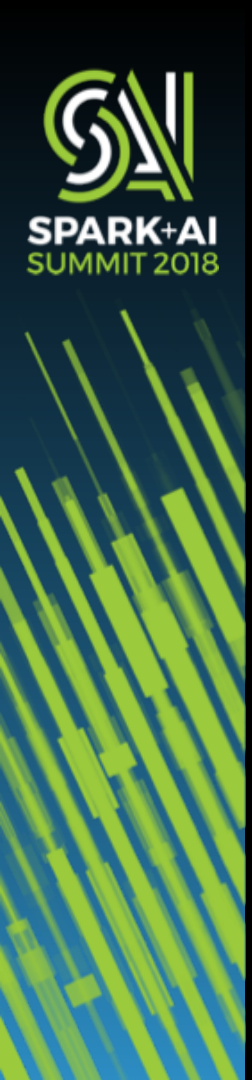


How to Use Millions of Mobile Activity Logs to Understand Our Customers, in Real Time!

Aaron Colcord, FIS Global

Kevin Mellott, FIS Global

#DevSAIS18

Who is FIS Global?

- One of the **largest global** FinTech companies
- Customers are banks and credit unions
- We're FIS Digital Finance, Mobile Data and Analytics
- Ecosystem of products and services **built around core banking**

The Evolution of Banking

Digital Banking

- Check our Account Balances
- Deposit a Check
- Pay Someone/Bill
- Get Money out of the ATM
- *We should be able to replace our actual wallets with the digital wallet.*
- *Let's talk about Fraud as an aspect of understanding*

Fraud Detection Datapoints

- Frequency of Transactions
- Location of the Transactions
- Pattern
- Items purchased
- Total Spend
- Transaction Amount

Fraud Detection has evolved too

- The Algorithms that fraud uses have only grown.(This is Anomaly Detection)
- The Accuracy of when something is fraud and not fraud has only grown more accurate
- Biggest Drawback happens on the backend.
  - After/During Transaction
  - Emphasis has been catching faster and notifying faster
  - Being Predictive about what transactions mean
  - Grabbing more Detail about the Transaction to make the prediction

This could be better

- We are emphasizing more work going faster to close our fraud.
- When Fraud is detected, We cut access. There is no Client feedback in the fraud loop, although technology is available.

With Mobile, is this the best we can do?

We can prove it is you by BioMetrics

We can reasonably assume you have your phone on you

We can track what security features you have enabled

Prove how you are and where you are

Enrich the Experience, Add Behavior and Feedback Loop

Scenarios

ONE	TWO	THREE
Behavioral Pattern	Is this your primary device?	Weird Transactional Pattern

Traditional Fraud Detection

- Supervised learning activity
- Trained using ALL transactions
- Anomaly detection (simplified)

Challenges

- Building a training dataset
- User behavior is unique
- Evolve what we already know

Scenario One

ONE	TWO	THREE
Behavioral Pattern	Is this your primary device?	Weird Transactional Pattern

Behavioral Patterns

- Is it normal for *this person*?
  - How do *they* use the app?
- Personalized anomaly detection
- Indirect correlation to transaction
- Unsupervised analysis

Physical Behavior

- When using our mobile app:
  - Wifi Network
  - Longitude & Latitude
  - Device Info (make/model/os)
  - App Info (installId/version)
- Metadata associated with every action

User Behavior

- Authentication Details
  - Biometric (touch, face)
  - 2FA (SMS, etc)
  - User/Pass
- Payment Method
- Device Used
  - Have we seen it before? When?

Time-based Behavior

- Repeating patterns
  - Pay landlord same amount each month
- Time/distance since last entry
  - Multiple concurrent sessions
  - Different locations, short time period
- User tendencies
  - Ex: Usual to purchase at 4am local time?

Scenarios

ONE	TWO	THREE
Behavioral Pattern	Is this your primary device?	Weird Transactional Pattern

Device Overload

- We live in a world of devices
  - Voice assistants, watches, phones, etc.
  - Will keep growing with IOT
  - Device security is federated
- People often use the same one for purchasing

Managing Devices

- Register upon first time use
  - Includes step-up authentication method
  - Provides a way to "activate" privileges
  - Establishes a baseline

Scenarios

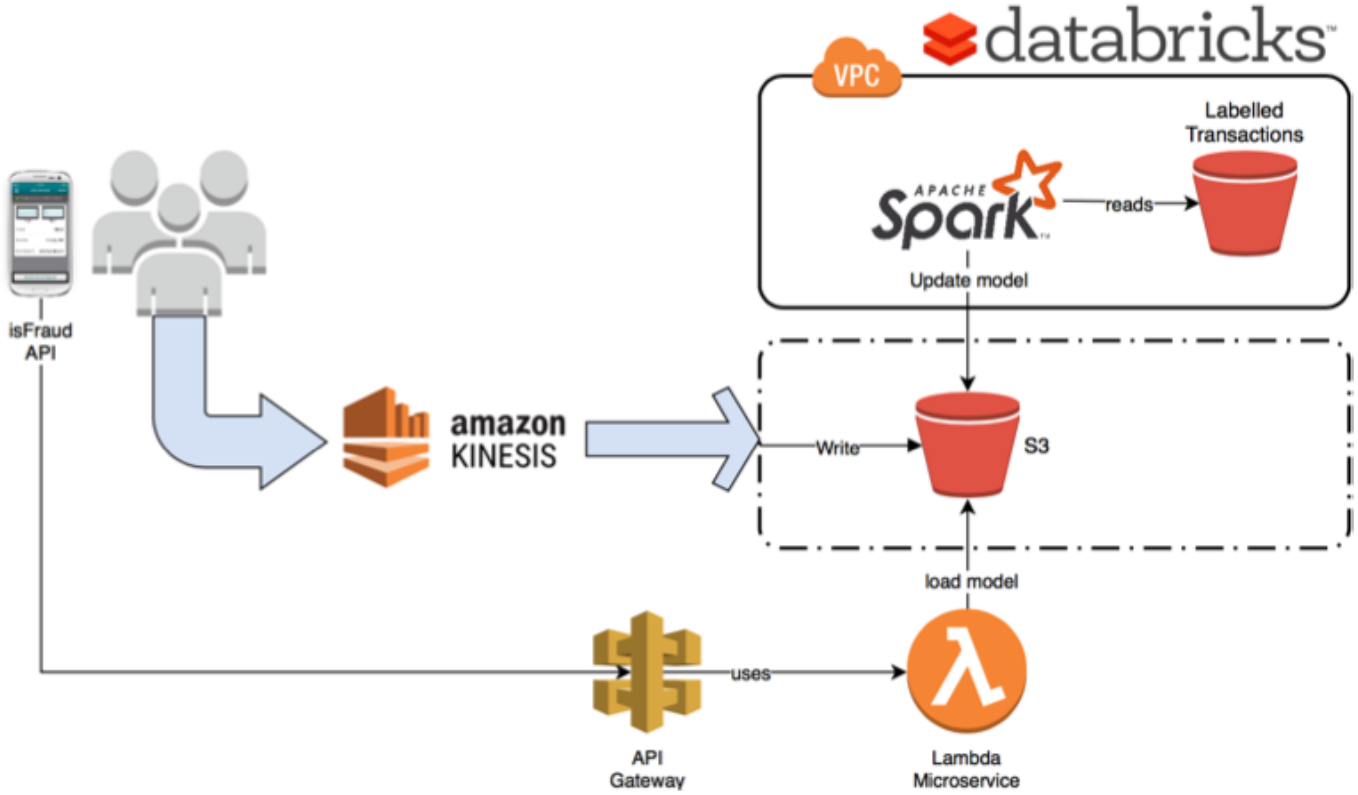
ONE	TWO	THREE
Behavioral Pattern	Is this your primary device?	Weird Transactional Pattern

Weird Transactions

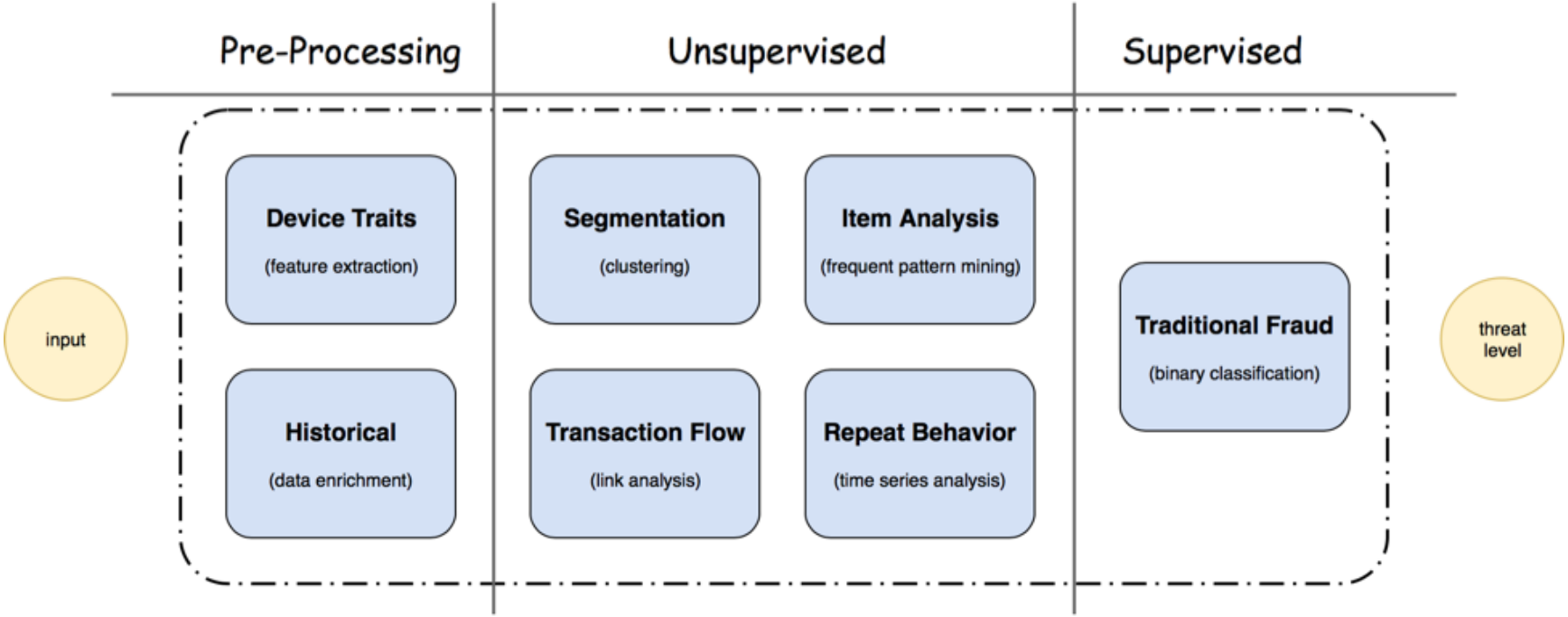
- Comparing a specific transaction
  - "Typical" for the merchant or customer
- Buying 20 laptops online
  - Normal for a business owner
  - Sketchy for an individual's account
- Establish customer profiles
  - Clustering technique
  - Collaborate with domain expert

How Does it Work?

Architecture



ML Pipeline


Pre-Processing
Unsupervised
Supervised
input
Device Traits
(feature extraction)
Historical
(data enrichment)
Segmentation
(clustering)
Transaction Flow
(link analysis)
Item Analysis
(frequent pattern mining)
Repeat Behavior
(time series analysis)
Traditional Fraud
(binary classification)
threat level

Demo

- Model Generation
- Real-time Predictions (Lagom demo)

Shift the Experience

- The Extra Element we are adding to Fraud is your actual behavior.
  - Your Active Location from mobile near Transaction
  - Your Distinct pattern either speed of type or the way you navigate.
  - Incorrect Device Usage
- Let's make Feedback an element of resolving or confirming fraud.

Thank You

www.fisglobal.com