SIEM-DRIVEN FINANCIAL FRAUD DETECTION: ENHANCING SECURITY AND RISK MITIGATION

Presented by Group B12
Akshay KR (20221094)
Nandulal Krishna (20221097)
Pravaal B Nath (20921038)
Rahul R (20221098)

OVERVIEW

- Abstract
- Introduction
- Literature Review
- System Architecture
- Use Case diagrams
- Hardware requirements
- Software requirements
- Conclusion

ABSTRACT

This project develops a real-time SIEM system to detect financial and cryptocurrency fraud. Using machine learning and external threat intelligence, it identifies suspicious behaviors and minimizes false positives.

Built for high performance with frameworks like Kafka and Flink, it processes large quantities of events per second. Its cloud-native architecture securely integrates with financial platforms, sending real-time alerts to SOCs for rapid response and enabling automated actions like account freezing. The system offers a scalable fraud detection solution for financial institutions and crypto exchanges.

INTRODUCTION

This project focuses on developing a scalable Security Information and Event Management (SIEM) system designed for real-time detection of financial and cryptocurrency fraud. Leveraging advanced machine learning algorithms and external threat intelligence, the system processes millions of events per second, ensuring rapid detection and response. Its cloud-native architecture integrates seamlessly with financial platforms and blockchain networks, providing a robust solution for fraud prevention.

LITERATURE REVIEW

1. SIEM Data Analysis with Machine Learning

- Research on IDS using machine learning (ML) within SIEM systems.
- It achieves high accuracy using Random Forest.
- Demonstrates real-time detection of anomalies.

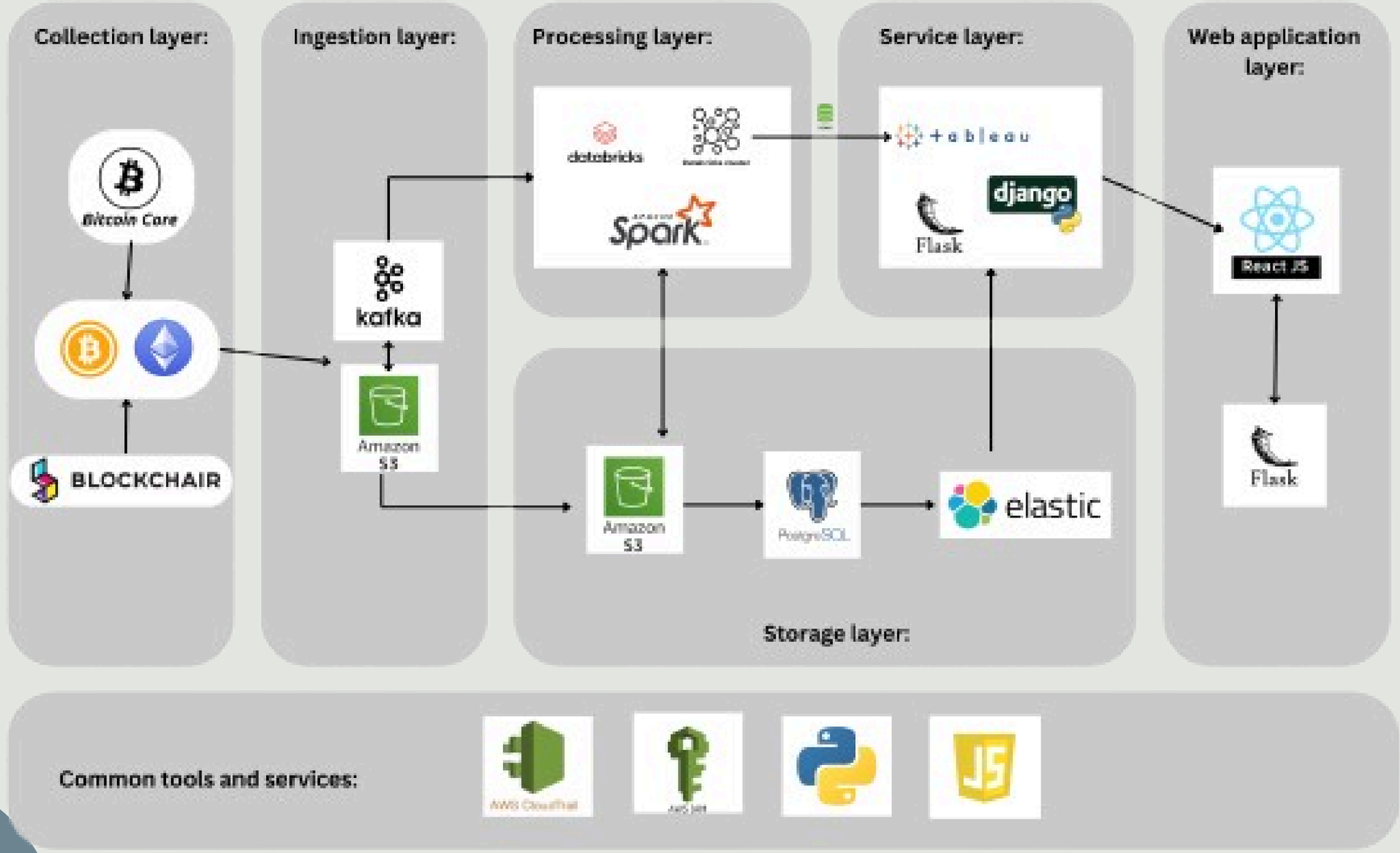
2. Hybrid Fraud Detection Model

- Introduces a hybrid fraud detection system using LightGBM and Keras neural networks.
- Improved accuracy, reduced false positives, and real-time fraud detection.

3. Adaptive Fraud Detection Systems

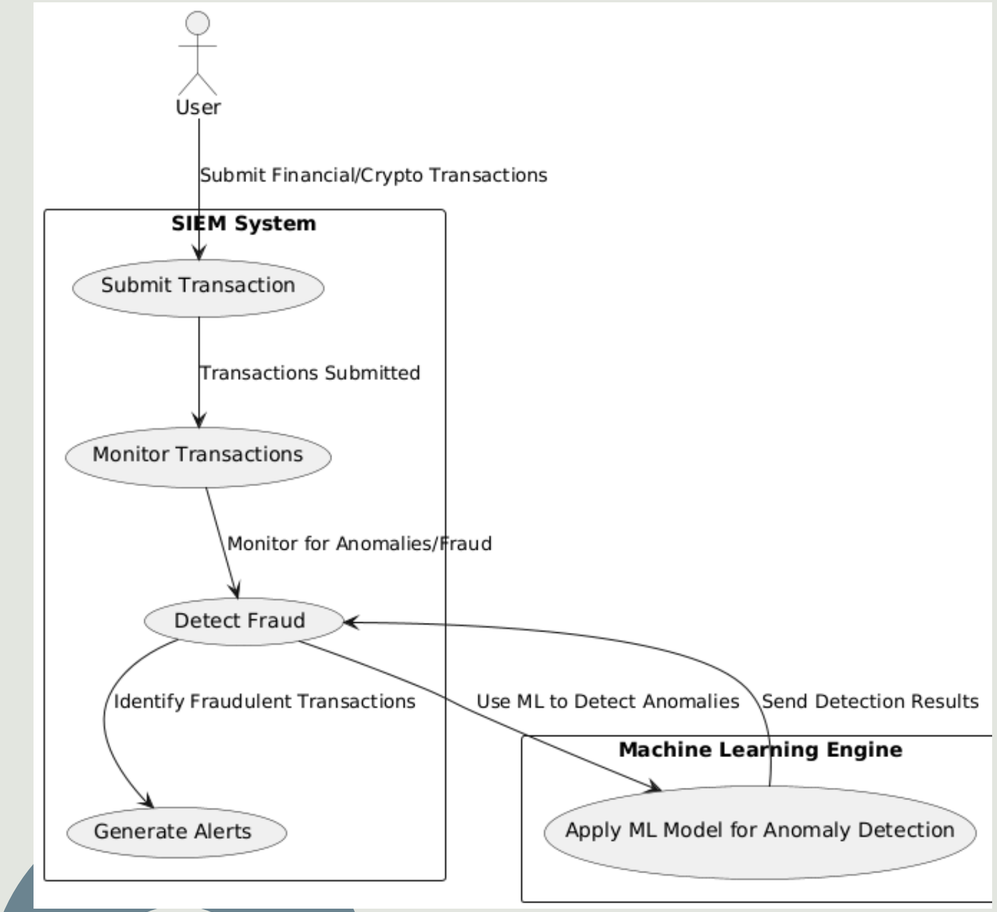
- focuses on adaptive fraud detection using real-time learning techniques.
- Handles concept drift and emerging fraud patterns.
- It combines One-Class SVM for anomaly detection with complex pattern recognition.
- Explores deep learning and privacy-preserving methods to enhance scalability and collaboration across institutions.

SYSTEM ARCHITECTURE

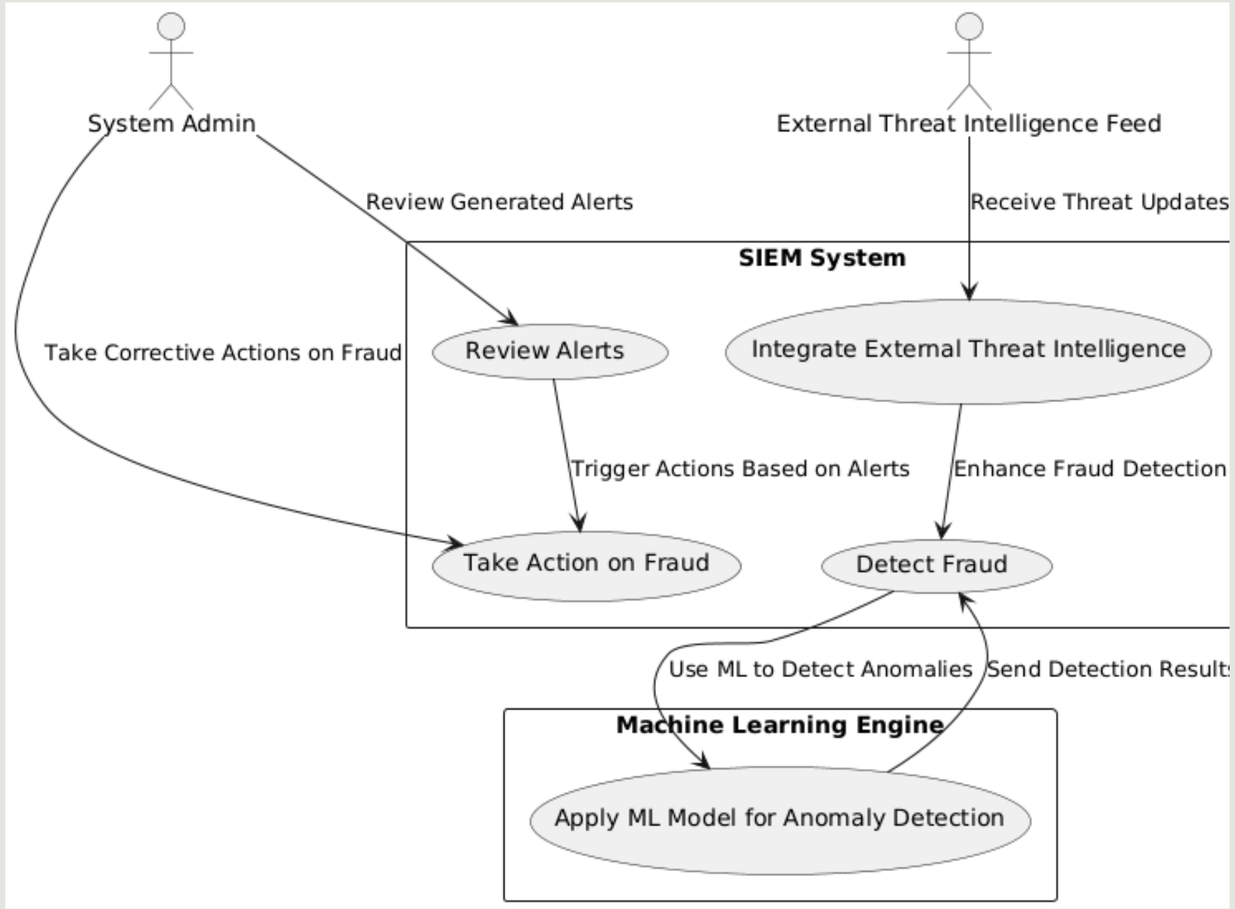


USE CASE DIAGRAMS

- USER POV



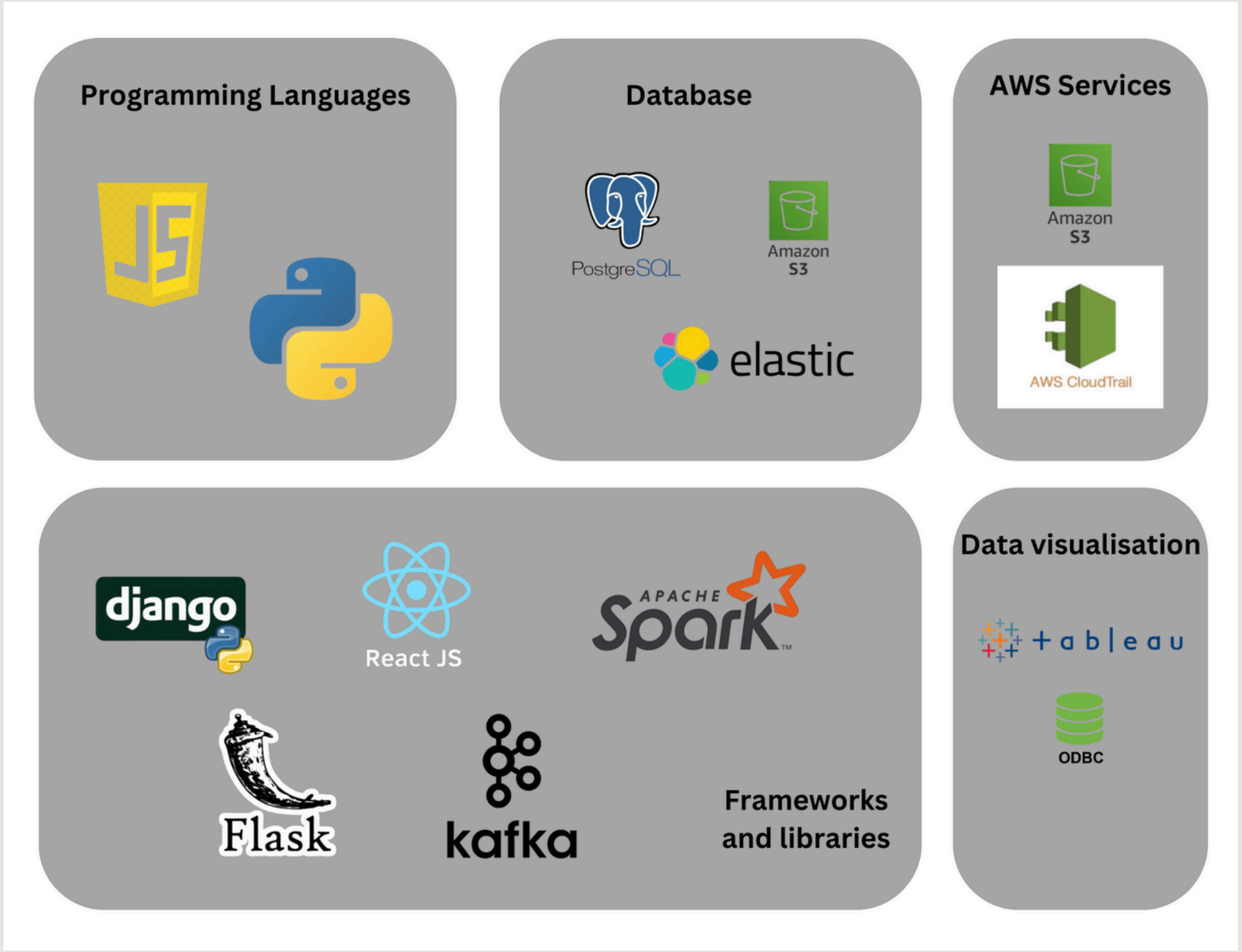
- ADMIN POV



HARDWARE REQUIREMENTS

- Processor: Multi-core (Intel Core i7 or AMD Ryzen 7 or higher) for large data processing.
- RAM: Minimum 16 GB (32 GB recommended) for high-performance machine learning.
- Storage: 500 GB SSD for fast operations, with additional cloud storage (e.g., Amazon S3).
- Network: High-speed internet for real-time data ingestion.
- Optional GPU: NVIDIA GTX 1660 or higher for machine learning tasks requiring GPU acceleration.

SOFTWARE REQUIREMENTS



CONCLUSION

- The proposed fraud detection system represents a major improvement in financial and cryptocurrency security, offering real-time fraud detection, automated alerts, and enhanced accuracy by integrating machine learning and threat intelligence. It addresses the limitations of traditional systems and ensures compliance management, making it adaptable to the evolving landscape of financial fraud.

- With a robust, scalable architecture and seamless data integration, the system is designed to meet current and future needs, fostering trust and security in financial institutions and cryptocurrency exchanges while maintaining regulatory compliance.

Thank You

For your attention