NEXT-GEN FINANCIAL SECURITY

AI Tool for Detecting Anomalies in Bank Transactions

Safeguarding the Future of Finance with Machine Learning Intelligence

COURSE:K.POORNACHANDER
INSTITUTION:SR UNIVERSITY
TEAM:2403A52379,2403A52382,2403A52391,2403A52396

The Escalating Threat Landscape

Surging Fraud Volume

Financial institutions face an unprecedented wave of fraud. Global losses are projected to exceed **$40.6 Billion** by 2027. The sheer velocity of digital transactions makes manual oversight obsolete.

Static Rule Failures

Traditional ”if-then” systems are rigid. They generate frustrating false positives for customers while failing to catch novel, AI-generated attack vectors like deepfake social engineering.

Enter AI-Powered Detection

Dynamic Learning

Unlike static rules, AI models learn dynamically. They analyze thousands of data points per transaction—location, device ID, typing speed—in milliseconds.

Proactive Defense

This enables a shift from ”reaction” to ”prevention,” flagging anomalies before funds ever leave the account, protecting both the bank’s assets and its reputation.

The Detection Pipeline

01. Ingest

Real-time streaming of transaction logs & metadata.

02. Analyze

Feature extraction & vector mapping of behavior.

03. Score

ML model assigns a risk probability (0-100).

04. Act

Instant block or step-up authentication trigger.

Core AI Methodologies

Supervised Learning

Models trained on labeled historical data. Ideal for spotting known fraud patterns like card cloning or chargeback fraud.

Unsupervised Learning

Detects outliers without prior labels. Crucial for identifying ”Zero-Day” attacks that have never been seen before.

Deep Learning

Neural Networks (RNN/LSTM) analyze sequential data to understand time-based patterns in user spending behavior.

Advanced Capabilities

- **Behavioral Biometrics:** Analyzes *how* a user interacts—typing cadence, mouse movements, phone angle—to verify identity beyond passwords.
- **Graph Network Analysis:** Maps hidden relationships between entities. It can instantly spot if 50 seemingly unrelated accounts are sharing one device ID.
- **Sub-Second Latency:** Delivers risk scores in under 300 milliseconds, ensuring a frictionless payment experience for legitimate customers.

Strategic Benefits

Speed

Real-time detection means stopping fraud *during* the transaction, not days later.

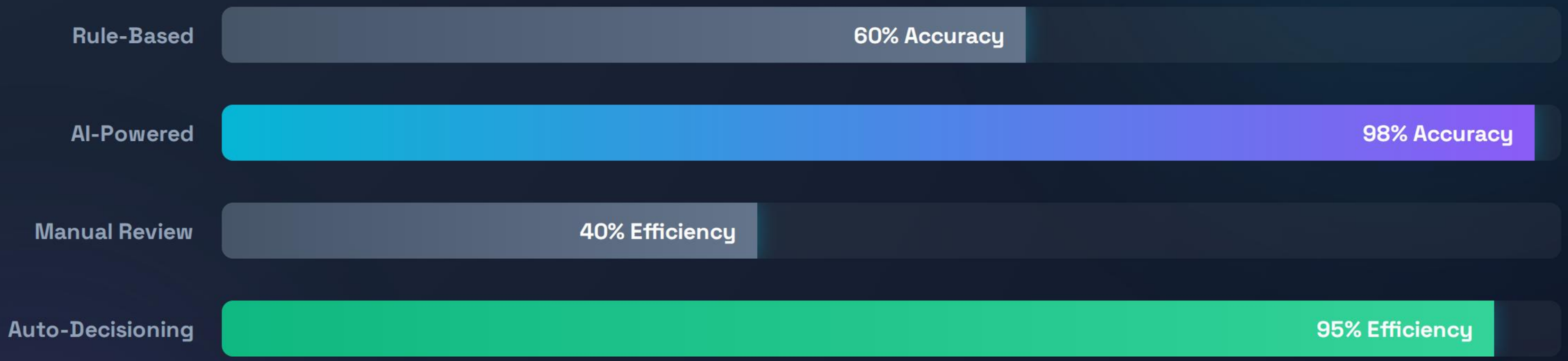
Cost Efficiency

Drastically reduces operational costs associated with manual reviews and chargeback fees.

Precision

Lowers false decline rates, ensuring legitimate customers aren’t embarrassed at checkout.

AI vs. Legacy Systems



AI systems outperform legacy rules in both detection rate and operational efficiency.

Impact by the Numbers

75%

Reduction in
Fraud Losses

10x

Faster Incident
Response

20%

Increase in
Approval Rates

Implementation Hurdles

The "Black Box" Paradox

Deep learning models are complex. Regulators require ”Explainable AI” (XAI)—banks must articulate exactly *why* a transaction was declined to ensure compliance and fairness.

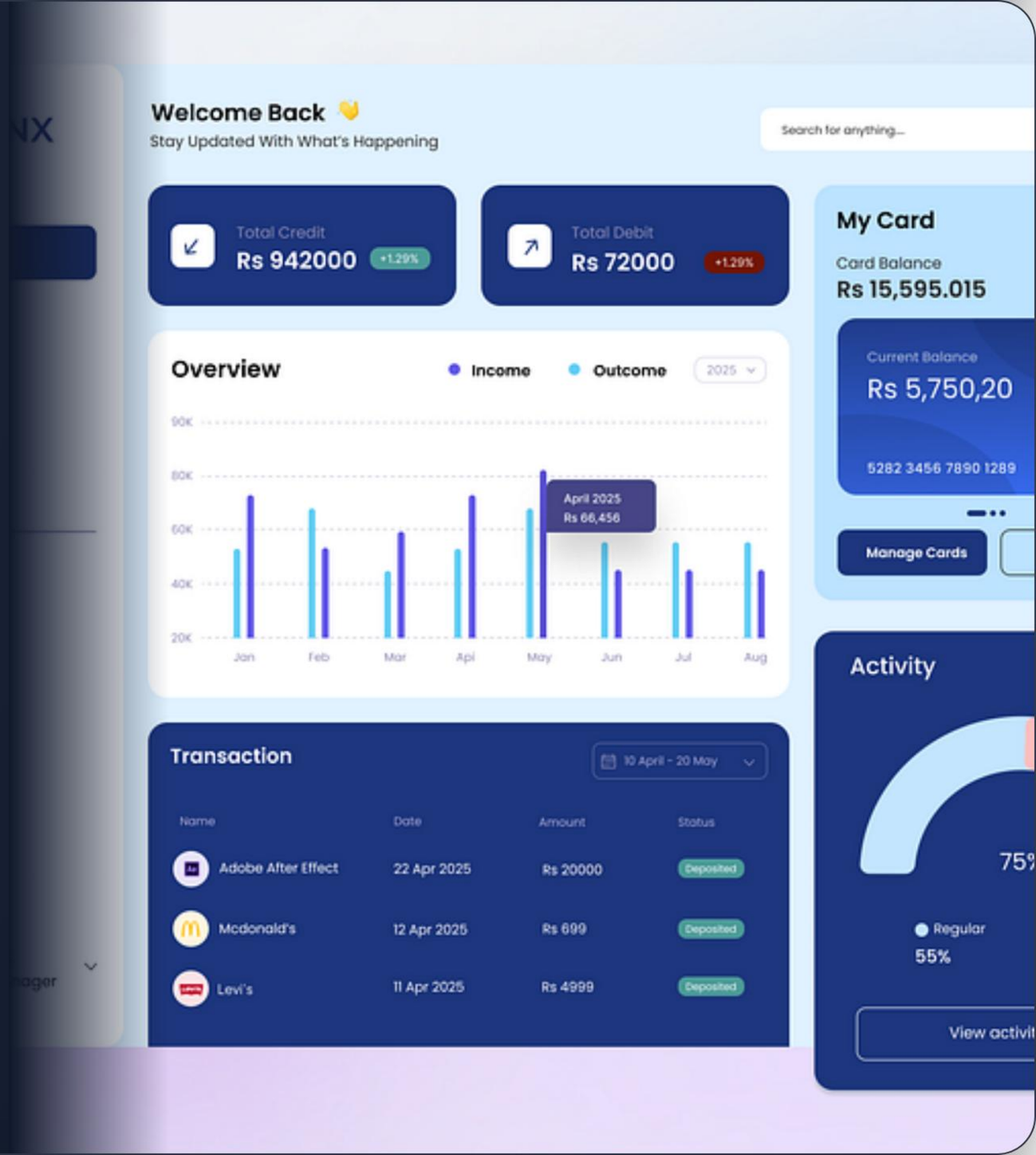
Data Privacy & Silos

Training models requires vast data. Navigating GDPR/CCPA while integrating modern AI engines with decades-old legacy banking mainframes creates significant technical debt.

The Future Horizon

The arms race continues. As fraudsters use Generative AI to create synthetic identities, banks are countering with **Adversarial AI** training.

The next frontier is **Federated Learning**—allowing institutions to share threat intelligence models without ever exposing the underlying private customer data.



Thank You

Securing the Digital Economy Together