Risk Reduction using MLOps

Linus Below Blomkvist

May 2022

1 Introduction

MLOps is a new tool that has only existed for eight years. With every new tool there are always a bunch of questions about it: What is MLOps and how does it differ from the classical DevOps? What are the challenges of MLOps? Are there any know applications of it today? What are the risks involved with machine learning? Can MLOps be used for reducing the risks that comes with machine learning projects?

The purpose of this essay is to answer the leading questions above and thereby providing the reader the knowledge of MLOps and the benefits it has for machine learning projects. The main focus in this essay is about the risk that comes with regular machine learning projects and how MLOps can be used for efficency and risk reduction.

2 MLOps vs DevOps

2.1 MLOps

DevOps is the composition of Development and Operations in order to improve the efficiency of the development and maintenance of a product. So a DevOps team are the ones that coordinates the work in order to improve the workflow and ensure the quality of the product.

MLOps, Machine Learning Operation, has the same purpose as DevOps. It can basically be described as application of DevOps principles and practices to the machine learning work flow where it covers all the steps from data collection to model management, where the goals for MLOps are:

- Faster experimentation and model deployment
- Faster deployment of updated models into production
- Quality assurance

While MLOps and DevOps are similare in their purpose for product development there is one critical differences between DevOps and MLops: deploying software code into production is not the same as deploying a machine learning models into production.

The data that machine learning works with always changes. So a machine learning system constantly needs to change and adapt (hence the name) based on the inputs. The complexity of these constant updates and changes are what makes MLOps all the more necessarry for macine learning project. [5] For that steps like continuous integration, continuous delivery and continuous training are needed. Continuous training is the part where MLOps differs from DevOps since it's not a part of the DevOps system. With continuous training the model always trains in order to adapt to the new data.[8]

So MLOps is the intersection of Machine Learning, DevOps and Dataengineering. In others words, MLOps is DevOps applied for machine learning projects. [6]

3 Risk of Machine Learning projects

For every new tool there involves some kind of risk. However when it comes to machine learning a majority of organizations can't seem to properly identify and handle the risks involving it, according to the global McKinsey survey [3].

With ability for the algorithms to adapt there are chances of it to not always make the ethical and accurate decision. The risk involves everything from input data to security[2]:

1. Data: One of the major risk factors with machine learning is the data. Sometimes the data can be quite poor (so called "dirty data") where, for example, a few more extreme values can alter the average or that data with no structure can't be correctly interpreted by the model. There are also other data-errors like overfitting, where to-good-data doesn't give the algorithm any chance to learn and biased data where human interference's has altered the data and thereby ruined it's outcome. [3]

2. Another risk area that is more of an human error but just as relevant: Defining the Minimal Viable Product (MVP). This is for determining the minimum need for the capability of the machine learning tool to be useful. This is an area for the data scientist to be the bridge between the engineers and the stakeholders.[1]. There are several other humans errors, such as misinterpretation of the output.

3. Another interesting risk factor in machine learning involves the Dynamic model calibration. What this means is that machine learning algorithms

will dynamically modify their parameters to reflect the patterns in the data. However the risk involved in this calibration is that if the model would overemphasis on the short term patterns the long-term performance of the model could be ruined. For that reasoned it is necessary to have control of the dynamic model calibration and many organizations always manually decide when the model is allowed for dynamic recalibration.[7]

4. One risk factor which is relevant for DevOps has to do with production readiness. Machine learning models are algorithmic and require a lots of computation for the production system to be able to support them. But this is an area that is many times overlooked in the development process. As in one example in the article from [7] one US bank spent resources on a project to develop a machine learning model that is able to predict transaction fraud. However when they deployed it they discovered that the model did not meet the required latency standards. So a machine learning engineer needs to have a large scope for several factors like the volume of data and the required runtime.[7]

5. Model degradation. As soon as a machine learning model is deployed it starts to degrade. Not all in the same degree of course. Mostly for models based on time-varying data and static data. What happens when a model starts to degrade is that it interact with real world data and does not have the ability to make any sense of it. It all comes from when failing to predict how the data is going to change over time.
   All of this stems from a phenomenon called concept drift. Which means that the accuracy of a machine learning model is at it's best until it starts being used. What it basically means is that statistical properties that the model is trying to predict changes over time in unforeseen ways. This will of course cause problems since the predictions will be less accurate over time. [4] Many of these sorts of failures occur when the model only is able to see patterns in data that is very similar to the training data

4 Usage of MLOps today

Nowadays MLOps is used to produce machine learning model and includes several steps in their cycle:

- Model Lifecycle management: In the process the MLOps tools are required of management of model deployment, deployment training and mode of operation.
- Model versions and Variations: Today MLOps also works with providing data models from the development environment to the users. By sending notifications and alerts to the users they get an update of the new version of their tool
- Model Monitoring

5 Cons of MLOps

One of the cons of introducing MLOps could possibly be the short term cost. MLOps is a tool that also requires a higher skill in engineering and data science since it's a combination of DevOps, machine learning and computer science.

However the major coon for this has more to do with the risk of human error. If MLOps have been implemented incorrectly the amount of tools and skills needed could be overwhelming. For that reasons the demands are high for an experienced MLOps architect.

Another con of MLOps, which is more a human factor, is that many businesses are skeptical towards replacing huamans in some working areas with only automated machine learning models. Because for many people the model is more of a "black box" rather then a program. It takes quite a high level of knowledge to understand how it works.

Another challenge for MLOps is the assessment and consideration of model risks that occur when a machine learning model is implemented. One famous incident that is a useful example for this kind of challenge is the blue-or-white dress. Which shows that if even humans cannot provide an answer with absolute certainty then there must be room for an artificial intelligence to also make mistakes.[12]

6 Risk reduction and time effiency with MLOps

There are several risks involed when implementing artificial intelligence and machine learning since these are algorithms that are not only programmed by humans. The main purpose of machine learning is to detect patterns in the future by algorithms that learns from previous data. The problem with this method is that how these pattern detections are made are sometime unknown. In one survey from 2020 36% of the participants said that data scientist spend up to 25% of their work time deploying machine learning models [9]. This is an area where MLOps can speed up the process and help deploying machine learning models more efficiently.

The main purpose behind MLOps is to give support to the development of machine learning project by setting standards and tools for each stage of the project. Some of these techniques includes: CI/CD, hyperprameters, testing of data and models and infrastructures and model development and production monitoring.[11].
By setting these standard and tools for each stage of the development process there will be significant reduction in time and cost.

There are several areas where MLOps could be applied for risk reduction.

In the regular machine learning development the lifecycle goes in the following order:
Data ingestion and wrangling → Model engineering → Model Deployment → Periodical audit → Data ingestion and wrangling

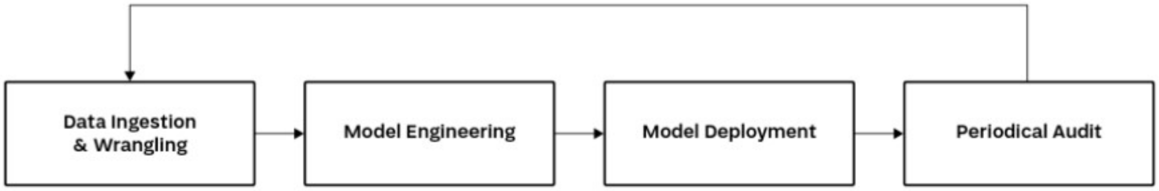

Figure 1: Figure from article [9]

One risk in this development process is lack of tools to deal with boundary situations. For example: implementing solutions for model registry to be able to restore the system in the event of a bug or a failure. It is also common in projects for repetitive task to be done manually instead of being replaced with automation.

These staged can be expanded and improved in efficiency with MLOps as it implements continuous integration to validate the models and data, continuous deployment to update the operating website on the latest model, continuous monitoring to secure the quality of the system and continuous training to allow the model to be able to retract to earlier stage if necessary. [9]

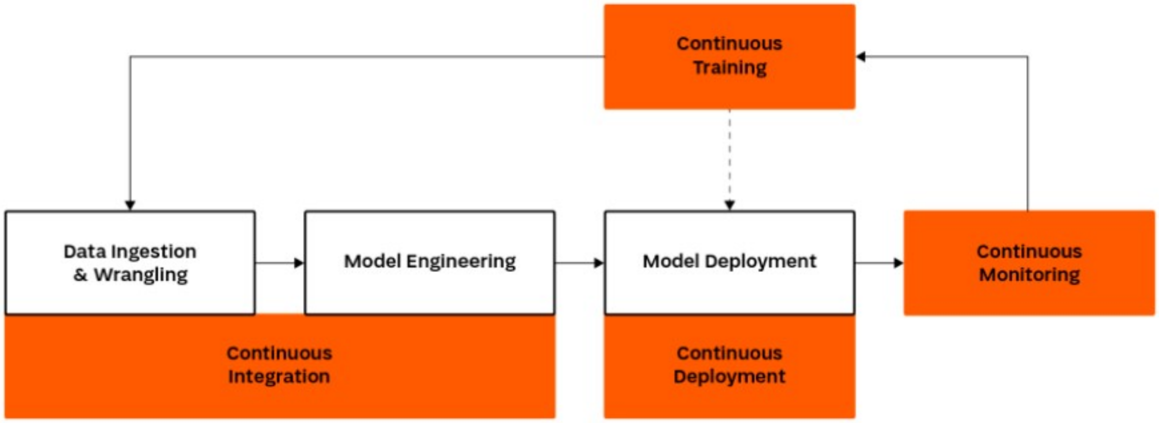

Figure 2: Figure from article [9]

The biggest change with the continuous integration is at the model deployment stage. Developer nowadays can use platforms as MLflow, which is an open-source platform for handling the machine learning lifecycle, to allow experimentation, test different versions and deployment. Another platform is one called Kubeflow, which is also an open-source platform meant for simplifying the development and deployment of machine learning systems.
These and other platsforms offers several benefits when deploying machine learning models such as: reproducing experiments with versioning of data, monitoring the project thru its work history and sharing of the trained models. [9]

The last stage in the machine learning life cycle is the monitoring of the production version of the model. With MLOps tools can be used to analyze the quality in real-time instead of having to do cyclical auditing.
One benefit with this is that it makes it possible to avoid the risk of system errors and identify the moments when predictions made by the model does not comply with the standards set by the developers. Which thereby means that it is time to update and train the next version of the model.
So all of this can be set with the continuous training mechanism that will automatically train and build new models from the new data and then set it's deployment in it's production environment.[9] So these parts show how MLOps so far can be used to improve the implementation of machine learning systems.[10]

Another area where MLOps is a solution is the risk for model degradation. For those type of risks it is necessary to monitor the machine learning models. Monitoring machine learning models is a bit different from monitoring regulars website but both use Application Performance Management (APM) principles. With the usage of APMs the following metrics are examined: error occurrence, response time, hardware resources and availability of the application.
When applying it to machine learning models it is necessary to extend it's scope to further elements: analyze the distribution of input feature and the predictions that are made to detect data drift, monitoring statistical values and automatic alerts in the case of the results exceed the anticipated domain. [10]
This part cover how the usage of monitoring machine learning systems proactively can be used to get a better control of the deliverance of the product.

In most cases machine learning is used more as an optimization tool then a tool for a part of the development for new services and products. According to the IDC (International Data Corporation) 88% of all AI and machine learning projects fail during the test phase. With the implementation of MLOps for these projects MLOps can offer support for the planning and implementation phase.

The cause of this huge failure rate has much to do with that companies don't take the time to analyze and get a clear picture of how a machine learning project is to be implemented and thereby accidentally oversee the complexity

of an ML-project.
So the key strength for MLOps in this area is that is can automate the modelling process of an machine learning project. So by using MLOps companies can integrate machine learning more efficiently into their processes.

One other area which we mentioned earlier is the deployment phase. With the usage of MLOps model deployment can be made by other teams than the data scientist, since the users of the MLOps system doesn't need any knowledge about the technology behind the model when inserting it in the system.[12]

7 Reflection

Thru the writing of this essay it can be quite easy to become overconfident in the new area of MLOps when you should always be a bit careful when it comes to new methods for technology that itself is fairly new. MLOps first came in 2015 and most of the sources that you find about it is from the last 4 years. While it is exciting to learn how a innovating and exciting area like machine learning can be more efficiently developed and deployed, it is legit to be skeptical of having artificial intelligence automate process that humans normally do like the model degradation as mentioned earlier. However this essay has presented how MLOps can be used and is meant for increasing the efficiency for the model development and risk reduction of the model deployment of machine learning.

One other aspect that is also worth reflecting about is that many of the articles that has been referenced in this essay are from companies who developes MLOps platforms. Which means that they could be biased since they want to more or less present and sell their platform after giving a introduction to general concepts and pros and cons of MLOps. It was quite difficult to find any academic papers about MLOps. There are plenty of academics papers when it comes to machine learning and the risks involved with machine learning. So one other area where it was hard to find any information was risk in machine learning where MLOps could not serve as a solution. However this is a small part of the essay. The core of the essay is about the risk following machine learning projects and how MLOps can be a solution. And all the sources used could offered one aspect about risk or risk reduction using MLOps.

References

[1] Benjamin Cohen. *Three Risks in Building Machine Learning Systems.* https://insights.sei.cmu.edu/blog/three-risks-in-building-machine-learning-systems/. 2020.

[2] Harold Figueroa G. McGraw R. Bonett V Shepardson. *Top 10 Security Risks of ML.* https://ieeexplore.ieee.org/abstract/document/9107290/authors#authors. 2020.

[3] Galvanize. *Understanding the Risks of Machine Learning.* https://www.wegalvanize.com/risk/understanding-the-risks-of-machine-learning/. 2021.

[4] Alexandre Gonfalonieri. *Why Machine Learning Models Degrade In Production.* https://towardsdatascience.com/why-machine-learning-models-degrade-in-production-d0f2108e9214. 2019.

[5] M Treveil N Omont C Stenac K Lefevre D Phan J Zentici A Lavoillotte Ma Miyazaki L Heidmann. *Introducing MLOps.* https://www.oreilly.com/library/view/introducing-mlops/9781492083283/. 2020.

[6] Safwan Islam. *MLOps vs. DevOps: What is the Difference?* https://www.phdata.io/blog/mlops-vs-devops-whats-the-difference/. 2022.

[7] Bernhard Babel Kevin Buehler Adam Pivonka. *Derisking machine learning and artificial intelligence.* https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/derisking-machine-learning-and-artificial-intelligence. 2019.

[8] Gaurav Sharma. *MLOps vs DevOps: Let's Understand the Differences?* https://www.analyticsvidhya.com/blog/2022/01/mlops-vs-devops-lets-understand-the-differences/. 2022.

[9] Mateusz Szczesny. *How Does MLOps Support Building of ML Models?* https://billennium.com/blog/how-does-mlops-support-building-of-ml-systems/. 2021.

[10] Mateusz Szczesny. *Monitoring ML models using MLOps.* https://billennium.com/blog/monitoring-ml-models-using-mlops/. 2021.

[11] Mateusz Szczesny. *Risk in ML Projects. Is MLOps the Solution?* https://billennium.com/blog/risk-in-ml-projects/. 2021.

[12] Sofiia V. *MLOps Benefits That Make it an Upcoming Industry Trend.* https://geniusee.com/single-blog/mlops-practices-and-its-benefits. 2020.