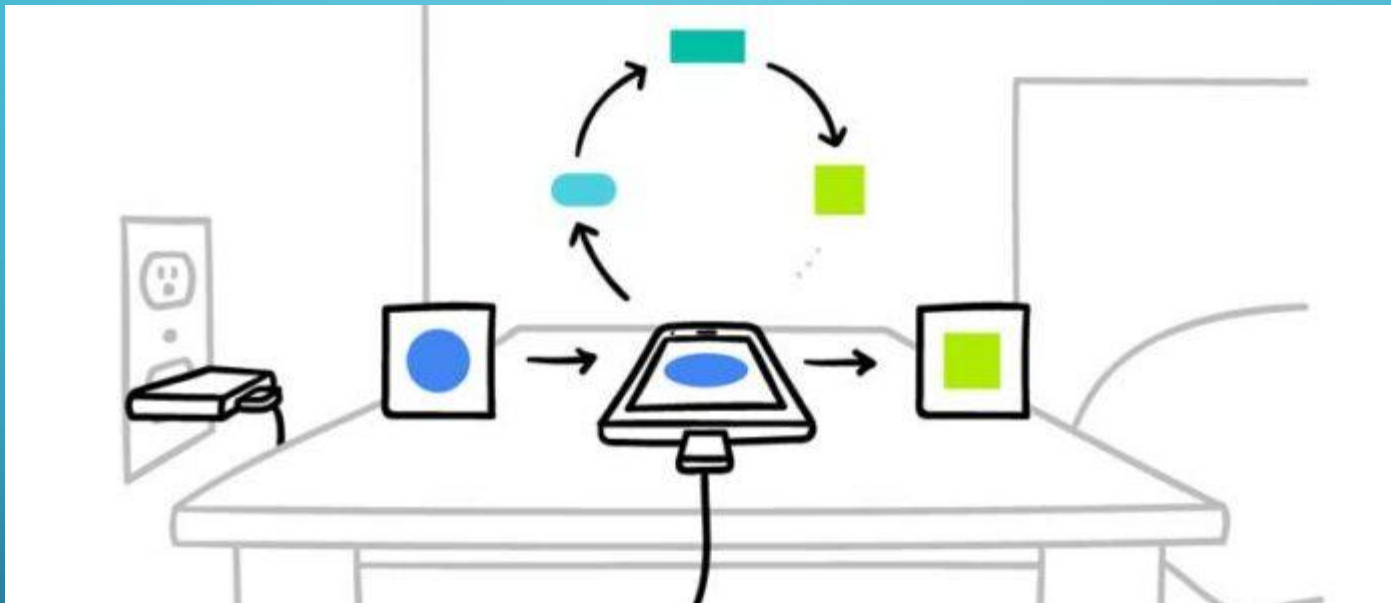


APRENDIZAJE FEDERADO



CARLOS SANTIAGO SÁNCHEZ MUÑOZ

ÍNDICE

- Introducción
- Aprendizaje Federado
- Desde el ruido hacia la verdad
- Cifrado homogéneo
- Funcionamiento
- Tipos
- Ventajas/Desventajas
- Utilidades
- Aplicaciones reales
- Herramientas
- Ejemplo
- Conclusiones

INTRODUCCIÓN

El Aprendizaje Profundo significa el acceso a los datos de entrenamiento.

Los datos de los que se aprende son increíblemente personales.

Un modelo de Aprendizaje Profundo puede estudiar miles de vidas para comprender la tuya.

Dificultades a la hora de poseer esa información tan valiosa.

En 2017, Google publicó un artículo que hizo una mella significativa. No necesitamos centralizar un conjunto de datos para entrenar un modelo sobre él. ¿y si en lugar de llevar todos los datos a un solo lugar, pudiéramos llevar el modelo a los datos?

"Los amigos no espían; la verdadera amistad también se trata de privacidad" Stephen King.

APRENDIZAJE FEDERADO

¿Qué pasa si en lugar de llevar el corpus de datos de entrenamiento a un lugar para entrenar un modelo, pudiera llevar el modelo a los datos donde sea que se generen?

Entrenar modelos valiosos en el cuidado de la salud, la gestión personal y otras áreas sensibles

Panorama competitivo: competencia empresarial

No es necesario tener acceso a un conjunto de datos para aprender de él.

Desafío

Rendimiento y privacidad

- Ataques o fallos de nodos.
- Mucho tiempo enviando el modelo.



DESDE EL RUIDO HACIA LA VERDAD

¿Responderías sinceramente si has cometido un crimen?

Privacidad diferencial: nivel de probabilidad de que una respuesta venga de un ruido aleatorio en lugar de un individuo protege su privacidad.

Agregación segura

CIFRADO HOMOMÓRFICO

Inteligencia Artificial + Criptografía ➡ Encriptación Homomórfica

El cifrado homomórfico permite realizar cálculos sobre valores cifrados.

```
public_key, private_key = phe.generate_paillier_keypair(n_length=1024)

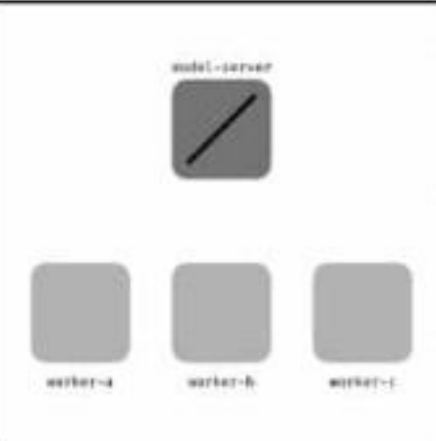
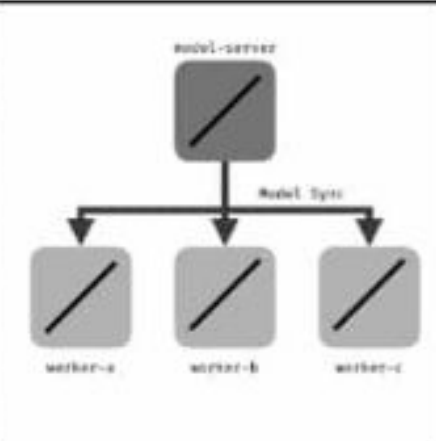
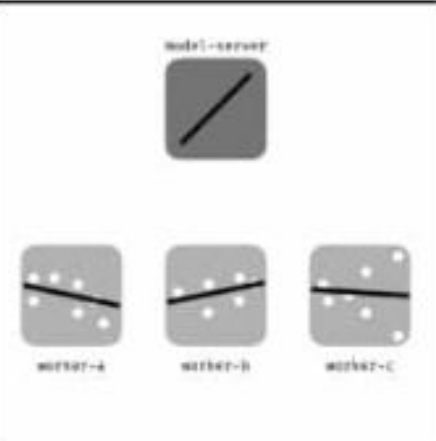
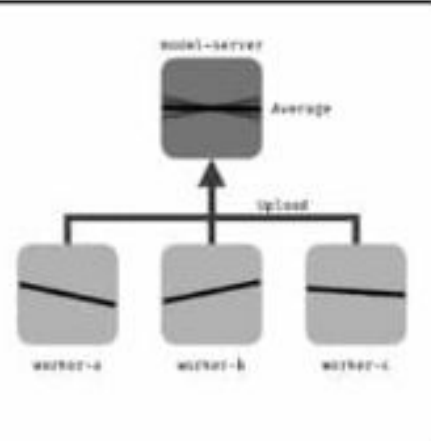
# Se encripta el número 5
x = public_key.encrypt(5)

# Se encripta el número 3
y = public_key.encrypt(3)

# Se suman los dos valores encriptados
z = x + y

# Se desencripta el resultado
z_ = private_key.decrypt(z)
print('The Answer: ' + str(z_))
```

FUNCIONAMIENTO

Step 1	Step 2	Step 3	Step 4
			
Central server chooses a statistical model to be trained	Central server transmits the initial model to several nodes	Nodes train the model locally with their own data	Central server pools model results and generate one global mode without accessing any data

TIPOS

- **Aprendizaje Federado Horizontal**

Dividiendo los datos en varias divisiones. Introduciendo conjuntos de datos similares en un espacio comparable.

- **Aprendizaje Federado Vertical**

Diferentes conjuntos de datos comparten identificaciones de muestra similares pero espacios de características diferentes.

VENTAJAS

- Privacidad de los datos: modelos locales se añaden a la red y ayudan a un modelo general
- Minimizando los inconvenientes que enfrentan los usuarios.
- Ofrece modelos algorítmicos tanto globales como personalizados.
- Termina transfiriendo menos datos en general que en los modelos tradicionales.
- No necesidad de almacenamiento de los datos en un servidor central.
- Se reducen las latencias y el coste de intercambiar datos con un servidor.

DESVENTAJAS

- Depende de la capacidad del dispositivo local para ser entrenado.
Condicionado a las limitaciones de los dispositivos locales en los que se ejecuta.
- Disponer de datos etiquetados para el entrenamiento local.
- Riesgos de posibles ataques o fallas de nodos.
- Aprendizaje Problemas de conectividad en los nodos.
- Hasta ahora, la falta de herramientas.

UTILIDADES

Transporte: Conducción autónoma



Industria 4.0: Fabricación Inteligente

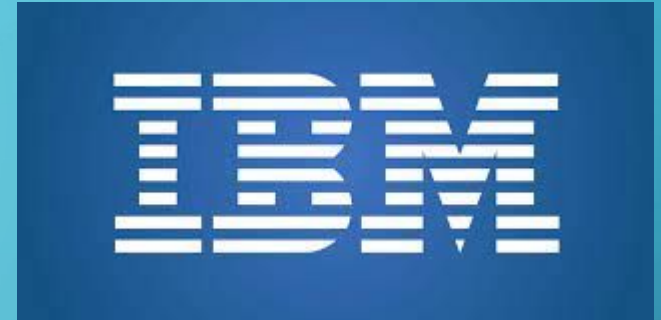


Medicina



APLICACIONES REALES

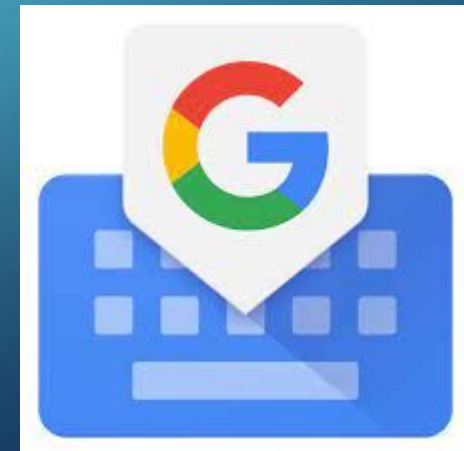
IBM Research



MELLODDY



Google Gboard



HERRAMIENTAS

TensorFlow Federated

PySyft

Federated AI Technology Enabler (FATE)

Sherpa.ai Federated Learning and Differential Privacy Framework

EJEMPLO

```
bob = (train_data[0:1000], train_target[0:1000])
alice = (train_data[1000:2000], train_target[1000:2000])
sue = (train_data[2000:], train_target[2000:])
```

Entrenando:

```
for i in range(3):
    print('Starting Training Round...')
    print('\tStep 1: send the model to Bob')
    bob_model = train(copy.deepcopy(model), bob[0], bob[1], iterations=1)

    print('\n\tStep 2: send the model to Alice')
    alice_model = train(copy.deepcopy(model), alice[0], alice[1], iterations=1)

    print('\n\tStep 3: Send the model to Sue')
    sue_model = train(copy.deepcopy(model), sue[0], sue[1], iterations=1)

    print('\n\tAverage Everyone's New Models')
    model.weight.data = (bob_model.weight.data + alice_model.weight.data
                        + sue_model.weight.data)/3

    print('\t% Correct on Test Set: ' + str(test(model, test_data, test_target)*100))

    print('\nRepeat !!\n')
```

Resultados:

```
Starting Training Round...
Step 1: send the model to Bob
Loss:0.21908166249699718

.....

Step 3: Send the model to Sue
Loss:0.015368461608470256

Average Everyone's New Models
% Correct on Test Set: 98.8
```

CONCLUSIONES

- Uno de los avances más emocionantes en el Aprendizaje Profundo
- Desbloqueará nuevos conjuntos de datos sensibles
- Convergencia entre el cifrado y la investigación en IA
- Un paso más hacia la Inteligencia Artificial confidencial.

¡GRACIAS POR SU ATENCIÓN!

- [1] Dementium. *Aprendizaje federado: ¿es realmente mejor para su privacidad y seguridad?* url: <https://dementium2.com/seguiridad-de-informacion/aprendizajefederado-es-realmente-mejor-para-su/>.
- [2] O'reilly. *Deep learning on unseen data: introducing federated learning*. url: https://www.oreilly.com/library/view/grokking-deep-learning/9781617293702/kindle_split_023.html
- [3] ICHI PRO. *Aprendizaje federado: ¿por qué y cómo empezar?* url: <https://ichi.pro/es/aprendizaje-federado-por-que-y-como-empezar-141963632002703>.
- [4] MIT Technology Review. *Aprendizaje federado: la nueva arma de IA para asegurar la privacidad*. url: <https://www.technologyreview.es/s/11017/aprendizajefederado-la-nueva-arma-de-ia-para-asegurar-la-privacidad>.
- [5] Paloma Recuero de los Santos. *Aprendizaje federado: IA con privacidad*. url: <https://empresas.blogthinkbig.com/aprendizaje-federado-ia-con-privacidad/>.
- [6] Data Science. *Aprendizaje federado*. url: <https://datascience.eu/es/aprendizajeautomatico/aprendizaje-federado/>.
- [7] Andrew W. Trask. *Grokking Deep Learning*.
- [8] Wikipedia. *Aprendizaje Federado*. url: https://es.wikipedia.org/wiki/Aprendizaje_federado.