DATA PRIVACY AND SECURITY

PROJECT PROPOSAL

Title: Confidential Market Basket Analysis for Enhanced Retail Insights

Team Members:

- **Satya Subhash Yellina(A20545769)**
- **Uday Kiran Muppavarapu(A20544881)**
- **Vivekananda Reddy Kotha(A20548456)**

Overview:

The goal of this project is to create a secure and confidential framework for conducting market basket analysis, a method utilized by retailers to identify correlations between concurrently purchased items. The framework will empower retailers to extract insights into consumer buying patterns while safeguarding the privacy of individual transactions.

Attack Scenario:

We will explore a scenario in which a retailer seeks to analyze transaction data to pinpoint items frequently bought together and determine item associations for marketing and inventory management purposes, all while maintaining the confidentiality of individual customers' transaction data.

Dataset:

A publicly accessible market basket dataset will be employed, such as the Online Retail dataset, which comprises anonymized transaction data from a UK-based online retail store.
https://www.kaggle.com/code/hassanamin/market-basket-analysis-for-online-retail-dataset/input?select=OnlineRetail.csv

Proposed Application:

The application will carry out market basket analysis to ascertain association rules and frequent itemsets within the transaction data, all while upholding the privacy of individual transactions. The analysis will be executed in a manner that preserves the privacy of customers' purchasing data.

Anticipated Building Blocks:

Cryptographic Schemes: Secure multi-party computation (SMPC) techniques will be utilized to facilitate joint computations on encrypted transaction data, ensuring the confidentiality of the raw data.

Anonymization Mechanisms: Data anonymization techniques will be implemented to guarantee that individual transactions are indistinguishable in the aggregated data.

Differential Privacy: To offer a robust privacy assurance, differential privacy techniques will be applied to introduce noise to the analysis results, ensuring that the output does not disclose sensitive information about any specific transaction.

Expected Outcomes:

- A confidential and secure system for market basket analysis that protects customers' privacy while delivering valuable insights into purchasing patterns.
- An assessment of the system's efficacy in terms of privacy protection and the usefulness of the analysis results for retail decision-making.
- A demonstration of how the system can be seamlessly integrated into retail analytics platforms for secure and privacy-preserving market basket analysis.