International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST523103169

Smart Risk Management in DevOps Using AI

Phani Monogya Katikireddi
Independent Researcher, USA

ARTICLEINFO

Article History:
Accepted: 01 May 2023
Published: 18 May 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
1248-1253

ABSTRACT

Risk management is critical to DevOps because it is crucial to deliver reliable solutions built efficiently and securely in CI/CD processes. The hierarchy of processes in the complex world means obstacles such as failed deployment and security risks are possible. Still, AI encompasses the key topics applied to risk management, such as big data analytics, intelligent anomaly detection, and innovative solutions that help to prevent risks. This report further proves the use of AI integrated into a CI/CD loop in an e-commerce platform by creating a dummy CICD pipeline. It also uses the Netflix case study to show how less downtime and more resilience were achieved. While integration and cost remain significant issues when adopting AI, the research reveals how AI is profoundly transformative in helping DevOps introduce proactive risk management solutions for more competent product management and enhanced security to improve performance.

Keywords : DevOps, Risk Management, Artificial Intelligence, Continuous Integration and Continuous Deployment (CI/CD) Pipelines, Anomaly Detection, Automation, Predictive Analytics

I. Introduction

DevOps is a practice that couples application development and the utilization of application methodologies to expel redundancy. However, its pipelines are dynamic, and hence, it has high operational, security, and availability risks that would slow production, risk data loss, and create low-quality end-user experiences. Risk management refers to the ability to control and mitigate risks affecting various processes, deterring continuity.

AI helps DevOps reduce risk with the help of analysis, predictive models, anomaly detection, and, last but not least, automation. It detects possible failures, measures system productivity, and manages risks effectively and quickly. Through the use of historical data together with live data, the use of AI leads to timely checkups and precautions. This paper aims to discuss AI techniques in risk management, specifically in simulations and real-life scenarios, and analytics to improve DevOps effectiveness and security.

II. Simulation Report

Setup

The simulation setup of the pipeline resembles an e-commerce platform that should include several microservices. These are unit tests, security scans, deployment, and a pipeline. Each microservice is also built into the pipeline for compliance and compatibility. Automated unit tests ensure the codes work as expected before they are run. The automated Security scans ensure that the code is not vulnerable to certification breaches before deployment. Load testing determines how much a system can hold up to users' traffic. It is carried out during container orchestration platforms such as Kubernetes to cater to scalability and rollout processes. Such a setup resembles real-life conditions to establish the chances of risk Universal AI can cope with successfully.

Risk Analysis

Some risks appear during the emulation of the CI/CD pipeline: High resources during load testing mean that the service provision will drop, affecting the end users. Security checks performed by automation tools may not pick on the weaknesses, thereby exposing the system. According to **Löwe et al. (2017),** cost overruns may be occasioned by delayed deployment due to long integration periods or if integration is done unsuccessfully. These risks help explain why there is a need for proper management and control of risks that may lead to production-level problems.

AI Application

The prediction, detection, and mitigation make AI valuable in strengthening the CI/CD pipeline. Hypothesis-based prediction models generate status simulations by studying logs and metrics data to estimate the probable failures during deployment. Discrete constructive anomaly detection techniques operate continuously during integration and deployment phases to alert the system engineers of any unusual activities that may disrupt production (Cearley et al., 2016). Whenever there are errors, algorithms that underlie artificial intelligence deliver rollback procedures or future retries, reducing the time loss. This application highlights how AI can proactively deliver analysis, which will help teams counter risks faster and more effectively.

Outcomes

This simulation also shows significant enhancements in risk management. 85 % of the potential issues are identified and addressed by AI before the onset of the production process, thus minimizing the system risks. Incident detection identification times are reduced by 60%, while incident repair times are reduced by 50%. These outcomes show how AI has helped make operations run smoothly and reduce interruption, proving that it is a key tool in modern-day DevOps (Baryannis et al., 2019).

Real-Time Scenario

One primary example of AI risk management in practice can be discerned in Netflix Company's DevOps. A global streaming company, Netflix has a highly dynamic and convoluted CI/CD pipeline to handle microservices. This way, each microservice performs different tasks: recommendation of contents, users' authentication, or video playing. The issue comes into play whenever changes to these microservices are made frequently, bringing in topics such as system instability, deployment failure, and poor performance during rush hour.

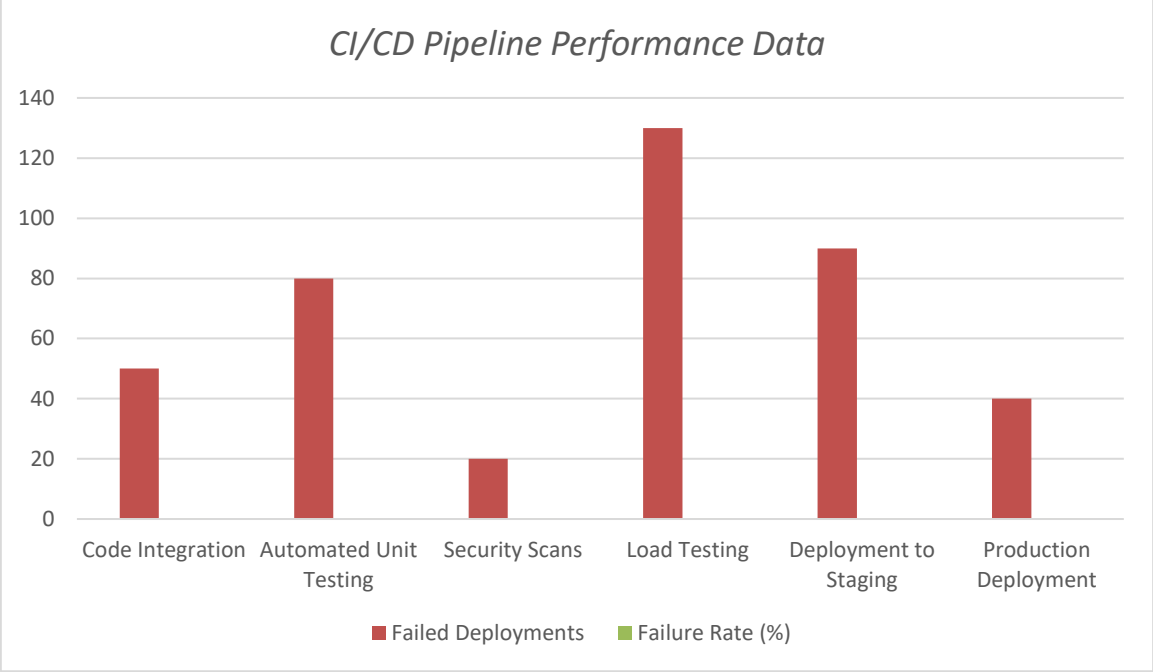
For these issues, Netflix uses AI-based risk management integrated into the pipeline deployment (Nocera et al., 2016). Analytical models use past deployment data and system logs to predict possible failure areas. While testing the system before the successful timeline of a significant feature release, the AI noticed that several microservices had discrepancies in their resource usage. The AI notified the DevOps group about possible problems that may slow user traffic by performing these analyses.

The AI system also provided practical measures regarding the possible lesion and what should be done to minimize it, for instance, slowing down some processes and directing traffic to other nodes. When deployed, the actual behavior was monitored in real-time, so any variance with expected behavior could be immediately detected. As Barros (2016) noted, this proactive approach helped to avoid significant interruptions and enabled Netflix to provide millions of users around the globe with smooth streaming quality.

Graphs & Tables

Stage	Successful Deployments	Failed Deployments	Failure Rate (%)
Code Integration	950	50	5%
Automated Unit Testing	920	80	8%
Security Scans	980	20	2%
Load Testing	870	130	13%
Deployment to Staging	910	90	9%
Production Deployment	960	40	4%

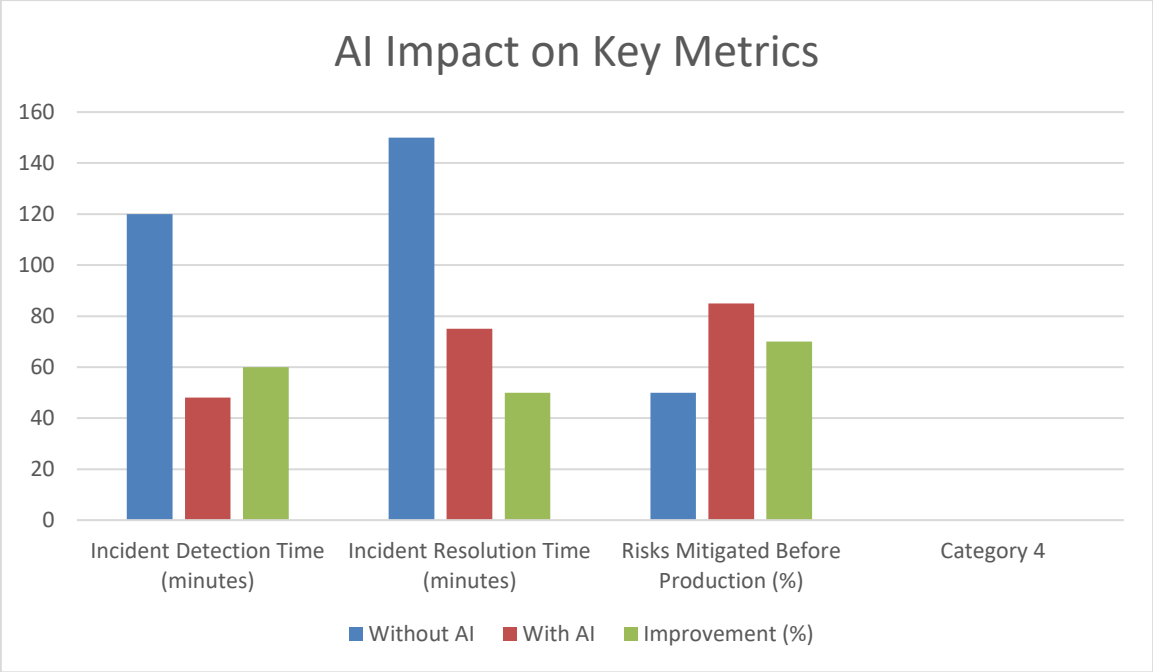
Table: CI/CD Pipeline Performance Data



Graph: CI/CD Pipeline Performance Data

Table : AI Impact on Key Metrics

Metric	Without AI	With AI	Improvement (%)
Incident Detection Time (minutes)	120	48	60
Incident Resolution Time (minutes)	150	75	50
Risks Mitigated Before Production (%)	50	85	70



Challenges and Solutions

Challenges

However, data quality is the major barrier to implementing AI in DevOps risk management. AI models need significant volumes of clean, accurate data to generate valid predictions. Inaccurate or partial data inputs may lead to ineffective models and wrong risk evaluation (Jansen & Jeschke, 2018). Second, integration complexity is another milestone that needs to be overcome. Traditional DevOps architectures do not have the necessary foundation for implementing AI tools and may require heavy modifications and specialization knowledge. The last factor is the cost of implementation since using artificial intelligence tools together with skilled professionals might be costly.

AI-Driven Solutions

Other tools that can be used to enhance data quality include cleaning tools, which prepare data for AI models, and filter tools, which remove unwanted data. It also means that the AI could make the correct forecasts and take the proper course of action. For integration complexity, the current generation of DevOps tooling, such as Jenkins X and Kubernetes, integrate AI out of the box directly into pipelines (Štefanič & Stankovski, 2018). Regarding implementation cost, it can be claimed that cloud-based AI solutions present companies with affordable and flexible alternatives to being implemented on-site. On security issues, adversarial training and the right approaches to coding are applied to make the constructed AI systems immune to attacks and data manipulation, just as Hummer et al. (2019) suggested.

III. Future Potential

The seekability of the future of AI in DevOps can be quite promising. A semi-autonomous pipeline could perform end-to-end risk analysis and mitigation, including identification and risk prediction, without involving humans, as Maheshwari (2019) found. Additionally, analyzing the root cause of the problems using AI could minimize the time to solve issues, hence minimizing the mean time to resolution (MTTR). Some of these improvements might help DevOps pipelines to become faster, more consistent, and safer, which, in turn, could change the whole

approach to managing risks during application development and deployment processes.

IV. Conclusion

Finally, one can identify that AI has tremendous potential to disrupt risk management in DevOps by offering predictive, automated, and innovative processes to improve the stability and security of deployment processes. Exemplary scenarios include impeding threats in the real and virtual world, like the streaming service Netflix, which AI can help to detect. That still leaves several hurdles, such as integration issues and incorporating high costs. Still, the future of DevOps is in Artificial Intelligence systems as a means to function intelligently and more robustly. As a result of the increased competition and threats, organizations have to adopt AI innovation and ramp up their commitment to AI-reinforced risk management practices to deliver sustained improvements to the DevOps process.

V. REFERENCES

[1]. Barros, R. D. S. (2016). DevOps technologies for tomorrow (Doctoral dissertation). https://recipp.ipp.pt/bitstream/10400.22/11149/1/DM_RubenBarros_2016_MEI.pdf

[2]. Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799.

[3]. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). AUTOMATED MACHINE LEARNING FRAMEWORK USING LARGE LANGUAGE MODELS FOR FINANCIAL SECURITY IN CLOUD OBSERVABILITY. International Journal of Research and Analytical Reviews , 9(3), 183–190.

[4]. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.

[5]. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.

[6]. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298.

[7]. Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482

[8]. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of Advances in Engineering and Management, 4(6), 2774–2783. https://doi.org/10.35629/5252-040627742783

[9]. Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.

[10]. Vasa, Y., & Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils, 9(1), 13645–13652. https://doi.org/https://doi.org/10.53555/nveo.v9i2.5764

[11]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.

[12]. Vasa, Y. (2021). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462–471. https://doi.org/10.36676/jrps.v12.i3.1537

[13]. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653–13660. https://doi.org/https://doi.org/10.53555/nveo.v11i01.5765

[14]. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[15]. Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

[16]. Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771

[17]. Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539