# AI-Powered Fraud Detection and Privacy-Preserving Payment System

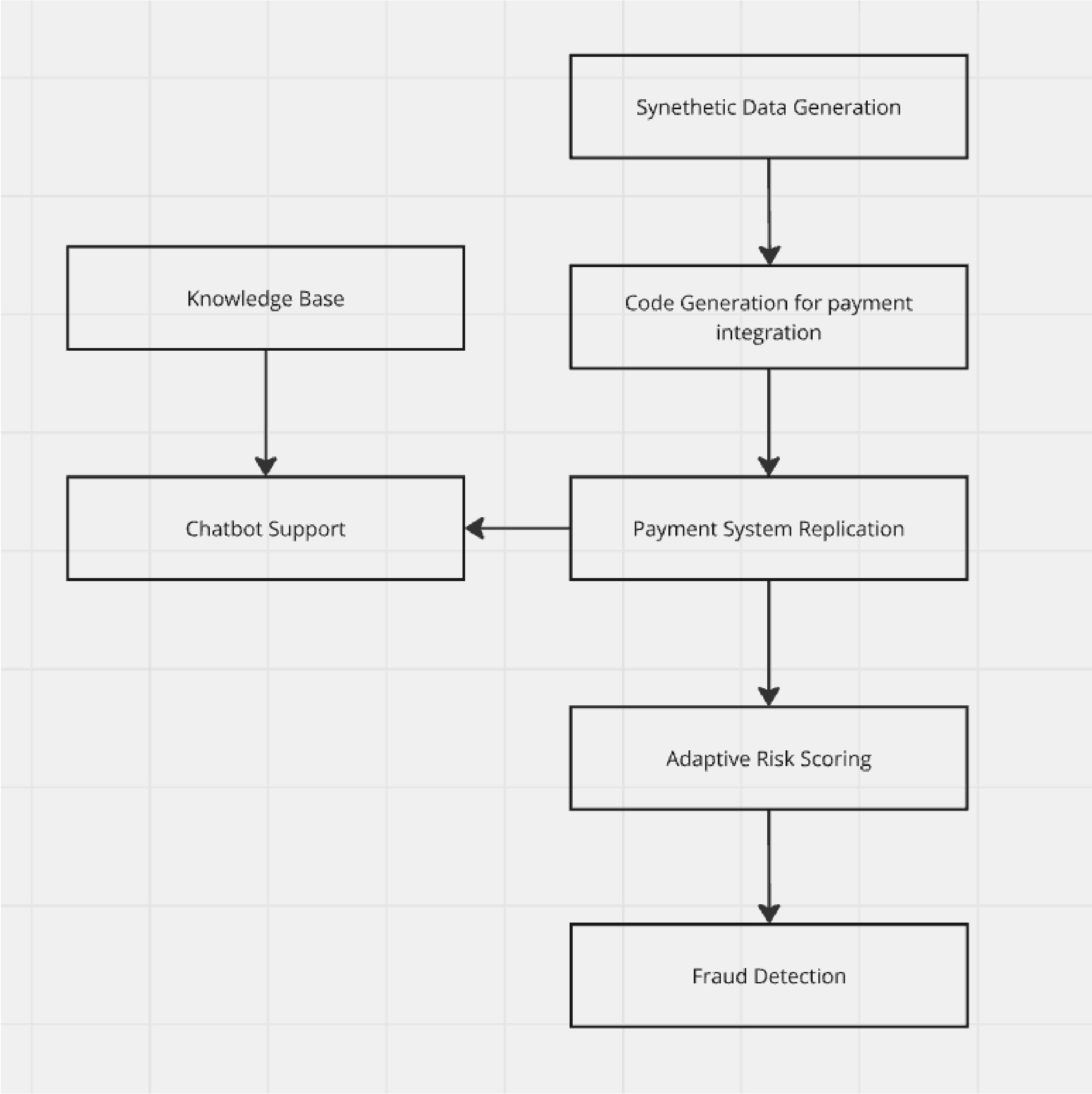
## Problem Description

The financial sector faces increasing threats from fraudsters leveraging sophisticated techniques to manipulate payment systems. Traditional fraud detection models struggle due to data scarcity, evolving fraud tactics, and privacy concerns in data sharing. Existing systems rely heavily on rule-based mechanisms that fail to adapt quickly to emerging fraud patterns. Moreover, the need for secure yet effective fraud detection across multiple financial institutions necessitates privacy-preserving AI techniques to maintain compliance with regulations such as GDPR.

## Introduction to the Solution

Our proposed system integrates **Generative AI and Privacy-Preserving AI** to enhance fraud detection and risk assessment in payment systems. By leveraging synthetic data generation, hybrid federated learning, conversational AI, and real-time transaction monitoring, we aim to create a scalable and adaptive solution. The system focuses on:

1. **Synthetic Data Generation** using **Duo-GAN with Diffusion Models** to train fraud detection models on realistic yet privacy-preserving datasets (Fraud Detection with Duo-GAN).
2. **Hybrid Federated AI for Collaborative Fraud Detection**, enabling multiple financial institutions to detect cross-entity fraud patterns without sharing raw data (Privacy-Preserving Financial Data Sharing).
3. **Adaptive Risk Scoring and Real-Time Fraud Detection** using deep learning models to flag high-risk transactions dynamically (Cost-Sensitive Learning & Isolation Forest).
4. **Conversational AI for Customer Support** to assist users with payment-related queries while ensuring security and compliance.
5. **Automated Code Generation for Payment Integrations** to simplify payment gateway integrations for developers.


Synethetic Data Generation
Knowledge Base
Code Generation for payment integration
Chatbot Support
Payment System Replication
Adaptive Risk Scoring
Fraud Detection

# Key Features

## 1. Synthetic Data Generation for Fraud Detection

**Objective:** Generate high-quality synthetic datasets to improve fraud detection models without exposing real transaction data.

**Technique Used: Duo-GAN with Diffusion Models**

- Traditional GANs suffer from mode collapse, making them unreliable for fraud detection.

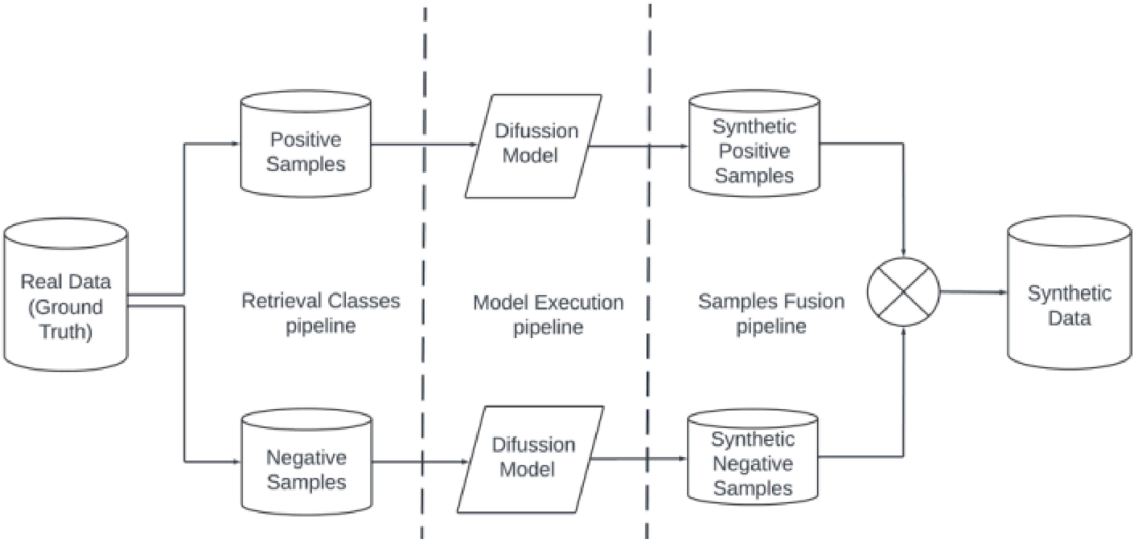
- Duo-GAN, combined with **diffusion models**, ensures that synthetic transactions mimic real-world fraud and non-fraud patterns accurately.
- Two separate diffusion blocks learn independently from fraud and non-fraud transactions, capturing class-conditional distributions.

**Privacy Considerations:**

- Synthetic data removes sensitive details, ensuring compliance with **GDPR** and financial privacy regulations.
- The **IEEE-CIS Fraud Detection Dataset** is suggested as a source for real transaction structures.

**GitHub Repository:**

- Credit Card Fraud Detection GAN



## 2. Fraud Detection using Generative AI

**Objective:** Develop an AI model capable of detecting fraud patterns by learning from real and synthetic data.

**Techniques Used:**

- **CNN & LSTMs** to analyze spatial and temporal patterns in transaction sequences.
- **Graph Neural Networks (GNNs)** to identify hidden fraud patterns across multiple entities.
- **SHAP & LIME** for Explainability ensures compliance with regulatory bodies by making fraud predictions interpretable.

**How It Works:**

1. GNN matches incoming transactions against generated synthetic fraud data.

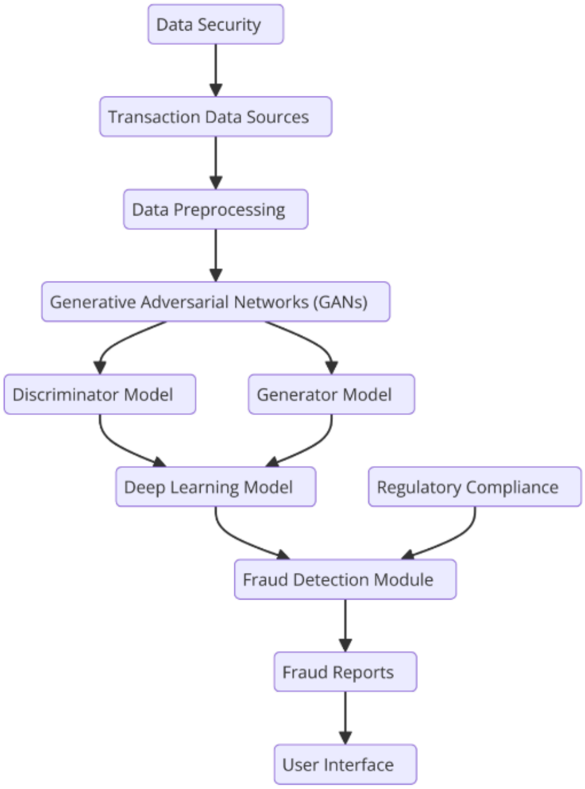
2. CNN detects high-risk regions for fraudulent transactions.
3. LSTM analyzes transaction frequency and behavioral deviations.
4. A final **risk score** is assigned, and flagged transactions are further reviewed.

**Research Paper References:**

- Optimizing Fraud Detection Models with Synthetic Data.
- Duo-GAN for Fraud Detection.

**GitHub Repository:**

- AI-Based Fraud Detection



## 3. Adaptive Risk Scoring & Transaction Monitoring

**Objective:** Assign real-time risk scores to transactions to enable proactive fraud detection.

**Implementation Details:**

- **Model: Anomaly Detection using Isolation Forest + XGBoost**.
- **Process:**
  - When a transaction is initiated, it is scored in real time (0-1 scale).

    - If the risk score is high, the system halts the transaction and requires additional verification.
    - Once the payment is complete, it is re-evaluated using full transaction data and flagged if necessary.

**Optimization:**

- **Edge computing** is used to reduce latency for instant fraud detection.
- Model continuously updates risk thresholds based on new fraud patterns.

**Paper Reference:**

- Cost-Sensitive Learning & Isolation Forest.

### 4. Hybrid Federated AI for Collaborative Fraud Detection

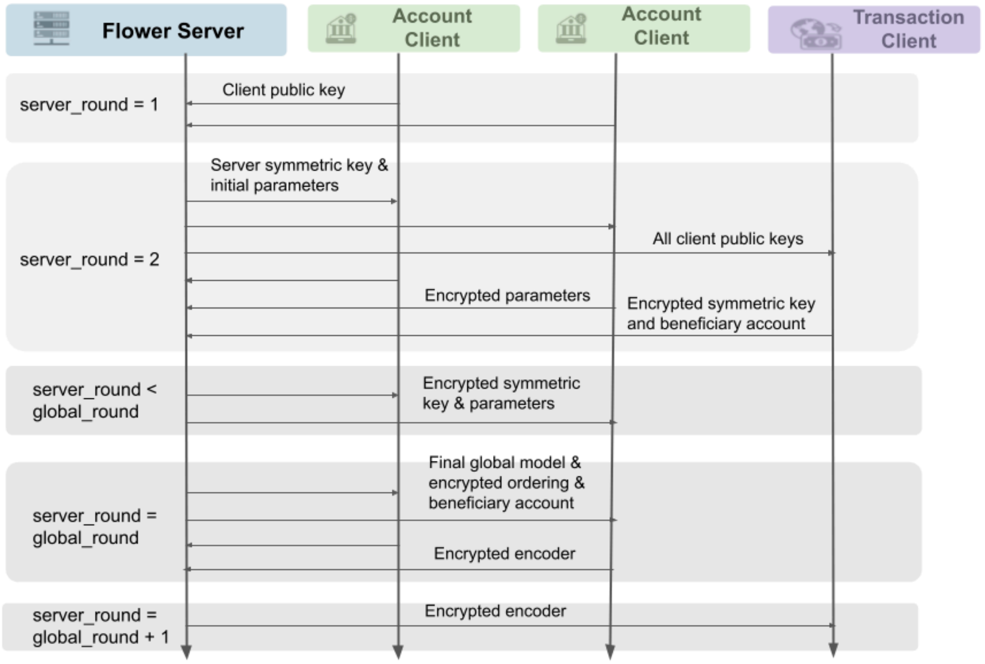
**Objective:** Enable financial institutions to detect fraud collectively while preserving customer privacy.

**Technique Used: Hybrid Federated Learning with Homomorphic Encryption**.

- Unlike traditional federated learning, our approach integrates **statistical data sharing** and **model updates** while maintaining privacy.
- **Homomorphic encryption** ensures that no private data is exposed, allowing secure cross-entity fraud detection.

**Research-Based Implementation:**

- Based on **this research paper**: Privacy-Preserving Financial Data Sharing.
- GitHub repository for implementation: HyFL - Hybrid Federated Learning.


Flower Server
Account Client
Account Client
Transaction Client
server_round = 1
Client public key
server_round = 2
Server symmetric key & initial parameters
All client public keys
Encrypted parameters
Encrypted symmetric key and beneficiary account
server_round < global_round
Encrypted symmetric key & parameters
server_round = global_round
Final global model & encrypted ordering & beneficiary account
Encrypted encoder
server_round = global_round + 1
Encrypted encoder

## 5. Conversational AI for Customer Support

**Objective:** AI chatbot for handling payment-related queries, transaction troubleshooting, and fraud alerts.

**Implementation:**

- Uses **open-source LLMs** such as **Llama 3, Mistral, or Falcon** trained on payment FAQs and troubleshooting logs.
- Real-time access to transaction history and risk scores to provide instant fraud explanations.
- Can be deployed locally to ensure **data privacy and security**.

## 6. Automated Code Generation for Payment Integrations

**Objective:** Simplify payment API integrations for developers.

**How It Works:**

- Uses **open-source LLMs** such as **StarCoder or CodeLlama** trained on financial API documentation to generate secure code snippets.
- Developers can enter API parameters, and the system generates:
  - **Payment gateway integration code**
  - **Error-handling scripts**
  - **Automated test cases**
- Designed for **local execution** to enhance security and privacy.

## Unique Selling Proposition (USP)

1. **Hybrid Federated Learning for Privacy-Preserving AI**.
2. **Adaptive Real-Time Fraud Detection** with self-learning AI.
3. **Comprehensive Payment AI Ecosystem** covering fraud detection, integrations, and customer support.