Deployment Automation with MLOps Practices & Ethical Deployment

AI Masters Capstone Project - Presentation 4

Jonathan Agustin

November 2024

What We'll Cover Today

- CI/CD pipeline integration for streamlined updates
- Infrastructure automation with Terraform, Docker, and AWS
- Ethical deployment: security, compliance, SBOMs, privacy considerations
- A holistic MLOps approach linking all pipeline stages

From code to customers, we'll ensure ethical, secure, and scalable model delivery.

CI/CD Pipeline Integration

- Automate code integration, testing, and deployment with GitHub Actions
- Trigger pipelines on commits or pull requests, ensuring continuous feedback
- Rapid, reliable releases that keep models current and aligned with ethical standards

CI/CD brings agility and trustworthiness, reducing risk and manual effort.

Infrastructure Automation

- Use Terraform for Infrastructure as Code: reproducible, version-controlled setups
- Docker for containerization: consistent runtime environments
- AWS integration: scalable, secure cloud deployments with minimal friction

Infrastructure automation ensures stable foundations for reliable and ethical ML services.

Ethical Deployment: Security & Compliance

- Automated security scans identify vulnerabilities early
- SBOM creation ensures transparency of all components & dependencies
- Compliance checks enforce privacy laws (e.g., GDPR) and industry regulations

Ethical deployment safeguards trust, protects user rights, and prevents damaging missteps.

A Holistic MLOps Strategy

- Continuous monitoring: track model drift, fairness shifts, and performance drops
- Incremental updates: roll out changes gradually, gathering feedback safely
- Comprehensive documentation and audits: maintain transparency, accountability

MLOps weaves ethics into the fabric of operations, ensuring long-term trust and value.

Next Steps

- Next Presentation: Code Quality, Security & Ethical Implications in ML Development
- Strengthening the final layer of assurance and responsibility

With our pipeline set, let's refine quality, security, and ethical codes for truly responsible AI.

Temporary page!

LaTeX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, becau LaTeX now knows how many pages to expect for this document.