International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Automating Security Compliance in DevSecOps Through AI-Driven Policy Enforcement

Ayobami Olwadamilola Adebayo *

Computer Science, Landmark Metropolitan University, Buea, Cameroon.

International Journal of Science and Research Archive, 2025, 15(02), 670-675

Publication history: Received on 06 April 2025; revised on 11 May 2025; accepted on 13 May 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.2.1457

Abstract

This study explores the integration of Artificial Intelligence (AI) in automating security compliance within DevSecOps pipelines. As organizations increasingly embrace DevSecOps to enhance security throughout the software development lifecycle, AI-driven tools are being leveraged to streamline policy enforcement, detect vulnerabilities, and ensure compliance with regulatory requirements. This research employs a descriptive methodology, using a questionnaire to gather insights from 100 professionals in the DevSecOps field. The findings reveal that while AI tools are widely adopted and have shown significant benefits in improving the efficiency of security audits and mitigating security threats, challenges such as a lack of skilled personnel, high implementation costs, and data quality issues persist. The study concludes that AI has the potential to revolutionize security compliance but recommends further investments in training, improved data management, and fostering a culture of AI adoption within organizations to fully unlock its benefits.

Keywords: DevSecOps; Artificial Intelligence; Security Compliance; Policy Enforcement; Automation; Vulnerability Detection; Regulatory Compliance; AI Tools; Security Audits; Data Quality

1. Introduction

In the rapidly evolving landscape of software development, security has emerged as a critical concern, especially with the increasing complexity of cloud-based environments, microservices, and continuous integration/continuous deployment (CI/CD) pipelines. DevSecOps, the practice of integrating security practices within DevOps processes, aims to address this challenge by embedding security into every phase of software development (Sharma et al., 2021). However, while DevSecOps is widely adopted to improve security resilience, the manual enforcement of security policies often leads to inconsistencies, inefficiencies, and slow response times to emerging threats (Reinhardt et al., 2020). In response to these challenges, artificial intelligence (AI) is being increasingly integrated into DevSecOps pipelines to automate various security processes, particularly the enforcement of security compliance policies. AI-driven tools can perform tasks such as identifying vulnerabilities, automating threat detection, and ensuring compliance with regulatory standards—tasks that would traditionally require significant manual oversight (Crawford et al., 2022). AI has the potential to not only reduce the workload of security teams but also to provide more precise and timely compliance enforcement, ensuring that security policies are continuously adhered to without the need for constant manual intervention.

Moreover, as regulatory requirements in sectors such as finance, healthcare, and technology continue to become more stringent, organizations must ensure that their security measures align with evolving legal and regulatory frameworks (Bertino et al., 2021). AI technologies, particularly machine learning (ML) and natural language processing (NLP), can play a pivotal role in automating the process of compliance checks by continuously monitoring security policies and

* Corresponding author: Ayobami Olwadamilola Adebayo

adapting to new regulations in real time. This automation not only increases the efficiency of policy enforcement but also ensures a higher level of consistency and accuracy in meeting compliance standards.

This paper explores the intersection of AI and DevSecOps, focusing on how AI-driven automation can enhance security compliance through policy enforcement. By examining existing research and case studies, this study aims to provide insights into the current state of AI adoption in DevSecOps pipelines, the benefits and challenges associated with AI-driven security compliance, and the future outlook of this emerging field.

2. Literature Review

2.1. DevSecOps: Concept and Evolution

The concept of DevSecOps has evolved as a response to the growing demand for enhanced security within DevOps pipelines. Traditionally, security was treated as a separate function at the end of the software development lifecycle (SDLC). However, the increasing sophistication of cyber threats and the speed at which software is developed today has made it imperative to integrate security practices throughout the entire SDLC. DevSecOps emerged as a philosophy that ensures security is embedded from the outset of development, automating the integration of security measures into the CI/CD pipelines (Sharma et al., 2021). The main goal of DevSecOps is to foster a collaborative environment between development, security, and operations teams, allowing for more rapid identification and mitigation of vulnerabilities (Reinhardt et al., 2020).

Despite its growing adoption, one of the major challenges faced by DevSecOps is maintaining consistent security compliance across complex, distributed systems, especially with the increasing scale of modern applications. Security policy enforcement in DevSecOps often relies on manual checks and interventions, which are error-prone, slow, and difficult to scale (Harris & Lambert, 2021). This gap has paved the way for artificial intelligence (AI) to play a crucial role in automating compliance processes and improving security posture.

2.2. AI-Driven Automation in DevSecOps

Artificial Intelligence, specifically machine learning (ML) and natural language processing (NLP), has been increasingly applied to automate tasks such as vulnerability scanning, risk management, and compliance auditing in DevSecOps pipelines (Crawford et al., 2022). ML algorithms can analyze large volumes of code and security logs to identify potential vulnerabilities and threats that might otherwise go unnoticed in manual reviews. These AI-driven tools help organizations identify patterns, predict emerging threats, and automate remediation strategies based on predefined security policies (Bertino et al., 2021).

A critical area where AI is particularly beneficial is in the automation of compliance checks. Regulatory standards such as GDPR (General Data Protection Regulation) and PCI DSS (Payment Card Industry Data Security Standard) require organizations to adhere to stringent security measures, and ensuring compliance can be a complex and resource-intensive task. AI tools can automate the process of monitoring and auditing security configurations, ensuring that the application adheres to the required security policies in real time (Harris & Lambert, 2021). For instance, AI can automatically check if a cloud deployment adheres to the appropriate compliance standards, flagging any misconfigurations that could lead to data breaches or non-compliance penalties.

2.3. AI-Driven Policy Enforcement: Tools and Frameworks

A range of AI-driven tools and frameworks have emerged to help enforce security policies in DevSecOps pipelines. Tools such as Checkmarx, Snyk, and SonarQube use AI to analyze source code for vulnerabilities and compliance issues before deployment (Crawford et al., 2022). These tools integrate seamlessly into DevSecOps pipelines, running automated security scans and enforcing security policies in real-time. For example, Checkmarx uses AI-powered static application security testing (SAST) to scan code and identify security flaws, while Snyk focuses on open-source vulnerability management and integrates with CI/CD tools to automate security compliance checks.

In addition, AIOps (Artificial Intelligence for IT Operations) is an emerging concept that leverages AI and machine learning to automate the detection, resolution, and prevention of incidents in real time. AIOps can integrate with DevSecOps pipelines to enforce compliance and security policies more efficiently, providing proactive responses to threats rather than waiting for human intervention (Chaudhary et al., 2020). By automating routine security tasks such as log analysis and anomaly detection, AIOps helps teams maintain security compliance while reducing operational overhead.

2.4. Challenges in AI-Driven Security Compliance

While AI presents significant opportunities to improve security compliance in DevSecOps, its adoption is not without challenges. One of the main obstacles is the complexity of AI models and the need for accurate, clean data. Machine learning algorithms are heavily dependent on the data they are trained on, and without high-quality, well-labeled data, AI tools may produce inaccurate results, leading to false positives or undetected vulnerabilities (Crawford et al., 2022). Furthermore, AI-driven tools require continuous training and fine-tuning to adapt to evolving security threats and compliance requirements.

Another challenge is the lack of skilled professionals who can effectively implement and manage AI-driven DevSecOps solutions. Although many organizations are adopting AI tools, there is a shortage of cybersecurity experts with the expertise to integrate these tools effectively into their DevSecOps pipelines (Reinhardt et al., 2020). Additionally, AI tools are not always intuitive and may require significant effort to configure and maintain, which can be resource-intensive.

Finally, trust and transparency are significant issues when it comes to AI in security compliance. Since AI tools often operate as "black boxes," it can be difficult for security teams to understand how a particular decision was made, which may hinder trust in the tool's capabilities (Bertino et al., 2021). This lack of transparency can pose a challenge in environments where decision-making must be auditable, particularly in highly regulated industries such as finance and healthcare.

2.5. Future Directions

The integration of AI in DevSecOps is still in its early stages, but the potential for future advancements is significant. Future research should focus on improving the interpretability of AI models, creating more transparent and explainable AI systems to foster trust among security professionals (Chaudhary et al., 2020). Additionally, the combination of AI with blockchain technology for immutable logs and decentralized security policy enforcement could provide a further layer of security and compliance for sensitive data in DevSecOps pipelines.

Moreover, continued collaboration between AI and human expertise will be essential. While AI can handle repetitive and data-intensive tasks, human oversight remains critical in making strategic security decisions and managing complex compliance requirements (Sharma et al., 2021). A hybrid model that combines AI's automation capabilities with human judgment may provide the most effective approach to security compliance in DevSecOps.

3. Methodology

This study employs a descriptive research design to explore the use of AI-driven policy enforcement for automating security compliance in DevSecOps. The research relies on questionnaires as the primary data collection method. The questionnaire is designed to gather quantitative data regarding the experiences, perceptions, and challenges faced by IT professionals, developers, and security experts in implementing AI-based solutions for security compliance in DevSecOps pipelines.

3.1. Population and Sampling

The target population for this study includes professionals working in organizations that have adopted DevSecOps practices, with a specific focus on those responsible for security compliance and automation. A random sampling technique was used to select participants from a pool of DevSecOps professionals. A total of 100 respondents were invited to participate in the survey.

3.2. Data Collection Instrument

The primary instrument used for data collection is a structured questionnaire. The questionnaire consists of both closed-ended and Likert scale questions, designed to assess participants' familiarity with AI tools in security compliance, the challenges they face, and their satisfaction with AI-driven automation in DevSecOps environments. The questionnaire also includes demographic questions to gather basic information about the respondents, such as their job role, experience level, and organization size.

3.3. Data Analysis

The data collected from the completed questionnaires were analyzed using descriptive statistical methods. Frequency distributions and percentages were used to summarize and interpret the responses. The analysis focuses on identifying patterns and trends regarding the adoption and effectiveness of AI tools for security policy enforcement in DevSecOps.

3.4. Ethical Considerations

In conducting this study, ethical guidelines were adhered to, including ensuring the confidentiality and anonymity of respondents. Informed consent was obtained from all participants, and they were assured that their participation was voluntary.

4. Results and Findings

4.1. Demographic Information

Table 1 Demographic Profile of Respondents

Demographic Variable	Frequency	Percentage (%)
Gender		
Male	60	60%
Female	40	40%
Age Group		
18-30	30	30%
31-40	50	50%
41-50	15	15%
51+	5	5%
Job Role		
Developer	40	40%
Security Expert	30	30%
IT Manager	20	20%
Other	10	10%
Years of Experience		
Less than 5 years	25	25%
5-10 years	50	50%
11-15 years	15	15%
16+ years	10	10%

The majority of respondents were male (60%), aged between 31-40 years (50%), and held roles as developers (40%) or security experts (30%). Most participants have 5-10 years of experience in their respective fields (50%).

4.2. Findings on AI Integration for Security Compliance

Table 2 Use of AI Tools for Security Compliance

Statement	Frequency	Percentage (%)
AI tools are integrated into the organization's DevSecOps pipeline	75	75%
AI tools are used for vulnerability detection and management	70	70%

AI tools help automate compliance with regulatory requirements	65	65%
AI tools are effective in detecting and mitigating security threats	60	60%
AI tools reduce the manual effort in compliance auditing	50	50%
AI tools provide real-time compliance monitoring	45	45%

A significant proportion of respondents (75%) reported that AI tools are integrated into their DevSecOps pipeline, with 70% indicating that these tools assist in vulnerability detection. However, only 45% reported real-time compliance monitoring, suggesting that this feature may not be fully utilized in all organizations.

Table 3 Challenges in Using AI for Security Compliance

Challenge	**Frequency**	**Percentage (%)**
Lack of skilled personnel to manage AI tools	55	55%
High initial cost of implementing AI tools	50	50%
Difficulty in training AI models to adapt to new security threats	45	45%
Limited transparency in AI decision-making	40	40%
Data quality issues affecting AI performance	35	35%
Resistance to AI adoption from staff	30	30%

The most commonly reported challenges in using AI for security compliance were the **lack of skilled personnel** (55%) and the **high initial cost** (50%). These findings suggest that while AI tools are widely adopted, organizations struggle with the resources and expertise required for effective implementation.

Table 4 Impact of AI on Security Compliance and Efficiency

Impact Statement	**Frequency**	**Percentage (%)**
AI has significantly improved the efficiency of security audits	70	70%
AI has helped to ensure compliance with industry regulations	65	65%
AI has reduced the number of security breaches	60	60%
AI has helped identify potential security risks more quickly	55	55%
AI has improved the collaboration between development and security teams	50	50%

The majority of respondents (70%) reported that AI has **improved the efficiency** of security audits. 65% felt that AI has positively impacted **compliance** with industry regulations, while 60% observed a reduction in security breaches. This suggests that AI is effectively supporting security compliance and improving operational efficiency.

4.3. Summary of Findings

The findings indicate that AI tools are widely used in DevSecOps pipelines to enhance security compliance, with a notable focus on vulnerability detection and regulatory compliance. However, challenges such as lack of skilled personnel, high implementation costs, and data quality issues continue to hinder the full utilization of AI. Despite these obstacles, AI has made a positive impact on the efficiency of security audits and threat detection.

5. Conclusion

The integration of Artificial Intelligence (AI) in DevSecOps pipelines has proven to be a game-changer in automating security compliance and enhancing the overall security posture of organizations. The results of this study indicate that a significant number of organizations have adopted AI tools for vulnerability detection, regulatory compliance, and threat mitigation. The efficiency of security audits has notably improved, and organizations report reduced security

breaches as a result of AI integration. However, challenges such as the lack of skilled personnel, high initial costs, and data quality issues remain barriers to the widespread and effective use of AI tools.

While AI-driven policy enforcement has demonstrated substantial potential in optimizing security compliance processes, it is clear that organizations still face difficulties in fully exploiting the capabilities of these tools due to factors like limited transparency in AI decision-making and the resistance to AI adoption among some staff members. These challenges highlight the need for improved training, better data management practices, and a more seamless integration of AI into existing workflows.

Recommendations

Based on the findings of this study, the following recommendations are made to enhance the adoption and effectiveness of AI-driven security compliance in DevSecOps:

- **Invest in Training and Skill Development**: Organizations should prioritize training programs to upskill their personnel in the use of AI tools for security compliance. This includes technical training on AI implementation, as well as training on how to manage and interpret AI-driven insights effectively.
- **Address the High Initial Costs**: To encourage wider adoption, organizations can explore **cost-effective AI solutions** or **cloud-based AI tools** that lower the upfront costs of implementation. Additionally, companies should consider the long-term savings in terms of reduced breaches, operational efficiency, and regulatory fines.
- **Improve Data Quality and Integration**: Organizations should invest in improving the quality and consistency of their data. High-quality data is critical for AI tools to function optimally, and without proper data management, the effectiveness of AI in compliance tasks could be compromised.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Bertino, E., Sandhu, R., & Li, N. (2021). *Security and Privacy in Cloud Computing*. Springer Nature.

[2] Chaudhary, N., Soni, P., & Joshi, A. (2020). A Survey of AI in Cybersecurity: Tools, Techniques, and Trends. *Journal of Cybersecurity and Privacy*, 1(4), 198-217.

[3] Crawford, P., Sanders, T., & Gupta, R. (2022). AI in Cybersecurity: Leveraging Machine Learning to Enhance Security Protocols. *Journal of Cybersecurity Technology*, 4(2), 45-61.

[4] Harris, A., & Lambert, D. (2021). DevSecOps: A Holistic Approach to Security. *International Journal of Information Security*, 12(3), 101-118.

[5] Reinhardt, J., Gomez, H., & Patel, V. (2020). DevSecOps: Integration and Automation for Security in Continuous Delivery. *International Journal of Information Security*, 19(6), 112-129.

[6] Sharma, D., Arora, A., & Kumar, P. (2021). A Comprehensive Overview of DevSecOps: Practices, Tools, and Challenges. *Software Engineering Journal*, 39(4), 202-217.

[7] Watson, J., & Davis, M. (2021) 'Security and compliance automation: A new era with AI', Journal of Information Security, 22(4), pp. 302-314.

[8] Wilson, J., & Thompson, P. (2019) 'AI in DevSecOps: The future of automated security', Journal of Information Technology & Security, 27(1), pp. 78-93.

[9] Yuan, F., & Wang, H. (2020) 'AI-driven policy enforcement in security compliance: Case studies and challenges', Cybersecurity Policy Review, 14(2), pp. 99-112.