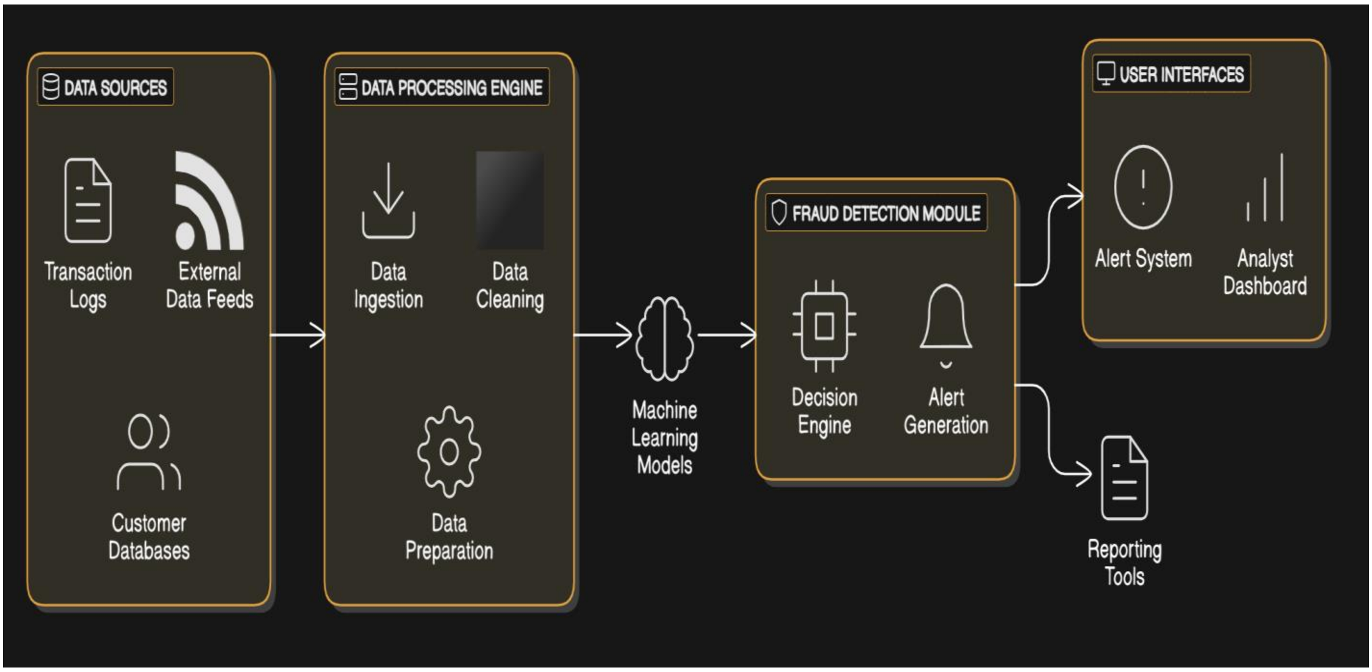
Fraud Detection in Banking System: Architecture and Design Document

Technology Architecture

Architecture Diagram:



Flow of Information Between Blocks:

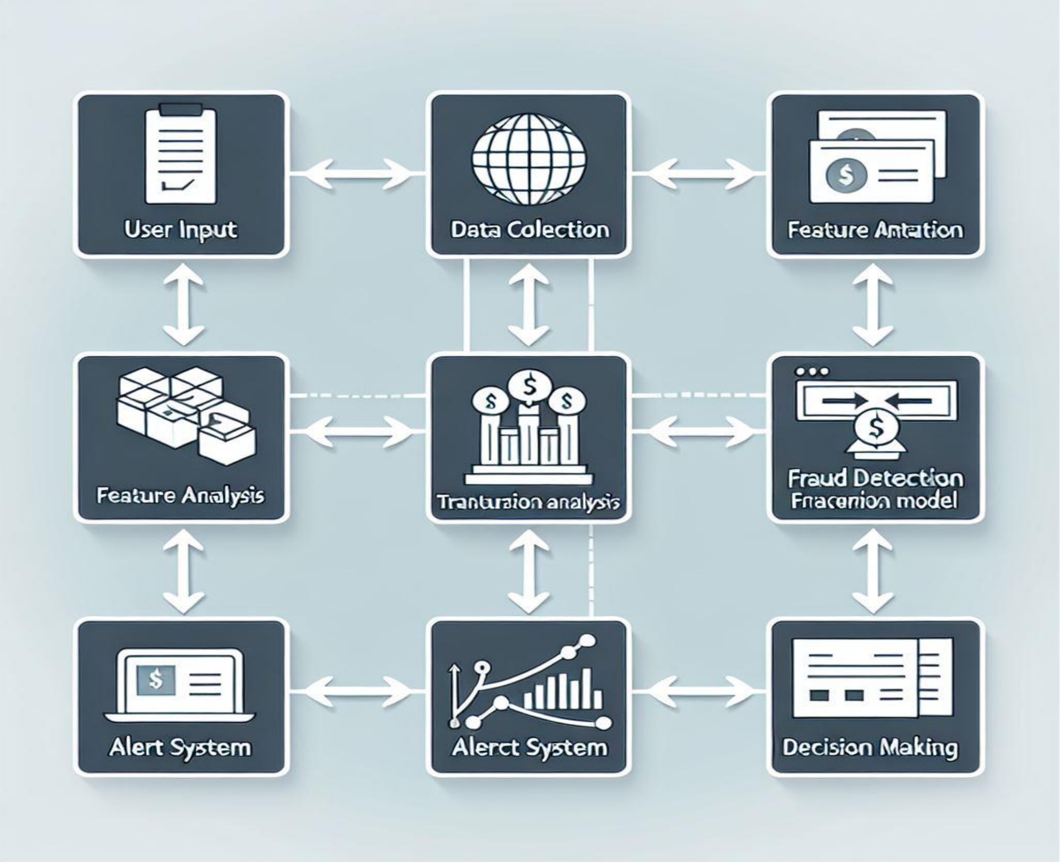
- User Interface: The user (bank employee or customer) interacts with the system through a web or mobile interface.
- Application Server: The requests from the user interface are processed by the application server, which handles business logic and communicates with the data processing component.
- Data Processing: This component analyzes transactions and other data to detect potential fraud. It may involve machine learning algorithms and data analytics.
- Database: The database stores transaction data, user information, and fraud detection models.

Explanation of the Blocks in the Block Diagram and the Flow of Information

- User Interface: Allows users to input data, view alerts, and manage their accounts.
- Application Server**:** Processes user requests, applies business logic, and routes data to the appropriate components.
- Data Processing: Analyzes transaction data using fraud detection algorithms to identify suspicious activities. It communicates findings to the application server.
- Database: Stores all relevant data, including transaction history, user profiles, and fraud detection results.

Technology Design

Architecture Diagram:



Flow of Information Between the Components / Blocks

1. **Data Sources**: Collects data from various sources such as transaction logs, customer information, and external data feeds.
2. **Data Ingestion**: Processes and ingests data into the system in real-time or batch mode.
3. **Data Storage**: Stores the ingested data in a secure and scalable database.
4. **Data Processing**: Analyzes the stored data using various algorithms and models to detect potential fraud.
5. **Fraud Detection Engine**: Applies machine learning models and rule-based systems to identify suspicious activities.
6. **Alert Management**: Generates alerts for detected fraud and sends them to the appropriate channels.
7. **User Interface**: Provides a dashboard for analysts to review and manage alerts.
8. **Reporting and Analytics**: Generates reports and analytics for further investigation and compliance.

Explanation of the Blocks in the Block Diagram and the Flow of Information

1. **Data Sources**:
    - **Description**: This block represents the various sources from which data is collected. These sources include transaction logs, customer information, and external data feeds such as credit scores and blacklists.
    - **Flow**: Data flows from these sources into the Data Ingestion block.
2. **Data Ingestion**:
    - **Description**: This block is responsible for processing and ingesting data into the system. It can handle both real-time streaming data and batch data.

- **Flow**: Ingested data is then sent to the Data Storage block.

3. **Data Storage**:
   - **Description**: This block stores the ingested data in a secure and scalable database. It ensures data integrity and availability for processing.
   - **Flow**: Stored data is accessed by the Data Processing block for analysis.
4. **Data Processing**:
   - **Description**: This block analyzes the stored data using various algorithms and models to detect potential fraud. It includes data cleaning, transformation, and feature extraction.
   - **Flow**: Processed data is sent to the Fraud Detection Engine block.
5. **Fraud Detection Engine**:
   - **Description**: This block applies machine learning models and rule-based systems to identify suspicious activities. It uses historical data and patterns to detect anomalies.
   - **Flow**: Detected fraud cases are sent to the Alert Management block.
6. **Alert Management**:
   - **Description**: This block generates alerts for detected fraud and sends them to the appropriate channels such as email, SMS, or a monitoring dashboard.
   - **Flow**: Alerts are displayed on the User Interface block for analysts to review.
7. **User Interface**:
   - **Description**: This block provides a dashboard for analysts to review and manage alerts. It allows users to investigate and take action on potential fraud cases.
   - **Flow**: Analysts can interact with the system and update the status of alerts.

8. **Reporting and Analytics**:
    - **Description**: This block generates reports and analytics for further investigation and compliance. It provides insights into fraud trends and system performance.
    - **Flow**: Reports and analytics are accessible through the User Interface block.