**Capstone Project Report: Mobile Money Fraud Detection in Rwanda**

**1. Introduction**

This capstone project focuses on detecting fraudulent mobile money transactions in Rwanda using machine learning techniques. We used a synthetic dataset sourced from Mendeley Data and applied anomaly detection to identify suspicious activities.

**2. Dataset Overview**

The dataset used contains approximately 1.7 million transactions with 10 columns, including transaction amounts, timestamps, balances, and fraud indicators. The data was structured in CSV format and required preprocessing before analysis.

**3. Methodology**

The project was conducted in the following steps:  
- Data cleaning using pandas (e.g., handling missing values, datetime parsing)  
- Exploratory Data Analysis (EDA) using matplotlib and seaborn  
- Anomaly Detection using Isolation Forest algorithm  
- Visualization of fraud detection results using Python and Power BI

**4. Key Graphs and Visuals**

The following charts were generated during EDA and anomaly detection:

- Transaction Amount Distribution

- Fraud vs Non-Fraud Count

- Boxplot of Amount by Fraud Status

- Correlation Heatmap

- Anomaly Scatter Plot (Red = Fraud, Blue = Legitimate)

- confusion matrix

- Transaction amount over time

- Anomaly vs Normal transaction

Additional visualizations were built in Power BI for dashboard reporting.

**5. Conclusion**

Machine learning, specifically Isolation Forest, proved effective in identifying anomalous transactions. Visual tools like Power BI enhanced interpretability and allowed stakeholders to explore suspicious patterns interactively. This project demonstrates how data science can improve financial security and fraud prevention in digital economies like Rwanda.

**6. Tools Used**

• Python (pandas, seaborn, matplotlib, scikit-learn)  
• Power BI  
• Mendeley Data  
• VS Code & GitHub