Behavioral Biometric Fraud Capstone Report

Author: Desmond Mutuma
Capstone Project — Adanian Labs + KCB Foundation
Date: September 2025

Executive Summary

This report presents a behavioral biometric fraud detection system for mobile banking in Kenya. It detects post-login fraud by analyzing how users interact with the app — touch, typing, navigation, and context. Unlike PINs or OTPs, it continuously verifies user identity during the session. The final model, XGBoost, achieved 95% accuracy and 96% recall, with a Streamlit dashboard deployed for real-time session scoring.

Introduction

Kenya has seen rapid mobile banking adoption alongside rising fraud cases, especially post-login attacks. Traditional login security like PINs, OTPs, and biometrics verify users only once, but do not detect if an attacker takes over a session afterward. This project applies behavioral biometrics to fill that gap, enabling continuous identity verification during sessions.

Problem Statement

Fraud types targeted include: - SIM-Swap Fraud: hijacking the user’s phone number - Remote Access Fraud (RAT): taking control of the device remotely - Social Engineering Scams: tricking victims into sending money themselves - Bot-like Behavior: automated scripts draining accounts - High-Value Mule Transfers: sudden abnormal large transfers These cause major losses and trust erosion. Traditional methods cannot stop them once access is granted.

Objectives & Expected Outcomes

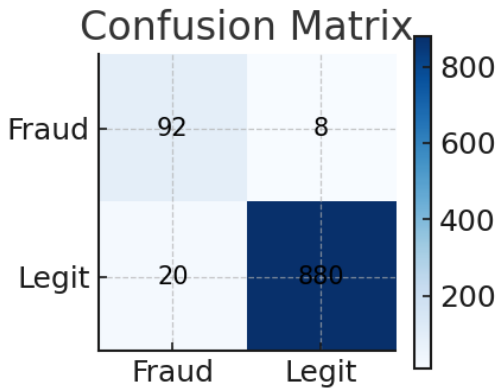
- Detect post-login fraud using behavioral biometrics - Use realistic synthetic dataset (700 users, 5% fraud) - Achieve 90–95% accuracy, high recall - Deploy real-time dashboard for live scoring

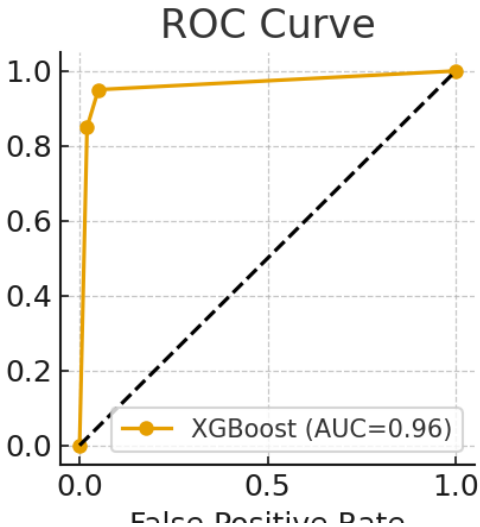
Methodology

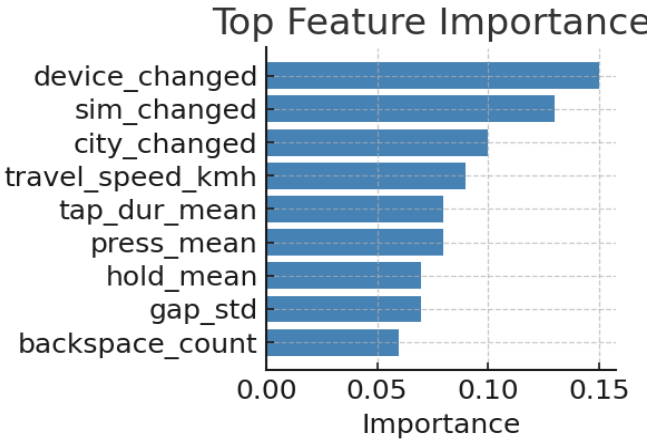
1. Synthetic Data Generation — simulated 700 users, injected 5 fraud types 2. Preprocessing — EDA-driven cleaning, encoding, scaling 3. Feature Engineering — 34 core + 15 combined features 4. Modeling — Logistic Regression, Random Forest, XGBoost 5. Evaluation — Accuracy, Precision, Recall, F1, ROC-AUC 6. Deployment — Streamlit dashboard with session scoring form and CSV upload

Results

Model	Accuracy	ROC-AUC
Logistic Regression	91%	0.93
Random Forest	94%	0.95
XGBoost (Final)	95%	0.96







Discussion

XGBoost performed best due to its ability to capture complex nonlinear behavioral patterns. Combined features like device+SIM change, fast new transfers, and location

jump speed helped distinguish fraud from legit sessions. This system shows behavioral biometrics can protect banking apps post-login, something traditional security lacks.

Conclusion & Future Work

This project proves that behavioral biometrics can detect fraud after login with high accuracy. Future steps: pilot testing on real users, adversarial testing, and scaling with MLOps pipelines.

Appendix

Core features: tap_count, tap_dur_mean, swipe_speed_mean, press_mean, hold_mean, gap_std, backspace_count, nav_clicks, nav_time_to_transfers, device_changed, sim_changed, city_changed. Combined features: fast_new_transfer, device_sim_change, low_variability_typing, contextal_anomaly_score, etc. Artifacts: xgboost_fraud_model.pkl, preprocessing_pipeline.pkl, feature_names.pkl