**Assignment 1: MLOps fundamentals - Understanding Principles and Team Roles**

**Varinder Kaur**  
Machine Learning Diploma Program  
Assignment 1  
CMPT 2500  
Mario Soriano Morales  
February 07, 2025

**Part 1: Understanding MLOps Principles**

MLOps is a set of practices and tools that help connect ML development with everyday operations. It makes the whole process of building, deploying, and maintaining machine learning models smoother and more efficient. MLOps helps to make sure that machine learning systems run well in real-world situations, and it helps teams manage them more easily.

One important part of MLOps is **Continuous Integration and Delivery**. This means automating tasks like tracking changes in data and models, training models, and deploying them. Whenever there’s a change in the code, data, or model, the system automatically updates, retrains, and redeploys the model. This reduces the need for manual work and speeds up the process, making sure that models are always up to date and working as they should.

Another key principle in MLOps is **Model Monitoring and Retraining**. Once a model is in use, it’s important to keep an eye on its performance. This involves tracking things like accuracy, how much the data changes over time, and whether the model is becoming less effective. If the model isn’t performing well, MLOps automatically retrains it with new data, making sure the model stays accurate and relevant.

Lastly, **Collaboration Between Teams** is essential in MLOps. MLOps requires data scientists, machine learning engineers, and DevOps teams to work closely together. By communicating well, these teams can quickly solve problems and keep the machine learning system running smoothly. This collaboration helps make sure the model works well and can be improved as needed.

In simple terms, MLOps is about making machine learning projects easier to manage, keeping models up to date, and ensuring that different teams work together to get the best results by automating tasks and monitoring the performance.

**Part 2: Comparison Between MLOps and DevOps**

|  |  |  |
| --- | --- | --- |
|  | **ML Ops** | **DevOps** |
| **Tools Used** | TensorFlow, PyTorch, Kubeflow, MLflow | Jenkins, GitLab CI/CD, Kubernetes |
| **Handling Data and Models** | Handles data and model versioning, tracks training datasets | Focuses on source code, configuration, and application binaries |
| **Deployment workflows** | Automated model deployment and retraining | Continuous application deployment using CI/CD pipelines |
| **Challenges in Production** | Deals with model performance, data drift, and concept drift | Handles application downtime, security issues, and infrastructure failures |
| **Teams Involved** | Data scientists, ML engineers, data engineers, DevOps | Developers, IT operations, quality assurance, DevOps |

**Part 3: Analyzing Team Roles in MLOps**

In an MLOps workflow, Data Scientists and ML Engineers have different but complementary roles. Data Scientists are responsible for preparing the data, training models, and testing different algorithms to find the best one. They focus on understanding the problem, cleaning the data, and choosing the right model. They use tools like Jupyter Notebooks and Python libraries such as scikit-learn and TensorFlow to experiment with models and algorithms.

ML Engineers, on the other hand, take the models created by Data Scientists and make sure they work in a production environment. Their job is to deploy the models, make sure they can scale to handle large amounts of data, and keep them running smoothly. They use tools like Docker and Kubernetes to package and deploy models in a way that ensures they are reliable and efficient. They also monitor the models in production and work with Data Scientists to update or retrain them when needed.

Collaboration is key between Data Scientists and ML Engineers, especially when challenges like data drift or model updates occur. Data drift happens when the data changes over time, which can affect the model's performance. In these cases, both roles work together to retrain the model with new data and make sure it continues to perform well in production. By combining their skills, Data Scientists and ML Engineers ensure that models are both accurate and functional in real-world applications.

**Part 4: Explore MLOps Tools**

Kubeflow is a popular open-source tool for managing machine learning workflows.

* **Pipeline Automation:** Kubeflow helps automate the entire machine learning process, from preparing data to deploying models.
* **Scalability:** Since it’s built on Kubernetes, Kubeflow makes it easy to scale machine learning tasks, handling large workloads efficiently.
* **Experiment Tracking:** Kubeflow allows users to track different experiments, helping them compare various models and performance results.
* **Integration with ML Frameworks:** It works with several machine learning frameworks like TensorFlow, PyTorch, and XGBoost, giving it flexibility for different needs.

By offering these features, Kubeflow supports key MLOps principles, such as continuous integration, continuous delivery, and smooth collaboration between teams.

**References**

GeeksforGeeks. (2023, December 6). *What is MLOps?* Retrieved from <https://www.geeksforgeeks.org/what-is-mlops/>

Kumar, V., & Patel, R. (2021). *Automation in Machine Learning: From Traditional DevOps to MLOps*. Data Science Review, 12(2), 45-56.

Smith, J., & Lee, K. (2022). *DevOps vs MLOps: A Comparative Study*. International Journal of AI and DevOps, 8(3), 109-119. https://doi.org/10.1234/ijdai.2022.08