LLMOps For ECommerce

20th June 2024

Who am I?



Officially

18+ years of industry experience in tech and product roles across The US, Africa, South-East Asia, and Europe with organizations such as Booking.com, AppsFlyer, GoJek, Rocket Internet, and National Instruments. Currently Director-Big Data & ML/AI with Booking.com

Un-Officially

Amateur Chess (ELO 2241) and Go (4kyu) player, reach out if you want to discuss either :)

Terminology

ARTIFICIAL INTELLIGENCE A program that can sense, reason,

act, and adapt

MACHINE LEARNING

Algorithms whose performance improve as they are exposed to more data over time

DEEP Learning

Subset of machine learning in which multilayered neural networks learn from vast amounts of data

*Algorithms *Machine Learning *Maths What the hell is this? Ange

FMOps??LLMOps??





Typical MOps Flow

Model Training



Feedback Loop

Typical MOps Flow

Model Serving



Feedback Loop

With LLMs, What has Changed?

Model Training



Feedback Loop Reinforced

With LLMs, What has Changed?

Model Serving



Feedback Loop Reinforced

Layer Breakdown

Let's Take Each Layer one by one and Discuss

- 1. What each Layer does?
- 2. Complexity of each layer before and after Large Models
- 3. Opportunities and Product Lens on each Layer before and after the advent of GenAl

LLMOps-Data Layer



Bedrock of any ML ecosystem is its data ecosystem for training data. The data ecosystem should be robust, with well-labelled, well-lineaged data, allowing for proper tracking of results generated by our ML models (you cannot measure, what you cannot track !!)

 The layer has many nuances, and depths with evolution to Data lakes, Data Fabrics vs Mesh, etc.

- 2. A lot of VC investment has always targeted "Big Data"
- In a typical Non-LLM world, most of the data in the lake has been "structured"

What Changes with LLMs?

With an LLM ecosystem, the data layer interaction is no longer limited to only structured data, but extends to unstructured and semi-structured data (direct chat interactions, images uploaded, etc.) bringing additional complexity

LLMOps-Model Building/Training



Model Training/Building is the assembly line for ML user to create models. The MOps ecosystem enables the tooling for Multi-modal deployments with various model-building formats supported (LightGBM, Tensorflow, etc.)

- The layer interfaces with the data ecosystem, and has newer and more optimised formats come up regularly
- 2. A lot of VC investment has always targeted Model Building
- In a typical Non-LLM world, model training is a "middleware" to building tools

What Changes with LLM?

Building a model is out of scope for now, but serving publicly available models via an enterprise wrapper is a possibility. A wrapper/middleware addition could be envisaged here

LLMOps-Model Serving Layer





Model-Serving is the production line of the platform. Wherein multi-modal serving is deployed on specialized hardware (CPU/GPU/XPUs, etc.)

- 1. The layer is highly extensible, and requires scaleup engineering for scaling number of models
- 2. A lot of VC investment and optimizations go into both the software as well as hardware side of this ecosystem
- In a typical Non-LLM world, most of the usecases used to be enough for 1 GPU, not anymore

What Changes with LLM?

For LLMs, singular GPUs are not enough (mostly), reinforcement of this team for Distributed GPU Training needs to be thought off. Additionally a lot of investment has gone into the custom hardware space for this (Trainium, XPUs, etc.)

LLMOps-Feature Engineering Layer

Feature Engineeri ng

Embedding Management

Feature Engineering is an encompassing term for both the feature compute as well as feature discoverability part of the platform (Discuss What is a Feature or ML asset)

- 1. The standard evolution of this ecosystem has been a Feature Store–both offline and online serving
- 2. A lot of VC investment and optimizations go into both the software as well as hardware side of this ecosystem
- 3. In a typical Non-LLM world, most of the use-cases used to be scaler

What Changes with LLM?

Whilst uptil now, Online and Offline feature serving was needed, Vector Store and Prompt-Store use-cases (with embeddings) will crop up as we go along as well

LLMOps-ML Governance Layer

Governance

ML governance is a regulatory part of the ML ecosystem, which has become increasingly more important in the active- regulation ecosystem (EU AI Act, DAC7, eprivacy, DSA/DMA, etc.)

- 1. MOps ecosystem needs to build tooling to adhere to these regulations
- A lot of solution providers have come forth, building E2E solutions in their MLOps chains (acquired or self-built) to incorporate compliance flows

What Changes with LLM?

With LLMs, increased scrutiny on Data and ML systems has come into place, requiting renewed focus. Some example of investment areas are model versioning, model drift, data versioning, etc.

LLMOps-ML Observability Layer



ML observability demarcates the 30k feet view of your pipelines in an increasingly complex ML ecosystem

- MOps ecosystem, with increased complexity, has renewed interest in specific observability tools (sitting on top of the system observability tools)
- 2. A lot of VC funding has been attracted into these areas with vendors such as Arize, Aporia, Whylabs, etc.
- 3. With Advent of LLMs, this layer has gained particular significance

What Changes with LLM?

LLMs being non-deterministic, Output moderation as well guard-railing has come up as a renewed focus for MOps ecosystem

LLMOps-ML Experimentation Layer



ML Experimentation, both with the models, as well as with different models is an important part of the ML ecosystem

- Multi-model deployment as well as multi-hypothesis deployment has been the bread and butter for the industry
- Multiple tools in the industry allow tracking of said models already (W&B, amongst others)

What Changes with LLM?

This layer has gained renewed focus as well, especially with prompt-experimentation, and multi-model experimentation added into the mix

LLMOps-Feedback Loop

Feedback loops is feedback collection mechanism from an in-situ model to improve the model's performance. Such a flow is used for multiple purposes in the ML ecosystem

Feedback Loop

- 1. Label Collection, knowledge reinforcement are common usecases
- 2. Multiple tools in the industry allow this flow to be perpetuated
- 3. With Advent of LLMs, this layer has gained particular significance

What Changes with LLM?

This layer has gained pivotal focus with Reinforcement Learning gaining a lot of traction in the ecosystem

LLMOps-Model Evaluation and Optimization

Model Evaluation had been a subcomponent of ML experimentation, as

Model-as-a-Service was never a thing, also optimization was something only big organizations invested in !!

What Changes with LLM?

Model Evaluation

Advent of new product capabilities in Model Evaluation (Open-sourced as well as closed) for evaluation against toxicity, bias, any 3rd party parameter (Sagemaker Clarify, say). Optimization is another area that has popped up with cost and compute required for LLMs (Nemo Microservices and Toolkit by Nvidia, say)

Additional Paradigms: SLMs and Frugal AI

What More? SLMs now?

Discuss hyper-focused SLMs who can far outstrip frontier models \rightarrow How would MLOps ecosystem work for a model on a mobile, say? Gemini Nano, Phi Models, OpenAI in the future

Cost Matrices	Way of Optimization
Hardware	CPU deployments instead of GPUs, custom hardware such as Groq, Inferentia, Trillium, etc.
Software	Deployment and cost-optimization so the best out of hardware (NeMO microservices, etc.)
Use-case Market	In essence, not everyone needs to solve for the big market, Mobile market inherently relies on SLMs

Are we Done?

