INSTITUTO TECNOLÓGICO AUTÓNOMO DE MÉXICO

DISEÑO E IMPLEMENTACIÓN DE MODELOS DE REGRESIÓN QUE PRESERVAN LA PRIVACIDAD DE LOS DATOS A TRAVÉS DE UN ESQUEMA DE CRIPTOGRAFÍA HOMOMÓRFICA

OBJETIVOS:

- Diseñar un sistema capaz de entrenar y evaluar modelos de aprendizaje sobre datos encriptados.
- Extender el sistema a uno multicliente en donde se pueda entrenar un modelo común sin que ningún cliente tenga acceso a la información de otro.
- Investigar un esquema de encriptación que permita el cálculo privado en la nube.

DISEÑO E IMPLEMENTACIÓN:

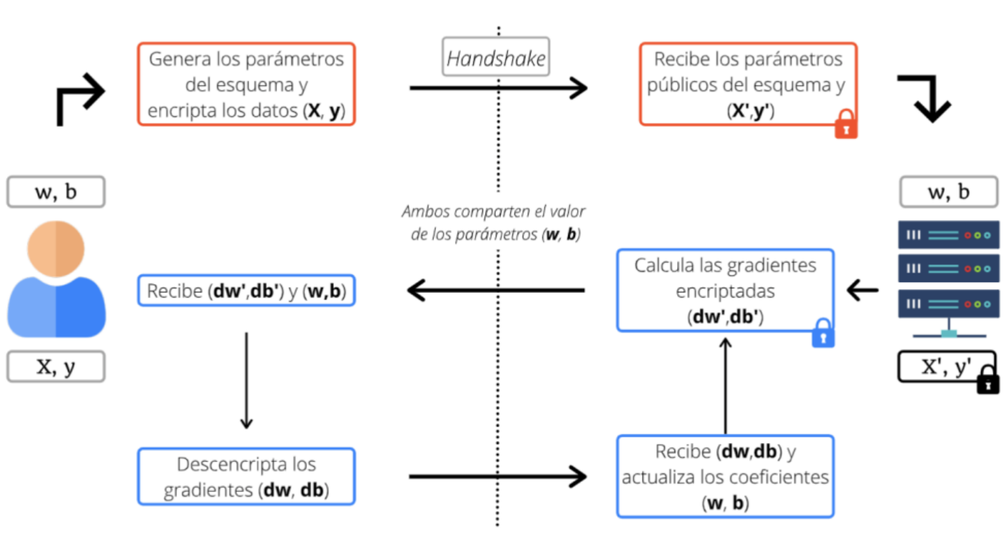

Figura 4.1. Sistema de regresión lineal cliente servidor

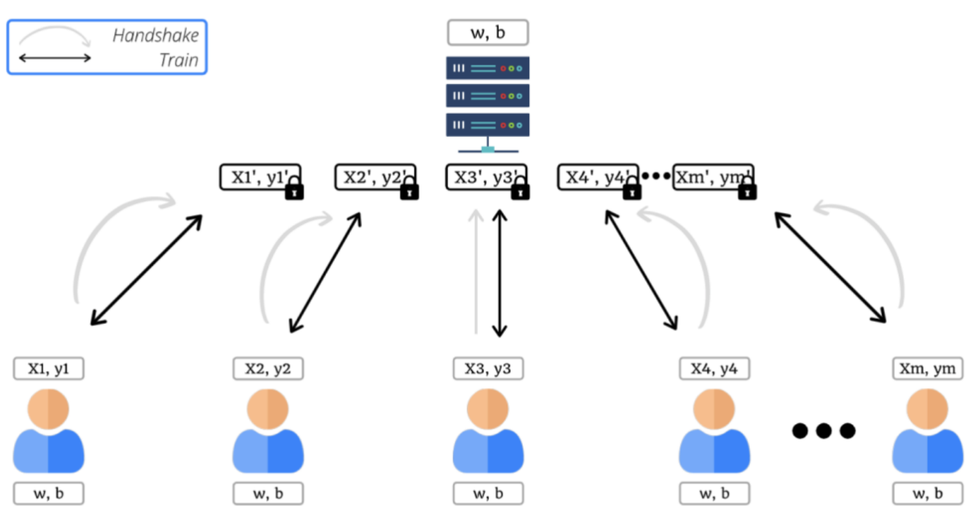

Figura 4.2. Sistema de regresión lineal multi cliente servidor

- Se diseña e implementa un servicio funcional multi cliente con el esquema BFV para entrenar un modelo común de regresión lineal múltiple.

RESULTADOS:

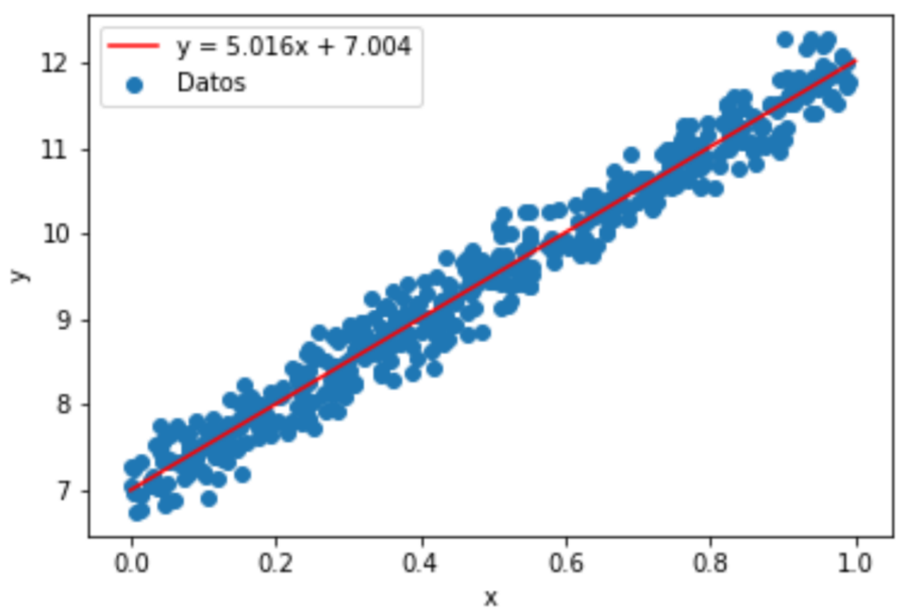

Figura 6.5. Predicción de datos usando el sistema de regresión lineal privado

- El sistema es un módulo en Python cuyo uso es amigable y similar a los modelos de las librerías más populares de aprendizaje de máquina.

CONCLUSIONES:

- Se probó que el sistema calcula una buena aproximación de los mejores coeficientes del modelo de regresión lineal, tanto en modelo cliente servidor como el modelo multi cliente.
- El esquema de cifrado utilizado induce una sobrecarga de tiempo muy considerable (alrededor de mil veces más tardado que el tradicional).

REFERENCIAS:

- Carey, A. (2020). *On the Explanation and Implementation of Three Open-Source Fully Homomorphic Encryption Libraries.*
- Laine, K. (2019) *Homomorphic Encryption with Microsoft SEAL.*
- Benaissa, A. *et al.* (2021). *TenSEAL: A library for Encrypted Tensor Operations Using Homomorphic Encryption*

Alumno: Juan Carlos Sigler Priego
Asesor: Dr. Carlos Fernando Esponda Darlington
Carrera: Ingeniería en Computación
Semestre: Primavera 2022