DOI: 10.53469/jtpes.2024.04(02).05

Enhancing Security in DevOps by Integrating Artificial Intelligence and Machine Learning

Penghao Liang[1, *], Yichao Wu[2], Zheng Xu[3], Shilong Xiao[4], Jiaqiang Yuan[5]

[1] Information Systems, Northeastern University, San Jose, CA, USA
[2] Computer Science, Northeastern University, San Jose, CA, USA
[3] Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA
[4] Computer Science, Hebei Normal University, Shijiazhuang City, CN
[5] Information Studies, Trine University, Phoenix, AZ, USA
**Correspondence Author, phliang2021@gmail.com*

Abstract: ***In modern software development and operations, DevOps (a combination of development and operations) has become a key methodology aimed at accelerating delivery, improving quality and enhancing security. Meanwhile, artificial intelligence (AI) and machine learning (ML) are also playing an increasingly important role in cybersecurity, helping to identify and respond to increasingly complex threats. In this article, we'll explore how AI and ML can be integrated into DevOps practices to ensure the security of software development and operations processes. We'll cover best practices, including how to use AI and ML for security-critical tasks such as threat detection, vulnerability management, and authentication. In addition, we will provide several case studies that show how these technologies have been successfully applied in real projects and how they have improved security, reduced risk and accelerated delivery. Finally, through this article, readers will learn how to fully leverage AI and ML in the DevOps process to improve software security, reduce potential risks, and provide more reliable solutions for modern software development and operations.***

Keywords: Data security; DevOps; Machine Learning; Artificial Intelligence.

1. INTRODUCTION

When it comes to the relevance of DevOps and AI/ML, it is worth noting that they can enhance and complement each other, resulting in a more efficient software development and operations process. DevOps focuses on automation and process improvement, while AI and ML technologies can be used to automate testing, monitoring, and troubleshooting to improve delivery speed and quality. In addition, AI and ML are able to analyze large data sets to provide insights that help DevOps teams make more informed decisions while promoting a culture of continuous improvement. As a result, the synergy of DevOps and AI/ML is expected to help organizations better respond to rapidly changing software delivery needs.

DevOps software development model solves the problem of long iteration cycle by strengthening the collaboration between teams through an integrated platform. In the whole development life cycle, the work progress and work output information are shared and displayed by the platform. From software design, development, testing, release to business operation, all links of the team work together to shorten the development life cycle of the entire application. Dev0ps implements the concept of "shift left," shifting the responsibility for delivering high-quality products to all members of the development and operations teams. As a result, productivity is improved, and programs can be iterated quickly to meet changing business requirements.

As for why security is critical in DevOps, this is mainly because DevOps focuses on fast delivery, but this can lead to the introduction of security vulnerabilities. Inadequate security can lead to problems such as data breaches, malicious intrusions, and reputational damage. By integrating security measures into the DevOps process, you can ensure continuous monitoring and feedback to quickly detect and respond to potential security threats. In addition, compliance requirements and regulations impose higher standards on data security, so ensuring that security is compliant with regulations is also critical. Ultimately, maintaining security helps reduce costs, as it is often more expensive to fix security breaches than to prevent them. Therefore, in DevOps practice, ensuring security is an important part of ensuring the quality, compliance, and reliability of software delivery.

2. RELATED WORK

2.1 DevOps

DevOps (a combination of Development and Operations) is a set of processes, methods, and systems used to facilitate communication, collaboration, and integration between development (application/software engineering), technical operations, and quality assurance (QA) departments. IT is a culture, movement, or practice that values communication and collaboration between "software developers (Dev)" and "IT operations technicians (Ops)." Build, test, and release software faster, more frequently, and more reliably by automating the processes of "software delivery" and "architecture change."

The traditional Dev focus is different from the Ops focus, where Dev focuses on how to develop and test to deliver new functionality, while Ops focuses on ensuring stable and high-performance application performance. The direct contradictions are manifested in the following two aspects:

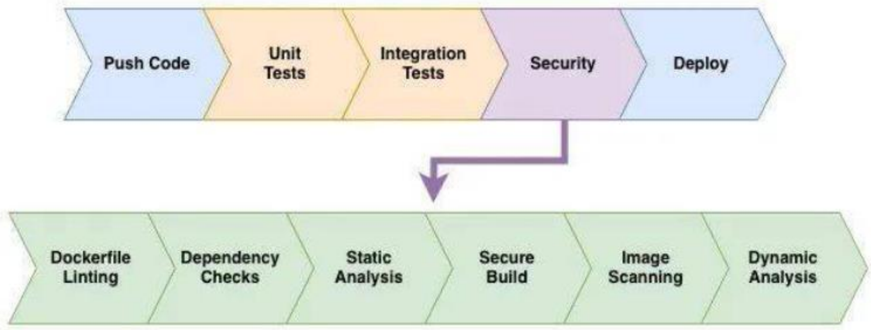


Figure 1: The cornerstone of DevOps is the continuous integration step.

(a) Ops downstream of the value stream determines that the non-functional quality of Dev software upstream of the value chain does not meet the requirements and therefore blocks changes.

Dev upstream of the value stream does not have access to the real operating environment of Ops downstream of the value chain, and therefore cannot improve the quality of delivery.

As a result, it gradually fell into a dead circle of "unable to improve quality" and "non-functional quality does not meet the requirements", and the final result is the separation and opposition between the development stage and the operation and maintenance stage in the software life cycle. Development does not consider operation and maintenance operations, only after the development of the most basic functions are delivered, but how to operate and maintenance is not considered at all, and even how to install and upgrade there is no documentation; In turn, operations does not provide hardware/network configuration/release environment information for development, and always raises questions to prevent changes and releases.

2.2 AI and Machine Learning Transform DevOps

Artificial intelligence and machine learning bring new automation capabilities to DevOps, and for that, an example of how these technologies can optimize an organization's operations needs to be understood. DevOps engineering is designed to accelerate the software development process to deliver value to customers faster without compromising code quality. Traditional DevOps has come a long way in the last decade and now allows many organizations to implement continuous integration (CI)/ continuous deployment (CD) pipelines. However, in most cases, organizations still rely on a combination of manual processes and human-driven automated processes and are not optimized.

2.3 Application of Artificial Intelligence and Machine Learning in DevOps

DevOps has also seen the rise of artificial intelligence and machine learning techniques. These tools are emerging as strong candidates for integration into the traditional DevOps tool stack. From decision process improvements to automated operations and code quality enhancements, the future of DevOps is promising with the help of artificial intelligence and machine learning. Here are seven trends and changes to watch:

(1) Code review is automated

In the early stages of software development, starting with the coding itself, AI and machine learning tools are already capable of performing automated code review and code analysis based on thought datasets (inputs to machine learning and responsive machine learning algorithms). These helps reduce human involvement. In addition, using code management and collaboration tools, users can automatically spread the workload of reviews among team members. The end result is earlier detection of code defects, security issues, and code-related defects that these algorithms can easily find. These tools can also reduce noise in code reviews. In addition to detecting defects, automated code review enforces coding and security standards.

(2) Automation of code analysis tools

Intelligent tools powered by AI and machine learning, such as code analysis and improvement, can learn from repositories of millions of lines of code. These tools can then understand the intent of the code and record the changes made by the developer. There, these smart tools can make recommendations for every line of code they analyze. Other developers take a different approach to code analysis. After analyzing millions of pieces of code from open-source projects, the code powered by machine learning tools focuses on performance and helps find lines of code that can cause significant losses, which can hurt an application's response time. These tools can detect problems in code, such as resource leaks, potential concurrent race conditions, and wasted CPU cycles, and they can also integrate with continuous integration (CI)/ continuous deployment (CD) pipelines during the code review phase and application performance monitoring phase.

In the same category, after coding the new functionality, developers began working on automated unit testing innovations powered by artificial intelligence and machine learning. Build. This can save developers about 20% of their time.

(3) Self-repair test

The next stage in post-build acceptance and integration coding is functional and non-functional testing. Here, the use of AI and machine learning for code creation as well as self-healing test code and maintenance has become a reality in the DevOps space. Test automation can be a huge bottleneck and is often the cause of project delays. Unreliable automation can affect the testing process. One of the root causes of unreliable test automation is the constant change of the application under test and the elements used in the test. Smart technology can help identify these changes and adjust the test to make it more stable and reliable.

2.4 Security Vulnerabilities in DevOps Processes

DevOps also talks about automating different dashboards and alerts, so people monitoring applications in real time can get better intelligence when security occurs. This is what we've been doing in software for a long time. I think DevOps is demanding more of it and putting a nice name in front of it, and at least in my world, trying to add more security to it and make it as automated as possible.

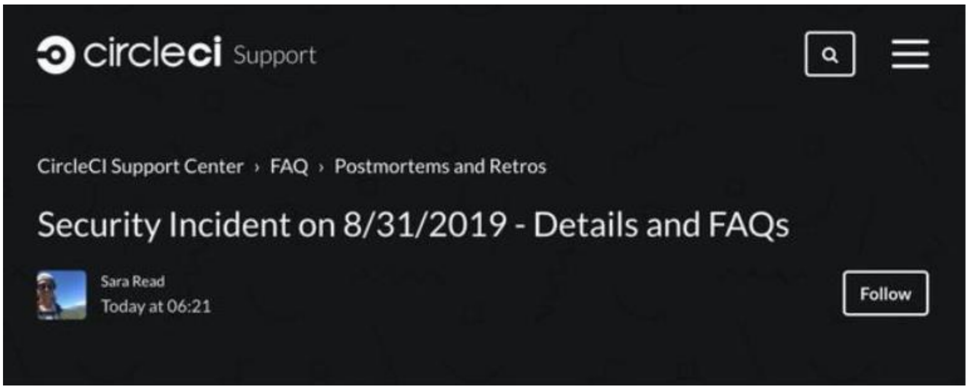
Now, the flip side is that certain elements of application security don't translate well to automation. Like, especially if you want to, if you want to use turnkey tools, there's always going to be a finding that tools, especially those that can cause access control issues, business logic issues, or deeper issues that pen testing might find, aren't always that good. You can tune it to work quickly in a DevOps environment, and perhaps only one in five people will find that manual operations may miss issues. The dark side of DevOps is that we still need people. We can't just automate everything. I think we still need people who are involved in deep vetting to really provide a deeper level of security assurance if you need it.

3. DEVOPS SECURITY CASE

3.1 Real Events:

Circleci, a well-known DevOps service provider, found abnormal behavior in its partner's account on August 31, and immediately terminated the account's access rights, and now released a security investigation report after an investigation, Circleci said that the user's source code and authorization credentials were not leaked, so users do not need to update their passwords. The disclosure affected all users who accessed the Circleci platform between June 30, 2019, and August 31, 2019, and Circleci has proactively notified these users by email and provided recommendations for necessary actions.

As a result, CircleCI received an email notification from a third-party analytics vendor on August 31 that the vendor's account was performing abnormal activity, CircleCI immediately disabled the affected account, and the CircleCI engineering team also detected the addition of an abnormal database to the system. Once it was confirmed that the database was not a CircleCI resource, the database was deleted immediately.



CircleCI Support Center › FAQ › Postmortems and Retros

Security Incident on 8/31/2019 - Details and FAQs

Sara Read
Today at 06:21

Figure 2: DevOps data is abnormal, and information is exposed on the page.

3.2 Events Description

This incident highlights the importance of security in DevOps and the need for vulnerability disclosure. Here are some perspectives on the event:

Security incidents are hard to avoid: Even well-known DevOps service providers can be affected by security incidents. This shows that regardless of the size of an organization, there is a constant need to focus on security and take steps to counter potential threats.

The importance of quick response and measures: CircleCI took immediate action upon discovering the abnormal behavior, suspending the affected accounts and conducting an investigation. This rapid response is key to limiting potential risks and harms.

Transparency and vulnerability disclosure: CircleCI chose to publicly disclose the details of the incident, which helps users understand what happened and can take the necessary precautions. Transparency is important for building trust and maintaining open communication with users.

User education and advice: CircleCI not only informed the affected users, but also provided advice and guidance to help them take the necessary steps. This user education is essential to ensure users' security awareness and actions.

Continuous improvement: After the incident, CircleCI may further improve its security measures to avoid future security incidents. This reflects the principle of continuous improvement in DevOps, improving safety through learning and adaptation.

In summary, this incident highlights the need for both service providers and users to always focus on security in DevOps and to have a plan in place to respond to security incidents. Vulnerability disclosure and rapid response are key, while transparency and user education help maintain trust and reduce risk. Continuous improvement of security measures is also a key step in ensuring future security.

However, in the process of DevOps practice, many enterprises are faced with many pain points, including culture, team, security, technology, etc. Some people start from DevOps security and believe that DevOps security team and continuous delivery team often operate independently, and information interaction is frequent and low efficiency leads to difficult quality assurance. The unplanned workload of safety problem rectification is large. At the same time, the communication work also relies on manual work, and automated tools only play the role of detection and execution, resulting in information asymmetry and untimely communication pain points. Another view focuses on the DevOps pain points of the cloud-native era, arguing that DevOps is integrated by relying on cloud-native, workflow, and people organization, but it is still difficult to get the desired business value from it. Value and management and maintenance costs are not equal, there is a difficult balance between efficiency and cost pain points. But more data shows that the choice and application of DevOps tools has become the most difficult area for many enterprises.

3.3 DevOps Development Dilemma

1) DevOps skills shortage

Making DevOps improvements and the lack of relevant domain experts are emerging as the biggest hindrance to organization-level DevOps transformation, who, in addition to relevant technical skills (automation skills, infrastructure knowledge, software development of processes, source code control, and analysis, etc.), Soft skills - such as collaboration, problem solving and interpersonal skills - are also required, as is hands-on experience with watermelon. The lack of experts with DevOps experience has led to slow and slow progress. With the continuous complexity of Internet technology and the rapid development of technology, the technical gap between development and operation and maintenance has become increasingly prominent and deepening. For most of the country's IT companies, relying on the concept of DevOps does not bridge this gap. The implementation of DevOps is highly dependent on talents and requires very high basic quality of personnel, which means that many IT companies have to fail in the practice of DevOps. There is an urgent need for a more efficient platform to make DevOps concepts and related technologies more reliable.

2) I am not sure about the development path and transformation direction of DevOps

The "China DevOps Status Survey Report" shows that there are still many enterprises in the research and development efficiency improvement, product quality, delivery efficiency and customer satisfaction indicators to measure the success of DevOps transformation. By focusing too much on such metrics, companies often overlook the impact of culture. But in reality, an important part of building a great DevOps process is understanding the cultural and organizational changes required for success and making them a priority.

3) It is difficult to build an appropriate work specific system, and DevOps has many technical challenges

Many DevOps practitioners in enterprises said that the pain points of DevOps landing in the cloud native era are more about the degree of automation and insufficient operation and maintenance capabilities, the operation and maintenance challenges brought by technological changes such as microservices and containers, and the tool and technical problems such as the disconnection of the application delivery tool chain. When companies decide to introduce DevOps tools, they have three options: directly use open-source tools, purchase commercial tools, or develop tools themselves.

4. CONCLUSION

This article delves into the interaction between DevOps and artificial intelligence (AI) and machine learning (ML), highlighting how together they can provide more efficient and secure solutions for modern software development and operations processes. First, the article introduces the fundamentals and importance of DevOps, emphasizing its value for accelerating delivery, improving quality, and enhancing security. The paper then focuses on the role of AI and ML in cybersecurity, especially in mission-critical applications such as threat detection, vulnerability management, and authentication. It further provides a set of best practices detailing how AI and ML technologies can be seamlessly integrated into DevOps practices to ensure the security of software development and operations processes. These practices include automated code review, automated code analysis, automated unit testing, and so on. In addition, the article presents multiple case studies that highlight the successful use of these technologies in real-world projects and how they have improved safety, reduced risk, and accelerated delivery.

Finally, this article highlights the critical importance of security in DevOps practices. Because DevOps focuses on fast delivery, inadequate security measures can lead to issues such as data breaches, malicious intrusions, and reputational damage. Therefore, by integrating security measures, continuous monitoring and feedback can be ensured to quickly detect and respond to potential security threats. In addition, compliance requirements and regulations impose higher standards on data security, so ensuring that security is compliant with regulations is also critical. Ultimately, maintaining security helps reduce costs, as it is often more expensive to fix security breaches than to prevent them. Therefore, in DevOps practice, ensuring security is an important part of ensuring the quality, compliance, and reliability of software delivery.

In the future, DevOps security will continue to evolve and evolve, facing new challenges and opportunities. As technology continues to advance, artificial intelligence (AI) and machine learning (ML) will play a greater role in DevOps, helping to automate threat detection, vulnerability management, and security audits. At the same time, the widespread adoption of cloud-native and container technologies will introduce new security considerations, requiring adaptive security measures. In addition, as compliance requirements continue to increase, DevOps security will focus more on meeting regulatory requirements, emphasizing data privacy and compliance. Ultimately, DevOps security in the future will require more cross-team collaboration and continuous improvement to ensure security, compliance, and reliability of software delivery.

ACKNOWLEDGEMENT

At the end of the article, I would like to sincerely thank Hengyi Zang for her article 'Strategic Application of AI Intelligent Algorithm in Network Threat Detection and Defense'. Their excellent research provides valuable inspiration and profound insights for this paper and provides a solid theoretical foundation for our research. In addition, I would like to give special thanks to [Hengyi Zang], whose research/work has provided important reference and inspiration for this article, and finally I would like to thank all the relevant literature and studies cited in this article, which provide important context and support for our research.

REFERENCES

[1] “Based on Intelligent Advertising Recommendation and Abnormal Advertising Monitoring System in the Field of Machine Learning”. International Journal of Computer Science and Information Technology, vol. 1, no. 1, Dec. 2023, pp. 17-23, https://doi.org/10.62051/ijcsit.v1n1.03.

[2] Yu, Liqiang, et al. “Research on Machine Learning With Algorithms and Development”. Journal of Theory and Practice of Engineering Science, vol. 3, no. 12, Dec. 2023, pp. 7-14, doi:10.53469/jtpes.2023.03(12).02.

[3] Liu, Bo, et al. "Integration and Performance Analysis of Artificial Intelligence and Computer Vision Based on Deep Learning Algorithms." arXiv preprint arXiv:2312.12872 (2023).

[4] Yu, L., Liu, B., Lin, Q., Zhao, X., & Che, C. (2024). Semantic Similarity Matching for Patent Documents Using Ensemble BERT-related Model and Novel Text Processing Method. arXiv preprint arXiv:2401.06782.

[5] Huang, J., Zhao, X., Che, C., Lin, Q., & Liu, B. (2024). Enhancing Essay Scoring with Adversarial Weights Perturbation and Metric-specific AttentionPooling. arXiv preprint arXiv:2401.05433.

[6] Tianbo, Song, Hu Weijun, Cai Jiangfeng, Liu Weijia, Yuan Quan, and He Kun. "Bio-inspired Swarm Intelligence: a Flocking Project With Group Object Recognition." In 2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE), pp. 834-837. IEEE, 2023.DOI: 10.1109/mce.2022.3206678

[7] Liu, B., Zhao, X., Hu, H., Lin, Q., & Huang, J. (2023). Detection of Esophageal Cancer Lesions Based on CBAM Faster R-CNN. Journal of Theory and Practice of Engineering Science, 3(12), 36–42. https://doi.org/10.53469/jtpes.2023.03(12).06

[8] Liu, Bo, et al. "Integration and Performance Analysis of Artificial Intelligence and Computer Vision Based on Deep Learning Algorithms." arXiv preprint arXiv:2312.12872 (2023).

[9] “Implementation of Computer Vision Technology Based on Artificial Intelligence for Medical Image Analysis”. International Journal of Computer Science and Information Technology, vol. 1, no. 1, Dec. 2023, pp. 69-76, https://doi.org/10.62051/ijcsit.v1n1.10.

[10] K. Jin, Z. Z. Zhong and E. Y. Zhao, "Sustainable Digital Marketing Under Big Data: An AI Random Forest Model Approach," in IEEE Transactions on Engineering Management, vol. 71, pp. 3566-3579, 2024, doi: 10.1109/TEM.2023.3348991.

[11] “Enhancing Computer Digital Signal Processing through the Utilization of RNN Sequence Algorithms”. International Journal of Computer Science and Information Technology, vol. 1, no. 1, Dec. 2023, pp. 60-68, https://doi.org/10.62051/ijcsit.v1n1.09.

[12] Dong, Xinqi, et al. “The Prediction Trend of Enterprise Financial Risk Based on Machine Learning ARIMA Model”. Journal of Theory and Practice of Engineering Science, vol. 4, no. 01, Jan. 2024, pp. 65-71, doi:10.53469/jtpes.2024.04(01).09.

[13] Tan, Kai, et al. “Integrating Advanced Computer Vision and AI Algorithms for Autonomous Driving Systems”. Journal of Theory and Practice of Engineering Science, vol. 4, no. 01, Jan. 2024, pp. 41-48, doi:10.53469/jtpes.2024.04(01).06.

[14] “A Deep Learning-Based Algorithm for Crop Disease Identification Positioning Using Computer Vision”. International Journal of Computer Science and Information Technology, vol. 1, no. 1, Dec. 2023, pp. 85-92, https://doi.org/10.62051/ijcsit.v1n1.12.

[15] Wang, Sihao, et al. “Diabetes Risk Analysis Based on Machine Learning LASSO Regression Model”. Journal of Theory and Practice of Engineering Science, vol. 4, no. 01, Jan. 2024, pp. 58-64, doi:10.53469/jtpes.2024.04(01).08.

[16] Jin, Keyan. "Impacts of Word of Mouth (WOM) on E-Business Online Pricing." JGIM vol.31, no.3 2023: pp.1-17. http://doi.org/10.4018/JGIM.324813.

[17] Wei, Kuo, et al. “Strategic Application of AI Intelligent Algorithm in Network Threat Detection and Defense”. Journal of Theory and Practice of Engineering Science, vol. 4, no. 01, Jan. 2024, pp. 49-57, doi:10.53469/jtpes.2024.04(01).07.

[18] Zheng, Jiajian, et al. “The Credit Card Anti-Fraud Detection Model in the Context of Dynamic Integration Selection Algorithm”. Frontiers in Computing and Intelligent Systems, vol. 6, no. 3, Jan. 2024, pp. 119-22, https://doi.org/10.54097/a5jafgdv.

[19] Qian, Jili, et al. “Analysis and Diagnosis of Hemolytic Specimens by AU5800 Biochemical Analyzer Combined with AI Technology”. Frontiers in Computing and Intelligent Systems, vol. 6, no. 3, Jan. 2024, pp. 100-3, https://doi.org/10.54097/qoseeQ5N.

[20] Song, Tianbo, et al. “Development of Machine Learning and Artificial Intelligence in Toxic Pathology”. Frontiers in Computing and Intelligent Systems, vol. 6, no. 3, Jan. 2024, pp. 137-41, https://doi.org/10.54097/Be1ExjZa.

[21] Du, Shuqian, et al. “Application of HPV-16 in Liquid-Based Thin Layer Cytology of Host Genetic Lesions Based on AI Diagnostic Technology Presentation of Liquid”. Journal of Theory and Practice of Engineering Science, vol. 3, no. 12, Dec. 2023, pp. 1-6, doi:10.53469/jtpes.2023.03(12).01.