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

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean semper non orci at fringilla. Etiam fermentum in diam vestibulum pellentesque. Nam volutpat, velit ut euismod mollis, ipsum erat facilisis justo, et tempor est lectus nec massa. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Sed accumsan viverra neque eu blandit. Suspendisse in fermentum felis, id iaculis mi. Quisque maximus quam lacus, non lobortis libero tincidunt at. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Maecenas lectus nibh, sagittis ut felis non, fermentum ullamcorper leo. In hac habitasse platea dictumst. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Fusce est dui, dapibus ultricies ipsum quis, ultrices maximus dolor. Proin finibus, lorem vulputate maximus convallis, quam tellus posuere magna, sed maximus nunc eros quis ipsum. Cras dignissim cursus lectus ac auctor. Donec suscipit vestibulum neque, sed lobortis est rhoncus non.

Praesent ut neque eros. Praesent vitae augue at diam tincidunt sagittis. In cursus lorem nec neque condimentum dictum. Morbi vel tristique orci. Cras luctus tempus elit tincidunt hendrerit. Proin bibendum arcu et sapien finibus vulputate sed eget leo. Duis at bibendum massa, sit amet ornare lorem. Donec dictum finibus fringilla. Duis accumsan lectus dolor, eu maximus ligula semper vel. Proin a sem tincidunt, mollis magna eget, consequat tortor. In sodales justo et varius scelerisque. Aliquam sit amet lacus mollis, tincidunt erat vitae, lacinia sem. Maecenas vel erat sagittis, semper ex in, commodo libero.

Integer malesuada quis elit eu eleifend. Suspendisse non vestibulum est, a fermentum urna. Donec ligula tortor, ultrices varius nisi eget, dictum malesuada augue. Fusce lacus orci, eleifend quis luctus dictum, ultricies id turpis. Vestibulum et auctor orci. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Integer facilisis neque quis dui dapibus dictum.

Descriptors
Lorem, ipsum, dolor, sit, amet

Índice general

1. Objetivos y Alcance **1**
1.1. Objetivos 1
1.1.1. Generales 1
1.1.2. Específicos 1
1.2. Alcance 3
1.2.1. Dentro del alcance 3
1.2.2. Fuera del alcance 3

2. Metodología **5**
2.1. Consideraciones 5
2.2. Metodología de Investigación 5
2.3. Metodología de desarrollo 7
2.4. Conclusión 8

3. Bases para el desarrollo **9**
3.1. Sistemas de recomendación 9
3.2. Federated Learning 10
3.2.1. Información general 10
3.2.2. Fundamentos y Protocolo 11
3.2.3. Problemas presentes 12

Índice de figuras

2.1. Ciclo empírico de A.D. de Groot (Fuente: Wikipedia[1]) 6
2.2. Modelo en el Espiral, Autor Desconocido (Fuente: Blog[2]) 7
2.3. Metodología de trabajo del proyecto final de grado (Autor: Ibai Guillén) 8

3.1. Recomendaciones de Amazon (Fuente: Amazon[**AmazonEsCompra**]) 10
3.2. Diagrama de una red de Federated Learning 11

Índice de tablas

Capítulo 1

Objetivos y Alcance

1.1. 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 independientemente del estado en que encuentren y 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.

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 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.

1.1.2. Específicos

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

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 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.

1.1.2.3. 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

1.2. 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.

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.

Se recogera el desarrollo de todo el proyecto en la memoria técnica 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

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.

2.1. 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.

2.2. 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.2.1). 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.2.3).

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.

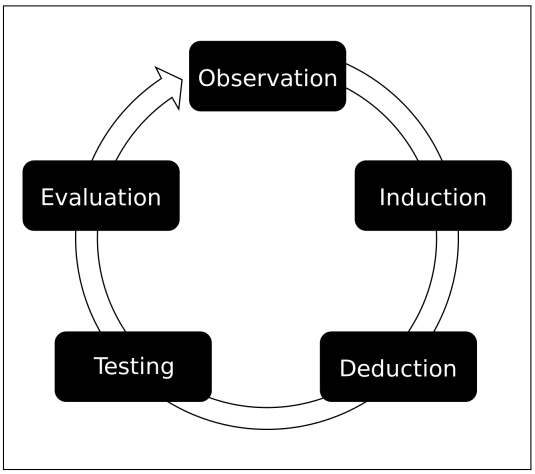

Fig. 2.1: Ciclo empírico de A.D. de Groot (Fuente: Wikipedia[1])

2.3. Metodología de desarrollo

El modelo en espiral (Fig.2.2) 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.

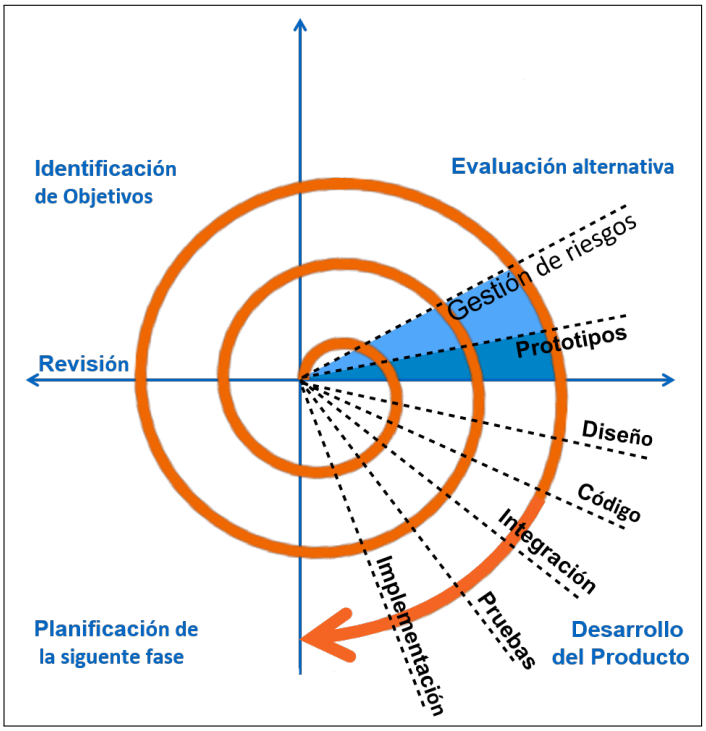

Fig. 2.2: Modelo en el Espiral, Autor Desconocido (Fuente: Blog[2])

2.4. 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 2.3.

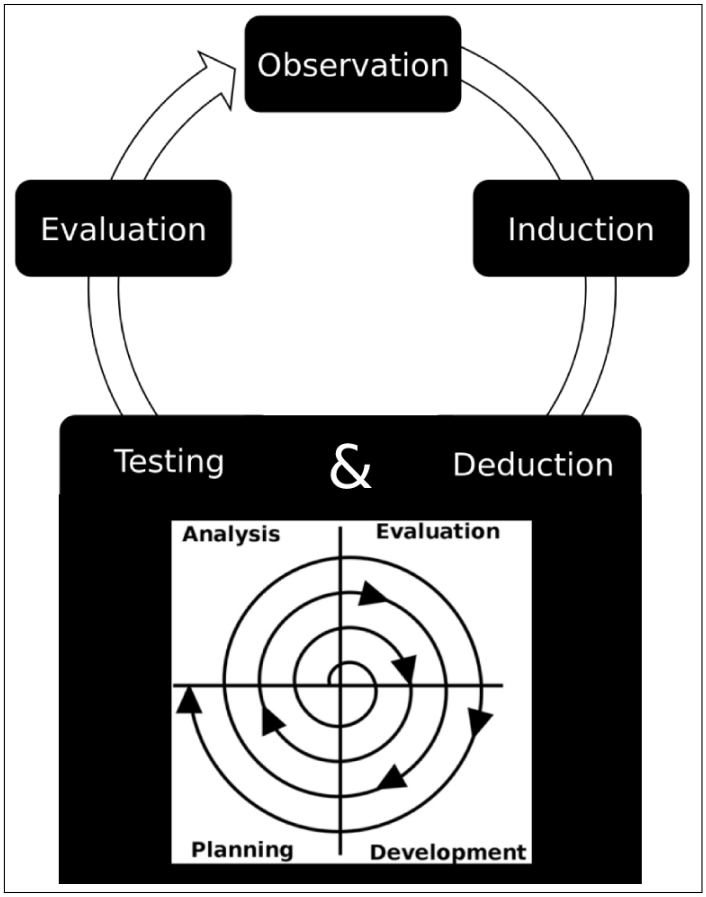

Fig. 2.3: Metodología de trabajo del proyecto final de grado (Autor: Ibai Guillén)

Capítulo 3

Bases para el desarrollo

En el siguiente capítulo se introducirán y explicarán los conceptos importantes sobre los que parte el proyecto. Es de gran importancia comprender y conocer lo que son los sistemas de recomendación y el Federated Learning para entender tanto el desarrollo, como la resolución de los problemas y retos que supone su implementación.

3.1. Sistemas de recomendación

Los sistemas de recomendación son sistemas de filtrado de información, que se basan en una gran cantidad de datos, tanto del usuario como de los elementos a recomendar, para predecir cuál será el elemento más apropiado para este. Estos sistemas están estrechamente relacionados con el marketing, ya que el objetivo es conseguir recomendar un elemento que sea del agrado e interés del usuario con los datos que se tienen de él, lo que en la mayoría de los casos va ligado al consumo de bienes o servicios.

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 (Fig3.1).

Fig. 3.1: Recomendaciones de Amazon (Fuente: Amazon[**AmazonEsCompra**])

3.2. Federated Learning

3.2.1. 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 (Fig3.2). 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, puesto 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

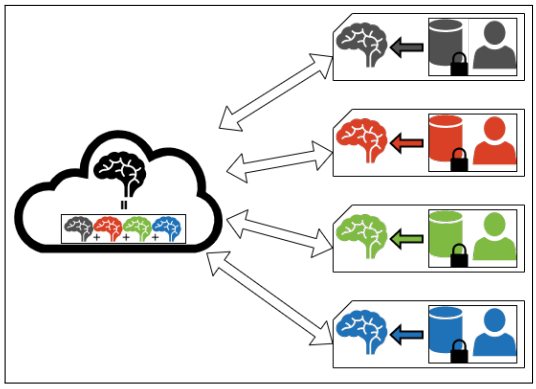

Fig. 3.2: Diagrama de una red de Federated Learning

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.

3.2.2. 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 [**bonawitzFederatedLearningScale2019** 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.

3.2.3. 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.

Bibliografía

[1] *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).

[2] *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).