Talking to the Machines: Monitoring Production Machine Learning Systems

Ting-Fang Yen, Director of Research, DataVisor
September 12, 2019
Machine Learning Applications Everywhere
Production ML Pipeline is Complex

“The required surrounding infrastructure is vast and complex.”

Machine Learning Pipeline at DataVisor

Real-time fraud detection service powered by unsupervised machine learning (UML) technology
Billions of application-level events processed daily

Data Collection and Storage

Raw Data

Case Management UI / API

Correlation engine of billions of users

Temporal
Event seq
Velocity / freq
Spatial / geo
Domain attributes
Graph attributes

Data Processing

Feature Generation

UML Clustering Analysis

Supervised Machine Learning

Automated Rule Engine

GIN

DataVisor Global Intelligence Network
What Can Go Wrong?

- **Misconfigurations / Buggy pipeline**
  - Input and output location
  - Module dependencies
  - Version control

- **Resource Management**
  - Out of memory
  - Out of disk
  - Job scheduling
  - Other job failures

- **Data Issues**
  - Data upload problems
  - Data format or parsing error

- **Bugs in code**
  - Runtime exceptions

- **Model accuracy**
  - ...

![Diagram of Data Processing Life Cycle](image-url)
Monitor Production ML Pipelines
Monitor Production ML Pipelines

#prod-status

⚠️ | ✅ | 🔴 O | P0 production status only

**AlertManager** APP 08:21

[PAGER][RT] 🚨 QPS is too low. QPS is 0.0 of last week's 0.1 quantile. Click [link](#) to check all alerts status.

**AlertManager** APP 08:29

[PAGER][RT] 🚨 QPS is too low. QPS is 0.0 of last week's 0.1 quantile. Click [link](#) to check all alerts status.

**AlertManager** APP 02:01

[PAGER][RT] 🚨 Asynchronous client RT requests accumulated in DLQ or reprocess queue. Queue size is 22072. Click [link](#) to check all alerts status.
Making Job Scheduling/Dependencies Simpler

DataVisor SparkGen: One job per cluster

- High utilization
- No inter-job interference
- Maximize job concurrency
- Low maintenance

Sequential

A B C D E F G H I J K L M

Multiple Clusters

A B D E H J L M

C F G I K

One Job Per Cluster

H

B E I L

A C F G J

D K M
What About Model Prediction Quality?

Common approaches for measuring model prediction quality
- Labeled data
- Holdout testing
- Business metrics
- Manual review

Can we come up with other metrics for evaluating machine learning models?
Defining Model Quality…

- Comparing with another model (the “surrogate”)
  - For example, a “simplified” model is used for better runtime performance. Run the “full” model to monitor performance of “simplified” model

- Goodness of clustering
  - E.g., Silhouette index, prediction boundaries

- Quantify model “drift”

- Model-specific metrics?
  - Meta-data about model internals and output
    - Detections triggered by each feature
    - Number of other users a given user is associated with
    - Detection volume by attack type / category
    - Prediction score distribution
    - …
Our Approach

An anomaly detection problem

- Assume model at deployment time is “good”
- Monitor for subsequent changes in model output
Time Series Decomposition

Seasonal decomposition of time series by Loess (STL)

- Additive decomposition: $Y_t = T_t + S_t + R_t$

References:
Time Series Decomposition – with Trend Replacement

Residual (Rt) = Original (Yt) – Trend (Tt) – Seasonal (St)

References:
Time Series Anomaly Detection: Residual Component

MAD statistic: Median absolute deviation
• Median value of the difference between each data point and the median
• A robust measure of data variability

Anomalies: Distance to median > X * MAD
Breakouts: Gradual Changes

Could indicate subtle changes in model behavior

Apply heuristics on “trend” component
- Derivative of signal has the same sign over multiple, consecutive data points
- Recent rate of change is large
Putting it Together
Investigating Anomalies

Group together “similar” time series

• (Pearson) Correlation distance

\[ 1 - \frac{(u - \bar{u}) \cdot (v - \bar{v})}{\| (u - \bar{u}) \|_2 \| (v - \bar{v}) \|_2} \]

• Clustering

• Rank time series in the same cluster as anomalous time series
Investigating Anomalies (cont’d)

- Multidimensional scaling (MDS) for plotting
Investigating Anomalies (cont’d)

Store results as Parquet files
Load as PySpark dataframe (supports SQL-like operations)
Lowers technical barrier for debugging machine learning models
Lessons Learned

• **Build resilient, modular pipelines**
  • Decouple model decisions from data engineering
  • Decouple data from code, features from data

• **Establish process for incident response, assign module owners**

• **Encourage cross-team communication**

• **Explore alternative model evaluation metrics that fit your application/business goals**
Thank you!

https://www.datavisor.com

info@datavisor.com
“By 2021, 50% of enterprises will have added unsupervised machine learning to their fraud detection solution suites.”

- Begin Investing Now in Enhanced Machine Learning Capabilities for Fraud Detection’, Gartner Research