CAPSTONE DESIGN EXPO | Computer Science | CS 25-340

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.

Project Goals:

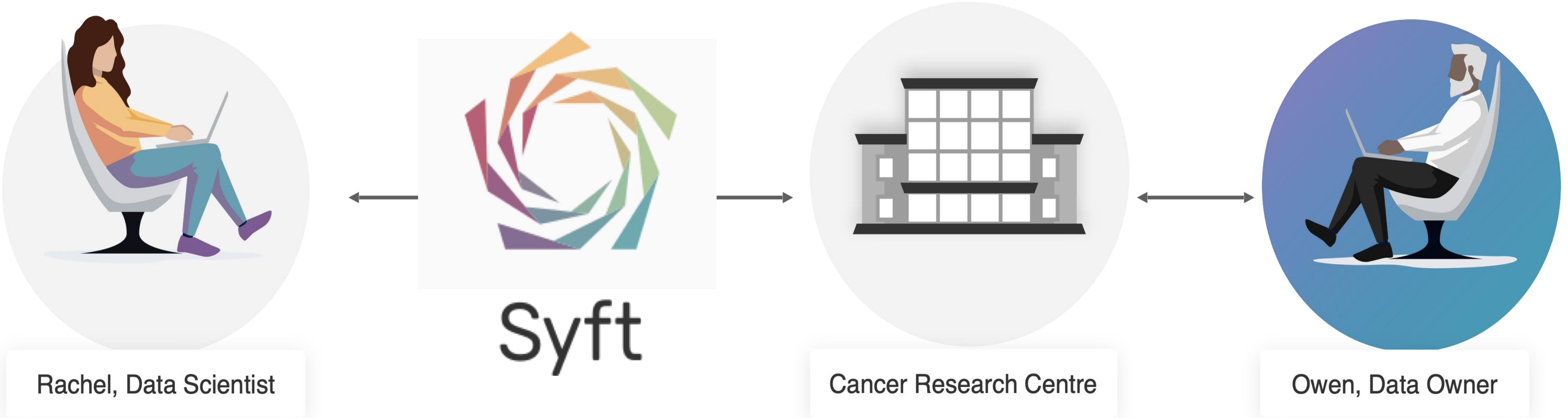
- Design a privacy-preserving machine learning system that protects sensitive data during computation.
- Utilize homomorphic encryption to enable computations on encrypted data without decryption.
- Ensure compliance with data privacy regulations like GDPR and HIPAA.
- Minimize the impact of privacy techniques on model performance.

Design Objectives:

- Implement homomorphic encryption and secure multi-party computation for data protection.
- Balance data utility with privacy preservation.
- Develop a scalable architecture for multiple data sources.
- Ensure usability for non-expert users.

Design Specifications and Constraints:

- **Data privacy:** Prevent exposure of sensitive data during training or inference.
- **Performance:** Maintain model accuracy, limiting reduction to under 10% due to privacy-preserving methods.
- **Compliance:** Adhere to standards like GDPR and HIPAA.
- **Scalability:** Enable the system to handle large datasets with minimal latency impact.
- **Usability:** Allow model deployment with minimal cryptography expertise.



Codes and Standards:

- GDPR (General Data Protection Regulation)
- HIPAA (Health Insurance Portability and Accountability Act)
- ISO/IEC 27001: Information security standards
- FIPS 140-2: Cryptography standards for sensitive data protection

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