[?????? MLOps ???]

?????? MLOps ???

???Mrinal Chakraborty

MLOps began as a set of best practices, but it has slowly evolved into an independent approach to Machine Learning lifecycle management. It is focused on the lifecycle of model development and aspects of machine learning model operationalization. MLOps seeks to make ML development more reliable by defining the processes of its development and deployment.

The core aspects of MLOps include:

- **Model Lifecycle Management for Scaling Enterprise-grade Adoption** - Similar to the needs for application development processes in traditional “DevOps” methodology, MLOps methodology helps to manage the lifecycle for model development, training, deployment, and operationalization. It's predominantly pivoted to provide consistent processes for moving models from the data science environment to the production environment.
- **Model Versioning & Data Realization** - As models are built, they will most likely be iterated and versioned to deal with the nuances of data and iterative engineering. Machine Learning models that perform well in theory, may change based on new training or real-world data. MLOps can operationalize this whole workflow by providing solutions for different versions of models, supporting multiple versions in operation as needed, provide notification to model

users of version changes, visibility into model version history, and can help make sure that obsolete models are systemically flushed out.

- **Model Monitoring and Management** - Continuous training is done to get the model from 'Sample' data to 'Real' data. MLOps solutions need to monitor and manage model usage while this transitioning of data realization. MLOps traces the consumption and results of models to make sure that their accuracy and performance continue to provide acceptable results. This is much needed for visibility into data and prevent model “drift,” while keeping an eye on various measures of model performance against thresholds and benchmarks.
- **Model Governance** - Models that are used for enterprise consumption needs to be tied to business outcomes. As such, MLOps platforms provide auditing, compliance, governance, and access control through the entire process. This includes features for model and data audit-trails (tracing data changes to model change), model access control, prioritizing model access. Its ensures to provide transparency into how models use data, and any regulatory or compliance needs for model usage.
- **Model Discovery and Parameterization** - While the enterprise matures in advanced MLOps adoption, the MLOps methodology may also provide model registries (and parameterization templates) or catalogs for models produced within the development ecosystem. A searchable intra-enterprise-marketplace can provide a way to locate consumable models, both internally developed as well as third-party models. This capability for model discovery should enable users to ascertain the relevance, quality, data origination, transparency of model generation, and other factors for a particular model.
- **Model Security with Cloud Security Features** - Machine Learning models are the IP that need to be protected as enterprise data-assets. MLOps solutions, borrowing from its cloud-native security features, can provide the functionality to protect models from being corrupted by un-reliable data, DOS (denial of service attacks) and Role-based access.

The MLOps practice is still in its infancy with technology solutions emerging only in the last year or two for the effective implementation of MLOps for enterprise-wide adoption. However, it is predicted that the MLOps market will be over $4 Billion in just a few years, and as such promises to be a major component of the AI solution landscape shortly. Centific can help leverage MLOps to deliver solutions that Data Science and IT Ops teams need to work together to deploy, monitor, manage, and govern ML/AI models in production.

Centific can help global brands get enterprise-grade models into production. With services across the full spectrum of the ML lifecycle, our experienced data scientists and data-engineers help with all the capabilities needed to establish the MLOps practice in your enterprise. This essentially leads to a systematic approach to: build, train, and deploy ML models, then ensure those models continue delivering value — without requiring you to build your own team of ML/AI specialists.

If you would like to learn more how MLOps fits in your organization workflow, feel free to **contact us**. We would love to hear from you.

-
-
-
-
-