Privacy Preserving Machine Learning

Team members: David Tran, Bryan Soerjanto, Amaris Young-Diggs, Minh Nguyen | **Faculty adviser:** Hong-Sheng Zhou, Ph.D. | **Sponsor: VCU College of Engineering** | **Mentor:** Hong-Sheng Zhou

Executive Summary

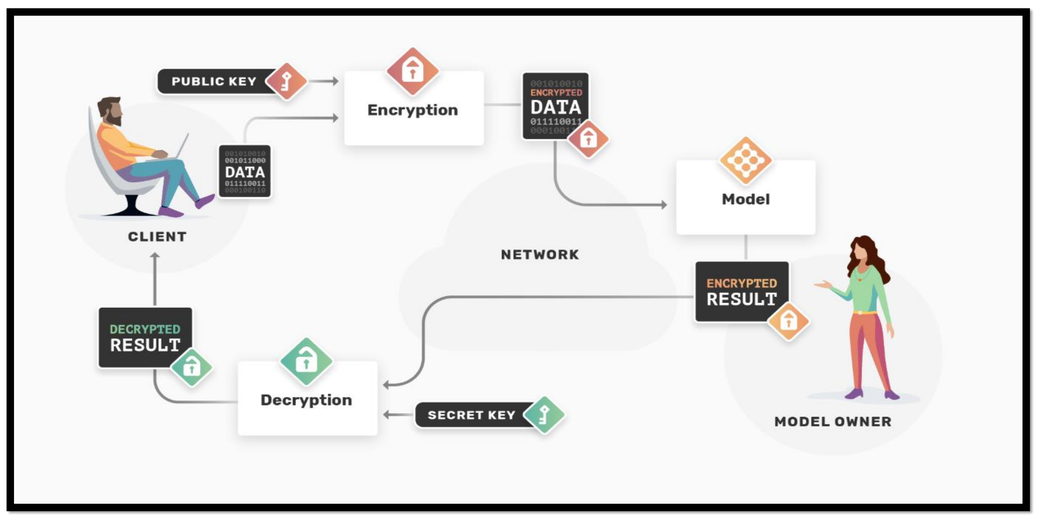
This project focuses on developing a Privacy-Preserving Machine Learning (PPML) system that ensures the protection of sensitive data throughout the entire machine learning lifecycle. Using advanced cryptographic techniques such as homomorphic encryption and secure multi-party computation, this system 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.

Problem Statement

As machine learning expands across industries, privacy concerns about sensitive data like healthcare records and financial transactions are growing. Regulations like GDPR and HIPAA demand data analysis without violating privacy. Traditional methods such as anonymization and aggregation are often inadequate, as they can still lead to re-identification risks. Cryptographic methods, such as homomorphic encryption and secure multi-party computation, offer solutions by enabling computations on encrypted data. The PySyft framework, for example, integrates these techniques to facilitate privacy-preserving machine learning.

Homomorphic Encryption is a form of encryption that allows computations to be performed on encrypted data without needing to decrypt it. This is particularly useful in privacy-preserving machine learning as it enables data scientists to work on sensitive information without exposing the original data. In essence, homomorphic encryption allows functions or algorithms to run on encrypted inputs, producing an encrypted output that can later be decrypted to reveal the final result. This makes it ideal for scenarios where sensitive data must be kept secure throughout the computation process, such as in healthcare or finance.

Secure Computing refers to a variety of techniques and frameworks that protect sensitive data during computation. This often includes multi-party computation (MPC) and secure enclaves. In multi-party computation, multiple parties can collaborate on data without revealing their private inputs, ensuring that only the final result is shared. Secure enclaves provide hardware-based security, creating isolated environments that protect the data and computations within from external interference. These secure computing methods are critical for privacy-preserving applications, as they allow computations to happen without exposing raw data to potentially insecure environments.



Encrypt Data with TenSEAL: Sensitive data is encrypted using TenSEAL's homomorphic encryption techniques. This allows computations to be performed on encrypted data directly. For example, data tensors (multi-dimensional arrays commonly used in machine learning) are encrypted so that they can be used in training or inference without exposing the raw values.

Criterion	Homomorphic Encryption	Federated learning	Hybrid Approach
Data privacy	Higher	Medium	High
Performance Impact	High	Low	Medium
Scalability	Medium	High	Medium
Implementation Complexity	High	Medium	High

PySyft Framework:

PySyft enables a new way to do data science, where you can use non-public information, without seeing nor obtaining a copy of the data itself. All you need is to connect to a Datasite!

Datasites are like websites, but for data. Designed with the principles of structured transparency, they enable data owners to control how their data is protected and data scientists to use data without obtaining a copy. PySyft supports any statistical analysis or machine learning, offering support for directly running Python code - even using third-party Python libraries.

PySyft

VCU College of Engineering