

Monitoring and explainability of models in production

Janis Klaise^{* 1} Arnaud Van Looveren^{* 1} Clive Cox¹ Giovanni Vacanti¹ Alexandru Coca¹

Abstract

The machine learning lifecycle extends beyond the deployment stage. Monitoring deployed models is crucial for continued provision of high quality machine learning enabled services. Key areas include model performance and data monitoring, detecting outliers and data drift using statistical techniques, and providing explanations of historic predictions. We discuss the challenges to successful implementation of solutions in each of these areas with some recent examples of production ready solutions using open source tools.

1. Introduction

In recent years, the problem of how to deploy and scale machine learning models has been made easier by open source tools such as Seldon Core (Cox et al., 2018), KFServing (KFServing, 2019), KubeFlow (KubeFlow, 2018) and MLFlow (Zaharia et al., 2018). One of the big challenges in MLOps is to design systems that monitor live deployments and take action or raise alerts when events impacting model performance are encountered (Diethe et al., 2019). Traditional application monitoring involves logging such core metrics as request latency, frequency and server load with the intention of ensuring uninterrupted, high quality service. On the other hand, it is more demanding to maintain the same level of service for machine learning applications. We identify four additional areas following model deployment which are key for the success of the application:

1. Monitoring model performance
2. Monitoring metrics related to incoming data
3. Detecting outliers and drift
4. Explaining model predictions

^{*}Equal contribution ¹Seldon Technologies Ltd, London, United Kingdom. Correspondence to: Janis Klaise <jk@seldon.io>, Arnaud Van Looveren <avl@seldon.io>.

Firstly, it is critical to ensure model performance does not degrade in a production setting. Inability to detect model performance degradation can lead to stale models and increased technical debt (Breck et al., 2017; Sculley et al., 2015). Whilst trained models usually come with performance metrics on offline test sets, this does not guarantee similar performance in live systems.

Secondly, measuring model performance implies having timely access to labels for live data which are seldom available due to operational and financial constraints. In the absence of labels it is critical to monitor the statistics of input data and output predictions as these can serve as a proxy for model performance (Breck et al., 2017).

Thirdly, to be truly useful the monitoring system requires functionality to determine when significant changes to data and predictive distributions happen, also known as drift detection. A related task is to identify incoming data points which fall outside the training data distribution, also known as outlier detection. These questions are statistical in nature and often require separate models which makes it more difficult to provide general solutions.

Finally, it is important to build trust in machine learning systems and make the decision process transparent. Many models are often “black boxes” whose internal processing is not well understood even by trained data scientists. The field of explainable AI provides numerous approaches to the problem of explaining model predictions, some of which are uniquely suited for deployed models.

In the following sections we discuss the key challenges in these areas from an algorithmic as well as infrastructure perspective and point to existing solutions using open source technologies.

2. Monitoring

2.1. Performance and metrics

Ensuring high model performance in live deployments is arguably the most important aspect of monitoring machine learning systems. However, performance metrics used to develop the models depend on the availability of labels. For live data the number and frequency of collected labels depends on the application. For example, in high-frequency

time-series prediction or internet ad serving labels are automatic and near real-time whilst for many other applications labels are expensive to produce, potentially unreliable and with long time delays following a prediction. For instance, consider a medical diagnostic system based on image recognition. Labelling even small samples of the data presented to such a system can be challenging since it is time consuming and requires domain knowledge. Label noise can also occur due to disagreements between annotators (Louie et al., 2010; Khoo et al., 2012; Bridge et al., 2016). It is however still crucial to report metrics which inform whether the performance of the deployed model is satisfactory.

In the perfect scenario of full and immediate label availability the calculation of performance metrics is straightforward, however some challenges remain on the infrastructure and decision making level. Firstly, the labels have to be fed into some system that then calculates metrics on the fly. This can be a separate system or as part of the model deployment. For example, Seldon Core provides a dedicated `/send-feedback` API endpoint accepting labels and performing user-defined metric calculations which can be standard ML metrics (e.g. accuracy for classification models) or custom, business-specific metrics (e.g. key KPIs derived from performance metrics). Secondly, metrics are inherently stateful—updating a metric with new values involves using the metric value from the previous step. This is in contrast with deployed models which are static over the lifetime of the model. Whilst recent open source libraries provide solutions to such *online* learning of metrics and histograms (Bolmier et al., 2019), the engineering effort of ensuring a metrics component does not lose its state and does not go out of sync (e.g. if the metrics component is scaled up to multiple instances) remains. Thirdly, one must decide on appropriate time periods for calculating metrics. For some use cases metrics over the lifetime of the deployment are most useful while for others static or dynamic time windows based on real time or request frequency are more appropriate. Finally, even with accurate knowledge of label-dependent metrics one must set some threshold or decision rule for when to raise alerts when metrics deteriorate. Such thresholds require domain knowledge and can be difficult to set appropriately to limit the number of false alarms. Alternatives based on change-point detection may prove to be more robust (Bifet, 2017).

In the more common scenario of scarce labels it is common to use label-independent metrics as a proxy for model performance (Breck et al., 2017). This includes designing metrics for monitoring live input data and model predictions. In contrast to performance metrics, appropriate metrics depend on the data type. Image, text and tabular data will have different metrics of interest. Even in the widespread case of tabular data, metrics will be different based on the type of features. For example, whilst we can monitor the

feature-wise moments and order statistics of numerical features, frequency based measures are more appropriate for categorical features. Going beyond pointwise metrics, fast algorithms for approximate online histograms (Ben-Haim & Tom-Tov, 2010) can provide much richer insight into the live data distributions. Nevertheless, a fundamental drawback of univariate metrics is that correlations between features are not captured. Multivariate metrics such as covariance matrices and multivariate histograms remain difficult to implement due to the increased computational cost and curse of dimensionality as well as the need for an online update rule. We discuss multivariate approaches in the context of detecting drift in Section 2.3.

2.2. Outlier detection

Machine learning models often fail to generalize outside of the training data distribution (Recht et al., 2019; Engstrom et al., 2019; Hendrycks & Dietterich, 2019). Furthermore, models are typically not well calibrated (Guo et al., 2017) which can lead to overconfident predictions on out-of-distribution instances (Lakshminarayanan et al., 2017). Outlier detection is therefore key to flag anomalies whose model predictions we cannot trust and should not use in a production setting. The type of outlier detector for a specific application depends on the modality and dimensionality of the data, availability of labeled normal and outlier data, and whether the detector is pre-trained (offline) or updated online. The pre-trained detector can be deployed as a separate static machine learning model while the online detector is deployed as a stateful application. Labeled outlier data is often scarce, making the problem semi-supervised at best. Open source libraries such as Alibi Detect (Van Looveren et al., 2020) and PyOD (Zhao et al., 2019) provide a wide range of mainly unsupervised off-the-shelf outlier detectors which can be tailored to the specific problem setting.

It is important to note that the problem of unsupervised anomaly detection for real-world data (e.g. natural images or noisy time series) is far from solved. At the heart the problem is one of reliable density estimation. The quality of the estimator however depends on the modality and the data set. Different studies on image data (Nalisnick et al., 2019; Choi et al., 2018) also illustrate that generative density models can assign higher likelihood values to out-of-distribution instances compared to inlier data. Contrary to most machine learning tasks, the unsupervised training objective is only a proxy for the actual performance of the detector.

2.3. Drift detection

While outliers refer to individual instances, data drift or shift detection checks whether two samples are drawn from the same underlying distribution or not via a statistical hypothesis test. The goal of the drift detector is therefore to identify

when the distribution of the requests for the deployed model starts to diverge from the training data and model predictions become unreliable. We can further distinguish *covariate shift* from *label shift* of the model predictions. In the case of *covariate shift* the input data distribution $p(x)$ changes while the conditional label distribution $p(y|x)$ remains unchanged. *Label shift* happens when $p(y)$ changes but the conditional $p(x|y)$ does not.

Target drift

Concept drift: actual relationship between X and y ($P(y|x)$)Source: <https://madewithml.com/courses/mlops/monitoring/>

In order to make drift detection work in practice on high-dimensional data such as images, the incoming data first undergoes a dimensionality reduction step before applying the hypothesis test. Rabanser et al. (2019) observe that randomly initialized encoders and *black box dimensionality reduction* introduced by Lipton et al. (2018) are promising pre-processing methods. This is followed by a two-sample test such as the *maximum mean discrepancy* (Gretton et al., 2012) for the multivariate case in combination with a permutation test to obtain p-values. Alternatively, a feature-wise Kolmogorov-Smirnov test (Smirnov, 1939) is run with Bonferroni or False Discovery Rate (Benjamini & Hochberg, 1995) p-value correction for multivariate data.

Drift detection informs the user when the model should be retrained which is especially important in applications where model performance feedback is not readily available. Malicious data drift, which significantly harms model performance, is of special importance. Vacanti & Van Looveren (2020) show that drift detection on an instance level adversarial score is effective at identifying underlying malicious data shift. Alibi Detect (Van Looveren et al., 2020) provides all the aforementioned drift detection functionality under a common API.

2.4. Deploying model monitoring

The techniques discussed above need to be deployed alongside the running models but in a manner which does not adversely affect their core performance. Recent inference deployment projects such as KFServing and Seldon Core which run on the Kubernetes container orchestration platform solve this by utilizing the eventing based project KNative (KNative, 2019) which allows serverless components to be connected to event streams. The serverless KNative project makes it possible to scale services down to zero if no requests are being received and scale up as demand increases. This allows monitoring components to scale as needed. Figure 1 shows the resulting architecture.

Incoming low latency requests run as normal with a payload logging solution sending events containing model request and response payloads to a KNative *broker* which can farm these out as desired via programmable *triggers* to serverless components such as outlier, drift and adversarial detection modules. Further eventing components can be added to feed off events produced by these components to send onwards to,

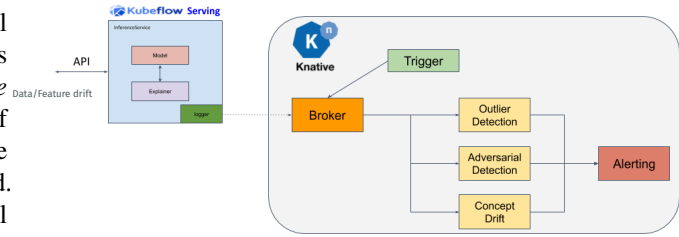


Figure 1. Asynchronous ML monitoring implementation with KFServing and KNative eventing.

for example, alerting or storage modules. The architecture provides a clean separation of concerns between the model and its later analysis components each of which can be scaled separately.

3. Explainability

3.1. The need for model explanations

Instance level machine learning model explanations are desirable for multiple reasons. They allow the user to build trust in the predictions made by the deployed machine learning system and improve transparency. The user can verify which factors contributed to certain predictions, introducing a layer of accountability. Model introspection is also increasingly important with the rise of pre-trained models (e.g. Kolesnikov et al. (2019) for computer vision or Wolf et al. (2019) for language tasks) which are only fine-tuned for a specific downstream task. The data used during the pre-training stage is not curated by the user of the downstream task and can create harmful model biases, potentially leading to unfair outcomes. Buolamwini & Gebru (2018) highlight the importance of representative and unbiased training sets in computer vision to avoid discrimination while Bolukbasi et al. (2016) reveal that even the pre-trained word embeddings *Word2Vec* contain societal gender bias. Model introspection goes hand in hand with other monitoring practices such as anomaly or drift detection. When an instance is flagged as an outlier, explanation methods can help determine whether the model prediction on the instance can be trusted and acted on.

The suitability of an explanation method depends on the data modality, type of model (e.g. tree-based or neural network) and prediction task (e.g. classification or regression). Most commonly used explanation methods also need heuristics and make assumptions about key components of the explanation generating process such as the background values for each feature (e.g. SHAP (Lundberg & Lee, 2017), Integrated Gradients (Sundararajan et al., 2017), Anchors (Ribeiro et al., 2018), Contrastive Explanations (Dhurandhar et al., 2018)), local model behaviour (e.g. local linearity for

LIME (Ribeiro et al., 2016)) or feature interactions (PDP (Friedman, 2001)). In order to overcome method-specific pitfalls, it is important to obtain a holistic explanation for each instance, combining the complementary strengths of different techniques. The overall explanation sheds light on the impact of the training data, relative feature importance, the key features to maintain the original prediction as well as the minimal changes to the features that will cause the prediction to change. Explanation techniques based on influence functions (Koh & Liang, 2017; Barshan et al., 2020) highlight which training instances had the most impact on a specific prediction at inference time. This allows the user to check whether the most influential training data contain relevant features compared to the explained instance in production. We also want to know which features are key to ensure a model prediction for a given instance regardless of the values of the other features in the form of Anchor explanations (Ribeiro et al., 2018). The opposite and complementary counterfactual approach (Wachter et al., 2018) finds the minimal change to the original instance which flips the model prediction while still respecting the class-conditional data distribution (Van Looveren & Klaise, 2019). Finally, feature attribution methods such as LIME, SHAP or Integrated Gradients evaluate the relative feature importances with respect to a model prediction.

Explanation algorithms can be grouped into *white-box* and *black-box* methods. Whereas white-box methods assume access to model internals such as being able to take gradients with respect to the input (Sundararajan et al., 2017), black-box methods do not assume anything beyond being able to access the prediction API endpoint. This is a natural scenario for deployed models as any information related to model internals is typically inscrutable and the only way to interact with the model is by requesting predictions. In the following section we motivate the usage of black-box explanations for models in production.

3.2. Deploying black-box explanations

Black-box explanation algorithms work by taking an input instance whose prediction is to be explained and by repeatedly querying the model with modified versions of the input to approximate its predictive behaviour. The actual query strategy, definition of modified instances and explanation output is specific to each algorithm. In production this translates to having two deployments, the original model and the explainer, exposing a prediction endpoint and an explanation endpoint respectively (fig. 2). When the prediction endpoint is called with a data point, a prediction is returned as usual, but when the explanation endpoint is called with the same data point, this triggers the black-box explanation algorithm to internally query the model and produce an explanation.

This pattern provides an infrastructure abstraction for re-

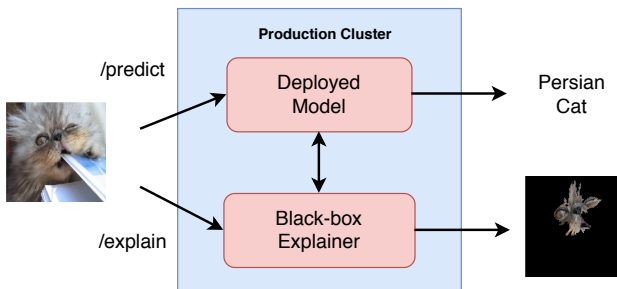


Figure 2. Design pattern for black-box explanation methods in production. A production cluster contains a deployed model which exposes a `/predict` endpoint as well as a deployed explainer which stores a reference to the model’s `/predict` endpoint and exposes an additional `/explain` endpoint. An explanation can be requested on-demand by calling the `/explain` endpoint which triggers the black-box algorithm to interact with the model and produce an explanation.

questing on-demand explanations for any black-box explanation algorithm. It has the advantage of using the underlying infrastructure to auto-scale the model deployment if a high volume of explanations is requested. Alternatively, this pattern can be implemented on a carbon copy of the model so as to separate production prediction requests from introspective explanation requests. This pattern is implemented using the Seldon Core (Cox et al., 2018) and KFServing (KFServing, 2019) deployment platforms, together with the Anchor explanation technique (Ribeiro et al., 2018) implemented in Alibi (Klaise et al., 2019) on tabular, text and image classification tasks. Figure 2 shows an example explanation of a prediction made by a deployed InceptionV3 (Szegedy et al., 2016) model on an ImageNet (Deng et al., 2009) instance.

4. Conclusion

In this paper we discussed key areas and challenges surrounding monitoring and explaining deployed models. We highlighted open source solutions for the algorithmic challenges (Klaise et al., 2019; Van Looveren et al., 2020; Bolmier et al., 2019) and the infrastructure (Cox et al., 2018; KFServing, 2019) to support these capabilities. One of the main open research topics is to more directly relate the label-independent measures obtained from the metrics, outlier and drift detectors to the model performance. Best practices are still being established in the MLOps community and we feel that in order to succeed, the open source tools need to be general enough to cover a majority of use cases whilst being flexible enough to allow for use case specific customization.

References

- Barshan, E., Brunet, M.-E., and Dziugaite, G. K. Relatif: Identifying explanatory training samples via relative influence. In Chiappa, S. and Calandra, R. (eds.), *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*, volume 108 of *Proceedings of Machine Learning Research*, pp. 1899–1909, Online, 26–28 Aug 2020. PMLR. URL <http://proceedings.mlr.press/v108/barshan20a.html>.
- Ben-Haim, Y. and Tom-Tov, E. A streaming parallel decision tree algorithm. *Journal of Machine Learning Research*, 11(28):849–872, 2010. URL <http://jmlr.org/papers/v11/ben-haim10a.html>.
- Benjamini, Y. and Hochberg, Y. Controlling the false discovery rate: A practical and powerful approach to multiple testing. *Journal of the Royal Statistical Society. Series B (Methodological)*, 57(1):289–300, 1995. ISSN 00359246. URL <http://www.jstor.org/stable/2346101>.
- Bifet, A. Classifier concept drift detection and the illusion of progress. In *International Conference on Artificial Intelligence and Soft Computing*, pp. 715–725. Springer, 2017.
- Bolmier, G., Halford, M., Sourty, R., Vaysse, R., and Zouitine, A. creme, a Python library for online machine learning, 2019. URL <https://github.com/creme-ml/creme>.
- Bolukbasi, T., Chang, K.-W., Zou, J. Y., Saligrama, V., and Kalai, A. T. Man is to computer programmer as woman is to homemaker? debiasing word embeddings. In Lee, D. D., Sugiyama, M., Luxburg, U. V., Guyon, I., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 29*, pp. 4349–4357. Curran Associates, Inc., 2016. URL <http://papers.nips.cc/paper/6228-man-is-to-computer-programmer-as-woman-is-to-homemaker-debiasing-word-embeddings.pdf>.
- Breck, E., Cai, S., Nielsen, E., Salib, M., and Sculley, D. The ml test score: A rubric for ml production readiness and technical debt reduction. In *Proceedings of IEEE Big Data*, 2017.
- Bridge, P., Fielding, A., Rowntree, P., and Pullar, A. Intraobserver variability: Should we worry? *Journal of medical imaging and radiation sciences*, 47(3):217–220, 2016.
- Buolamwini, J. and Gebru, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In Friedler, S. A. and Wilson, C. (eds.), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, volume 81 of *Proceedings of Machine Learning Research*, pp. 77–91, New York, NY, USA, 23–24 Feb 2018. PMLR. URL <http://proceedings.mlr.press/v81/buolamwini18a.html>.
- Choi, H., Jang, E., and Alemi, A. A. Waic, but why? generative ensembles for robust anomaly detection. 2018.
- Cox, C., Sunner, G., Saucedo, A., Dawson, R., Gonzalez, A., and Skolasinski, R. Seldon Core: A framework to deploy, manage and scale your production machine learning to thousands of models., 2018. URL <https://github.com/SeldonIO/seldon-core>.
- Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., and Fei-Fei, L. ImageNet: A Large-Scale Hierarchical Image Database. In *CVPR09*, 2009.
- Dhurandhar, A., Chen, P.-Y., Luss, R., Tu, C.-C., Ting, P., Shanmugam, K., and Das, P. Explanations based on the missing: Towards contrastive explanations with pertinent negatives. In Bengio, S., Wallach, H., Larochelle, H., Grauman, K., Cesa-Bianchi, N., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 31*, pp. 592–603. Curran Associates, Inc., 2018. URL <http://papers.nips.cc/paper/7340-explanations-based-on-the-missing-towards-contrastive-explanations-with-pertinent-negatives.pdf>.
- Diethe, T., Borchert, T., Thereska, E., Balle, B., and Lawrence, N. Continual learning in practice, 2019.
- Engstrom, L., Tran, B., Tsipras, D., Schmidt, L., and Madry, A. Exploring the landscape of spatial robustness. In Chaudhuri, K. and Salakhutdinov, R. (eds.), *Proceedings of the 36th International Conference on Machine Learning*, volume 97 of *Proceedings of Machine Learning Research*, pp. 1802–1811, Long Beach, California, USA, 09–15 Jun 2019. PMLR. URL <http://proceedings.mlr.press/v97/engstrom19a.html>.
- Friedman, J. H. Greedy function approximation: A gradient boosting machine. *The Annals of Statistics*, 29(5):1189–1232, 2001. ISSN 00905364. URL <http://www.jstor.org/stable/2699986>.
- Gretton, A., Borgwardt, K. M., Rasch, M. J., Schölkopf, B., and Smola, A. A kernel two-sample test. *Journal of Machine Learning Research*, 13(25):723–773, 2012. URL <http://jmlr.org/papers/v13/gretton12a.html>.
- Guo, C., Pleiss, G., Sun, Y., and Weinberger, K. Q. On calibration of modern neural networks. In Precup, D. and Teh, Y. W. (eds.), *Proceedings of the 34th International*

- Conference on Machine Learning*, volume 70 of *Proceedings of Machine Learning Research*, pp. 1321–1330, International Convention Centre, Sydney, Australia, 06–11 Aug 2017. PMLR. URL <http://proceedings.mlr.press/v70/guo17a.html>.
- Hendrycks, D. and Dietterich, T. G. Benchmarking neural network robustness to common corruptions and perturbations. In *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019*. OpenReview.net, 2019. URL <https://openreview.net/forum?id=HJz6tiCqYm>.
- KFServing. KFServing: Serverless inferencing on kubernetes, 2019. URL <https://github.com/kubeflow/kfserving>.
- Khoo, E. L., Schick, K., Plank, A. W., Poulsen, M., Wong, W. W., Middleton, M., and Martin, J. M. Prostate contouring variation: can it be fixed? *International Journal of Radiation Oncology* Biology* Physics*, 82(5):1923–1929, 2012.
- Klaise, J., Van Looveren, A., Vacanti, G., and Coca, A. Alibi: Algorithms for monitoring and explaining machine learning models, 2019. URL <https://github.com/SeldonIO/alibi>.
- KNative. KNative, 2019. URL <https://knative.dev>.
- Koh, P. W. and Liang, P. Understanding black-box predictions via influence functions. In *Proceedings of the 34th International Conference on Machine Learning*, volume 70, pp. 1885–1894, 06–11 Aug 2017. URL <http://proceedings.mlr.press/v70/koh17a>.
- Kolesnikov, A., Beyer, L., Zhai, X., Puigcerver, J., Yung, J., Gelly, S., and Houlsby, N. Big transfer (bit): General visual representation learning, 2019.
- Kubeflow. Kubeflow, 2018. URL <https://www.kubeflow.org/>.
- Lakshminarayanan, B., Pritzel, A., and Blundell, C. Simple and scalable predictive uncertainty estimation using deep ensembles. In Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 30*, pp. 6402–6413. Curran Associates, Inc., 2017. URL <http://papers.nips.cc/paper/7219-simple-and-scalable-predictive-uncertainty-estimation-using-deep-ensembles.pdf>.
- Lipton, Z. C., Wang, Y.-X., and Smola, A. Detecting and correcting for label shift with black box predictors, 2018.
- Louie, A. V., Rodrigues, G., Olsthoorn, J., Palma, D., Yu, E., Yaremko, B., Ahmad, B., Aivas, I., and Gaede, S. Inter-observer and intra-observer reliability for lung cancer target volume delineation in the 4d-ct era. *Radiotherapy and Oncology*, 95(2):166–171, 2010.
- Lundberg, S. M. and Lee, S.-I. A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems 30*, pp. 4765–4774. 2017. URL <https://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions>.
- Nalisnick, E., Matsukawa, A., Teh, Y. W., Gorur, D., and Lakshminarayanan, B. Do deep generative models know what they don’t know? In *International Conference on Learning Representations*, 2019. URL <https://openreview.net/forum?id=H1xwNhCcYm>.
- Rabanser, S., Günnemann, S., and Lipton, Z. Failing loudly: An empirical study of methods for detecting dataset shift. In Wallach, H., Larochelle, H., Beygelzimer, A., d’Alché-Buc, F., Fox, E., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 32*, pp. 1396–1408. Curran Associates, Inc., 2019. URL <http://papers.nips.cc/paper/8420-failing-loudly-an-empirical-study-of-methods-for-detecting-dataset-shift.pdf>.
- Recht, B., Roelofs, R., Schmidt, L., and Shankar, V. Do ImageNet classifiers generalize to ImageNet? In Chaudhuri, K. and Salakhutdinov, R. (eds.), *Proceedings of the 36th International Conference on Machine Learning*, volume 97 of *Proceedings of Machine Learning Research*, pp. 5389–5400, Long Beach, California, USA, 09–15 Jun 2019. PMLR. URL <http://proceedings.mlr.press/v97/recht19a.html>.
- Ribeiro, M. T., Singh, S., and Guestrin, C. “Why should I trust you”: Explaining the predictions of any classifier. In *Proceedings of the 22Nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1135–1144, 2016. ISBN 978-1-4503-4232-2. doi: 10.1145/2939672.2939778. URL <https://doi.acm.org/10.1145/2939672.2939778>.
- Ribeiro, M. T., Singh, S., and Guestrin, C. Anchors: High-precision model-agnostic explanations. In *AAAI Conference on Artificial Intelligence*, 2018. URL <https://www.aaai.org/ocs/index.php/AAAI/AAAI18/paper/view/16982>.
- Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J.-F., and Dennison, D. Hidden technical debt in machine learning systems. In Cortes, C., Lawrence, N. D., Lee, D. D., Sugiyama, M., and Garnett, R. (eds.),

- Advances in Neural Information Processing Systems* 28, pp. 2503–2511. Curran Associates, Inc., 2015. URL <http://papers.nips.cc/paper/5656-hidden-technical-debt-in-machine-learning-systems.pdf>.
- Smirnov, N. V. Estimate of deviation between empirical distribution functions in two independent samples. *Bulletin Moscow University*, 2(2):3–16, 1939.
- Sundararajan, M., Taly, A., and Yan, Q. Axiomatic attribution for deep networks. In *Proceedings of the 34th International Conference on Machine Learning - Volume 70*, ICML17, pp. 3319–3328. JMLR.org, 2017.
- Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., and Wojna, Z. Rethinking the inception architecture for computer vision. In *2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, June 27-30, 2016*, pp. 2818–2826. IEEE Computer Society, 2016. doi: 10.1109/CVPR.2016.308. URL <https://doi.org/10.1109/CVPR.2016.308>.
- Vacanti, G. and Van Looveren, A. Adversarial detection and correction by matching prediction distributions. *arXiv preprint arXiv:2002.09364*, 2020. URL <https://arxiv.org/abs/2002.09364>.
- Van Looveren, A. and Klaise, J. Interpretable counterfactual explanations guided by prototypes. *arXiv preprint arXiv:1907.02584*, 2019. URL <https://arxiv.org/abs/1907.02584>.
- Van Looveren, A., Vacanti, G., Klaise, J., and Coca, A. Alibi-Detect: Algorithms for outlier and adversarial instance detection, concept drift and metrics., 2020. URL <https://github.com/SeldonIO/alibi-detect>.
- Wachter, S., Mittelstadt, B., and Russell, C. Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard journal of law & technology*, 31:841–887, 04 2018. URL <https://arxiv.org/abs/1711.00399>.
- Wolf, T., Debut, L., Sanh, V., Chaumond, J., Delangue, C., Moi, A., Cistac, P., Rault, T., Louf, R., Funtowicz, M., and Brew, J. Huggingface’s transformers: State-of-the-art natural language processing. *ArXiv*, abs/1910.03771, 2019.
- Zaharia, M., Chen, A., Davidson, A., Ghodsi, A., Hong, S. A., Konwinski, A., Murching, S., Nykodym, T., Ogilvie, P., Parkhe, M., Xie, F., and Zumar, C. Accelerating the machine learning lifecycle with mlflow. *IEEE Data Eng. Bull.*, 41:39–45, 2018.
- Zhao, Y., Nasrullah, Z., and Li, Z. Pyod: A python toolbox for scalable outlier detection. *Journal of Machine Learning Research*, 20(96):1–7, 2019. URL <http://jmlr.org/papers/v20/19-011.html>.