Apéndice A

Protección de Datos en la Unión Europea y España

A.1. Preludio

Ante la llegada de las Tecnologías de la Información y la Comunicación (TIC), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) decidió definir unas directrices el 23 de septiembre de 1980 que regulen *".. la protección de la privacidad y el flujo transfronterizo de datos personales ... "* [1, págs.1]. Este fue uno de los primeros intentos de regular la gestión y utilización de los datos personales.

No llegaron medidas concretas a Europa hasta el 24 de octubre de 1995, cuando el Parlamento Europeo y el Consejo Europeo publicaron la *"Directiva 95/46/CE"* [2] con el objetivo de crear un marco jurídico que garantizase la protección de los datos y la libre circulación de estos[1]. Por eso, en España se creó la *"Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal"* [3] más conocida por sus siglas LOPD, que era la encargada de garantizar el cumplimiento de la directiva europea en España.

Ante la ausencia de leyes que garantizaran el cumplimiento de los derechos humanos en internet, algunos autores empezaron a definir los derechos digitales. Una de las primeras declaraciones de derechos fundamentales tecnológicos fue la de Robert B. Gelman, que en 1997 difundió una propuesta de *"Declaración de los Derechos Humanos en el Ciberespacio"*, basada en la Declaración Universal de los Derechos Humanos de 1948.

[1]Las directivas de la UE no son legalmente vinculantes para los ciudadanos, se dirigen a todos los estados miembros y cada uno deberá transponer la directiva a las leyes locales

Sin embargo, aunque el trabajo de Robert B. Gelman fue ampliamente apoyado por una gran comunidad de expertos, no ha sido hasta la entrada en el siglo XXI (cuando las TIC ya han conseguido una gran relevancia en la sociedad) que se ha empezado a atisbar la necesidad de derechos digitales inherentes de vivir en una sociedad tecnológica. Tanto es así, que varios autores empezaron a escribir sobre la necesidad de una nueva generación de derechos humanos que incluyese el campo de la tecnología.

La corriente pro derechos digitales llegó inclusive a la Unión Europea, que en el año 2000 redactó la *Çarta de los Derechos Fundamentales de la Unión Europea"* [4] en Niza con el objetivo de *"... reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos."* [4, págs.5]. El problema es que no pasó a ser jurídicamente vinculante hasta el año 2009 junto con el Tratado de Lisboa. Esta carta es especialmente innovadora en cuanto a la protección de datos de carácter personal, puesto que establecía como derecho fundamental la protección de estos en el artículo 8. En este artículo se establecía que además, estos se tratarían de modo leal y con el consentimiento de la persona afectada. Asimismo, la persona afectada tendría derecho a acceder a los datos recogidos, así como a la rectificación de los mismos.

A.2. Legislación

La legislación vigente en Europa cambió radicalmente en el 2016, el parlamento europeo adoptó nuevas medidas para la era digital.

El 5 de mayo de 2016 entró en vigor la Directiva (UE) 2016/680 [5], reconocida como la Directiva sobre protección de datos en el ámbito penal, *"... relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos ..."* [5, págs.1]. La Comisión Europea define esta medida en su página web [6] como:

> *"... protege el derecho fundamental de los ciudadanos a la protección de sus datos cuando los utilicen las autoridades policiales y judiciales a efectos de aplicación de la ley. Más concretamente, la Directiva garantizará que se protejan adecuadamente los datos personales de víctimas, testigos y sospechosos de delitos, además de facilitar la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo."*

El 24 de mayo de 2016 el Reglamento (UE) 2016/679 [7], reconocido como el Reglamento General de Protección de Datos (RGPD). *"... relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ..."* [7, págs.2]. La Comisión Europea define esta medida en su página web como:

> *"... es una medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital. Además, la existencia de una norma única pone fin a la fragmentación en distintos sistemas nacionales y a las cargas administrativas innecesarias."*

Esta legislación no sería aplicable hasta dos años más tarde, el 6 y 25 de mayo de 2018 respectivamente. Dos años durante los cuales cualquier empresa de la unión o cualquier empresa que tenga negocios en la Unión Europea se debía adaptar a la nueva normativa.

El objetivo principal de este reglamento era proteger a las personas físicas en cuanto al tratamiento de sus datos personales y a la libre circulación de estos. Estos datos son de naturaleza sensible, puesto que pueden revelar la identidad de la persona, ya sea mediante el nombre completo, la dirección de su domicilio, el número de tarjeta bancaria, etc.

Entre las cuestiones más relevantes del RGPD destacan:

- La transparencia: obliga a las organizaciones a comunicar a los usuarios el tratamiento que se realiza a sus datos.

- El derecho a la rectificación y borrado: cada usuario tendrá derecho a pedir que se rectifiquen sus datos en caso de ser inexactos. Además, los usuarios tendrán derecho a que las organizaciones borren sus datos y rescindir el consentimiento

de tratamiento de ellos.

- Derechos sobre el procesamiento: cada usuario podrá solicitar la limitación de procesamiento de sus datos, así como negarse a que se usen en tomas de decisiones o en perfiles automatizados, aparte, también podrá solicitar que le entreguen sus datos en formato estructurado cuando sea posible.

La directiva sobre protección de datos en el ámbito penal y el RGPD dejaron obsoleta la LOPD española, por lo cual, para adaptarse al nuevo marco jurídico europeo el 7 de diciembre de 2018 entró en vigor la *"Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales"* [8] (LOPD-GDD), acorde con el RGPD.

Esta ley transpone el RGPD europeo a la legislación española, incluyendo medidas como:

- La incorporación del término privacidad desde el diseño, lo que quiere decir que deben elaborarse procesos empresariales teniendo en cuenta la LOPD-GDD desde un primer momento.
- El consentimiento, donde se obliga a las organizaciones a obtener el consentimiento explícito para el tratamiento de datos de las personas, estas personas, además, podrán solicitar la portabilidad de sus datos o la eliminación de los mismos.

Sin embargo, la LOPD-GDD no se ciñe únicamente a adaptar el RGPD a la legislación Española, fue la primera ley europea de protección de datos en incluir explícitamente los derechos digitales de las personas en los entornos digitales.

A.3. Derechos fundamentales

Como se ha comentado en el apartado anterior, con la entrada en vigor de la LOPD-GDD España se convirtió en el primer país europeo en garantizar los derechos digitales. Estos derechos digitales llegaron en 2018 en el Título X de la LOPD-GDD, titulado *"Garantía de los derechos digitales"*, en respuesta a la Carta de los Derechos Fundamentales de la Unión Europea y a las nuevas medidas del Reglamento (UE) 2016/679 y de la Directiva (UE) 2016/680.

Varios de los derechos recogidos en la LOPD-GDD fueron:

- El derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

- El derecho a la desconexión digital en el ámbito laboral.
- Derecho al olvido en búsquedas de Internet.
- El derecho al testamento digital.

Este paso adelante por parte del estado español incentivó a que un año después de la entrada en vigor de la LOPD-GDD, el Ilustre Colegio de la Abogacía de Barcelona (ICAB) presentase la *Çarta de Barcelona por los Derechos de la Ciudadanía en la Era Digital"* [9], apoyada por universidades y entidades de la sociedad civil.

A la vista de la relevancia e impacto del tema, el gobierno español (representado por el Ministerio de Asuntos Económicos y Transformación Digital), se inspirará en la carta del ICAB para redactar la pionera *Çarta de Derechos Digitales"* [10] de España, que contribuirá con los objetivos ya avanzados en el Título X de la LOPD-GDD. Se prevé que sea aprobada antes de 2022 para la estrategia España Digital 2025.

Esta carta cuenta con 25 puntos de alta relevancia entre los que están los recogidos en el anteriormente mencionado Título X de la LOPD-GDD, y entre otros, algunos de especial impacto en el desarrollo de este proyecto: los derechos ante la Inteligencia Artificial (Derecho XXIII) y el derecho a no ser localizado y perfilado (Derecho V).

El derecho a no ser localizado y perfilado deja claro que cada persona tiene derecho a la *"... libre autodeterminación individual (...) a no ser objeto de localización, ni a ser sometido a análisis de la personalidad o conducta que impliquen el perfilado de la persona"*, además, añade que sólo se podrán realizar *"... tratamientos de información personal con el consentimiento de la persona afectada ..."*.

En cuanto al derecho ante la Inteligencia Artificial expone como primer punto que, en lo que concierne al desarrollo y ciclo de vida de esta, *"Se deberá garantizar el derecho a la no discriminación algorítmica ..."*. Además. en procesos de decisión automatizada las personas tienen derecho a *"Solicitar una supervisión e intervención humana"* o *Ïmpugnar las decisiones automatizadas o algorítmicas"*.

La carta, al no estar aprobada aún, no es legalmente vinculante, por lo que no es de obligado cumplimiento. Sin embargo, deja clara la orientación que van a tomar los derechos digitales en los próximos años.

Referencias

[1] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, es. OECD, feb. de 2002, ISBN: 978-92-64-19719-0 978-92-64-19639-1. dirección: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (visitado 28-03-2021).

[2] *DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995*. dirección: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES (visitado 28-03-2021).

[3] *LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*. dirección: https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf (visitado 28-03-2021).

[4] "Carta de los Derechos Fundamentales de la Unión Europea," pág. 17,

[5] "DIRECTIVA (UE) 2016/ 680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016," es, pág. 43,

[6] *La protección de datos en la UE*, es, Text. dirección: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (visitado 27-03-2021).

[7] *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016*. dirección: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=ES (visitado 27-03-2021).

[8] M. B. Samper, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, es, 1.ª ed. Dykinson, sep. de 2020, ISBN: 978-84-13-77085-7 978-84-13-77029-1. dirección: http://www.jstor.org/stable/10.2307/j.ctv17hm980 (visitado 28-03-2021).

[9] *Carta de Barcelona por los Derechos de la Ciudadanía en la Era Digital*. dirección: https://www.icab.cat/export/sites/icab/.galleries/documents-noticies/2019/documento-carta-de-barcelona-por-los-derechos-de-la-ciudadania-en-la-era-digital-21-02-2019.pdf (visitado 01-04-2021).

[10] *Carta de Derechos Digitales*. dirección: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIACartaDerechosDigitales.pdf (visitado 30-03-2021).

Apéndice B

Documentos adicionales

En este apartado se adjuntan los documentos que debido a su tamaño puede que no se puedan observar con claridad en la memoria del proyecto.

B.1. Planificación del Proyecto

En la siguiente hoja se adjunta el diagrama GANTT de la planificación del proyecto a tamaño completo.

EDT	TÍTULO DE LA TAREA	FASE UNO															FASE DOS															FASE TRES															FASE 4													
		SEMANA 1					SEMANA 2					SEMANA 3					SEMANA 4					SEMANA 5					SEMANA 6					SEMANA 7					SEMANA 8					SEMANA 9					SEMANA 10					SEMANA 11					SEMANA 12				
		L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V
0	Registrar proyecto																																																																			
0.1	Definición de título y descripción																																																																			
0.2	Registro del proyecto a través del formulario																																																																			
1	Formación																																																																			
1.1	Formación sobre conceptos de Machine Learning																																																																			
1.2	Fornación sobre conceptos de los sistemas de recomendación																																																																			
1.3	Formación sobre conceptos de Federated Learning																																																																			
1.4	Formación sobre LightFM																																																																			
1.5	Familiarización con el sistema de recomendación de R.Sánchez																																																																		
2	Configuración del hardware																																																																		
2.1	Configuración de las RaspBerrys																																																																		
2.2	Configuración de la JetsonNano																																																																		
2.3	Aprovisionamiento de los Sistemas Operativos																																																																		
2.4	Instalar y ejecutar sistema de recomendaciones																																																																		
4	Adaptación del sistema de recomendación online a aprendizaje federado																																																																		
4.1	Guardado , cargado y envío de modelos de inteligencia artificial																																																																		
4.2	Agregación de los modelos de inteligencia artificial																																																																		
4.3	Recomendación para un único usuario																																																																		
4.4	Combinar recomendaciones para un único usuario																																																																		
4.5	Combinar recomendaciones para varios usuario																																																																		
4.6	Reentrenar modelos																																																																		
4.7	Visualización de los resultados de rendimiento por gráficas																																																																		
3	Desarrollo de la memoria																																																																		
3.1	Resumen																																																																		
3.2	Introducción																																																																	
3.3	Antecedentes y Justificación																																																																	
3.4	Objetivos y Alcance																																																																	
3.5	Consideraciones éticas																																																																	
3.6	Metodología																																																																	
3.7	Planificación																																																																	
3.8	Introducción al Federated Learning																																																																	
3.9	Desarrollo																																																																	
3.10	Presupuesto																																																																	
3.11	Conclusiones y Trabajo futuro																																																																	
3.12	Bibliografía																																																																	
3.13	Definiciones y Acrónimos																																																																	
3.14	Anexos																																																																	
5	Estudio del rendimiento																																																																	
5.1	Estudio del rendimiento de un sistema de recomendaciones centralizado																																																																	
5.2	Estudio del rendimiento de un sistema de recomendaciones de modelos agregados																																																																		
5.3	Estudio de rendimiento del sistemas de recomendaciones final																																																																	