UGANDA TECHNOLOGY AND MANAGEMENT UNIVERSITY

UTAMU

For an Open Mind

PROPOSAL FOR AN AI-DRIVEN ANOMALY DETECTION AND FRAUD PREVENTION SYSTEM IN UGANDA'S MOBILE MONEY SYSTEM

By
MIVULE NELSON AND ERECHO JONATHAN
SCHOOL OF COMPUTING AND ENGINEERING

A Concept Paper submitted to the School of Computing and Engineering in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Science in Computer Security and Forensics of Uganda Technology and Management University

Supervisor

Mr. Allan Ninyesiga
School of Computing and Engineering, Uganda Technology and Management University
aninyesiga@utamu.ac.ug, +25670437694

JULY 2025

Preface

This proposal outlines the development of an AI-driven anomaly detection and fraud prevention system specifically tailored for Uganda's rapidly expanding mobile money ecosystem. In an era where digital financial services are paramount for economic inclusion and growth, the escalating threat of sophisticated financial fraud poses a significant challenge. This document addresses the urgent need for a robust, adaptive, and privacy-preserving solution to safeguard mobile money transactions, protect vulnerable users, and reinforce public trust in digital finance.

Authored by Mivule Nelson and Erecho Jonathan from the School of Computing and Engineering at Uganda Technology and Management University, under the esteemed guidance of Mr. Allan Ninyesiga, this proposal represents a comprehensive approach to combating financial crime. It ransacks into the current landscape of mobile money fraud in Uganda, critically reviews existing global AI-driven fraud detection systems, and proposes a unique methodology centered on Federated Learning and collaborative intelligence. By integrating advanced machine learning models, multi-factor authentication, and a strong emphasis on data privacy, this system aims to provide a resilient defense against evolving threats, ensuring the integrity and security of Uganda's vital mobile money infrastructure.

This work is a testament to the commitment to leveraging cutting-edge technology for societal benefit, contributing not only to the security of financial transactions but also to the advancement of science, technology, and academia within the Ugandan context and beyond.

Declaration

We, Mivule Nelson and Erecho Jonathan declare that this is our original work and has never been submitted anywhere for any award.

Students Signature……. mivuleneslon and erechjonathan………... Date….17th July 2025…….

Approval

This work has been submitted for examination with the approval of

…..............................

Mr. Allan Aninyesiga

Department of Engineering and Computing

Contents

CHAPTER ONE: INTRODUCTION

1.0. Introduction

Uganda's fast-evolving digital financial sector especially its growing mobile money ecosystem is increasingly vulnerable to sophisticated fraud. This proposal presents an AI-driven system for detecting anomalies and preventing fraud in mobile money transactions. By applying advanced machine learning and privacy-preserving technologies, the solution ensures secure and adaptive protection. It is specifically designed to strengthen the integrity and resilience of Uganda's mobile money infrastructure. The project offers a smart, collaborative approach to combating financial crimes that heavily impact mobile money users.

1.1. Background

Uganda’s financial sector is grappling with a significant and growing threat from financial crimes, with mobile money services being a primary target. In 2024 alone, economic crimes including Cyber fraud and bank scams resulted in losses exceeding USD 272 million. A study by the Financial Intelligence Authority in June 2022 revealed that fraud was rampant and increasingly sophisticated, with Cyber fraud accounting for over 50% of high-value cases and annual losses more than doubling. The rapid expansion of digital financial services, especially mobile money, which saw registrations surge to 36.8 million in 2023, has inadvertently created a larger attack surface for criminals. This digital transformation, while offering convenience and bridging financial inclusion gaps, has led to a concerning statistic: one in three mobile money users reported being targeted by fraudsters in 2020. The Uganda Police Force Annual Crime Report further substantiates this trend, noting a 93% increase in Cybercrime from 2023 to 2024. In 2022, Uganda recorded financial losses of UGX 19.2 billion due to mobile money fraud alone.

The types of fraud prevalent in Uganda’s mobile money sector are diverse and continuously evolving. External threats include deceptive fake loan scams where fraudsters promise quick loans for an upfront “processing fee”. Fake supplier scams involve impersonating legitimate vendors to solicit upfront payments for goods that are never delivered. Phishing and fraudulent emails are widespread, with scammers mimicking legitimate entities to steal sensitive information. Money laundering involving the placement, layering, and integration of illicit funds remains a persistent challenge, as does terrorism financing. Digital threats have become particularly sophisticated, encompassing account takeover fraud, where login credentials are stolen to access victim accounts, and synthetic identity fraud, where criminals combine real and fabricated information to create entirely new identities. Mobile money users are frequently targeted by SIM card fraud, unauthorized access, identity theft, and social engineering tactics that manipulate individuals into revealing personal details like PINs. Internal fraud involving misappropriation of assets, manipulation of financial records, and embezzlement also contributes significantly to losses, often exacerbated by weak internal controls, poor remuneration, and inadequate monitoring within institutions, particularly Microfinance Institutions. The increasing sophistication of these schemes is underscored by fraudsters' growing use of advanced technologies, including generative AI, to craft highly convincing phishing emails and even generate functional malware, raising the stakes in the fight against financial crime.

Current fraud detection mechanisms in Uganda face significant limitations, particularly in the mobile money domain. Traditional rule-based systems and conventional machine learning models struggle to keep pace with the rapidly evolving fraud patterns and the immense volume of digital transactions characteristic of mobile money. These systems frequently produce high false positives, leading to legitimate customers being mistakenly flagged as fraudsters, which results in poor user experiences, abandoned transactions, and increased operational costs for mobile money operators and financial institutions. A substantial number of mobile money fraud incidents go unreported, hindering the development of a comprehensive understanding of the threat landscape and limiting the ability to learn from past events. While Uganda has established legal frameworks such as the Computer Misuse Act 2011 and the Data Protection and Privacy Act 2019, these regulations alone have proven insufficient in deterring digital fraud, highlighting the urgent need for a holistic, technology-driven approach. Recent legal rulings in Uganda emphasize a shared responsibility between financial service providers and customers in fraud prevention, yet these rulings also reveal instances where providers failed to implement adequate fraud detection systems or overlooked critical red flags such as mismatched account details. This situation underscores that the rapid expansion of mobile money services has outpaced digital literacy among some segments of the population, particularly vulnerable groups. When these individuals fall victim to mobile money fraud, they not only suffer direct financial losses but also lose trust in informal financial systems, potentially reverting to less efficient, cash-based transactions. This erosion of trust among the most susceptible users poses a systemic risk, capable of reversing the significant gains made in financial inclusion and impeding overall economic development. The ongoing dynamic where malicious actors leverage advanced AI tools to enhance their fraudulent activities means that any effective defense must be equally adaptive, continuously learning, and capable of countering these sophisticated AI-enhanced threats.

1.3. Problem statement

Uganda's mobile money sector is experiencing a surge in sophisticated fraud, driven by rapid digital growth and outdated detection tools. In 2024 alone, over $272 million was lost, weakening public trust and hindering financial inclusion for vulnerable users. Fraudsters are leveraging advanced AI, outpacing traditional systems and escalating an AI arms race. To protect the sector and build a fair digital economy, stronger fraud prevention is urgently needed and thus a proposal for an AI-powered solution, designed to counter these evolving threats in the Uganda's financial sector.

1.4. Main objective

To enhance the integrity and security of Uganda’s mobile money sector while preserving user privacy through an advanced collaborative AI-driven anomaly detection system and multi-factor authentication for every transaction.

1.4.1. Specific objectives

To develop robust AI models that detect various mobile money fraud types in real-time by analyzing diverse transaction data and behavioral patterns unique to mobile money usage.

To implement a privacy-preserving data collaboration framework like Federated Learning, allowing mobile money operators and other financial institutions to jointly train models without sharing sensitive customer data.

To establish a centralized hub for real-time sharing of anonymized mobile money fraud indicators and best practices among financial institutions and regulators, strengthening collective defense.

To enhance AI system efficiency by reducing false positives, minimizing customer disruption, and ensuring accurate mobile money fraud detection with high precision and recall.

To build local AI/ML expertise through training programs for financial staff and regulators, promoting continuous learning and adaptation to emerging mobile money fraud threats.

To integrate robust multi-factor authentication (MFA) mechanisms for every new transaction made on a given user account in any mobile money service, ensuring enhanced security and user verification.

2.0. Research Significance

This section articulates the profound impact of the proposed AI-driven anomaly detection and fraud prevention system across various dimensions, emphasizing its relevance to Uganda's unique mobile money context.

2.1. To Society

The surge in AI-driven fraud within Uganda's mobile money sector threatens national economic stability with over $272 million lost in 2024 alone. This undermines public trust especially among vulnerable groups and risks reversing gains in financial inclusion. Deploying an advanced AI solution is vital to protect livelihoods, strengthen digital trust and support equitable development across Ugandan society.

2.2. To Science and Technology

This project marks a major advancement in AI for financial crime prevention by developing cutting-edge privacy-preserving models tailored to the unique challenges of mobile money fraud in Uganda. IT introduces novel applications of Graph Neural Networks, Long Short-Term Memory networks (LSTMs) and Federal Learning to detect complex fraud patterns while safeguarding user data, setting a global benchmark for secure AI collaboration. The outcomes will contribute significantly to scientific innovation and offer scalable solutions for secure digital financial in developing nations worldwide.

2.3. To Academia

This project will generate vital empirical data on AI deployment in mobile money, addressing real-world challenges like imbalanced data, privacy and regulatory gaps in Uganda. It supports academic research across AI, law, economic and social sciences, enriching discourse on responsible AI in developing contexts. By fostering local expertise and interdisciplinary collaboration, it offers a model for African AI innovation and global academic advancement in ethical inclusive digital finance.

3.0. Research Scope

This section delineates the boundaries and focuses of the proposed AI-driven anomaly detection and fraud prevention system, outlining its technical, geographical, and temporal dimensions, with a specific emphasis on Uganda's mobile money transactions.

3.1. Technical Scope

This project’s technical scope focuses on building a robust scalable and adaptive AI system to detect mobile money fraud in real-time by analyzing transaction data and user behavior. It leverages advanced models such as LSTMs, Auto-encoders and Graph Neural Networks to uncover complex and evolving fraud patterns, while ensemble methods like XGBoost enhance accuracy in imbalanced datasets. Privacy-preserving techniques especially Federated Learning ensure regulatory compliance and enable secure collaboration across institutions without exposing sensitive customer data. Real- time processing and intelligent risk scoring minimize false positives and improve user experience, while multi-factor authentication adds a strong layer of traditional security. Designed for seamless integration and scalability, the system supports Uganda's rapidly growing mobile money sector and can be adopted broadly across financial institutions.

3.2. Geographical Scope

The project primarily targets Uganda, tailoring its AI system to the country's unique mobile money ecosystem including fraud types, regulatory frameworks and user behaviors. With over 36.8 million mobile money users and widespread digital adoption, Uganda presents a high-impact environment for fraud prevention innovation. The system is designed for diverse financial institutions including banks, microfinance institutions and mobile money operators. Its privacy-preserving, federated architecture enables secure collaboration and positions it for regional scalability across East Africa. This supports broader goals of cross-border fraud defense, Cybersecurity integration and positions Uganda as a regional leader in secure AI deployment for mobile finance.

3.3. Time Development Phases Scope

The project will follow a phased approach, typical for complex AI system development, ensuring iterative improvement and adaptation, with a focus on the mobile money ecosystem.

3.3.1. Phase 1: Assessment and Foundation (1-2 weeks)

The phase will focus on deeply understanding Uganda's mobile money ecosystem including data characteristics, regulation and stakeholder needs to ensure a context-specific solution. Key activities will include requirement gathering, literature review, stakeholder engagement and early data assessment for AI feasibility.

3.3.2. Phase 2: Pilot and Proof of Concept (4-6 weeks)

The pilot phase will validate the AI and privacy-preserving techniques by developing a minimum viable product focused on anomaly detection and Federated Learning with select mobile money operators. Using anonymized or synthetic data, this phase tests model performance on imbalanced datasets and privacy collaboration, identifying technical challenges and refining the system.

Successful outcomes will demonstrate real-world benefits, build stakeholder confidence and pave the way for full-scale deployment.

3.3.3. Phase 3: Software Development, Integration and Scaling (7-22 weeks)

This phase will focus on full-scale software development and integration of the AI fraud detection system across multiple mobile money operators and financial institutions in Uganda, ensuring seamless, privacy-preserving data flow. It includes refining AI models for continuous learning, adapting to emerging fraud pattens and scaling infrastructure to process high transaction volumes in real-time. Successful deployment will enable robust, collaborative defense through Federated Learning, overcoming legacy system challenges and strengthening nationwide fraud prevention.

3.3.4. Phase 4: Continuous Optimization and Capacity Building (Ongoing)

Given the evolving nature of mobile money fraud, the system requires continuous learning, regular AI models updates and ongoing monitoring to stay effective. The phase also emphasizes building local AI/ML expertise through financial staff and regulators, ensuring skilled human oversight and responsible governance. Sustained optimization and capacity building will secure the project’s long term impact and foster innovation in Uganda's mobile money sector.

CHAPTER TWO: LITERATURE REVIEW

2.0. Introduction

The global rise of digital financial services especially mobile money in developing countries like Uganda, has greatly improved financial inclusion but also increased sophisticated fraud risks. Traditional rule-based fraud detection struggles to keep up with evolving threats and transaction volumes. This literature review examines the shift to AI and Machine Learning solutions worldwide, highlighting their advancement and challenges particularly for mobile system.

2.1. Review of Existing AI-Driven Fraud Detection Systems

This section reviews six leading AI-based fraud detection systems used by major global financial institutions focusing on their features, mechanisms and limitations. It highlights gaps these systems leave unaddressed which the proposed solution for Uganda's mobile money aims to overcome.

2.1.1. JPMorgan Chase COiN (Contract Intelligence)

Developed by JPMorgan Chase in the USA n 2017, COiN is an AI system that uses Natural Language Processing and Machine Learning to automate the review of commercial loan documents, aiming to save over 360,000 legal hours annually. It scans and understands legal documents, extracts key clauses, structures unstructured data and learns from historical patterns to flag irregularities that may indicate fraud. While effective for internal document analysis, COiN is not designed for real-time fraud detection or high-volume transactions streams typical of mobile money systems. It lacks capabilities for analyzing behavior transaction patterns or operating across multiple financial institutions. The system is centralized, posing privacy and data-sharing concerns that conflict with Uganda's regulatory needs. CoiN also does not support privacy-preserving collaboration such as Federated Learning, critical for Uganda's multi-operator mobile money environment. Its scope is limited to structured legal data and does not adapt well to the dynamic, fast-paced nature of mobile money fraud. Therefore, it falls short of addressing the real-time, decentralized and privacy-sensitive requirements of Uganda's mobile financial ecosystem.

2.1.2. Bank of America Erica

Erica, Bank of America's AI assistant in the USA, is a leading chatbot in the banking industry, implemented to enhance customer service and help users manage their finances. While its specific launch date is not provided, it is an established AI assistant. The system was developed primarily to provide personalized financial insights and track transaction patterns, blending customer service with real-time fraud monitoring to boost customer trust. Erica uses Natural Language Processing (NLP) and Machine Learning (ML) to understand user queries, provide tailored information, and alert users to unusual activity instantly. It also helps users access security meter levels and learn about scam red flags. However, Erica's fraud detection capabilities are primarily focused on individual customer accounts within Bank of America's ecosystem. It does not facilitate collaborative intelligence sharing across different financial institutions or mobile money operators, which is crucial for detecting complex, multi-provider mobile money fraud schemes. Its current iteration does not use generative AI or large language models for its core AI, potentially limiting its adaptability to novel mobile money fraud tactics compared to more advanced AI systems.

2.1.3. HSBC Quantexa Partnership

HSBC, a global bank based in the UK, partnered with Quantexa, a UK-based company founded in 2016, to develop a fraud detection tool. HSBC became an early adopter of Quantexa's Q Assist technology suite, piloting it as part of Quantexa's Lighthouse Program, with Q Assist expected to be publicly available by early 2025. The partnership was formed to fight financial crime at scale, automate and augment decision-making for investigators, and move beyond rule-based solutions that produced high false positives. The aim is to streamline analysis, investigation, and reporting, and enhance the accuracy and reliability of generative AI models. Quantexa's Decision Intelligence Platform uses AI and machine learning, leveraging a knowledge graph capability, to connect siloed data and provide a contextual view of customers and counterparties. This helps identify and prevent financial crime, including money laundering, by flagging suspicious activity and reducing case volumes. While powerful in connecting internal data, the provided information does not explicitly detail a privacy-preserving mechanism for external collaboration with other financial institution mobile money operators to share fraud insights or models without sharing raw data, which is a key requirement for Uganda’s mobile money sector.

2.1.4. Rabobank's AI for Authorized Push Payment (APP) Fraud Prevention

Rabobank, a bank in the Netherlands, has been leveraging machine learning applications in financial economic crime (FEC) for many years. Over the past two-and-a-half years (from June 2025), Rabobank has re-engineered its compliance stack, integrating ML, advanced data platforms, and generative AI. This initiative was driven by the need to combat rising global fraud losses and money laundering, particularly Authorized Push Payment (APP) fraud, by enhancing detection, prevention, and workflow automation. Rabobank uses AI to analyze suspicious transaction patterns, account behavior, and timing to prevent APP fraud. Their approach integrates machine learning, data platforms, and generative AI to automate workflows like onboarding, case management, and reporting, and they are experimenting with AI-generated draft reports to allow compliance officers to focus on risk analysis. They also emphasize responsible AI governance frameworks with bias monitoring and drift detection. While Rabobank demonstrates strong internal AI capabilities, the available information does not indicate a mechanism for cross-institutional, privacy-preserving model training to detect fraud patterns that span multiple mobile money operators or banks, which is crucial for a collaborative system in Uganda.

2.1.5. Mastercard Decision Intelligence Platform

Mastercard, a global payment technology company, introduced its Decision Intelligence platform in December 2016 as the first use of AI implemented on a global scale directly on the Mastercard network. An even more advanced version, Decision Intelligence Pro, was rolled out in 2024. The platform was developed to increase the accuracy of real-time approvals for genuine transactions, reduce false declines, and prevent fraud, aiming to boost cardholder trust and loyalty while lowering operational costs. The Decision Intelligence platform processes over 1.3 billion transactions daily, analyzing more than 200 variables per authorization request. It uses AI and Machine Learning techniques, along with unique network insights, to generate a transaction score and reason code. It establishes a behavioral baseline from cardholders' historical shopping and spending habits to compare new transactions, moving beyond a "one-size-fits-all" approach. While operating at a global network level, Mastercard's system is proprietary and centralized within its network. It does not offer a framework for individual financial institutions or mobile money operators (especially those outside its direct network or in developing regions like Uganda) to contribute their private, raw transaction data to a shared, collaboratively trained model while maintaining data sovereignty, which is a core tenet of the proposed system for mobile money.

2.1.6. Feedzai Platform

Feedzai, a financial technology company founded in 2011, developed its platform to identify and eradicate financial crimes such as fraud in real-time, covering the entire financial crime lifecycle from account opening to AML compliance. The platform aims to reduce false positives and enhance fraud detection accuracy. Feedzai's AI-native platform leverages AI-based individual risk profiles and behavioral analytics to profile normal customer behavior, making it easier to spot abnormal, fraudulent events. It uses continuous and rapid evaluation of large amounts of data to identify suspicious activity and alert customers. The platform covers various payment types, channels, and geographies, providing real-time risk monitoring at scale. Feedzai also offers a Generative AI agent, ScamAlert, to help customers spot scams. While Feedzai is a comprehensive, AI-native platform, it is a commercial, centralized solution, typically requiring financial institutions to send their data to Feedzai's platform for processing. This contrasts with a decentralized, privacy-preserving model, which is particularly crucial in contexts like Uganda where mobile money data sharing trust and regulatory compliance are paramount.

2.3. Table of Existing and Proposed Systems

This table offers a comparative analysis of existing AI-based fraud detection systems and the proposed solution for Uganda's mobile money sector. It emphasizes the proposed system's unique strengths, especially its privacy-preserving collaborative design and specific alignment with mobile money fraud challenges.

2.3.1: Comparison of Existing and Proposed AI Fraud Detection Systems

Feature/System	**JPMorgan Chase COiN**	**Bank of America Erica**	**HSBC Quantexa**	**Rabobank AI**	**Mastercard Decision Intelligence**	**Proposed system**
Customer Service, Personal Finance	NO	YES	NO	NO	NO	YES
Financial Crime, Contextual Analytics	NO	NO	YES	NO	NO	YES
APP Fraud, Compliance Automation	NO	NO	NO	YES	NO	YES
Transaction Risk Monitoring, False Decline Reduction	NO	NO	NO	NO	YES	YES
NLP, ML	YES	YES	YES	YES	YES	YES
non-GenAI	NO	YES	NO	YES	NO	YES
Knowledge Graph, GenAI (Q	NO	NO	YES	NO	NO	YES

Assist)						
Internal legal documents	YES	NO	NO	NO	NO	YES
Internal customer data	NO	YES	NO	NO	NO	YES
Internal, connected data	NO	NO	YES	NO	NO	YES
Internal transaction/behavioral data	NO	NO	NO	YES		YES
Global network transaction data	NO	NO	NO	NO	YES	YES
Focus on Mobile Money Transactions	NO	NO	NO	NO	NO	YES
Supports Inter-institutional Privacy-Preserving Collaboration?	NO	NO	NO	NO	NO	YES
Integrates Multi-Factor Authentication (MFA)?	NO	NO	NO	NO	NO	YES
Addresses Imbalanced	NO	NO	NO	NO	NO	YES

Data?						
Uses Generative AI?	NO	NO	YES	YES	NO	YES
Real-time Transactional Fraud Detection?	NO	YES	YES	YES	YES	YES
Privacy Approach	NO	YES	YES	YES	YES	YES
Document Analysis, Compliance	YES	NO	NO	NO	NO	YES

The comparative analysis reveals a key architectural difference between the proposed system and existing solutions. While current AI-driven systems by major financial institutions effectively detect fraud internally, they rely on centralized data processing within isolated ecosystems, limiting inter-institutional collaboration. This is inadequate for addressing cross-entity fraud common in mobile money. The proposed system's use of Federated Learning and decentralized processing ensures privacy-preserving intelligence sharing crucial in Uganda's regulatory context.

2.4. Uniqueness of the Proposed System and the existing AI-driven systems

The proposed AI-driven fraud detection system for Uganda's mobile money sector stands out for its use of privacy-preserving and Federated Learning, enabling secure collaboration among financial institutions without sharing raw data. Unlike centralized models used by platforms like COiN, it aligns with Uganda's Data Protection and Privacy Act 2019. This approach addresses trust and regulatory concerns while enhancing collective fraud detection. A key innovation is the Collaborative Intelligence Hub which allows real-time sharing of anonymized fraud indicators and best practices across stakeholders. This structured collaboration goes beyond traditional threat feeds enabling a coordinated response to mobile money fraud. It fosters ecosystem-wide defense while safeguarding sensitive data sources. Designed specifically for Uganda's unique fraud landscape such as SIM swap scams and social engineering, the system integrates adaptive AI techniques like Graph Neural Networks. It continuously evolves to match fraudsters' generative AI tactics while reducing false positives. This balance protects users, sustains financial inclusion and builds trust in digital financial services.

2.5. Conclusion

The review of current AI-driven fraud detection systems shows progress in internal fraud management but highlights a major shortfall: lacking secure, privacy-preserving collaboration across institutions. Most rely in centralized data processing or proprietary networks which conflict with Uganda's **DATA PROTECTION AND PRIVACY ACT 2019,** specifically **SECTION 18-22** that restrict the sharing and processing of personal data without explicit consent or lawful basis. This renders many existing solutions unsuitable for Uganda's fragmented mobile money ecosystem. The proposed system addresses this gap through Federated Learning and a collaborative intelligence hub, enabling compliance with national law while enhancing fraud detection. It ensures both data privacy and operational effectiveness, fostering a safer and more inclusive digital economy.

CHAPTER THREE: METHODOLOGY

3.0. Introduction

This chapter presents a structured methodology for developing the AI-driven anomaly detection and fraud prevention system tailored to Uganda's mobile money sector. It follows four key phases: Requirement gathering and Research Design, System Design, Development and Testing. The phased approach ensure iterative, robust development grounded in AI/ML and software engineering best practices. It remains adaptive to the specific needs and challenges of Uganda's mobile money environment.

3.1. Requirement Gathering and Research Design

This phase is crucial for understanding the problem space in depth, defining clear objectives, and establishing a solid framework for the system's development, with a focus on mobile money.

3.1.1. Literature Review

The literature review aims to build a thorough understanding of AI/ML techniques for fraud detection including Graph Neural Networks and deep learning alongside privacy-preserving technologies like Federated Learning, Homomorphic Encryption and Secure Multi-Party Computation. It examines global financial sector applications with a focus on mobile money fraud and Uganda's legal and regulatory context. Sources include academic papers, industry reports and case studies (e.g. Monzo, BBVA). Uganda-specific insights on fraud trends, digital transformation and Cybersecurity guidelines are also reviewed. This ongoing review supports algorithm selection, architectural design and strategies to address challenges like imbalanced data and evolving fraud tactics.

3.1.2. Stakeholder Interviews

These aim to collect qualitative insights from key actors in Uganda's mobile money ecosystem including BOU, FIA, UMRA, MTN, Airtel and various financial institutions. These engagements explore regulatory expectations, data sharing practices and existing fraud detection challenges. Input from fraud analysts, IT security teams, consumer and adoption barriers. This ensures the system is technically robust, legally compliant and socially responsive. The insights also inform practical design choices and potential policy recommendations for harmonizing AI governance in Uganda’s mobile money sector.

3.1.3. Surveys and Questionnaires

These aim to gather quantitative data on mobile money fraud incidents, user experiences, digital literacy and perceptions of trust and security across Uganda's mobile money users. Structured surveys will target mobile money operator staff to assess internal fraud and control effectiveness while questionnaires will reach users to capture fraud exposure, behavior patterns and vulnerabilities like SIM fraud and PIN sharing. Analyzing this data will reveal trends, correlations and high-risk areas within the sector. These insights guide AI model development and feature prioritization for targeted fraud mitigation. Additionally, the data provides a benchmark for evaluating the system's long-term impact on fraud reduction and trust.

3.1.4. Brainstorming Sessions

These sessions are conducted to drive innovation by bringing together insights from technical peers, mobile money professionals and domain experts. They will explore creative AI/ML solutions for detecting emerging fraud types and handling imbalanced mobile money data. Key topics include Federated Learning strategies, secure data protocols and user-friendly UI/UX for institutional interfaces. This collaborative ideation helps translate complex challenges into practical, privacy-preserving solutions tailored to Uganda's mobile money context. It also fosters shared ownership and adaptability ensuring the project remains relevant and impactful.

3.1.5. Research Design

This outlines the overall methodologies for data collection, analysis and validation, ensuring both scientific accuracy and ethical handling of mobile money data. It involves defining key research questions around AI effectiveness, privacy and fraud reduction, while selecting suitable methods like experimental evaluation and case studies. Data governance protocols such as anonymizing and encryption ensure compliance with Uganda's Data Protection and Privacy Act 2019. Ethical AI principles including bias mitigation and transparency are embedded to maintain fairness and trust. A strong research design ensures credible, impactful results that support academic rigor and practical application.

3.2. System Design

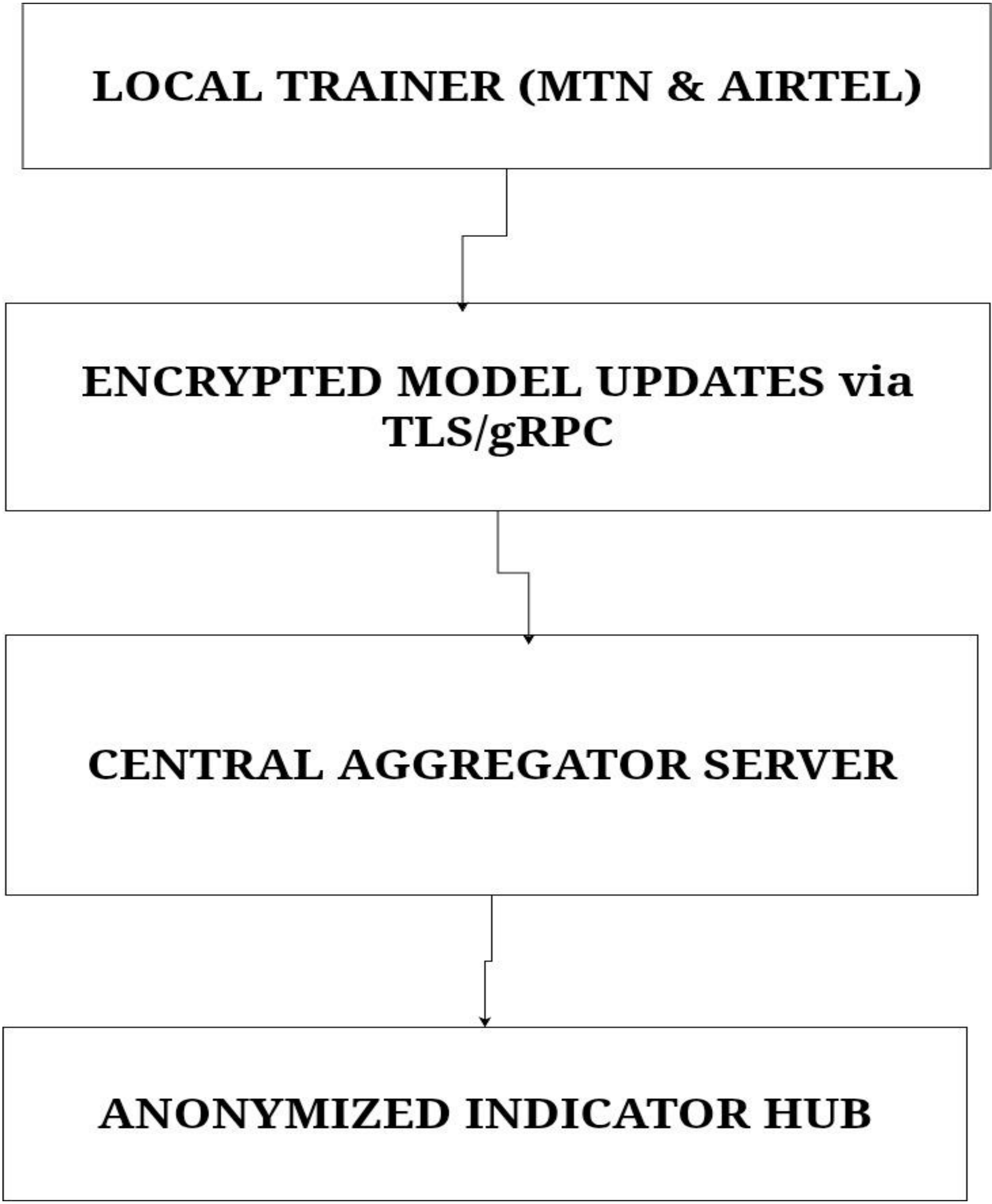
This section translates the gathered requirements into a detailed architectural blueprint for the AI-driven fraud detection system, with a strong emphasis on mobile money transactions.

3.2.1. Requirements Analysis

This phase focuses on refining and clarifying functional and non-functional requirements specific to mobile money ensuring they are precise, testable and aligned with project goals. Functional requirements include real-time fraud detection, anomaly scoring and fraud indicator sharing, while non-functional one's address performance, scalability, privacy and usability for agents and users. Requirements will be categorized, prioritized based on impact and feasibility and reviewed for conflicts or ambiguities in consultation with stakeholders. This structured analysis helps prevent scope creep and informs system architecture and design decisions. For instance, real-time detection demands high-speed processing and suitable AI models while privacy needs guide the use of Federated Learning and encryption. A well-documented requirement set ensures fewer design errors and smoother development. Ultimately, this leads to a solution that effectively addresses Uganda's mobile money fraud challenges.

3.2.2. System Architecture Design

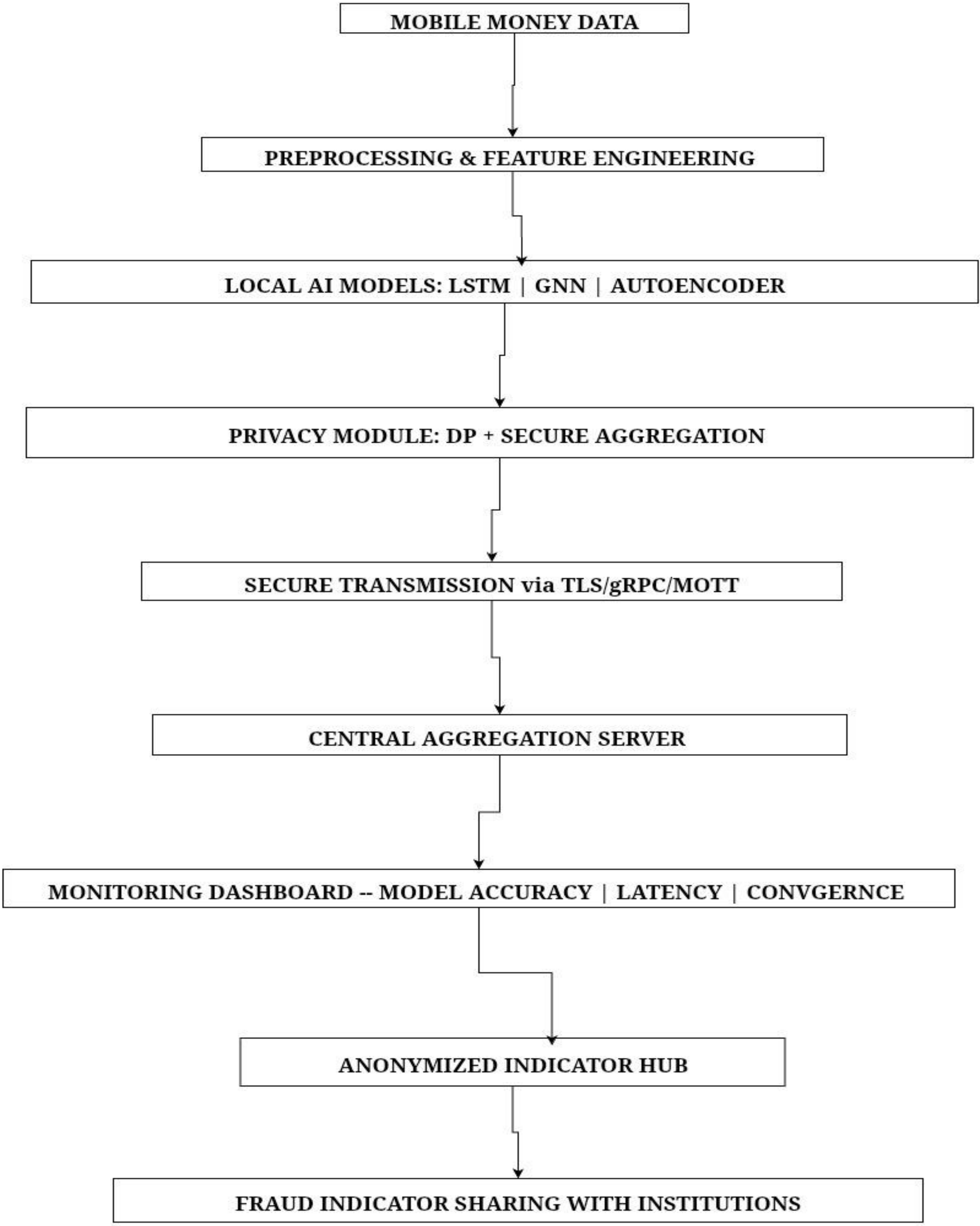
This section defines the system's high-level architecture, focusing on a distributed design tailored for Uganda's mobile money ecosystem. The architecture will support Federated Learning where local model trainers reside at each mobile money operator or financial institution and a central secure server aggregates model updates without accessing raw data. Communication protocols like TLS/SSL, gRPC and MQTT will ensure encrypted, low-latency data exchange. Data flow diagrams and methods such as the 4+1 architectural view model (logical, Development, Process, Physical and Scenarios) will be used for clarity. Cloud infrastructure will be integrated for scalability and asynchronous processing of high mobile money volumes. A centralized hub will be designed to share anonymized fraud indicators while preserving institutional data privacy. The architecture will be designed to meet key non-functional requirements such as scalability, fault tolerance and privacy.


LOCAL TRAINER (MTN & AIRTEL)
ENCRYPTED MODEL UPDATES via TLS/gRPC
CENTRAL AGGREGATOR SERVER
ANONYMIZED INDICATOR HUB

This structure ensures privacy-preserving collaboration, supports legal compliance and provides a scalable foundation for future growth.

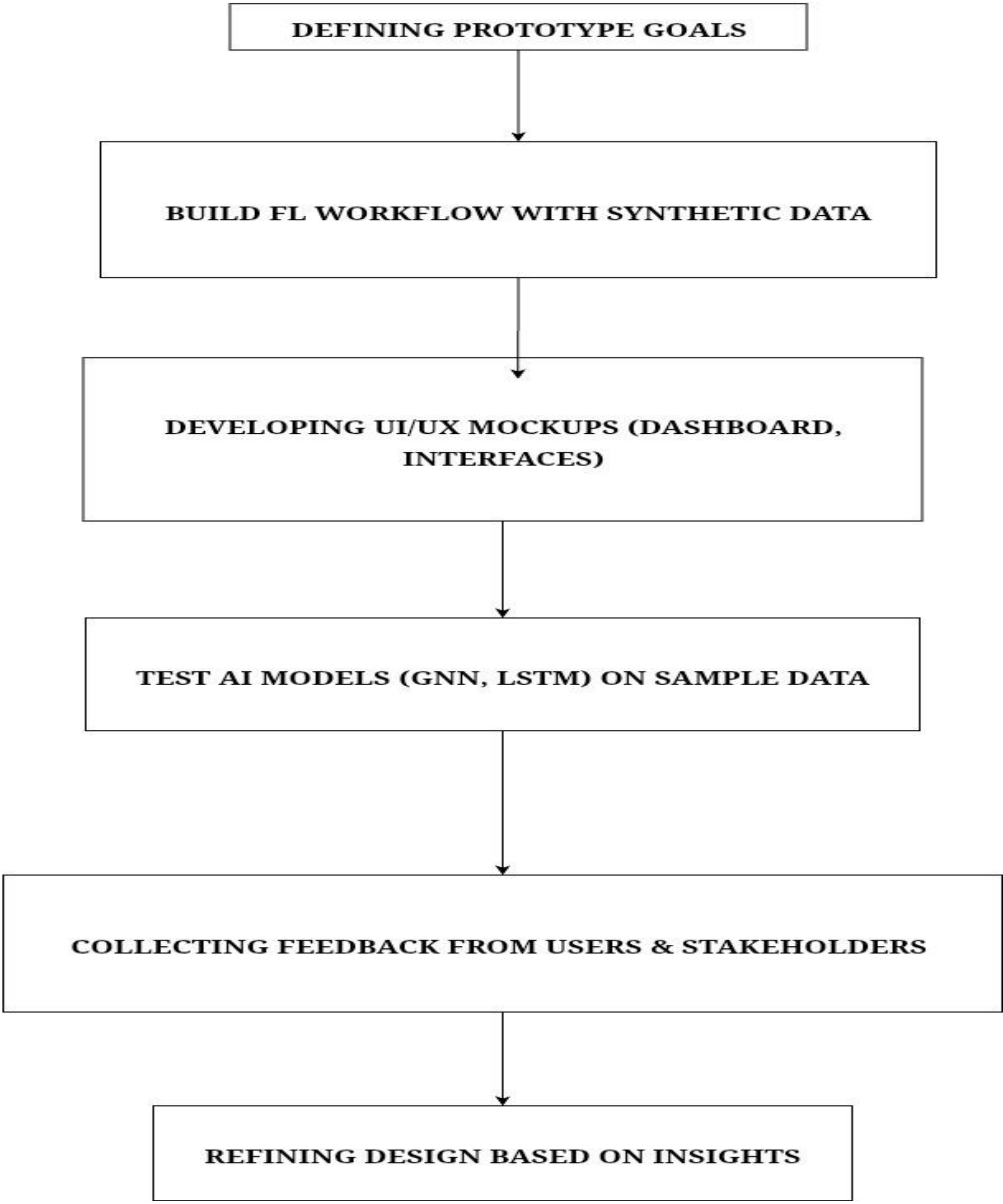
3.2.3. Component Design

This phase involves designing detailed system components focused on mobile money data including LSTM, Auto-encoders and GNNs for local fraud detection alongside preprocessing and feature engineering. Component like the Privacy Module will integrate differential privacy and secure aggregation while the Aggregation Server will use Federated Averaging to merge updates. Secure communication (TLS/SSL, gRPC, MQTT) and a Monitoring Dashboard (AWS CloudWatch, TensorBoard, Grafana) will ensure system reliability. The Centralized Hub will anonymize and share fraud indicators without exposing raw data. This modular, privacy-by-design approach ensures scalability, maintainability and legal compliance.


MOBILE MONEY DATA
PREPROCESSING & FEATURE ENGINEERING
LOCAL AI MODELS: LSTM | GNN | AUTOENCODER
PRIVACY MODULE: DP + SECURE AGGREGATION
SECURE TRANSMISSION via TLS/gRPC/MOTT
CENTRAL AGGREGATION SERVER
MONITORING DASHBOARD -- MODEL ACCURACY | LATENCY | CONVGERNCE
ANONYMIZED INDICATOR HUB
FRAUD INDICATOR SHARING WITH INSTITUTIONS

3.2.4. Prototyping

This step involves building early versions of key system components to validate design decisions, assess AI model performance and gather user feedback in mobile money contexts. It includes creating a working prototype of the Federated Learning workflow using anonymized data and mockups of dashboards and interfaces for operators. Core models like GNNs and LSTMs will be rapidly tested to evaluate fraud detection capabilities. This helps identify issues early, align with user needs and minimize costly changes later. Prototypes also server effective tools for stakeholder engagement and concept demonstration.

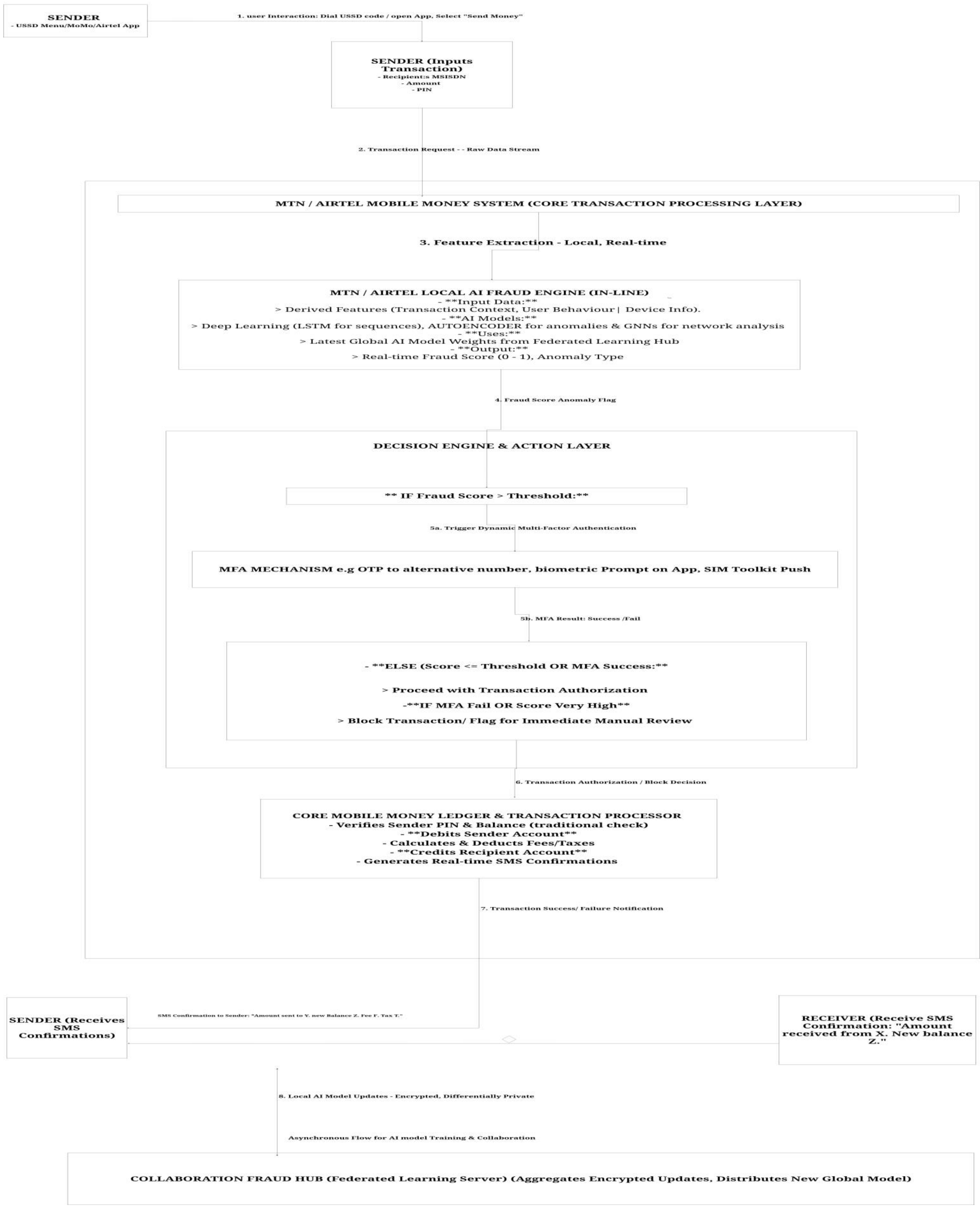

DEFINING PROTOTYPE GOALS
BUILD FL WORKFLOW WITH SYNTHETIC DATA
DEVELOPING UI/UX MOCKUPS (DASHBOARD, INTERFACES)
TEST AI MODELS (GNN, LSTM) ON SAMPLE DATA
COLLECTING FEEDBACK FROM USERS & STAKEHOLDERS
REFINING DESIGN BASED ON INSIGHTS

3.2.5. Design Documentation

Involves creating detailed records of the system's architecture, components, data models and technical specifications, specifically tailored for mobile money integration. This includes C4 and UML diagrams, component specs, API documentation and data schemas that support seamless integration with mobile money platforms. A design rationale log will capture key decisions and reasoning to ensure traceability. Well-structured documentation promotes collaboration, supports future maintenance, and simplifies on-boarding and audits. IT is crucial for long-term scalability and regional adaptation. This knowledge base enhances local AI/ML capacity within Uganda's mobile money ecosystem

3.2.6. Full System Architecture

PERSON -TO-PERSON TRANSFER FLOW WITH PROPOSED SYSTEM INTEGRATION


SENDER
- USSD Menu/MoMo/Airtel App
1. user Interaction: Dial USSD code / open App, Select "Send Money"
SENDER (Inputs Transaction)
- Recipient:s MSISDN
- Amount
- PIN
2. Transaction Request - - Raw Data Stream
MTN / AIRTEL MOBILE MONEY SYSTEM (CORE TRANSACTION PROCESSING LAYER)
3. Feature Extraction - Local, Real-time
MTN / AIRTEL LOCAL AI FRAUD ENGINE (IN-LINE)
- **Input Data:**
> Derived Features (Transaction Context, User Behaviour| Device Info).
- **AI Models:**
> Deep Learning (LSTM for sequences), AUTOENCODER for anomalies & GNNs for network analysis
- **Uses:**
> Latest Global AI Model Weights from Federated Learning Hub
- **Output:**
> Real-time Fraud Score (0 - 1), Anomaly Type
4. Fraud Score Anomaly Flag
DECISION ENGINE & ACTION LAYER
** IF Fraud Score > Threshold:**
5a. Trigger Dynamic Multi-Factor Authentication
MFA MECHANISM e.g OTP to alternative number, biometric Prompt on App, SIM Toolkit Push
5b. MFA Result: Success /Fail
- **ELSE (Score <= Threshold OR MFA Success:**
> Proceed with Transaction Authorization
-**IF MFA Fail OR Score Very High**
> Block Transaction/ Flag for Immediate Manual Review
6. Transaction Authorization / Block Decision
CORE MOBILE MONEY LEDGER & TRANSACTION PROCESSOR
- Verifies Sender PIN & Balance (traditional check)
- **Debits Sender Account**
- Calculates & Deducts Fees/Taxes
- **Credits Recipient Account**
- Generates Real-time SMS Confirmations
7. Transaction Success/ Failure Notification
SENDER (Receives SMS Confirmations)
SMS Confirmation to Sender: "Amount sent to Y. new Balance Z. Fee F. Tax T."
RECEIVER (Receive SMS Confirmation: "Amount received from X. New balance Z."
8. Local AI Model Updates - Encrypted, Differentially Private
Asynchronous Flow for AI model Training & Collaboration
COLLABORATION FRAUD HUB (Federated Learning Server) (Aggregates Encrypted Updates, Distributes New Global Model)

3.4. System Development

This phase involves the actual coding and implementation of the system components based on the approved design, with a focus on mobile money transaction processing.

3.4.1. Programming Languages and Tools Selection

The selection of programming languages and tools will prioritize robustness, scalability, community support, and compatibility with AI/ML frameworks and privacy-preserving libraries, suitable for high-volume mobile money environments.

3.4.1.0: Proposed Technology Stack

CATEGORY	LANGUAGE/TOOL	PURPOSE	WHY THE TECHNOLOGY
AI/ML & Backend	Python	-AI/ML model development (GNNs, Deep Learning, Federated Learning), mobile money data processing and logic	-Extensive libraries (TensorFlow, PyTorch, Scikit-learn, DGL, NetworkX, FastAPI) support AI/ML and backend APIs
Backend Services & APIs	Django	-Robust, scalable backend services, APIs & central aggregation server handling mobile money transaction loads	-Django provides high-performance suitable for secure communication layers (gRPC MQTT)
Frontend	HTML, CSS, JavaScript	-Developing UI of the centralized hub dashboard & institution interface for mobile money operators & regulators	-Standard web technologies for responsive, interactive web apps; frameworks like React or Vue.js support efficient UI development.
Database Management	PostgreSQL/MongoDB/Neo4j	- PostgreSQL for relational data (user profiles, audit logs) - Neo4j for graph-	PostgreSQL offers ACID compliance and robustness; Neo4j is optimized for graph data

		structured data (mobile money transaction networks - MongoDB for flexible unstructured data	critical for GNNs; MongoDB provides schema flexibility.
Version Control	Git with GitHub/GitLab	- Source code management - Change tracking and collaborative dev't	-Industry standard with strong branching and merging, essential for teamwork and code integrity.
Cloud Platform	AWS/Azure/Google Cloud	- Scalable infrastructure - GPU compute for AI training - Managed services (Kafka for real-time data streams) - Kubernetes for orchestration	-Elastic scalability, high availability, and broad managed services to support AI workloads and distributed systems.
Containerization	Docker/Kubernetes	- Packaging apps & dependencies into containers - Orchestration of containerized applications at scale	-Ensures consistent environments and simplifies deployment, scaling, and management of microservices.
Monitoring & Visualization	Grafana, Prometheus, TensorBoard, AWS CloudWatch	- Real-time monitoring of system performance - Model accuracy - Operational metrics	-Dashboards and alerts critical for tracking model convergence, latency, and overall health. -TensorBoard specializes in AI model visualization.
Privacy-preserving Libraries	PySyft, OpenFHE, MPC	- implement Federated Learning	-Pre-built cryptographic protocols and privacy-

		- Homomorphic Encryption - Secure multi-party computation on mobile money data	preserving AI tools in Python reduce development time and increase security robustness.

3.4.2. Coding and Implementation

This section involves translating the system design into functional modules tailored for mobile money fraud detection. Python will be used for developing AI models, Federated Learning Logic and data pipelines, ensuring modularity and privacy. Web technologies will support intuitive user interfaces while secure APIs and communication protocols will enable seamless, encrypted data exchange. This section emphasizes security, real-time processing and integration with existing mobile money infrastructure.

3.4.2.1. Local Model Training module

The development of local model training modules will be done primarily using Python, leveraging powerful AI/ML libraries such as PyTorch, TensorFlow and Deep Graph Library. These modules will implement Graph Neural Networks and deep learning models specifically designed to detect fraud patterns in mobile money transactions. The models will be trained on local data each mobile money operator or financial institution to preserve data privacy and improve detection accuracy tailored to Uganda's mobile money ecosystem.

3.4.2.2. Federated Learning Aggregation Logic

The core Federated Learning aggregation will be implemented on the central server, utilizing Python for seamless integration with the AI modules. This component will handle secure aggregation of locally trained model updates, ensuring that raw customer data never leaves the operators. Secure aggregation protocols will be carefully integrated to protect individual updates during transmission and combination, maintaining strict privacy compliance and enhancing collaborative fraud detection.

3.4.2.3. Secure Communication Layer

A robust communication layer will be developed to enable encrypted and reliable transmission of model updates between local trainers and the central server. Using protocols such as TLS/SSL, gRPC or MATT, this layer will ensure that all data exchanges are confidential, tamper-proof and performance, supporting real-time collaboration without risking exposure of sensitive mobile money data.

3.4.2.4. Centralized Hub Development

The web-based centralized hub, serving as the interface for sharing anonymized mobile money fraud indicators will be built using standard web technologies (HTML, CSS and JavaScript) alongside modern frameworks like React or Vue.js. This hub will provide mobile money operators, regulators and other stakeholders with an intuitive platform for monitoring fraud trends, accessing shared insights and coordinating responses while safeguarding user privacy.

3.4.2.5. API Integration

Seamless integration with existing mobile money operator systems will be achieved through well-defined RESTful APIs. These interfaces will enable secure data exchange, model update submissions and retrieval of aggregated insights ensuring that the new fraud detection system complements current operational workflows and data infrastructure without disruption.

3.4.2.6. Data Preprocessing Pipelines

Robust data preprocessing pipelines will be implemented to handle the diverse formats and quality issues typical of mobile money transaction data. These pipelines will clean, normalize and transform raw data into suitable inputs for AI models, addressing challenges such as missing values, inconsistent formats and noise, thereby enhancing model accuracy and reliability.

3.4.2.7. Handling Imbalanced Datasets

Given nature of mobile money fraud as a rare event, the system will employ advanced techniques to address imbalanced datasets such as adjusting class weights, oversampling minority classes or using synthetic data generation methods like SMOTE. These strategies will help ensure that the AI models remain sensitive to fraudulent activities without generating excessive false positives.

3.4.2.8. Code Quality and Security

High standards of code quality will be maintained through modular design, through testing and comprehensive error handling to ensure stability in real-time, high- volume environment. Security best practices including input validation, secure coding standards and regularly vulnerability assessments, will be strictly followed to protect sensitive mobile money data and comply with Uganda's privacy regulations, ultimately fostering trust among users and stakeholders.

3.4.3. Version Control

Version control will manage code changes, support developer collaboration and maintain a complete history of modifications. Git, hosted on platforms like GitHub or GitLab will be used with a branching strategy such as GitFlow to organize development. Regular code reviews ensure quality, security and adherence to standards. Effective version control is vital for preventing conflicts, enabling rollbacks and providing an audit trail essential for regulatory compliance in mobile money systems.

3.4.4. Testing Integration

Integration testing ensures that different system component like local model trainers, the privacy module, aggregation server and communication layer work smoothly together and with external systems such as mobile money platforms. Automated tests verify correct data flow and interface compatibility across these parts. Special focus is placed on ensuring that the centralized hub can share anonymized model insights and indicators securely. Testing also confirms seamless connectivity with mobile money operators. Since Federated Learning involves multiple parties, any integration failure could disrupt the entire system. Early and continuous testing helps catch such issues early, ensuring data flows correctly, models are aggregated accurately, and communication remains secure. This reduces risks, minimizes downtime and maintains system reliability in real-time environments.

3.4.5. Agile Development Practices

It ensures the mobile money fraud detection system evolves through short, flexible sprints allowing rapid delivery and continuous improvement. By holding regular stand-ups, sprint reviews and maintaining a prioritized backlog, the team will quickly respond to emerging fraud patterns and regulatory changes. Agile supports ongoing learning from real-world deployments and rapid adaption. Continuous integration and delivery keep the system functional and up to date. This approach fosters transparency and aligns development with stakeholder needs.

3.5. System Testing and Validation

This section ensures the system meets all specified requirements, performs optimally, and is secure and reliable for deployment in a live mobile money environment.

3.5.1. Functional Testing

To ensure that the mobile money fraud detection system performs all key task accurately including identifying various fraud types like SIM swap, social engineering and fake loans scams. It verifies real-time anomaly detection, risk scoring and privacy-preserving features of Federated Learning to prevent raw data leakage. The centralized hub’s ability to share anonymized indicators is also tested.

This therefore confirms that the system meets its core goal of secure and accurate fraud detection. Reliable functionality builds and institutional trust in the mobile money ecosystem.

3.5.2. User Acceptance Testing (UAT)

To ensure the mobile money fraud detection system meets the practical needs of fraud analysts, compliance officers and agents. By testing in a simulated environment with realistic data, users' usability, alert clarity and workflow integration. UAT ensures the system supports daily operation without disruption legitimate transactions. Gathering feedback helps refine the system to reduce false positives and improve user experience. A user-friendly, effective system increases adoption and strengthens mobile money fraud prevention efforts.

3.5.3. Performance Testing

To ensure the system handles Uganda's high and growing volume of mobile money transactions, its responsiveness, stability and scalability must be verified under varying loads. IT should process real-time fraud detection and alert generation quickly, even during peak transaction periods. The system's ability to update and aggregate models efficiently within the Federated Learning framework is essential. Efficient response use (CPU, memory, bandwidth) ensures smooth operation. A fast, reliable system helps mobile money operators prevent fraud without disrupting legitimate services.

3.5.4. Security Testing

To protect sensitive mobile money data and ensure system resilience, all components such as local trainers, aggregation servers and communication channels must be evaluated for vulnerabilities. Penetration attempts and simulated attacks will help uncover weaknesses, particularly in areas handling fraud detection and data aggregation. Privacy-preserving methods like Federated Learning, differential privacy and secure aggregation will be audited to guard against adversarial interference. The fraud, unauthorized access, data breaches and DDoS attacks. Compliance with Uganda's Data Protection and Privacy Act 2019 is essential. The system must also resist manipulation attempts that could mislead fraud models. Multi-Factor authentication will be checked for effectiveness in safeguarding transaction access. A secure and compliant system builds trust among users and regulators.

3.5.5. Validation Against Requirements

Before full deployment, the system must be thoroughly reviewed to confirm it meets all functional and non-functional expectations specific to mobile money fraud prevention. Each requirement will be linked to test results using a structured traceability approach, ensuring nothing is overlooked.

Stakeholder feedback, test outcomes and performance metrics will be accessed to confirm technical accuracy, user satisfaction and regulatory compliance. A final report will document how the system aligns with its original goals of improving mobile money integrity and security in Uganda. This process builds trust and ensures readiness for wide-scale adoption.

4.0. References

1. https://www.dataversity.net/mastercard-rolls-artificial-intelligence-across-global-network/
2. https://arxiv.org/abs/2009.02047
3. https://allafrica.com/stories/202507090430.html
4. https://info.bankofamerica.com/en/digital-banking/erica
5. https://www.bankofamerica.com/security-center/understand-merchant-compromise/
6. https://www.bbva.com/en/innovation/data-innovation/artificial-intelligence/
7. https://cipesa.org/2025/02/ugandas-ai-framework-a-rights-based-policy-playbook/
8. https://ctomagazine.com/ai-fraud-detection-bank-security/
9. https://eprcug.org/eprc-in-the-news/as-we-tap-and-click-our-way-to-convenience-digital-fraud-lurks/
10. https://www.feedzai.com/
11. https://www.feedzai.com/industries/government/
12. https://finovate.com/hsbc-taps-quantexa-for-decision-intelligence/
13. https://www.fraud.com/post/anomaly-detection
14. https://www.fraud.com/
15. https://www.fraud.com/glossary/federated-learning-for-fraud-detection
16. https://a-us.storyblok.com/f/1012896/x/75b2f9dc6f/hsbc-case-study-jennifer-calvery-financial-crime.pdf
17. https://www.imbankgroup.com/ug/information-security/sim-swap-fraud/
18. https://kcl.co.ug/ai-in-uganda-policy-and-regulatory-environment/
19. https://b2b.mastercard.com/ai-and-security-solutions/fraud-and-decisioning/decision-intelligence/
20. https://www.mastercard.com/globalrisk/en/resources/all-resources/detect.html
21. https://medium.com/@chenycy/fraud-detection-and-anomaly-detection-e65dd11a3146
22. https://medium.com/@arahmedraza/how-jpmorgan-uses-ai-to-save-360-000-legal-hours-a-year-6e94d58a557b
23. https://www.mi-3.com.au/13-06-2025/draft-ai-augmented-compliance-how-rabobank-rewiring-financial-crime-prevention-genai

24. https://ug.numida.com/blog/how-to-identify-scammers-and-protect-your-business-in-uganda

25. https://www.paloaltonetworks.com/cyberpedia/what-are-multi-factor-authentication-mfa-examples-and-methods

26. https://poverty-action.org/how-interactive-storytelling-protecting-ugandans-mobile-money-fraud

27. https://www.providence.bank/multifactor-authentication/

28. https://www.weforum.org/organizations/quantexa/

29. https://raboinvestments.com/portfolio/hawk-ai/

30. https://www.researchgate.net/publication/391399968_FEDERATED_LEARNING_FOR_PRIVACY-PRESERVING_FRAUD_DETECTION_ACROSS_FINANCIAL_INSTITUTIONS

31. https://www.researchgate.net/publication/390799136_Graph_Neural_Networks_for_Fraud_Detection_Modeling_Financial_Transaction_Networks_at_Scale

32. https://securiti.ai/uganda-data-protection-and-privacy-act/

33. https://seon.io/resources/fraud-detection-and-prevention/

34. https://stripe.com/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention

35. https://thebankingscene.com/opinions/generative-ai-in-banking-rabobank-a-conservative-start

36. https://www.wissen.com/blog/introduction-to-privacy-preserving-techniques-in-financial-ai

5.0. Appendix: Glossary of all the key words used in the proposal

This appendix provides definitions for short terms and key IT concepts used throughout this proposal, offering clarity and a comprehensive understanding of the technical and operational aspects discussed.

- **AI (Artificial Intelligence):** The simulation of human intelligence processes by machines, especially computer systems. These processes include learning, reasoning, and self-correction.
- **AI/ML (Artificial Intelligence/Machine Learning):** Refers to the combined fields of Artificial Intelligence and Machine Learning, emphasizing the use of algorithms that learn from data to make predictions or decisions.
- **AML (Anti-Money Laundering):** A set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.
- **Anomaly Detection:** The process of identifying data points, events, or observations that deviate significantly from most of the data, often indicating fraud or other unusual activity.
- **API (Application Programming Interface):** A set of defined rules that enable different software applications to communicate with each other.
- **APP Fraud (Authorized Push Payment Fraud):** A type of fraud where a victim is tricked into sending money directly from their bank account to an account controlled by a fraudster.
- **AWS (Amazon Web Services):** A comprehensive, broadly adopted, and widely used cloud platform, offering over 200 fully featured services from data centers globally.
- **BOU (Bank of Uganda):** The central bank of Uganda, responsible for maintaining monetary stability and supervising financial institutions.
- **C4 Model:** A set of diagrams for visually communicating software architecture, helping to describe a system's structure in an understandable way.
- **CPU (Central Processing Unit):** The electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logic, controlling, and input/output (I/O) operations specified by the instructions.
- **Cybercrime:** Criminal activities carried out by means of computers or the internet.
- **Cybersecurity:** The practice of protecting systems, networks, and programs from digital attacks.
- **DGL (Deep Graph Library):** An open-source Python package for deep learning on graphs, providing a framework for developing graph neural networks.
- **DDoS (Distributed Denial of Service) Attack:** A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- **Deep Learning:** A subset of machine learning in which artificial neural networks, inspired by the human brain, learn from large amounts of data.

- **Differential Privacy (DP):** A system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset.
- **Docker:** A platform that uses OS-level virtualization to deliver software in packages called containers.
- **FastAPI:** A modern, fast (high-performance) web framework for building APIs with Python 3.7+ based on standard Python type hints.
- **FEC (Financial Economic Crime):** A broad term encompassing various illegal activities related to finance, including fraud, money laundering, and terrorism financing.
- **Federated Averaging:** An algorithm used in Federated Learning to aggregate model updates from multiple clients.
- **Federated Learning (FL):** A machine learning technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples, without exchanging their data samples.
- **Feedzai:** A financial technology company that provides an AI-native platform to identify and eradicate financial crimes.
- **FIA (Financial Intelligence Authority):** The central national agency in Uganda responsible for receiving, analyzing, and disseminating financial information concerning suspected proceeds of crime and terrorist financing.
- **GNN (Graph Neural Network):** A type of neural network designed to operate on graph-structured data, effective for analyzing relationships and patterns in interconnected data.
- **Grafana:** An open-source platform for monitoring and observability, allowing users to query, visualize, alert on, and explore metrics, logs, and traces.
- **gRPC (Google Remote Procedure Call):** A modern open-source high-performance RPC framework that can run in any environment.
- **Homomorphic Encryption:** A form of encryption that allows computations to be performed on encrypted data without decrypting it first.
- **HTML (HyperText Markup Language):** The standard markup language for documents designed to be displayed in a web browser.
- **HSBC (Hongkong and Shanghai Banking Corporation):** A British multinational universal bank and financial services group.
- **JavaScript:** A programming language that enables interactive web pages.
- **JPMorgan Chase CoiN (Contract Intelligence):** An AI system developed by JPMorgan Chase that uses Natural Language Processing and Machine Learning to automate the review of commercial loan documents.

- **Kubernetes:** An open-source system for automating deployment, scaling, and management of containerized applications.
- **LLM (Large Language Model):** A type of artificial intelligence model that is trained on a massive amount of text data to generate human-like text, translate languages, write different kinds of creative content, and answer your questions in an informative way.
- **LSTM (Long Short-Term Memory):** A type of recurrent neural network (RNN) capable of learning order dependence in sequence prediction problems, often used for time series data.
- **Mastercard Decision Intelligence Platform:** A platform introduced by Mastercard that uses AI and Machine Learning to increase the accuracy of real-time approvals for genuine transactions and prevent fraud.
- **MCC (Mobile Money Operators):** Companies that facilitate mobile money services.
- **MFA (Multi-Factor Authentication):** An authentication method that requires the user to provide two or more verification factors to gain access to a resource.
- **ML (Machine Learning):** A subset of AI that enables systems to learn from data, identify patterns, and make decisions with minimal human intervention.
- **MongoDB:** A popular NoSQL database program, which uses JSON-like documents with optional schemas.
- **MQTT (Message Queuing Telemetry Transport):** A lightweight messaging protocol for small sensors and mobile devices, optimized for high-latency or unreliable networks.
- **MTN:** A major mobile money operator in Uganda.
- **NLP (Natural Language Processing):** A branch of AI that enables computers to understand, interpret, and generate human language.
- **Neo4j:** A graph database management system.
- **PIN (Personal Identification Number):** A numerical password used to authenticate a user to a system.
- **PostgreSQL:** A powerful, open-source object-relational database system.
- **Prometheus:** An open-source monitoring system with a dimensional data model, flexible query language, efficient time series database and modern alerting approach.
- **PySyft:** An open-source Python library for secure and private AI, enabling Federated Learning and other privacy-preserving techniques.
- **PyTorch:** An open-source machine learning framework that accelerates the path from research prototyping to production deployment.
- **Quantexa:** A UK-based company that provides a Decision Intelligence Platform leveraging AI and machine learning to connect siloed data and provide a contextual view.
- **Rabobank:** A Dutch multinational banking and financial services company.

- **RESTful APIs (Representational State Transfer Application Programming Interfaces):** A set of architectural principles for designing web services that are lightweight and easily maintainable.
- **Scikit-learn:** A free software machine learning library for the Python programming language.
- **Secure Multi-Party Computation (MPC):** A cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private.
- **SIM (Subscriber Identity Module) Card Fraud:** Fraudulent activities involving the unauthorized use or manipulation of a SIM card.
- **SMOTE (Synthetic Minority Over-sampling Technique):** An oversampling technique used to address imbalanced datasets by generating synthetic samples for the minority class.
- **Social Engineering:** The psychological manipulation of people into performing actions or divulging confidential information.
- **TensorBoard:** A suite of web applications for inspecting and understanding TensorFlow runs and graphs.
- **TensorFlow:** An open-source machine learning framework developed by Google.
- **TLS/SSL (Transport Layer Security/Secure Sockets Layer):** Cryptographic protocols designed to provide communications security over a computer network.
- **UAT (User Acceptance Testing):** The final phase of software testing where real users test the software to ensure it can handle required tasks in real-world scenarios.
- **UML (Unified Modeling Language):** A standardized general-purpose modeling language in the field of object-oriented software engineering.
- **UMRA (Uganda Microfinance Regulatory Authority):** An authority in Uganda responsible for regulating and supervising microfinance institutions.
- **UI/UX (User Interface/User Experience):** UI refers to the visual elements users interact with, while UX focuses on the overall experience a user has with a product or system.
- **Vue.js:** An open-source model–view–viewmodel JavaScript framework for building user interfaces and single-page applications.
- **XGBoost (eXtreme Gradient Boosting):** An optimized distributed gradient boosting library designed to be highly efficient, flexible, and portable.