Давидов Петро

Огляд публікації: «Machine Learning Operations (MLOps): Challenges and Strategies» автора Амандіпа Сінгла

1. *Вступ*

Публікація під назвою «Machine Learning Operations (MLOps): Challenges and Strategies» авторства Амандіпа Сінгла, опублікована в журналі *Journal of Knowledge Learning and Science Technology*, пропонує всебічне дослідження еволюційної дисципліни MLOps. У міру того як машинне навчання (ML) дедалі глибше інтегрується в процеси прийняття рішень та автоматизації в корпоративному середовищі, зростає потреба в надійних операційних фреймворках.

У статті розглядається ключове дослідницьке питання: *Як організації можуть ефективно впроваджувати MLOps для забезпечення масштабованості, надійності та ефективності на всіх етапах життєвого циклу ML?*

Основною метою дослідження є ідентифікація багатовимірних викликів - технічних, організаційних і культурних, які перешкоджають впровадженню MLOps, а також розробка стратегічних рішень, що сприятимуть сталому та масштабованому розгортанню ML-моделей. Автор наголошує на важливості інтеграції MLOps у наявні DevOps - практики, розвитку між функціональної співпраці та використанні інструментів з відкритим кодом для стандартизації робочих процесів.

2. *Методологія*

Методологія, застосована в цій публікації, має переважно якісний та аналітичний характер. Автор узагальнює висновки з сучасної академічної літератури, галузевих опитувань та кейси (практики) для класифікації викликів у сфері MLOps і формулювання практичних стратегій їх подолання. Огляд літератури охоплює джерела, зокрема arXiv, конференції IEEE та рецензовані наукові журнали, що забезпечує багато перспективне бачення впровадження MLOps у різних секторах.

Замість проведення емпіричних експериментів, автор використовує порівняльний аналіз і тематичне групування. Виклики поділяються на три категорії - технічні, організаційні та культурні, кожна з яких підкріплена посиланнями на джерела та практичними прикладами. Запропоновані стратегії

базуються на кращих практиках, спостережених у корпоративних ML-процесах, а також на внесках спільноти відкритого програмного забезпечення.

3. Результати

У публікації визначено кілька ключових висновків:

- ✓ *Технічні виклики:*

Серед основних технічних проблем - версіонування моделей, забезпечення відтворюваності в різних середовищах та узгодженість розгортання. Відсутність стандартизованих інструментів і фрагментована інфраструктура часто призводять до ненадійних результатів ML-моделей.

- ✓ *Організаційні виклики*

Співпраця між міжфункціональними командами ускладнена через ізольованість підрозділів та різноманіття інструментів. Інтеграція ML-процесів у традиційні пайплайни розробки програмного забезпечення залишається стійкою проблемою.

- ✓ *Культурні виклики*

Опір змінам, дефіцит навичок і відсутність спільного розуміння серед зацікавлених сторін гальмують впровадження MLOps. Багатьом командам бракує відповідного мислення та підготовки для переходу від експериментального ML до промислових систем.

Для подолання цих викликів автор пропонує багаторівневу стратегію:

- ✓ *Впровадження* контролю версій та контейнеризації
- ✓ *Створення* спеціалізованих MLOps-команд
- ✓ *Інтеграція* CI/CD-пайплайнів, адаптованих до ML
- ✓ *Сприяння* освіті та підвищенню кваліфікації
- ✓ *Використання* відкритих фреймворків для забезпечення сумісності

Ці стратегії спрямовані на покращення аудиту, повторюваності та надійності ML-систем.

4. *Ключові Інсайти*

I. Відтворюваність, як основа довіри

Акцент на відтворюваності є особливо релевантним у контексті кібербезпеки. У процесі пентестингу відтворюваність дозволяє послідовно демонструвати та підтверджувати вразливості. Аналогічно, у MLOps відтворюваність гарантує передбачувану поведінку моделей у різних середовищах. Це спостереження підкреслює важливість використання контейнеризації (наприклад, Docker) та систем контролю версій (наприклад, Git) як у ML, так і в безпекових робочих процесах.

II. Міжфункціональна праця - критична потреба

У статті наголошується на важливості співпраці між дата-сайентистами, інженерами та бізнес-стейкхолдерами. У сфері кібербезпеки, зокрема в операціях Red Team, взаємодія між атакувальними та захисними командами є ключовою. Це спостереження стимулює впровадження чіткої документації та спільних інструментів (наприклад, GitHub Actions, Jenkins) у міждисциплінарних командах, що дозволяє узгодити ML-моделі та безпекові рішення з організаційними цілями.

III. Моніторинг і цикли зворотного зв'язку як основа безперервного вдосконалення

Описаний у статті пайплайн розгортання включає надійні механізми моніторингу та зворотного зв'язку. У пентестингу безперервний моніторинг є критично важливим для виявлення аномалій та адаптації атакувальних стратегій. У контексті MLOps це означає застосування таких інструментів, як Prometheus і Grafana, для моніторингу продуктивності моделей та виявлення дрейфу даних - що є аналогом виявлення системних вразливостей у кібербезпеці.

5. *Висновок*

Ця публікація становить вагомий внесок у розуміння MLOps як дисципліни, що поєднує машинне навчання та розробку програмного забезпечення. Через класифікацію викликів і пропозицію стратегічних рішень автор формує певну дорожню карту для організацій, які прагнуть ефективно працювати з ML. Акцент на відтворюваності, співпраці та безперервній інтеграції узгоджується з ширшими тенденціями інновацій, що базуються на штучному інтелекті.

Перспективні напрями майбутніх досліджень включають вивчення перетину MLOps і кібербезпеки, зокрема в контексті атакуючого ML (adversarial ML), стійкості моделей та практик безпечного розгортання. Інтеграція принципів безпеки в MLOps-пайплайни залишається недостатньо дослідженою, але критично важливою сферою.

Персональна перспектива: інтеграція MLOps у практику кібербезпеки

У межах мого професійного розвитку орієнтуючись на напрямки *penetration testing* та *DFIR (Digital Forensics and Incident Response)***,** які тісно взаємопов'язані, розуміння принципів MLOps є важливим для майбутньої діяльності**.** У цьому огляді я прагнув поєднати концепції MLOps із практиками кібербезпеки, намагався поєднувати та знайти їхню взаємну цінність.

6. *Зв'язок із кібербезпекою та практикою пентестингу*

Теми, що порушені в цій публікації, мають безпосереднє прикладне значення. MLOps запроваджує операційну дисципліну в ML-системи - те, що є не менш важливим у проєктуванні безпечних систем та тестуванні захисту.

Приклади:

- ✓ *Версіонування моделей* у MLOps має аналог у відстеженні версій експлойтів у таких інструментах, як Metasploit.
- ✓ *Контейнеризація через Docker* використовується як для розгортання ML-моделей, так і для ізоляції середовищ атак.
- ✓ *Інструменти моніторингу*, такі як Prometheus і Grafana, активно застосовуються в лабораторіях різних навчальних платформах для пентестингу, для спостереження за поведінкою систем і виявлення аномалій.

- ✓ *CI/CD-пайплайни* можуть бути адаптовані для автоматизації сканування вразливостей та розгортання експлойтів.

У своїй практиці на різних платформах для тренування навичок пентестингу я часто використовую інструменти, такі як *Burp Suite*, *Nmap, OWASP ZAP* та скрипти для автоматизації розвідки та експлуатації. Принципи MLOps - *автоматизація, відтворюваність і моніторинг*, здатні суттєво покращити ці робочі процеси, додаючи структурованість і «трасування даних».

Крім того, *культурні виклики*, такі як *опір змінам і дефіцит навичок*, мають прямі паралелі з труднощами, які виникають у кібербезпекових командах під час переходу до DevSecOps. Формування культури навчання та міжфункціональної співпраці є одними з ключових чинників успіху.

Ця публікація не лише поглиблює розуміння MLOps як дисципліни, але й надихає на інтеграцію її принципів у практику кібербезпеки, зокрема у створення безпечних, масштабованих і можливих до аудиту пайплайнів для penetration testing.

Словник

MLOps - Операції машинного навчання (MLOps) - це дисципліна, що поєднує машинне навчання з розробкою програмного забезпечення та практиками DevOps. Вона охоплює автоматизацію та управління життєвим циклом ML-моделей: від розробки до розгортання, моніторингу та контролю.

Journal of Knowledge Learning and Science Technology - Академічний журнал, що публікує рецензовані дослідження у сферах систем знань, освітніх технологій та прикладних наук. Служить платформою для міждисциплінарних досліджень, зокрема у галузі MLOps та інтеграції ШІ.

DevOps - це набір практик, що об’єднує розробку програмного забезпечення (Dev) та IT-операції (Ops). Його мета - скоротити життєвий цикл розробки та забезпечити якісне програмне забезпечення через автоматизацію, співпрацю та безперервне постачання..

DevSecOps - це розширення DevOps з інтеграцією безпекових практик на всіх етапах життєвого циклу розробки. Він сприяє про активному управлінню ризиками, безпечному кодуванню та автоматизованому тестуванню безпеки в CI/CD-процесах.

arXiv - це відкритий репозиторій наукових статей у галузях комп’ютерних наук, фізики, математики тощо. Дозволяє дослідникам публікувати препринти до проходження рецензування, прискорюючи поширення знань.

IEEE conferences - Конференції IEEE - це міжнародні академічні заходи, організовані Інститутом інженерів електротехніки та електроніки. Вони презентують новітні дослідження в галузях інженерії, обчислень і технологій, включно з ШІ, кібербезпекою та MLOps.

CI/CD - Безперервна інтеграція та безперервне розгортання (CI/CD) - це практики, що автоматизують інтеграцію коду, тестування та постачання. Вони підвищують швидкість розробки, надійність і узгодженість між середовищами.

Pipelines - У програмних та ML-процесах пайплайни - це структуровані послідовності автоматизованих етапів для обробки даних, навчання моделей, тестування та розгортання. Вони забезпечують відтворюваність, масштабованість і операційну ефективність.

ML - Машинне навчання (ML) - це підгалузь штучного інтелекту, яка дозволяє системам виявляти закономірності в даних та приймати рішення без явного програмування. Широко використовується в автоматизації, аналітиці та кібербезпеці.

GitHub Actions, Jenkins - це інструменти автоматизації, що використовуються для побудови CI/CD-пайплайнів. Вони підтримують оркестрацію завдань, тестування та розгортання у програмних і ML-проектах.

Deployment - Розгортання - це процес випуску програмного забезпечення або ML-моделі в продуктивне середовище. Включає пакування, конфігурацію та інтеграцію для забезпечення готовності до експлуатації.

Deployment workflow - Пайплайн розгортання - це заздалегідь визначена послідовність кроків, що регулює випуск моделей або застосунків. Включає тестування, моніторинг, етапи перевірки та механізми відкату для забезпечення надійності.

Prometheus and Grafana - Prometheus - це система моніторингу з відкритим кодом, яка збирає метрики з застосунків та інфраструктури. Grafana - це інструмент візуалізації, що відображає ці метрики у вигляді дашбордів, підтримуючи аналіз продуктивності та виявлення аномалій.