Privacy-Preserving Machine Learning

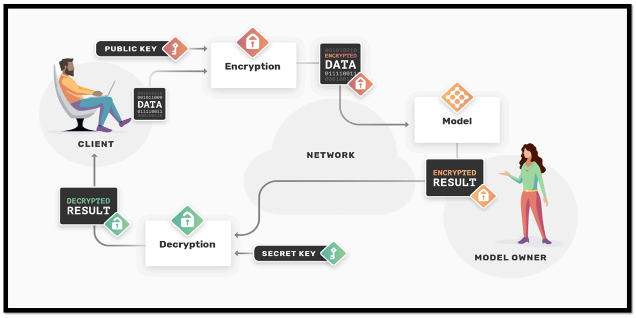
Project Team: David Tran, Minh Nguyen, Bryan Soerjanto, Amaris Young-Diggs
Computer Science
Project Number: CS 25-340

Faculty Advisor(s): Hong-Sheng Zhou, Ph.D.
Sponsor: College of Engineering
Mentor: Hong-Sheng Zhou

The growing demand for machine learning applications has raised significant concerns regarding data privacy in recent years. Traditional machine learning models often require direct access to sensitive data, posing risks of unauthorized exposure and data misuse. This project focuses on developing a Privacy-Preserving Machine Learning (PPML) system that protects sensitive data throughout the entire machine learning lifecycle. Using advanced cryptographic techniques such as homomorphic encryption and secure multi-party computation, this system allows organizations to extract valuable insights from data while maintaining privacy. This is particularly relevant for industries like healthcare, finance, and marketing, where the privacy of personal data is critical. Our solution integrates federated learning, which allows multiple parties to collaboratively train models on decentralized data, ensuring that raw data never leaves local devices.

Keywords: privacy, homomorphic encryption, TenSEAL, practical, machine learning

By combining efficiency, scalability, and robust privacy protection, our project offers a practical solution for organizations seeking to leverage machine learning while adhering to strict privacy regulations and protecting sensitive data. We evaluate the framework on real-world datasets, demonstrating that it achieves strong privacy guarantees with minimal impact on model accuracy. By combining TenSEAL encryption with federated learning and differential privacy, our project offers a scalable, efficient, and practical solution for organizations seeking to deploy privacy-preserving machine learning applications.


PUBLIC KEY
Encryption
ENCRYPTED
DATA
DATA
CLIENT
Model
NETWORK
ENCRYPTED
RESULT
MODEL OWNER
DECRYPTED
RESULT
Decryption
SECRET KEY