Fraud and Spam Call Detection Models Summary

1. CDR Fraud Detection Model

Model:	CDR Fraud Detection Model
Dataset:	data/CDR-Call-Details.csv
Features:	'Day Mins', 'Day Calls', 'Eve Mins', 'Eve Calls', 'Night Mins', 'Night Calls', 'Intl Mins', 'Intl Calls', 'CustServ Calls'
Target:	isFraud (1 = Fraud, 0 = Not Fraud)
Algorithm:	Random Forest Classifier (n_estimators=100)
Preprocessing:	Standard train-test split (80-20)
Performance Metric:	Accuracy and Classification Report
Model File:	cdr_fraud_model.pkl
Output:	Printed as: 'CDR Fraud Model Accuracy'

2. Spam Text Detection Model

Model:	Spam Text Detection Model
Dataset:	data/fraud_call.file
Label:	label (1 = Fraud, 0 = Not Fraud)
Preprocessing:	Special character removal, stopword removal
Feature Extraction:	TF-IDF Vectorization (max_features=500), saved as tfidf_vectorizer.pkl
Algorithm:	Support Vector Machine (SVM) with linear kernel
Performance Metric:	Accuracy and Classification Report
Model File:	spam_text_model.pkl
Output:	Printed as: 'Spam Detection Model Accuracy'

3. Adaptive Ensemble Approach

Ensemble Strategy:	Adaptive Ensemble Approach
Logic:	If either model predicts 1 (fraud/spam), final prediction = 'Fraud/Spam Call Detected', else 'Safe Call'
Benefit:	Leverages both numerical and textual features for improved detection
Final Prediction:	Based on OR logic between predictions of both models