Experiment – Suspicious Persons List matching with HE

# Overview

In this experiment, we explore a secure and privacy-preserving method for identifying and matching suspicious persons between two financial institutions using Fully Homomorphic Encryption (FHE). By leveraging FHE, we ensure that sensitive data remains confidential during processing, while still enabling meaningful analysis and machine learning inference.

# Scenario (Use Case)

In this experiment, we explore a secure and privacy-preserving method for identifying and matching suspicious persons between two financial institutions using Fully Homomorphic Encryption (FHE). By leveraging FHE, we ensure that sensitive data remains confidential during processing, while still enabling meaningful analysis and machine learning inference.

# How the Experiment will be run?

The following steps provide a guide on how the experiment will run:

1. **Data Generation**: Synthetic datasets for two financial institutions are created, each containing transaction patterns and labels indicating whether each individual is suspicious.
2. **Model Training**: A logistic regression model is trained on the combined plaintext data to classify transactions as suspicious or not, and the model's accuracy is assessed.
3. **Data Encryption**: The transaction patterns in the test set are encrypted using the SEAL library, ensuring data confidentiality during processing.
4. **Encrypted Inference**: Encrypted inference is performed by computing the linear combination of encrypted features and model coefficients directly on the encrypted data. The results are decrypted, and the sigmoid function is applied to obtain predictions.
5. **Matching Suspicious Persons**: IDs and predictions are encrypted and decrypted to match suspicious persons between the two banks, ensuring that the process remains secure and private.

# Conclusion

This experiment successfully demonstrates the potential of Fully Homomorphic Encryption (FHE) to enable secure and privacy-preserving data analysis in sensitive domains like financial fraud detection. By performing encrypted inference and matching, financial institutions can collaborate and identify suspicious activities without exposing raw data, thus maintaining privacy and compliance with data protection regulations. This approach ensures that sensitive information is kept secure throughout the analysis process, highlighting the practical application of FHE in real-world scenarios.