Seminario de Inteligencia Artificial de la Universidad de Sevilla

Aprendizaje Federado: conceptos, estado del arte, y retos en modelos no-deep learning.

Jose M. Moyano

28 noviembre 2023

Dpto. Ciencias de la Computación e Inteligencia Artificial

1. Introducción

2. Conceptos y fundamentos

3. FedAvg y caso de uso

4. Retos en la implementación de modelos no-deep learning

5. Conclusiones

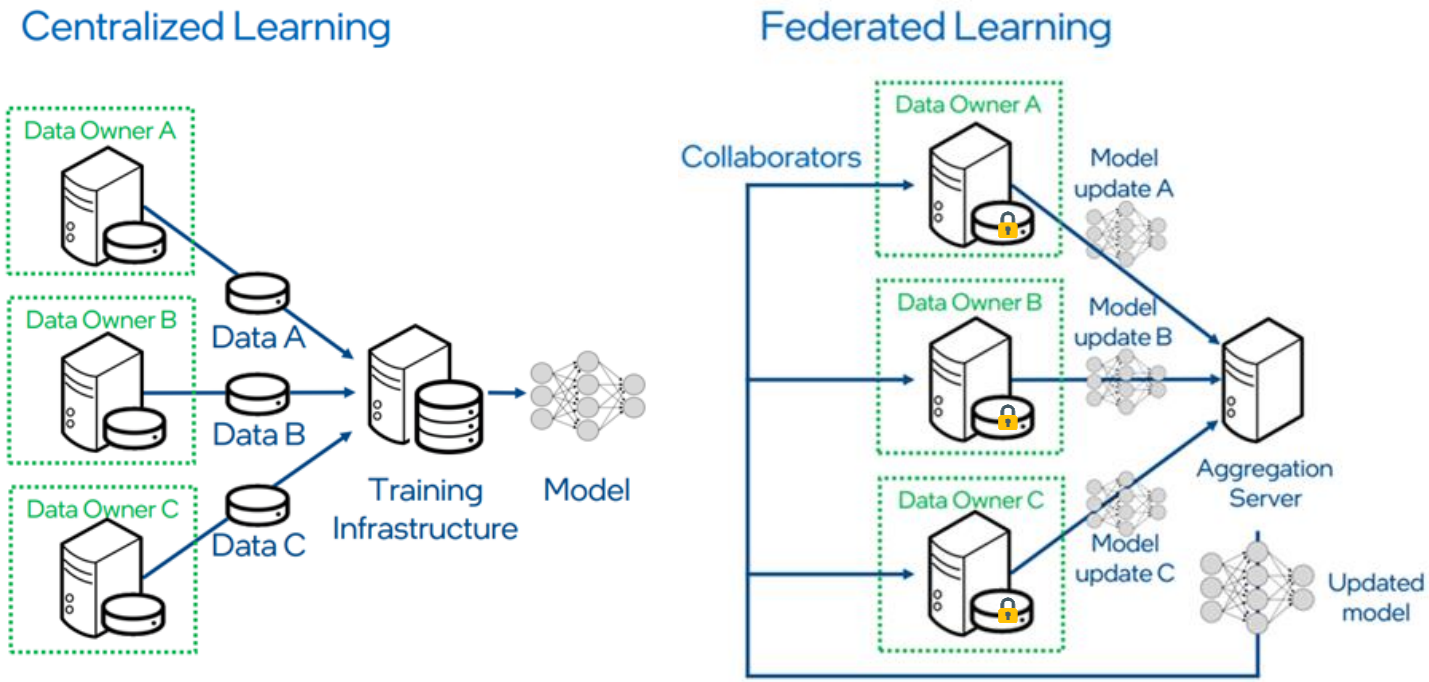
Motivación

- Crecimiento del uso de *machine learning* (ML) e IA en general.
- Necesidad de grandes cantidades de datos.
- Cada vez más regulaciones (y escepticismo) al compartir o liberar datos.
  - P.ej. *General Data Protection Regulation (GDPR)* en la Unión Europea

- Beneficios de colaboración entre entidades.
- Computación en *IoT*.

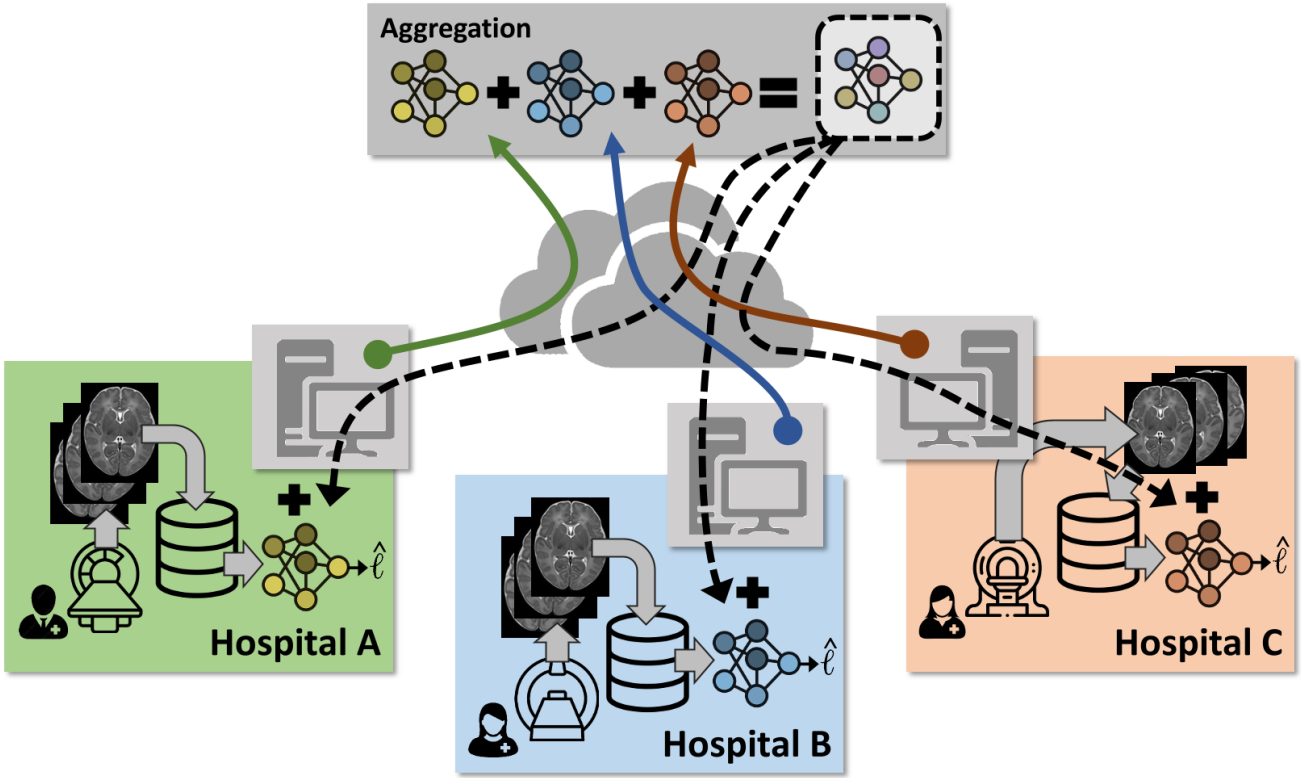
- **Aprendizaje Federado!** (*Federated Learning, FL*)

Aprendizaje Centralizado vs Federado



https://community.intel.com/t5/Blogs/Products-and-Solutions/HPC/Secure-and-Compliant-Data-Using-Embargoed-Confidential-and/post/1421771/

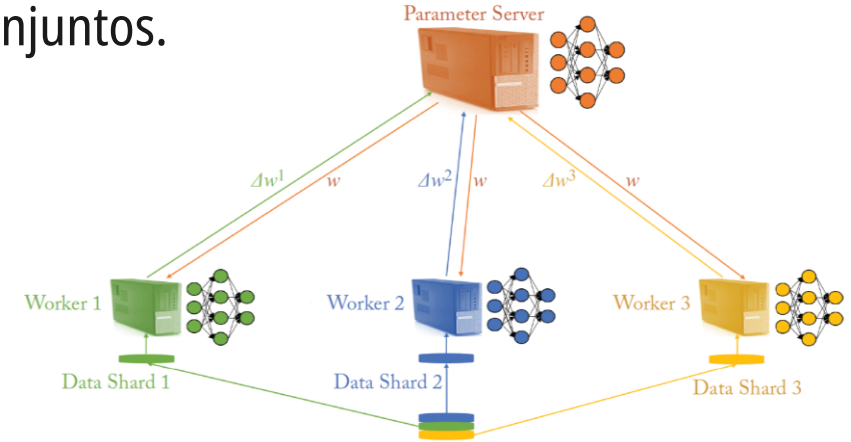
Aprendizaje Federado (FL)



Luzón M.V. *et al*. (2024). A Tutorial on Federated Learning from Theory to Practice: Foundations, Software Frameworks, Exemplary Use Cases, and Selected Trends. *IEEE/CAA J. Autom. Sinica*, 11(4).

Aprendizaje Federado vs Distribuido

- Los datos nunca están centralizados.
- No se puede conocer la distribución global de los datos.
- La potencia de los clientes viene posiblemente dada.
- Los datos se encuentran distribuidos originalmente, con lo que ello implica sobre el origen y tamaño de los conjuntos.



Yang Q. *et al*. (2020). Federated Learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*.

1. Introducción

2. Conceptos y fundamentos

3. FedAvg y caso de uso

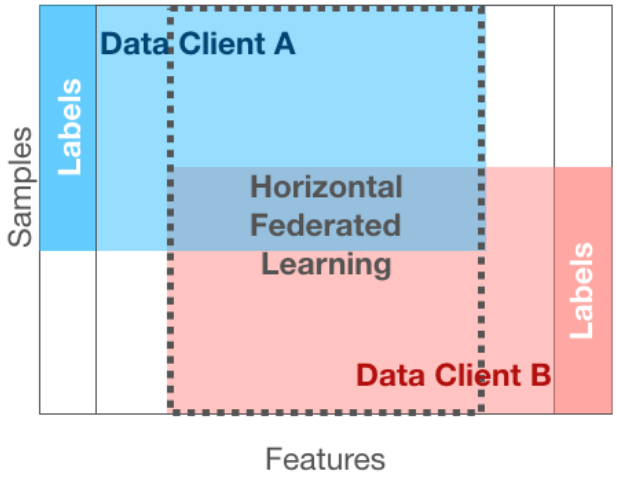
4. Retos en la implementación de modelos no-deep learning

5. Conclusiones

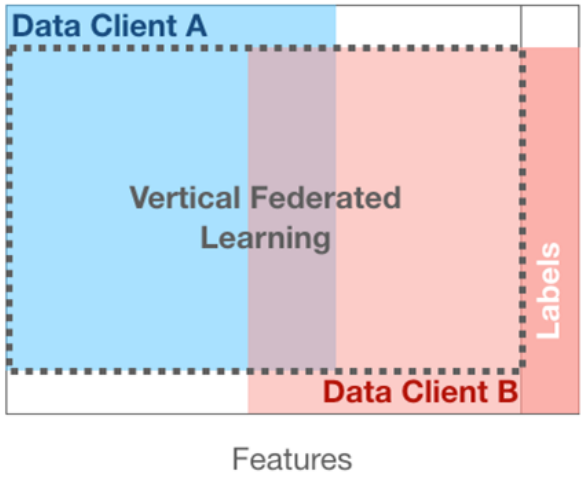
Definición de FL

- Marco algorítmico para construir modelos de ML.
- Hay dos o más **partes interesadas** (clientes) que quieren construir un **modelo** de ML **conjunto**.
  - Cada parte posee sus propios datos para contribuir al entrenamiento.
- Los **datos privados** no salen de cada parte durante el entrenamiento.
- Se pueden transferir partes del **modelo** bajo **encriptación**, de forma que las otras partes no puedan hacer ingeniería inversa para obtener los datos.
- El **rendimiento** del modelo resultante es una buena **aproximación** del modelo ideal centralizado.

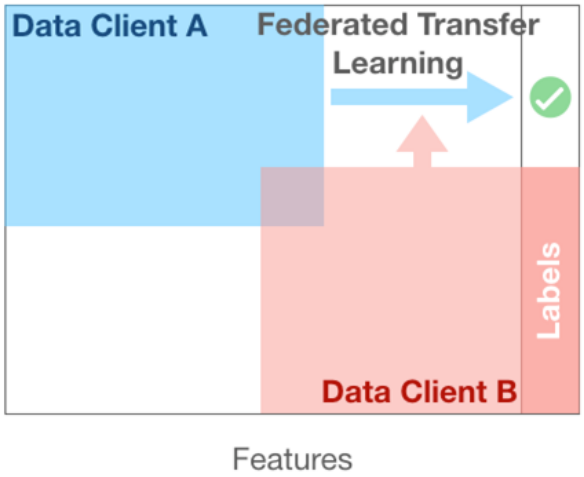
Tipos de FL



FL Horizontal
(HFL)



FL Vertical
(VFL)

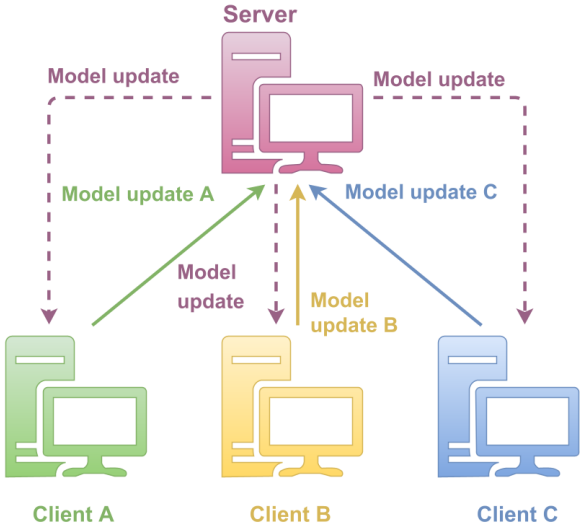


Transfer FL
(TFL)

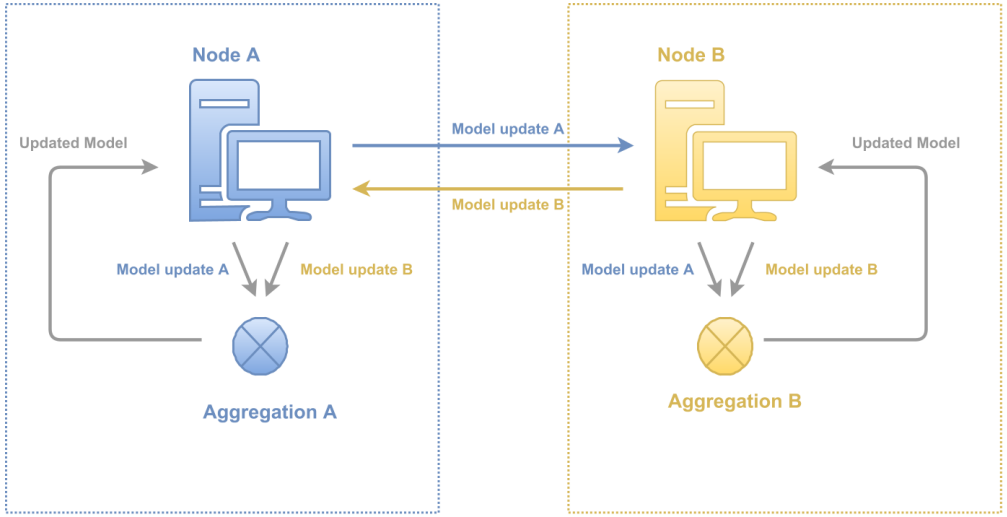
Yang Q. *et al*. (2020). Federated Learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*.

Luzón M.V. *et al*. (2024). A Tutorial on Federated Learning from Theory to Practice: Foundations, Software Frameworks, Exemplary Use Cases, and Selected Trends. *IEEE/CAA J. Autom. Sinica*, 11(4).

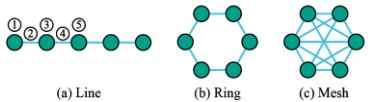
Arquitecturas principales



Cliente-servidor



Peer-to-peer (descentralizado)



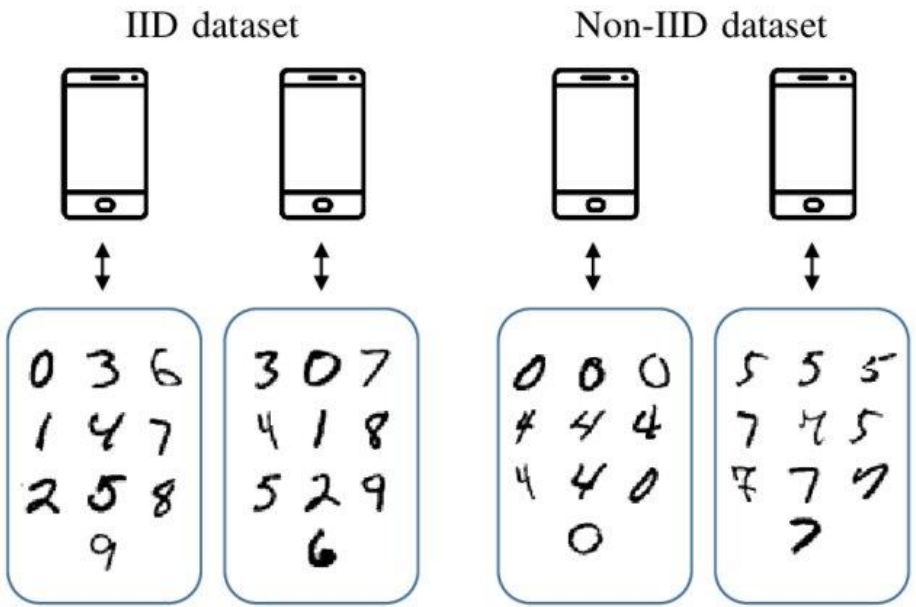
Yuan, L., Sun, L., Yu, P. S., & Wang, Z. (2023). Decentralized Federated Learning: A Survey and Perspective. *arXiv preprint arXiv:2306.01603.*

Luzón M.V. *et al*. (2024). A Tutorial on Federated Learning from Theory to Practice: Foundations, Software Frameworks, Exemplary Use Cases, and Selected Trends. *IEEE/CAA J. Autom. Sinica*, 11(4).

Modelo global / descentralizado / personalizado

- El concepto general gira entorno a tener un modelo global alojado en un servidor.
- En otras arquitecturas, el modelo puede estar alojado en diferentes sitios:
  - Cada cliente tiene una copia del mismo modelo
  - O el modelo debe estar, por restricciones, almacenado “por partes” entre todos los clientes.
- Personalización de modelos en cada cliente.

Distribución de los datos (IID / non-IID)



- Tamaño del dataset
- Diferentes clases (o diferente número de instancias por clase)
- Distintos orígenes
- Sesgo en los datos
- ...

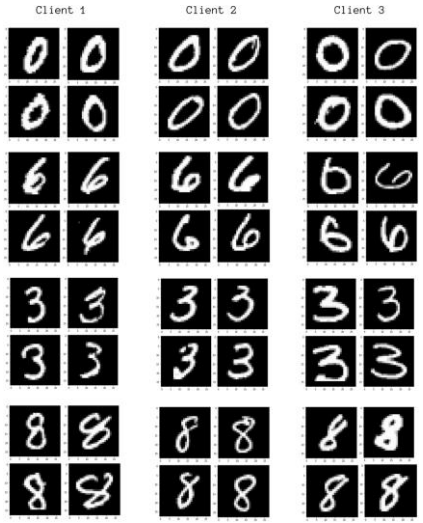
Hellström, H., Silva Jr, J. M. B. D., Amiri, M. M., Chen, M., Fodor, V., Poor, H. V., & Fischione, C. (2020). Wireless for machine learning. *arXiv preprint arXiv:2008.13492*.

Conjuntos de datos

- Inherentemente federados

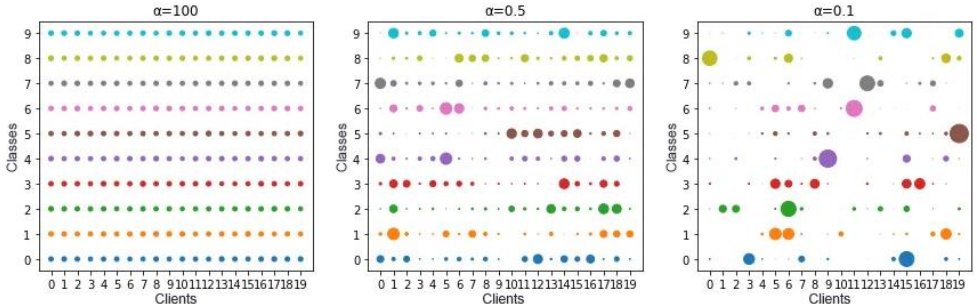
text string	date string	user string	sentiment int32
Ok, first assesment of the #kindle2 ...it fucking rocks!!!	Mon May 11 03:18:54 UTC…	chadfu	4
@kenburbary You'll love your Kindle2. I've had mine for a few…	Mon May 11 03:19:04 UTC…	SIX15	4
@mikefish Fair enough. But i have the Kindle2 and I think it's…	Mon May 11 03:21:41 UTC…	yamarama	4
@richardebaker no. it is too big. I'm quite happy with the Kindle2.	Mon May 11 03:22:00 UTC…	GeorgeVHulme	4
Fuck this economy. I hate aig and their non loan given asses.	Mon May 11 03:22:30 UTC…	Seth937	0

https://huggingface.co/datasets/**sentiment140**



https://github.com/aswarth123/Federated_Learning_**MNIST**

- Simulación



https://towardsdatascience.com/from-centralized-to-federated-learning-b0074793e9f

Frameworks

- TensorFlow Federated
  - https://www.tensorflow.org/federated
- Flower
  - https://flower.dev/
- FATE
  - https://fate.fedai.org/
- ...

Frameworks

	PyS	TFF	FAT	Pad	Flo	Xay	IBM	Sub	OFL	FML	FJx	101	FLb	SFL	EFL	TFL	AFL	NVF
Federated Learning:																		
Horizontal Federated Learning	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Vertical Federated Learning	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Federated Transfer Learning	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Support other ML frameworks	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sampling IID or non-IID distribution	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Federated aggregation mechanisms	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Adversarial attacks in FL:																		
Privacy attacks	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Defenses against Privacy attacks	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Attacks to the federated model	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Defenses against attacks to the model	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Differential Privacy (DP):																		
Mechanisms: Exponential, Laplacian...	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Subsampling methods to increase privacy	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Advanced DP Composition	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Advanced properties:																		
Interpretability / Explainability	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Personalization	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Documentation and tutorials	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
High-level API	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ability to extend the framework	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Actively maintained	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Luzón M.V. *et al*. (2024). A Tutorial on Federated Learning from Theory to Practice: Foundations, Software Frameworks, Exemplary Use Cases, and Selected Trends. *IEEE/CAA J. Autom. Sinica*, 11(4).

Desafíos

- Privacidad de los datos / encriptación
- Costes de comunicación y latencia
- Limitaciones en el acceso de los datos
- Distribución de los datos
- Selección del modelo / personalización
- Ataques maliciosos
- Entrada/salida de entidades, y asincronía en las actualizaciones
- Simulación
- Incentivos
- Evaluación
- ...

1. Introducción

2. Conceptos y fundamentos

3. FedAvg y caso de uso

4. Retos en la implementación de modelos no-deep learning

5. Conclusiones

Federated Averaging (FedAvg)

- HFL
- Cliente-servidor
- Redes neuronales
  - U otros modelos que puedan descomponerse como conjunto de pesos
- Asume:
  - Datos non-IID y desbalanceo
  - Gran número de clientes
  - Conexiones lentas y poco fiables

Federated Averaging (FedAvg)

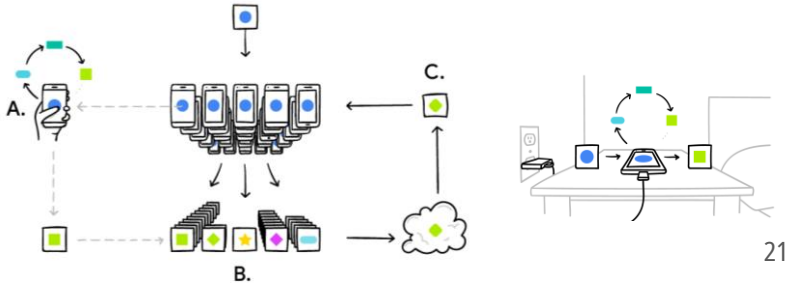
- **Servidor inicializa** el modelo, y lo envía a los K clientes.
- PARA cada ronda de entrenamiento federado:
  - Se selecciona un **ratio** ρ de **clientes** para participar en la ronda
  - Cada **cliente actualiza** el modelo con sus **datos locales** por S épocas, usando un mini-batch de tamaño M de su dataset D_k
  - Cada **cliente envía** al servidor los **pesos** actualizados (*model averaging*) o los **gradientes** obtenidos (*gradient averaging*).
  - **Servidor actualiza** calculando una media de los pesos/gradientes, obtiene un nuevo modelo global, y lo reenvía a los clientes.

Federated Averaging (FedAvg)

- Versión asíncrona
  - A la actualización del modelo recibida por el cliente se le asigna un peso.
  - Peso basado en cuánto ha tardado en devolver la actualización.
  - Evita incluir actualizaciones de modelos “antiguos”.

GBoard

- Desde 2017, comenzaron a utilizar FL para recomendación de la siguiente palabra.
- Primera incursión de Google en FL.
- No envía datos, y solo entrena mientras el móvil está cargando, conectado a WiFi, y sin usar.
- Usando FedAvg (primera propuesta de Google también)
- Usa una versión mini de TensorFlow en Android.



https://support.google.com/gboard/answer/12373137

https://www.searchenginejournal.com/google-personalize-gboard-search-results-using-cloud-based-machine-learning/194243/

1. Introducción

2. Conceptos y fundamentos

3. FedAvg y caso de uso

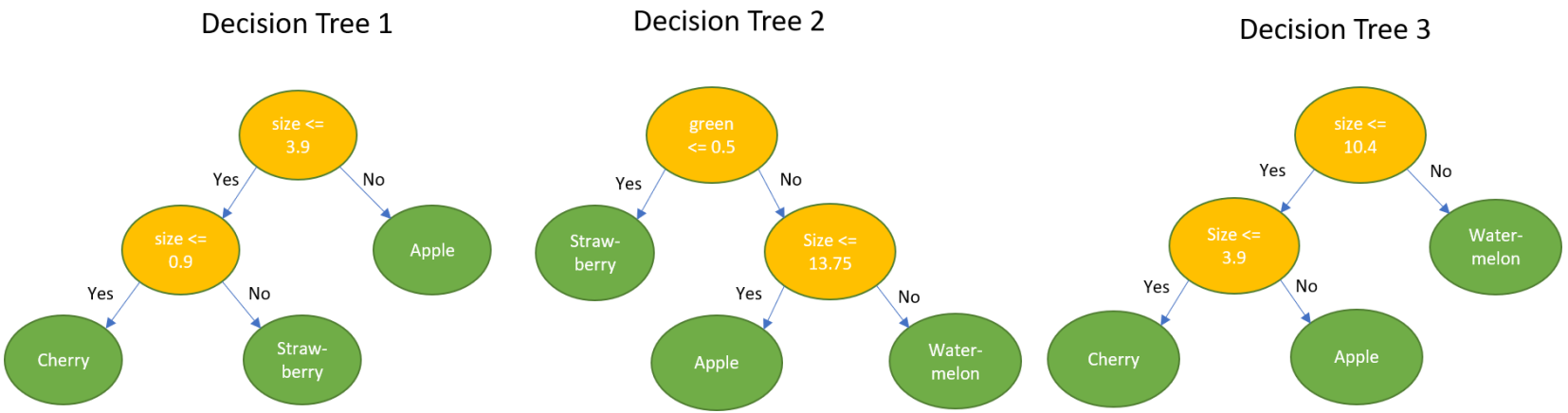
4. Retos en la implementación de modelos no-deep learning

5. Conclusiones

Retos

- No es trivial agregar modelos que no se compongan de un conjunto de pesos.
  - Árboles de decisión
  - Modelos de ensemble
  - K-means clustering
  - ...

Árboles de decisión



https://developer.nvidia.com/blog/accelerating-random-forests-up-to-45x-using-cuml

Árboles de decisión (HLF)

[Todos los clientes poseen los mismos atributos]

- El servidor almacena el árbol común
- Pide a los clientes que seleccionen el siguiente atributo para la partición
  - Deben enviar, además de la partición, alguna métrica que indique su bondad.
  - Si envía información sobre nº de patrones por clase, incluye ruido.
- El servidor puede:
  - Seleccionar la mejor partición de entre las recibidas
  - Obtener un consenso
- El servidor actualiza el árbol y pide a los clientes la siguiente partición
- En muchos casos puede que no haya datos suficientes en un nodo concreto

Árboles de decisión (VLF)

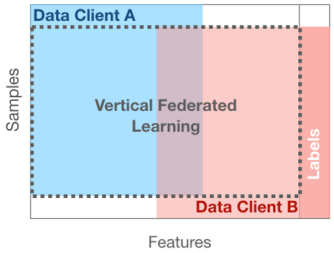
[Cada cliente tiene un subconjunto de atributos distinto]

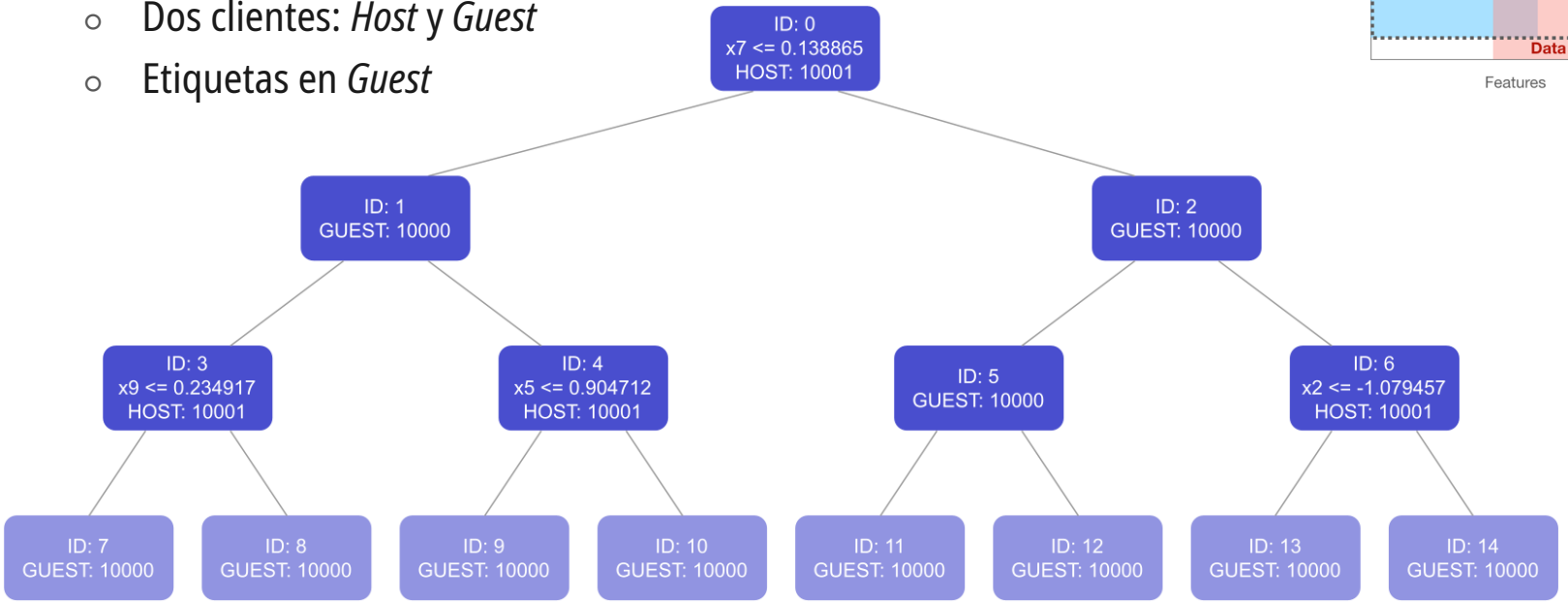
- El servidor (o cada cliente) almacena la estructura parcial del árbol.
- Cada cliente calcula la mejor partición entre sus atributos.
- Se selecciona la mejor partición de entre todas.
- Se almacena una estructura común con un id de atributo en cada nodo y qué cliente lo posee.
- Al predecir, deben participar todos los clientes.

Cheng, K., *et al*. (2021). Secureboost: A lossless federated learning framework. *IEEE Intelligent Systems*, 36(6), 87-98.

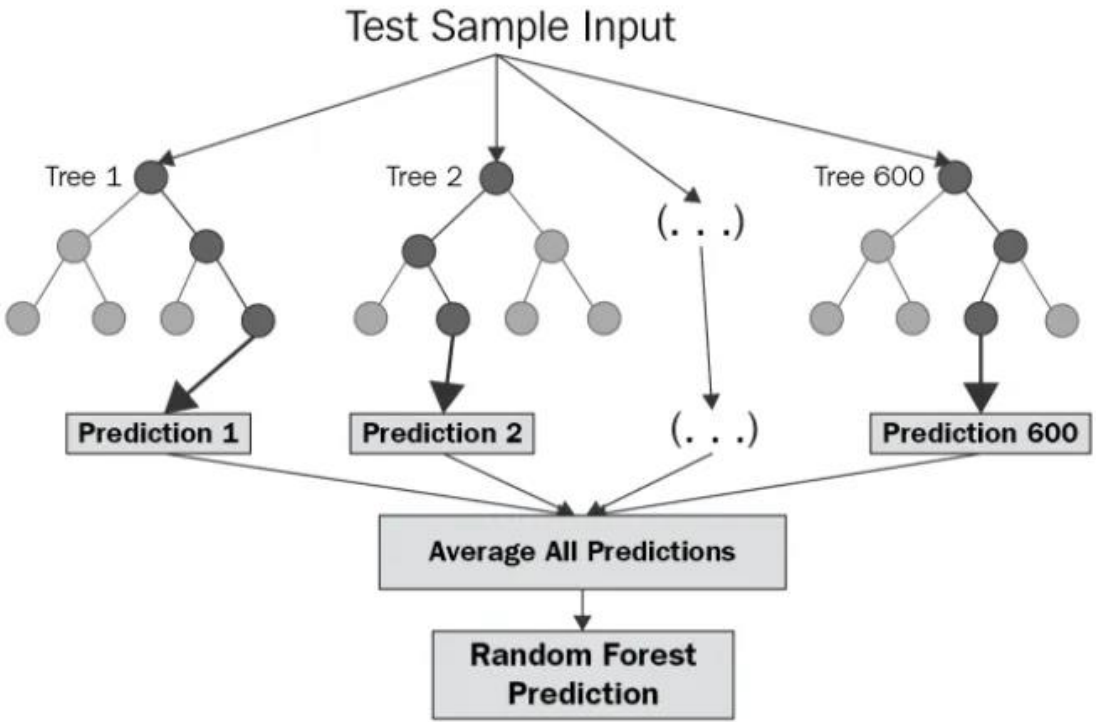
Árboles de decisión (VLF)

- Árbol de decisión en *Host*
  - Dos clientes: *Host* y *Guest*
  - Etiquetas en *Guest*





Random Forest



https://levelup.gitconnected.com/random-forest-regression-209c0f354c84

Basado en Random Forest

- Cada cliente entrena un número de árboles de decisión.
- Comparte los modelos con un servidor
  - No comparte información como tal de los clientes
  - Pero sí el número de instancias de cada clase, ya que envía los árboles completos
  - Aún revela cierta información que sería deseable que no
- El servidor envía a los clientes los árboles recibidos
  - Antes de incluir cada árbol en su propio *bosque*, lo evalúa sobre sus datos locales.
    - Evita posibles amenazas o ataques intrusos
    - Evita introducir modelos puntuales con mal rendimiento

de Souza, L.A.C., *et al*. (2020). DFedForest: Decentralized federated forest. In *2020 IEEE International conference on blockchain* (pp. 90-97).

Basado en *ensemble distillation*

- Se entrena un modelo global, basado en las salidas de los modelos locales
  - Es necesario que el servidor tenga un conjunto de datos que compartir con los clientes (pueden ser datos públicos, datos sin etiquetar, generados artificialmente, ...)
- Cada cliente entrena su modelo, y evalúa sobre los datos del servidor.
- El servidor colecciona las salidas de los modelos de cada cliente, y las usa como etiquetas para entrenar su propio modelo central.
- La estructura de los modelos no tiene por qué necesariamente ser la misma.

Lin, T., *et al*. (2020). Ensemble distillation for robust model fusion in federated learning. *Advances in Neural Information Processing Systems*, 33, 2351-2363.

Gong, X., *et al*. (202). Preserving privacy in federated learning with ensemble cross-domain knowledge distillation. In *Proceedings of the AAAI Conference on Artificial Intelligence* (36:11, 11891-11899).

Uso de datos sintéticos

- Cada cliente entrena una GAN y genera datos sintéticos.
- El servidor reúne los datos sintéticos y divide en entrenamiento-validación.
- Envía el conjunto sintético de entrenamiento a todos los clientes.
- Cada cliente entrena sus árboles (sobre sus datos locales y los sintéticos) y los comparte con el servidor.
- El servidor utiliza el conjunto de validación para entrenar hiperparámetros o seleccionar árboles del bosque, si es necesario.

Li, J., *et al*. (2020). A multicenter random forest model for effective prognosis prediction in collaborative clinical research network. *Artificial intelligence in medicine*, 103, 101814.

Ensemble iterativo

- En cada iteración, cada cliente construye varios modelos
- Se envían al resto de clientes para que lo validen sobre sus datos
- Se calcula el error medio de validación entre todos los clientes
- Se seleccionan los mejores para formar parte del modelo global

1. Introducción

2. Conceptos y fundamentos

3. Estado del arte

4. Retos en la implementación de modelos no-deep learning

5. Conclusiones

Conclusiones

- Restricción en la privacidad de los datos
- Construcción colaborativa de modelos de ML
- Variedad de categorizaciones y conceptos dentro de FL
- Hay muchos frameworks aunque queda trabajo por hacer
- Retos a los que enfrentarse

Conclusiones

- FedAvg como algoritmo clásico
- Aplicaciones en entornos reales con buenos resultados

- Mucho trabajo para redes neuronales
- Trabajo por hacer en otro tipo de modelos
    - Mención especial a modelos de ensemble

Seminario de Inteligencia Artificial de la Universidad de Sevilla

Aprendizaje Federado: conceptos, estado del arte, y retos en modelos no-deep learning.

Jose M. Moyano

jmoyano1@us.es

https://personal.us.es/jmoyano1/