MLOps Ölüyor !

Caner ŞEKERCİ

MLOps Evriliyor

MLOps (Machine Learning Operations):

- Geleneksel makine öğrenimi modellerinin üretime alınması ve izlenmesi süreçlerinde kritik bir role sahiptir. Örneğin, sahtekarlık tespit sistemleri gibi uygulamalarda yaygın olarak kullanılır.
- Ancak, karmaşıklığın artmasıyla birlikte evrilmesi gerekmiştir.

LLMOps (Large Language Model Operations):

- GPT-4 gibi büyük dil modellerinin yönetimine odaklanır.
- **Odak noktaları:** Prompt mühendisliği, RAG (Retrieval-Augmented Generation) boru hatları, etik uygunluk.
- Daha geniş ölçekli veri işleme gereksinimleri ve insan girdisini optimize etmek için yeni yöntemler gerektirir.

AgentOps (AI Agent Operations):

- Otonom yapay zeka ajanlarının karmaşık görevleri insan müdahalesi olmadan gerçekleştirmesini sağlar.
- **Örnekler:** Müşteri hizmetleri botları, iş akışı otomasyonu.
- MLOps'un bir ileri seviyesi olarak düşünülmektedir.

AI Agent: Kurumsal AI Geleceği

1. **Benimsenme Oranları:**
    - %51 oranında şirketin hali hazırda yapay zeka ajanlarını üretimde kullandığını, %78'inin ise kısa sürede kullanmayı planladığını belirterek, bu teknolojinin hızla yaygınlaştığını vurgulayabilirsiniz.
    - Bu veri, dinleyicinin dikkatini çekmek ve konunun güncel olduğunu göstermek için harika bir başlangıç.
2. **Kilit Kullanım Alanları:**
    - **Müşteri Hizmetleri:** CRM entegrasyonu ile çalışan otonom ajanlar müşteri sorularını çözmede hız ve doğruluk sağlıyor (ör. Salesforce Einstein Copilot).
    - **İş Akışı Otomasyonu:** İnsan kaynakları oryantasyonu, şifre sıfırlama gibi rutin görevlerde etkili.
    - **Kod Üretimi:** GitHub Copilot ve Replit gibi araçlar, gerçek zamanlı kodlama yardımı sunarak yazılım geliştirme sürecini hızlandırıyor.
    - **API'ler ve Erişim Kolaylığı:** OpenAI, Anthropic ve Google Gemini gibi platformlar, altyapı gereksinimlerini azaltarak daha hızlı yapay zeka uygulama dağıtımını mümkün kılıyor.

Modern MLOps'un Üç Temel Direği

Scalable Infrastructure (Ölçeklenebilir Altyapı):

- **Nedir?**: Sunucusuz mimariler (ör. AWS Lambda) ve dağıtık çerçeveler (ör. Ray), kaynak tüketimi yüksek LLM'lerin (Large Language Models) verimli çalışmasını sağlar.
- **Örnek:** Şirketlerin, veri talebine göre kapasiteyi artırıp azaltmasını sağlayarak maliyet etkin çözümler sunar.
- **Vurgu:** Yapay zeka modellerinin büyük veriyle başa çıkabilmesi için optimize edilmiş altyapılar zorunludur.

Monitoring & Safety (İzleme ve Güvenlik):

- **Araçlar:**
  - *NannyML*: Model drift (modelin zamanla doğruluğunu yitirmesi) tespiti.
  - *LIME/SHAP*: Yapay zeka ajanlarının kararlarını şeffaflaştırmak ve açıklanabilirlik sağlamak için kullanılır.
- **Örnek Kullanım:** Bir müşteri hizmetleri botu, yanlış bilgi yaymaya başladığında erken uyarı sistemleri devreye girer.

Ethical Compliance (Etik Uygunluk):

- **Nedir?**: Yapay zeka önyargılarını azaltma (ör. RLHF - Reinforcement Learning from Human Feedback) ve içerik filtreleme (ör. OpenAI Moderation API).
- **Düzenlemelere Uyum:** GDPR gibi yasal düzenlemelere uyum sağlama.
- **Örnek:** LangChain'in anketi, firmaların %45'inin doğruluk ve güvenliği önceliklendirdiğini gösteriyor.

AgentOps Döneminde Karşılaşılan Zorluklar

Performance Uncertainty (Performans Belirsizliği):

- **Nedir?**: Takımların %41'i, yapay zeka ajanlarının öngörülemeyen çıktılar üretmesini en büyük engel olarak görüyor.
- **Etkisi:** Bu durum, ölçeklenebilirlik önünde büyük bir bariyer oluşturuyor ve işletme süreçlerinin güvenilirliğini riske atıyor.
- **Örnek:** Öngörülemeyen bir chatbot'un müşteri ilişkilerinde yanlış bilgi vermesi gibi.

Integration Complexity (Entegrasyon Karmaşıklığı):

- **Sorun:** Farklı araçların parçalı yapısı ve yeniden kullanılabilir boru hatlarının eksikliği, uygulamaları yavaşlatıyor.
- **Örnek:** Bir şirket, AI ajanını CRM ve ERP sistemlerine bağlamada ciddi gecikmelerle karşılaşabilir.

Human-AI Collaboration (İnsan-Yapay Zeka İşbirliği):

- **Nedir?**: Yüksek riskli görevler (ör. finansal işlemler) için hâlâ insan gözetimine ihtiyaç duyuluyor.
- **Etkisi:** Bu durum, tam otomasyonun sağlanmasını zorlaştırıyor ve hibrit iş akışlarına olan ihtiyacı artırıyor.

Solution (Çözüm): Hybrid Workflows (Hibrit İş Akışları):

- **Örnek:** İnsanların devrede olduğu süreçler (human-in-the-loop) ile otonom sistemler arasında denge sağlanabilir.
- **Etkisi:** Hem kontrol hem de otonomi sağlanarak süreçlerin güvenilirliği artırılabilir.

2025 ve Sonrası: Ajan Merkezli Yapay Zeka Ekosistemi

Multi-Agent Systems (Çoklu Ajan Sistemleri):

- **Nedir?**: Birden fazla yapay zeka ajanının işbirliği içinde çalışarak görevleri çözmesi (ör. tedarik zinciri optimizasyonu).
- **Örnek:** Amazon'un tedarik zinciri lojistiğinde birden fazla yapay zeka modülünü kullanması.
- **Etkisi:** Karmaşık sistemlerin daha koordineli ve verimli çalışmasını sağlar.

Domain-Specialized LLMs (Alanlara Özgü Büyük Dil Modelleri):

- **Nedir?**: Sağlık (Med-PaLM 2), hukuk (ChatLAW) ve finans (BloombergGPT) gibi özel alanlara odaklanan modeller.
- **Avantaj:** Halüsinasyon (yanlış bilgi üretme) oranını düşürür.
- **Etkisi:** Endüstrilere özel, yüksek doğruluklu sonuçlar sunar.

Self-Improving Agents (Kendi Kendini Geliştiren Ajanlar):

- **Nedir?**: Google'ın sentetik veri teknikleriyle büyük dil modellerinin kendi eğitim boru hatlarını iyileştirmesi.
- **Etkisi:** Daha hızlı öğrenme ve performans artışı sağlar.
- **Örnek:** Bir yapay zeka, kullanıcı geri bildirimlerinden öğrenerek yanıtlarını daha da geliştirir.

Ethical AI Frameworks (Etik Yapay Zeka Çerçeveleri):

- **Nedir?**: Microsoft'un sorumlu yapay zeka standartları ve Anthropic'in Claude gibi etik standartları belirleyen framework'leri.
- **Etkisi:** Ajanların güvenli ve sorumlu bir şekilde dağıtılmasını sağlar.
- **Örnek:** GDPR ve benzeri düzenlemelere uygun içerik filtreleme.

Teoriden Gerçeğe: AI Ajanları ile Şirketler Nasıl Kazanıyor?

Healthcare (Sağlık):

- **Örnek:** Mayo Clinic'in yapay zeka ajanı, hasta geçmişlerini analiz ederek teşhis hatalarını %30 oranında azaltıyor.
- **Etkisi:** Daha doğru teşhisler, hasta güvenliğini artırır ve sağlık sisteminin maliyetlerini düşürür.
- **Vurgu:** LLM destekli sağlık çözümleri, tıbbi verilerin hızlı ve doğru şekilde analiz edilmesini sağlar.

Retail (Perakende):

- **Örnek:** Walmart'ın tedarik zinciri yapay zeka ajanı, olası aksaklıkları %95 doğrulukla tahmin ediyor ve GPT-4 API'ları ile MLOps boru hatlarını kullanıyor.
- **Etkisi:** Stok yönetiminde verimlilik ve müşteri memnuniyetinde artış sağlıyor.
- **Vurgu:** AI, tedarik zinciri yönetimini optimize ederek büyük maliyet tasarrufu sağlar.

Finance (Finans):

- **Örnek:** JPMorgan'ın COiN ajanı, yılda 12 milyondan fazla belge incelemesini otomatikleştirerek işlem süresini %90 oranında azaltıyor.
- **Etkisi:** Hukuki belgelerin işlenmesinde hız ve doğruluk sağlar.
- **Vurgu:** Otomasyon, finans sektöründe yüksek hacimli işlemleri hızlı ve hatasız şekilde yönetir.

Build vs. Buy: Yapay Zeka Devrimini Güçlendiren Araçlar

Open Source (Açık Kaynak):

- **LangChain:** Çok adımlı ajan iş akışlarını düzenler ve LLM entegrasyonlarını optimize eder.
  - **Örnek Kullanım:** Farklı görevleri sırayla çözen bir chatbot iş akışı tasarımı.
- **MLflow:** LLM sürüm kontrolü ve prompt takibi gibi modern özellikleri destekler.
  - **Örnek Kullanım:** Makine öğrenimi modelleri için uçtan uca izlenebilirlik sağlar.

Proprietary (Ticari/Özel):

- **Databricks Lakehouse AI:** Ajanların ölçeklenebilir bir şekilde dağıtımı için birleşik bir platform sunar.
  - **Avantaj:** Büyük ölçekli projelerde entegrasyon kolaylığı sağlar.
- **AWS Bedrock:** Anthropic, Cohere gibi popüler LLM'lere ve tescilli modellerine erişimi basitleştirir.
  - **Örnek Kullanım:** Bulut tabanlı LLM API'leri ile hızlı prototipleme.

Hibrit Yaklaşım:

- **Vurgu:** Modern AgentOps süreçleri, genellikle açık kaynak araçlar ile ticari bulut API'lerinin bir kombinasyonunu kullanır.
  - **Avantaj:** Esneklik ve maliyet etkinliği sağlar.

MLOps'un Ajan İş Akışlarına Uyumu

Development (Geliştirme):

- **Nedir?**: Prompt mühendisliği ve model özelleştirme (ör. OpenAI Fine-Tuning API).
- **Örnek:** Belirli bir alan için özelleştirilmiş bir dil modeli oluşturma.
- **Etkisi:** Daha yüksek doğruluk ve verimlilik sağlar.

Testing (Test):

- **Nedir?**: LangSmith gibi otomatik değerlendirme çerçeveleri, ajan mantığının doğruluğunu test eder.
- **Örnek:** Bir chatbot'un kullanıcı yanıtlarına verdiği cevapların bağlamını değerlendirme.
- **Etkisi:** Üretime alınmadan önce hataları önleme.

Deployment (Dağıtım):

- **Nedir?**: Kubernetes kümeleri, düşük gecikmeli ve ölçeklenebilir ajan tahmini sağlar.
- **Örnek:** Bir müşteri hizmetleri botunun yüksek trafik altında hızlı yanıt vermesi.
- **Etkisi:** Büyük ölçekli uygulamalarda kararlılık.

Monitoring (İzleme):

- **Nedir?**: WhyLabs gibi araçlar, LLM doğruluğunu ve API maliyetlerini gerçek zamanlı olarak izler.
- **Örnek:** Bir modelin performansının zamanla düşmesini fark etmek ve önlem almak.
- **Etkisi:** Model drift ve maliyet kontrolü sağlar.

Yeni Risklere Karşı Koruma: Veri Sızıntıları, Jailbreakler ve Daha Fazlası

Threats (Tehditler):

1. **Prompt Injection Attacks (Prompt Enjeksiyon Saldırıları):**
   - **Nedir?**: Kötü niyetli kullanıcıların, bir yapay zeka ajanını yanıltarak beklenmedik veya zararlı davranışlar sergilemesine neden olması.
   - **Örnek:** Chatbot'un, özel bir komutla hassas bilgilere erişmeye çalışması.
   - **Etkisi:** Sistem güvenliğini riske atar ve kullanıcı güvenini sarsar.
2. **Sensitive Data Exposure (Hassas Veri Sızıntıları):**
   - **Nedir?**: LLM çıktılarında kişisel tanımlayıcı bilgiler (PII) gibi hassas verilerin yanlışlıkla ifşa edilmesi.
   - **Örnek:** Bir yapay zeka ajanının, istemeden müşteri verilerini dışa aktarması.
   - **Etkisi:** GDPR ve benzeri düzenlemelerle uyumsuzluk ve potansiyel yasal cezalar.

Solutions (Çözümler):

1. **Azure AI Content Safety:**
   - **Nedir?**: Yapay zeka çıktılarında riskleri tarayan bir araç.
   - **Örnek:** Hassas verilerin veya uygunsuz içeriklerin dışa aktarılmasını engeller.
   - **Etkisi:** Güvenli yapay zeka dağıtımı için önleyici bir katman sağlar.
2. **NeMo Guardrails:**
   - **Nedir?**: Etik sınırları desteklemek için açık kaynaklı bir araç kiti.
   - **Örnek:** Ajanın belirli türde yanıtlar vermesini sınırlar ve etik uyum sağlar.
   - **Etkisi:** Güvenlik ve etik kurallarının daha iyi yönetilmesini sağlar.

AgentOps Dönemi için Yetenek Kazanımı

Technical Skills (Teknik Beceriler):

1. **Prompt Engineering Frameworks (Ör: DSPy):**
   - **Nedir?**: Yapay zeka modellerini daha verimli yönlendirmek için kullanılan teknikler.
   - **Etkisi:** Daha iyi model çıktıları elde etmek için hayati önem taşır.
   - **Örnek:** Bir müşteri hizmetleri botunun doğru sorular sormasını sağlama.
2. **LLM-Specific Infrastructure Tools (vLLM, Hugging Face TGI):**
   - **Nedir?**: Büyük dil modelleri için altyapı ve dağıtım araçları.
   - **Etkisi:** Bu araçlar, model dağıtımı ve performans optimizasyonu için kritik bir rol oynar.

Soft Skills (Sosyal Beceriler):

1. **Compliance için Hukuk Takımlarıyla İşbirliği:**
   - **Nedir?**: Yapay zeka çözümlerinin yasalara uygunluğunu sağlamak için multidisipliner işbirliği.
   - **Örnek:** GDPR gibi düzenlemelere uyumun sağlanması.
   - **Etkisi:** Yapay zeka projelerinin yasal sorunlardan kaçınmasını sağlar.
2. **Agent Kararlarını Teknik Olmayan Paydaşlara Açıklamak:**
   - **Nedir?**: Yapay zeka çıktılarının anlaşılabilir bir şekilde ifade edilmesi.
   - **Etkisi:** Daha fazla paydaş desteği ve güven oluşturur.
3. **Stat (İstatistik):**
   - **Veri:** MLOps profesyonellerinin %67'si, AgentOps becerilerinin maaşlarını %20'den fazla artırdığını belirtiyor.
   - **Etkisi:** AgentOps yeteneklerinin kariyer gelişimi için değerini vurgular.