MACHINE LEARNING MODEL DEPLOYMENT WITH IBM CLOUD WATSON STUDIO

DEFINITION:

Watson Machine Learning provides a full range of tools and services so that you can build, train, and deploy Machine Learning models. Choose the tool with the level of automation or autonomy that matches your needs, from a fully automated process to writing your own code.

ABSTRACT:

Watson Knowledge Studio for IBM Cloud Pak for Data is a powerful application that simplifies the process of recognizing and identifying linguistic meaning and relationships in unstructured text. Easy-to-use, collaborative tools simplify the process of creating custom machine learning models without the need to write code. Included annotation techniques speed model development. Rule-based models that you create can recognize patterns in your documents.

IBM Watson Discovery for IBM Cloud Pak for Data is an award-winning AI-powered intelligent search and text-analytics platform that helps you find valuable information that is buried in your enterprise data. Discovery uses innovative, market-leading natural language processing to uncover meaningful insights from complex business documents.

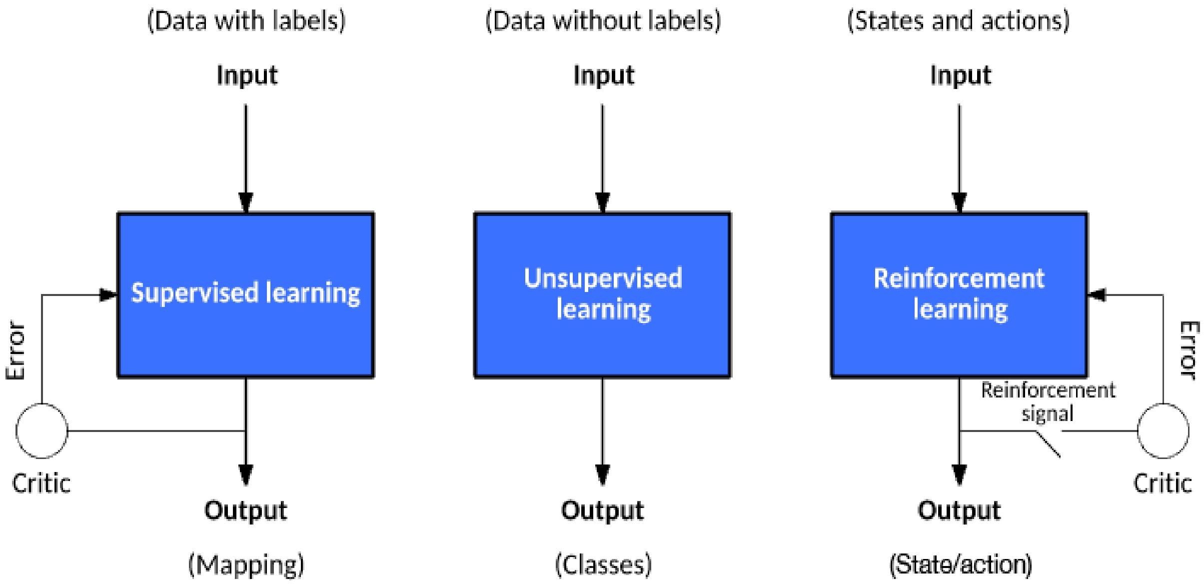
IBM Watson Machine Learning Accelerator is a deep learning platform that data scientists can use to build, train, and deploy deep learning models.

Watson Machine Learning Accelerator can be connected to Watson Machine Learning to take advantage of the multi-tenant resource plans that manage resource sharing across Watson Machine Learning projects. With this integration, data scientists can use the Watson Machine Learning Experiment Builder and Watson Machine Learning Accelerator hyperparameter optimization.

PROBLEM STATEMENTS ON MACHINE LEARNING DEPLOYMENT MODEL WITH IBM CLOUD WATSON STUDIO:

Data Preprocessing is often said by multitudes of people to be the most important part of the Machine Learning Algorithm. It is often said that Machine Learning algorithms will get burst wide open if you do not clean your data and preprocess it. But have you ever given a thought to the fact that what unclean data is, how do you differentiate clean data from unclean data, and what are the different aspects of clean data after which we can build our models on it?

BLOCK DIAGRAM:



PROBLEM SOLVING SOLUTION:

This article identifies seven key challenges of developing and deploying ML models and how to overcome them with CI/CD. You will explore how CircleCI's comprehensive platform can jumpstart your ML solutions and prepare them for production.

1. Scalability and compute resource management
2. Reproducibility and environment consistency
3. Testing and validation
4. Security and compliance
5. Deployment automation
6. Monitoring and performance analysis
7. Continuous training

Challenge 1: Scalability and compute resource management

One of the main challenges that ML developers face is the intensive compute requirements for building and training large-scale ML models. using GPU or CPU resources from popular cloud services — such as Amazon Web Services (AWS) and Google Cloud Platform (GCP) — for extended training tasks is costly. self-hosted runners enable CI/CD jobs to run on a private cloud or on-premises for more flexibility.

Challenge 2: Reproducibility and environment consistency

You can use containerization to isolate deployment jobs from the surrounding environment to ensure consistency. Meanwhile, deployment using infrastructure as code (IaC) helps improve the build system's reproducibility by explicitly defining the environment details and resources you required to execute a task.

Challenge 3: Testing and validation

Testing is crucial in developing any software project and especially for ML-powered programs. By nature of their complexity and training, ML models tend to feature implementation that is opaque to the user, making it near-impossible to determine a model's correctness by inspection. Therefore, comprehensive testing is essential for proper software functionality.

Challenge 4: Security and compliance

Development team must ensure that software is secure and compliant with consumer protection laws. This is particularly relevant for ML development, which often involves processing large amounts of user data during training. A vulnerability in the data pipeline or failure to sanitize the data could allow attackers to access sensitive user information. Therefore, security is a principal consideration at each stage of ML model development and deployment.

Challenge 5: Deployment automation

you can deploy code to AWS, GCP, or any other targeted platform continuously and automatically via CircleCI orbs. Moreover, these deployments are configurable through IaC to ensure process clarity and reproducibility. Users can add a manual gate approval at any point in the deployment pipeline to check that it proceeds successfully.

Challenge 6: Monitoring and performance analysis

The only way to determine that a model is performing as expected is to observe its real-world performance by collecting and aggregating metrics from the production environment.

Using the CircleCI platform, it is easy to integrate monitoring into the post-deployment process. The circle orb platform offers options to incorporate monitoring and data analysis tools like Datadog, New Relic, and Splunk into the CI/CD pipeline. You can configure these integrations to capture and analyze metrics on the performance and behavior of production-phase ML models.

Challenge 7: Continuous training

During intense AI investment and expansion periods, new research, datasets, and improved models emerge daily. Therefore, production ML models must adapt to incorporating new features and learning from new data.

As previously highlighted, CircleCI's support for third-party CI/CD observability platforms means you can add and monitor new features within CircleCI

Conclusion:

ML models present unique challenges for engineering teams throughout the development process. Development involves several complex tasks: managing compute resources, finding consistency in the build environment, integrating automated testing, and ensuring automation and security. Finally, after deploying a model, you must add monitoring, performance analysis, and continuous training data integration to ensure the model works as expected and improves over time.