MAJOR PROJECT PRESENTATION

FinSPY: SIEM-Driven Financial Fraud Detection

Enhancing Security and Risk Mitigation

PROJECT GUIDE

Mr. V. Damodaran

PRESENTED BY

Akshay K R, Nandulal Krishna,
Pravaal B Nath, Rahul R

Agenda

3	Introduction
4	Literature Review
5	System Analysis
6	System Study
7	System Design
8	Methodology
9	System Implementation
10	Conclusion & Future Scope

Introduction

Objective:

Real-time financial fraud detection SIEM: Integrates machine learning and threat intelligence for enhanced accuracy, ensuring regulatory compliance and minimizing fraud incidents.

Features:

- Real-time Transaction Monitoring
- Hybrid AI Model for Anomaly Detection
- Fraud Alerts and Response
- User and Admin Interfaces
- System Scalability and Performance

Literature Review

Enhancing Transaction Fraud Detection with a Hybrid Machine Learning Model. Zhao, Xin & Zhang, Qiong & Zhang, Chang. (2024)

- Advanced Fraud Detection: Combines LightGBM (gradient boosting) and Keras (deep learning) with Focal Loss to tackle imbalanced financial transaction data.
- Enhanced Real-Time Accuracy: Aims to significantly improve precision and adaptability in real-time fraud detection scenarios.

Security Information Event Management Data Acquisition and Analysis Methods with Machine Learning Principles.Tendikov, Noyan & Leila, Rzayeva & Saoud, Bilal & Shayea, Ibraheem & Bin Azmi, Marwan & Myrzatay, Ali & Alnakhli, Mohammad. (2024)

- AI/ML Enhanced SIEM: Integrates AI and machine learning into SIEM systems for improved network intrusion detection.
- Proactive Threat Detection: Demonstrates the effectiveness of ML models, like Random Forest, in accurately identifying security anomalies.

Literature Review

Adaptive Fraud Detection Systems: Real-Time Learning from Credit Card Transaction Data.Ahmad Amjad Mir.(2024)

- Dynamic Fraud Detection: Moves beyond static rules to adaptive, ML-driven systems for real-time credit card fraud detection.
- Adaptability & Accuracy: Emphasizes continuous learning to handle evolving fraud patterns, improving accuracy and customer trust.

Using the SIEM Software Vulnerability Detection Model Proposed. In-seok Jeon, Keun-hee Han, Dongwon Kim, Jin-yung Choi

- SIEM-Enhanced Vulnerability Detection: Integrates vulnerability databases (CVE, etc.) with SIEM for improved software vulnerability analysis.
- Improved Detection & Response: Utilizes big data analytics to increase detection rates, reduce false positives, and enable rapid response to software threats.

Literature Review

Why SIEM is Irreplaceable in a Secure IT Environment? O. Podzins and A. Romanovs

- SIEM for Centralized Security: SIEM integrates diverse security logs for real-time threat detection and automated response across IT infrastructure.
- Essential but Complex: While crucial for proactive cybersecurity, SIEM effectiveness depends on proper optimization and faces challenges like cost and false positives.

Identifying Fraudulent Credit Card Transactions Using AI. H. Cheddy and R. K. Sungkur

- ML for Credit Card Fraud: Evaluates ML models (XGBoost, Decision Tree, etc.) on synthetic data to detect fraudulent transactions.
- XGBoost Optimization & Deployment: Highlights XGBoost's performance, enhanced by techniques like SMOTE and hyperparameter tuning, and its deployment via Flask.

Literature Review

A Survey on Detection of Fraudulent Credit Card Transactions Using Machine Learning Algorithms. A. N. Ahmed and R. Saini

- ML for Imbalanced Fraud Data: Reviews and compares various ML algorithms, highlighting the effectiveness of ensemble methods (XGBoost, Random Forest) for credit card fraud detection.
- Data Preprocessing is Key: Emphasizes the importance of resampling techniques (SMOTE, undersampling) and data preprocessing to address data imbalance and improve model accuracy.

AI-Powered Fraud Detection in the Financial Services Sector: A Machine Learning Approach. M. Marripudugala

- ML Model Comparison: Evaluates Logistic Regression, Decision Tree, and MLP for mobile money fraud detection, highlighting strengths and weaknesses.
- Model Tuning & Strategy: Emphasizes the need for model fine-tuning and strategic selection, along with behavioral analytics and AI-driven approaches, to improve fraud detection.

Literature Review

Comparative Performance of Random Forest versus Gradient Boosting Machines in Detecting Financial Fraud. R. Sharma and D. Minhas

- Ensemble Models for Fraud: Compares Random Forest (RF) and Gradient Boosting Machines (GBM) for financial fraud detection, showing strong performance from both.
- GBM vs. RF Trade-offs: Highlights GBM's superior accuracy and AUC-ROC (0.95), but notes its higher computational cost compared to RF's faster, scalable approach.

System Analysis

Existing System:

- Blockchain based transactions models and rule based transaction verification models.
- Immutable Ledger: Ensures transactions are traceable and tamper-proof, enhancing fraud detection.
- Lack of Real-Time Detection: Blockchain alone cannot dynamically identify evolving fraud patterns at scale.

System Analysis

Proposed system:

- Implementation of SIEM ideology from network security in financial fraud detection.
- Hybrid AI Model: Combines XGBoost and artificial neural networks (ANNs) for enhanced fraud detection accuracy.
- Real-Time Adaptive Learning: Uses XGBoost's Updater feature to update models incrementally, reducing retraining time and computational costs.
- Scalable & Secure Architecture: Built on Flask and Django for efficient API development, ensuring high performance and regulatory compliance.

System Study

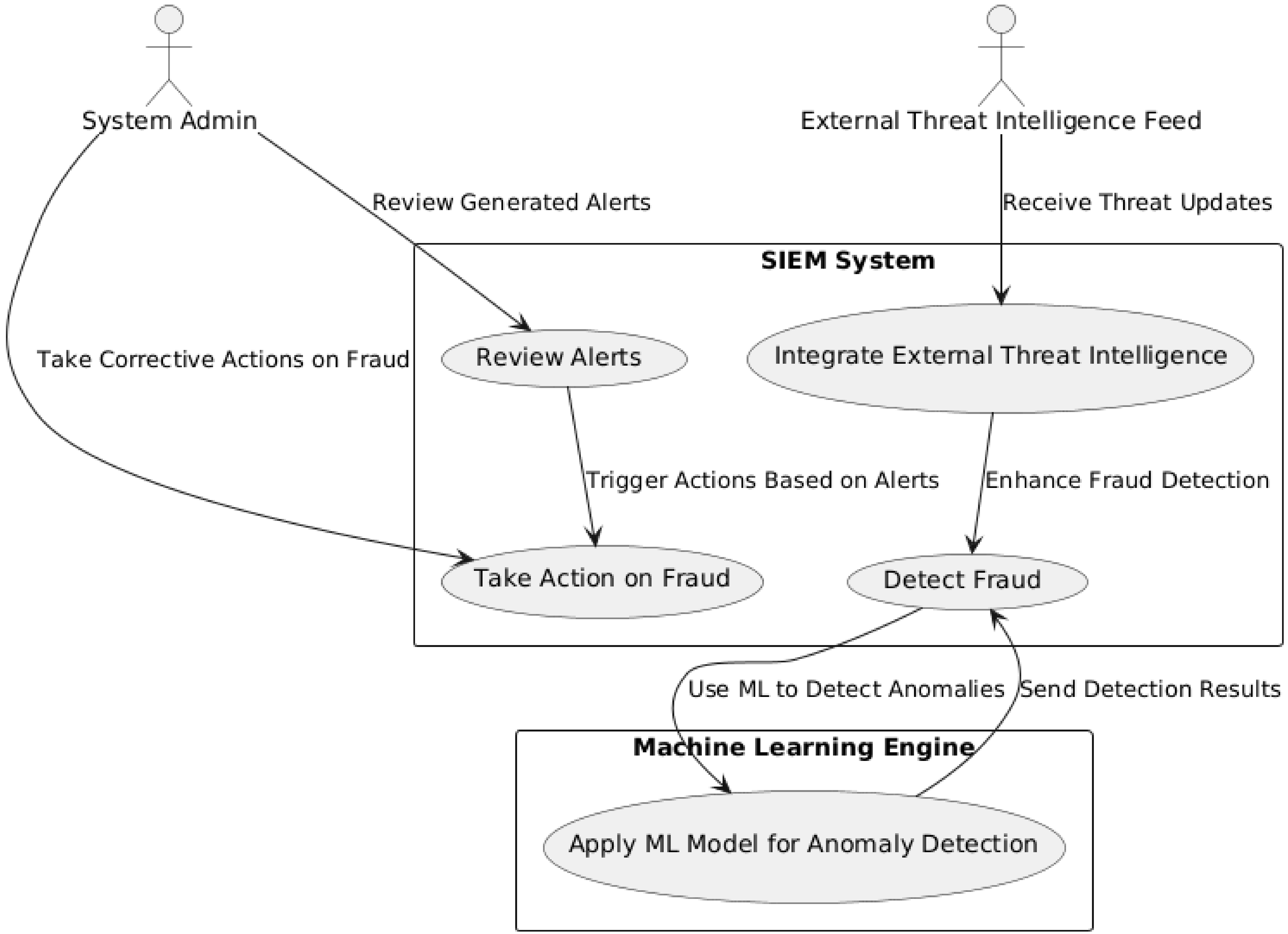
Purpose:

This project develops a real-time fraud detection system using hybrid AI and threat intelligence to monitor financial transactions, ensuring accuracy, compliance, and proactive alerts.

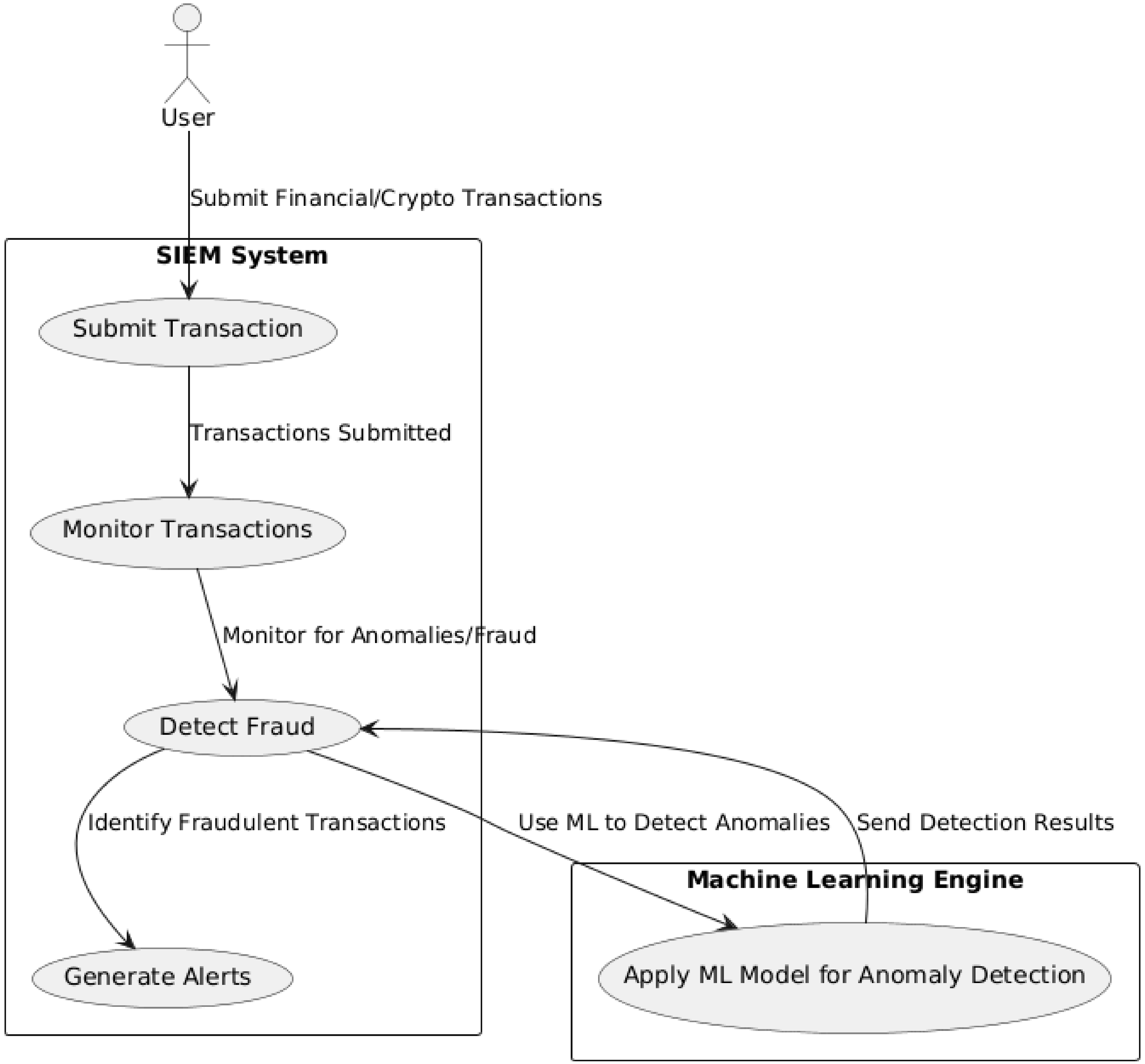
User Types:

1. Clients: Financial institutions implementing the framework for fraud detection.
2. Framework Administrators: Oversee system usage, model performance, and database health.

Usecase : Admin POV


System Admin
External Threat Intelligence Feed
Review Generated Alerts
Receive Threat Updates
SIEM System
Review Alerts
Integrate External Threat Intelligence
Take Corrective Actions on Fraud
Trigger Actions Based on Alerts
Enhance Fraud Detection
Take Action on Fraud
Detect Fraud
Use ML to Detect Anomalies
Send Detection Results
Machine Learning Engine
Apply ML Model for Anomaly Detection

Usecase : Client POV


User
Submit Financial/Crypto Transactions
SIEM System
Submit Transaction
Transactions Submitted
Monitor Transactions
Monitor for Anomalies/Fraud
Detect Fraud
Identify Fraudulent Transactions
Use ML to Detect Anomalies
Send Detection Results
Generate Alerts
Machine Learning Engine
Apply ML Model for Anomaly Detection

System Study

Functional Requirements

1. Real-time Fraud Detection
2. Data Collection
3. Anomaly Detection
4. Data Aggregation and Correlation
5. Data Visualization
6. Scalability and Performance

Non Functional Requirements

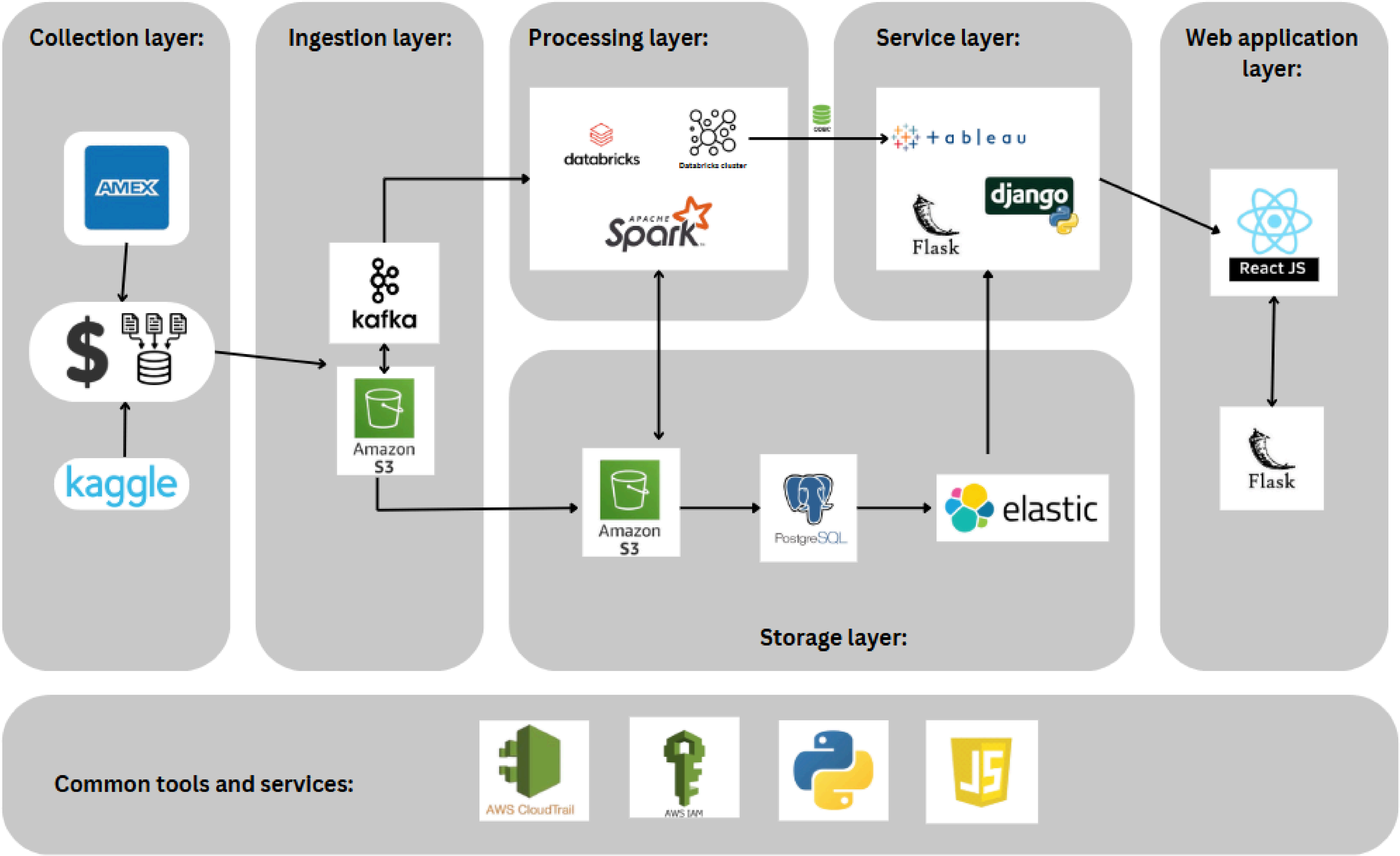
1. Performance
2. Scalability
3. Security
4. Reliability
5. Maintainability
6. Auditability
7. Extensibility

System Design

Hardware Requirements

- Processor: Intel Core i7+/AMD Ryzen 7+ (Multi-core) for real-time processing.
- RAM: Minimum 16GB (32GB recommended) for ML and data processing.
- Storage: 500GB+ SSD for fast operations; cloud storage (e.g., Amazon S3) for large datasets.
- Network: High-speed internet for real-time ingestion & threat intelligence updates.
- GPU (Optional): NVIDIA GTX 1660+ for ML acceleration.

System Design



Collection layer:

Ingestion layer:

Processing layer:

Service layer:

Web application layer:

Storage layer:

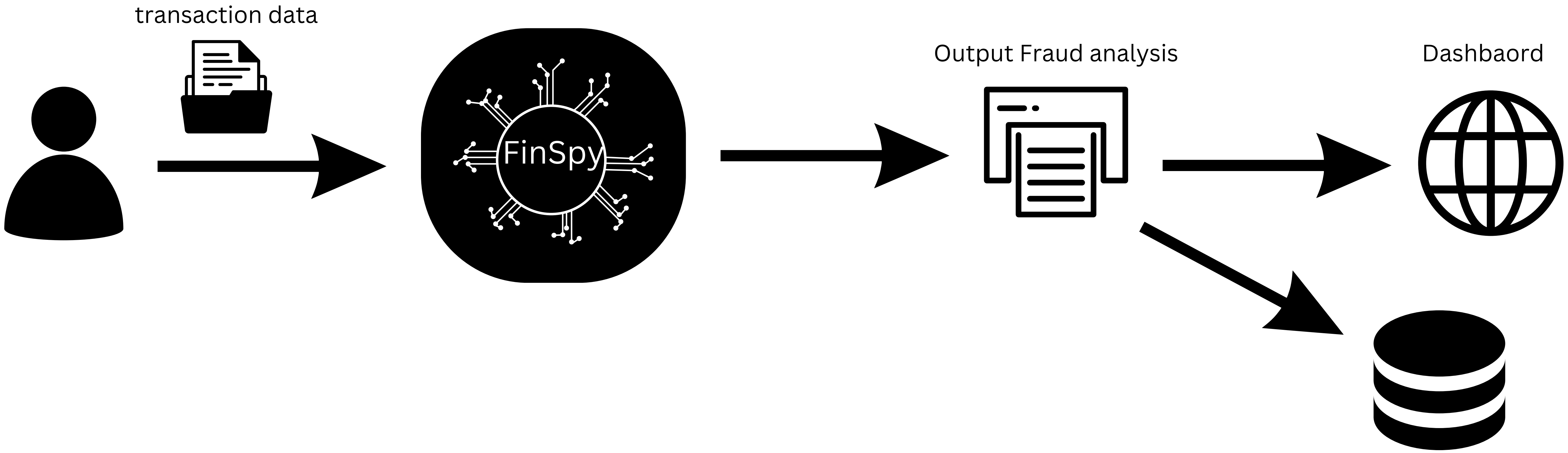
Common tools and services:

System Design

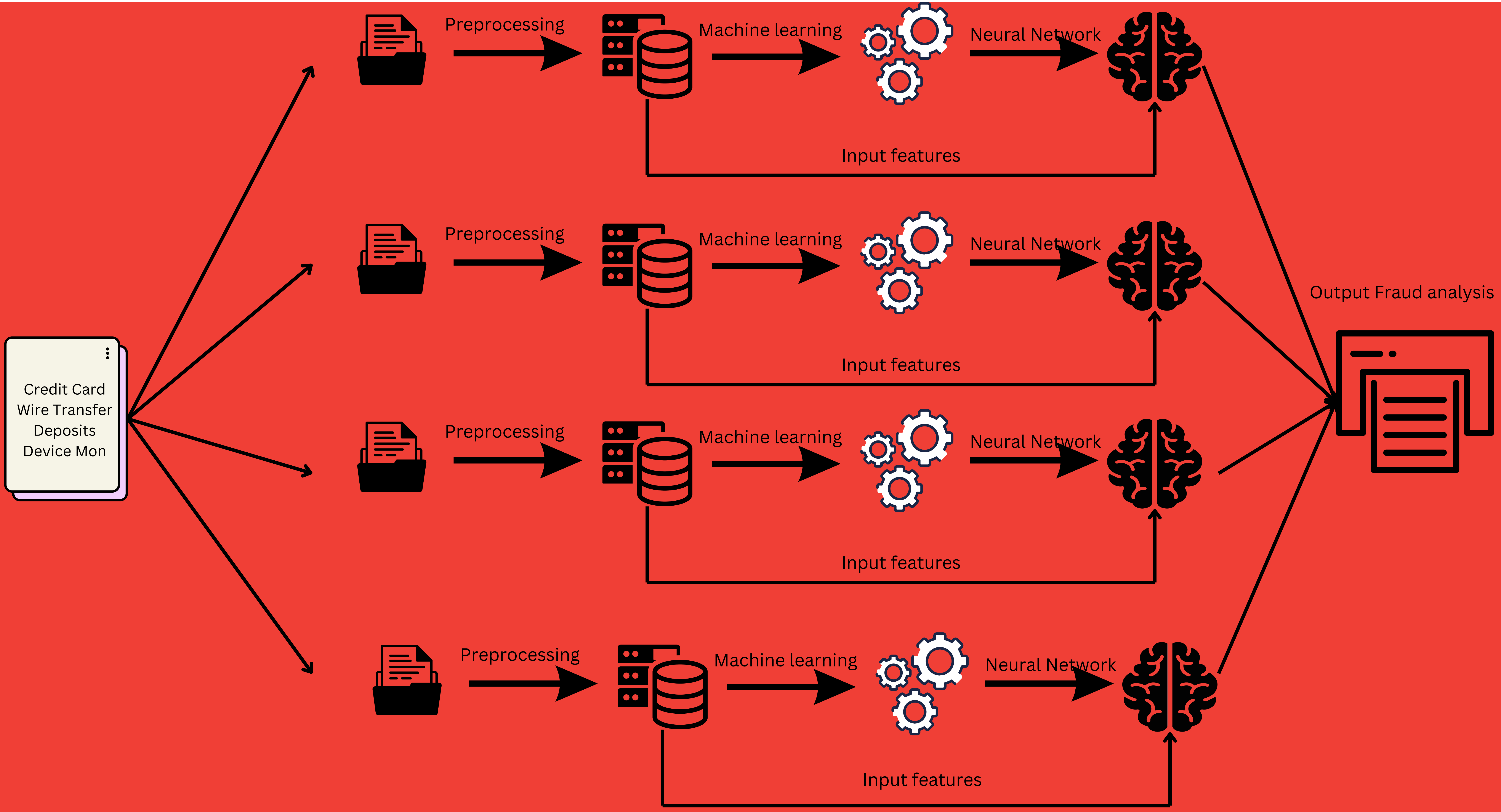
System Architecture:

1. Layered Design: Ensures scalability, efficiency, and seamless data flow.
2. Data Ingestion: Financial data from institutions (e.g., Amex, JP Morgan) & datasets (Kaggle)
3. AI Model: Hybrid AI (ML + ANN) runs in Spark for fraud analysis.
4. Storage: Amazon S3 & PostgreSQL ensuring ACID compliance.
5. Service Layer: Flask & Django handle business logic and APIs.

AI Logic Flow



AI Logic Flow



Methodology

Modules

- Data Pre-processing & Feature Engineering
- ML & ANN Model Training
- Model Updation & Retraining
- Authentication & User Management
- Client Dashboard
- Framework Administrator Dashboard
- Backend API Handling
- Database
- Data Visualization
- Navigation & Routing
- Error Handling & Notifications

System Implementation

- Frontend: React.js with Mistral AI for dynamic UI and AI-driven insights.
- Backend: Apache Spark & Django for advanced data processing and API handling.
- Database: PostgreSQL with AWS S3 for secure and scalable data storage.
- Data Visualization: Chart.js integrated with PostgreSQL for interactive analytics.
- AI Processing: Keras & Scikit-learn hybrid models for accurate fraud detection.

Tech Stack

- 📌 Frontend:
  - React.js + Redux Toolkit – Dynamic UI & state management.
  - Tailwind CSS + Chart.js – Modern styling & fraud analytics.
- 📌 Backend:
  - Python Django – API handling & business logic.
- 📌 Database & Storage:
  - PostgreSQL – Transaction storage.
  - AWS S3 – Scalable cloud storage.

Tech Stack

- 📌 Machine Learning & AI:
  - XGBoost + ANN (Keras, Scikit-learn) – Hybrid fraud detection.
- 📌 Security & Authentication:
  - OAuth2.0 + Auth0 – Secure user authentication.
  - AES-256 Encryption + RBAC – Data & access control.
- 📌 Cloud & DevOps:
  - Docker + Kubernetes – Scalable microservices.
  - AWS EC2 + CloudWatch – Performance monitoring.

Conclusion

The proposed fraud detection system revolutionizes financial security with real-time detection, compliance management, and proactive fraud mitigation. By leveraging hybrid AI models and external threat intelligence, it enhances accuracy and adapts to evolving threats. Its scalable architecture, automated alerts, and seamless API integration ensure compatibility across diverse infrastructures. Inspired by SIEM, the system monitors transactions rigorously, safeguarding financial assets and customer trust. This framework sets a new benchmark for fraud prevention, providing financial institutions with cutting-edge security solutions.

Future Scope

- Advanced AI Integration: Incorporate federated learning, self-supervised learning, and transformer-based models for enhanced fraud detection and privacy-preserving intelligence.
- Regulatory Adaptability: Expand support for global compliance standards and integrate AI-driven risk scoring for improved fraud prevention.
- Enhanced Interoperability: Integrate with SIEM systems and financial security platforms for a comprehensive fraud management solution.

Project Demonstration

References

1 Xin Zhao, Qiong Zhang, Chang Zhang, ”Enhancing Transaction Fraud Detection with a Hybrid Machine Learning Model,” in 2024 IEEE 4th International Conference on Electronic Technology, Communication and Information (ICETCI), Changchun, China, 2024, pp. 427-435.

2 Noyan Tendikov, Leila Rzayeva, Bilal Saoud, Ibraheem Shayea, Marwan Hadri Azmi, Ali Myrzatay, Mohammad Alnakhli, ”Security Information Event Management data acquisition and analysis methods with machine learning principles,” Results in Engineering, vol. 22, pp. 102254, 2024.

3 Ahmad Amjad Mir, ”Adaptive Fraud Detection Systems: Real-Time Learning from Credit Card Transaction Data,” Advances in Computer Sciences, vol. 7, pp. 1-10, 2024.

4 H. Cheddy and R. K. Sungkur, ”Identifying Fraudulent Credit Card Transactions Using AI,” 2024 4th International Conference on Information Communication and Software Engineering (ICICSE), Beijing, China, 2024, pp. 75-79

5 M. Marripudugala, ”AI-Powered Fraud Detection in the Financial Services Sector: A Machine Learning Approach,” 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 795-799

6 R. Sharma and D. Minhas, ”Comparative Performance of Random Forest versus Gradient Boosting Machines in Detecting Financial Fraud,” 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 2024, pp. 1027-1030

References

7 In-seok Jeon, Keun-hee Han, Dong-won Kim, Jin-yung Choi, ”Using the SIEM Software Vulnerability Detection Model Proposed.”

8 P. Nagpal, ”The Transformative Influence of Artificial Intelligence (AI) on Financial Organizations Worldwide,” 2023 IEEE International Conference on ICT in Business Industry Government (ICTBIG), Indore, India, 2023, pp. 1-4,

9 A. N. Ahmed and R. Saini, ”A Survey on Detection of Fraudulent Credit Card Transactions Using Machine Learning Algorithms,” 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, India, 2023, pp. 1-5,

10 Assefa, Samuel, ”Generating Synthetic Data in Finance: Opportunities, Challenges and Pitfalls”, 2020

11 O. Podzins and A. Romanovs, ”Why SIEM is Irreplaceable in a Secure IT Environment?,” 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2019, pp. 1-5

ALGORITHMIC ASSET ARCHITECTS

Thank you!

Github:

https://github.com/Algorithmic-Asset-Architects

The team:

Pravaal B Nath - AI Implementation
Nandu'lal Krishna - Backend speci*a*list
Akshay KR - Front-end Designer
and Rahul R - Front end wizards