**Full Homomorphic Encryption (FHE) Experiment**

**Introduction**

In this experiment, we explored the application of Full Homomorphic Encryption (FHE) to secure the results of a fraud detection model. The goal was to encrypt the predictions generated by a machine learning model, allowing secure communication of sensitive data between financial institutions and their customers.

**Synthetic Data Generation**

We manually generated synthetic data to simulate a scenario where all transactions are suspicious. The dataset consisted of five records, each containing details like the cardholder's name, customer ID, age, transaction amount, credit score, and a binary indicator of fraud (IsFraud). All records were marked as fraudulent, with high transaction amounts and low credit scores to reflect typical fraud patterns.

**Model Training and Evaluation**

A Linear Regression model was trained on the synthetic data to predict the likelihood of fraud. Despite the simplicity of the model and the small dataset size, we split the data into training and testing sets to maintain a structured approach. After training, the model's performance was evaluated using metrics like the Confusion Matrix and Classification Report. Since the test set contained only one class, the ROC AUC score was not applicable.

* Confusion Matrix: Showed that all predictions were correctly classified as fraudulent.
* Classification Report: Indicated perfect precision, recall, and F1-score, demonstrating the model's accuracy on this small dataset.

**Full Homomorphic Encryption (FHE)**

The predictions from the model were encrypted using the TenSEAL library, which supports the CKKS scheme for FHE. This allowed us to perform both addition and multiplication on the encrypted predictions, demonstrating the key capabilities of FHE. The encrypted results were serialized into a JSON format, making them suitable for transmission over the web.

**Risk Interpretation**

To make the encrypted results understandable to end users, we decrypted the results and provided risk interpretations. Transactions were classified as "High Risk," with a strong likelihood of being fraudulent. This classification was based on predefined thresholds applied to the decrypted values.

**Conclusion**

This experiment successfully demonstrated the use of FHE in securing model predictions for fraud detection. The encrypted data can be safely transmitted between institutions, ensuring privacy and security. The risk interpretations provide clear guidance to customers or institutions on the potential fraudulent nature of transactions.