INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

Advancing Retail Cloud Security: Integrating Devsecops, Ai-Driven Automation, And Compliance Strategies For Resilient Software Delivery

Dr. Mei-Ling Chen

University of Montreal, Canada

Abstract: The rapid digital transformation of retail enterprises, driven by cloud adoption and microservices architectures, has intensified the need for robust security frameworks that ensure compliance, operational resilience, and resistance to emerging threats. Traditional DevOps practices, while effective for accelerating delivery, often lack sufficient mechanisms for ensuring security throughout the software development lifecycle. In response, the DevSecOps paradigm integrates security practices directly into DevOps workflows, shifting security left and embedding continuous verification within continuous integration and continuous deployment (CI/CD) pipelines. This research article examines the theoretical foundations, empirical practices, and emerging innovations in DevSecOps, with an emphasis on the retail cloud domain where compliance and resilience are particularly critical due to sensitive customer data and regulatory constraints. Drawing on established literature and recent advances, including strategies for secure DevOps in retail cloud environments (Gangula, 2025), this work synthesizes a comprehensive understanding of how security tools, machine learning, and systemic organizational strategies coalesce to strengthen cloud security.

The study critically engages with themes such as automated security verification, machine learning integration, microservices intrusion detection, and secure development methodologies. By weaving insights from systematic reviews, architectural proposals, and methodology papers, the research illuminates the multifaceted challenges and practical solutions in contemporary DevSecOps adoption. Findings suggest that while automation and AI/ML tools provide substantial gains in threat detection and compliance monitoring, organizational culture, metrics frameworks, and model-based security design play indispensable roles. Furthermore, limitations remain in adequately securing dynamic microservices environments and aligning DevSecOps practices with evolving regulatory frameworks. The article concludes by proposing future research directions focused on adaptive security frameworks, enhanced interpretability of AI models, and cross-domain integrations capable of addressing emerging cyber threats in retail cloud infrastructures.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

Keywords: DevSecOps, cloud security, retail cloud, compliance, microservices, machine learning, secure software development

INTRODUCTION

The contemporary landscape of software engineering has witnessed a tectonic shift towards cloud-native architectures and agile delivery practices. Retail enterprises, in their quest to meet dynamic market demands, have increasingly adopted cloud platforms to host customer-facing applications, data analytics pipelines, and backend services. This transition underscores significant opportunities for scalability, agility, and operational efficiency. However, it also amplifies security vulnerabilities, particularly as retail systems manage vast repositories of personally identifiable information (PII), financial transactions, and supply chain data. Traditional DevOps practices, which emphasize rapid iteration and continuous delivery, have been instrumental in accelerating software deployment. Yet, they frequently under-emphasize integrated security measures, creating gaps that adversaries can exploit. In response, the DevSecOps paradigm has emerged as a vital evolution, embedding security practices within DevOps workflows to ensure continuous compliance and resilience in the face of sophisticated threats.

DevSecOps represents a cultural and technical shift, uniting development, operations, and security teams under shared responsibilities for secure software delivery. According to Gangula (2025), secure DevOps strategies for retail cloud environments emphasize compliance frameworks and resilience mechanisms that can withstand both external cyberattacks and internal misconfigurations. This integration of security into the CI/CD lifecycle ensures that vulnerabilities are identified and remediated early, thereby reducing the cost and risk associated with late discovery during production. However, the complexity of cloud environments — characterized by microservices, containerization, and distributed networks — presents novel challenges for embedding security seamlessly throughout the lifecycle. These challenges are compounded by regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and other region-specific mandates that impose stringent compliance obligations on data handling and privacy.

The academic discourse on DevSecOps highlights a convergence of theoretical underpinnings and practical strategies for achieving secure and compliant delivery pipelines. For instance, systematic literature reviews on real-time security monitoring for IoT systems underscore the necessity of continuous attack detection and automated responses within DevSecOps frameworks (Ahmed Bahaa et al., 2021). Similarly, research into the use of machine learning for enhancing intrusion detection within microservices architectures demonstrates that intelligent automation can play a critical role in identifying anomalous patterns indicative of security breaches (José Flora et al., 2023). These insights

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

foreground the need for DevSecOps frameworks that are both tool-driven and strategically aligned with organizational goals.

Despite growing attention, significant gaps persist. Existing studies often focus on individual components of DevSecOps, such as toolchains or security testing approaches, without holistically addressing how these elements interact within broader organizational and regulatory contexts. There is also limited scholarship on how AI and machine learning can be practically and ethically integrated into DevSecOps workflows without introducing new risks or biases. Furthermore, models that quantify and evaluate the effectiveness of DevSecOps practices, particularly in cloud-native retail systems, are insufficiently developed.

To address these gaps, this article synthesizes interdisciplinary research, integrating insights from secure software development methodologies, machine learning applications in security, and organizational strategies for cultivating DevSecOps culture. By doing so, it provides an in-depth examination of foundational theories, current practices, and emerging innovations that collectively enhance compliance and resilience in retail cloud infrastructures.

At its core, the study seeks to answer the following overarching research questions:

1. How do DevSecOps practices contribute to compliance and resilience in cloud-native retail environments?
2. What roles do automation and AI/ML tools play in strengthening security within DevSecOps workflows?
3. What organizational, cultural, and methodological factors influence successful DevSecOps adoption?

Addressing these questions requires a comprehensive exploration of the interplay between technology, process, and people. The remainder of the article is structured to provide theoretical context, articulate methodological frameworks for assessing DevSecOps practices, analyze current results from the literature, and discuss implications for both academia and industry. By situating the analysis within the specific exigencies of retail cloud environments — where compliance and resilience are paramount — the study offers nuanced insights that transcend generic DevSecOps discussions.

METHODOLOGY

The research methodology employed in this study is fundamentally qualitative and interpretive, designed to synthesize diverse scholarly perspectives on DevSecOps practices, particularly within cloud-native retail environments. The approach draws inspiration from established frameworks for systematic literature reviews and thematic synthesis in software engineering research.

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

The initial phase involved a comprehensive literature exploration spanning academic databases, conference proceedings, and peer-reviewed journals. This search prioritized works related to DevSecOps, secure software development, cloud security, and artificial intelligence applications in security. Emphasis was placed on recent publications to ensure relevance to contemporary cloud architectures and tooling. For instance, the integration of machine learning in DevSecOps to automate security monitoring and verification has gained prominence in recent years (Guzman Camacho, 2024; Cankar et al., 2023), necessitating its inclusion in the foundational corpus.

A critical component of the methodology was the adoption of inclusion and exclusion criteria. Studies were selected if they directly addressed one or more of the following elements: automation within DevSecOps pipelines; security verification tools; AI/ML applications in security; compliance frameworks for cloud systems; and organizational strategies for secure development. Research that focused solely on general DevOps practices without explicit security integration was excluded to maintain thematic coherence.

The analytical framework involved thematic coding and synthesis. Each selected work was meticulously reviewed, with salient constructs and insights categorized under thematic clusters. For example, studies emphasizing microservices security and intrusion detection (Flora et al., 2023; Kohyarnejadfard et al., 2022) were coded under automation and threat detection themes. Those focusing on secure development methodologies (Casola et al., 2024; Casola et al., 2020) were grouped under methodological rigor and design principles. This thematic clustering facilitated a structured analysis of how different strands of research contribute to overall DevSecOps objectives.

It is important to note that while this research predominantly synthesizes existing literature, it also critically engages with the content to identify tensions, gaps, and avenues for future inquiry. Rather than merely summarizing findings, the methodology emphasizes integration and interpretation. For instance, the role of AI/ML tools in security automation is juxtaposed against challenges related to interpretability and operational reliability, drawing on contrasting perspectives within the scholarly corpus.

Limitations of the methodology include potential biases inherent in literature selection and interpretation. Given the expansive nature of DevSecOps research, some relevant works may have been inadvertently omitted. To mitigate this, the search process was iterative, revisiting databases and cross-referencing citations within key papers to uncover additional sources. Another limitation is the qualitative nature of the analysis, which, while rich in interpretive insight, does not directly quantify outcomes or empirically test hypotheses. This underscores the study's orientation toward conceptual synthesis rather than empirical measurement.

RESULTS

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

The synthesis of literature reveals that DevSecOps practices significantly enhance compliance and resilience in cloud-native retail environments. Central to these practices is the early and continuous integration of security throughout the software development lifecycle, which results in reduced vulnerability exposure and improved adherence to regulatory mandates.

One of the key findings is that automation is indispensable for effective DevSecOps implementation. Automated security verification tools integrated within CI/CD pipelines detect vulnerabilities in real time, enabling rapid remediation. For example, microservice intrusion detection frameworks that leverage automated monitoring have demonstrated efficacy in identifying deviations from normal operational patterns (Flora et al., 2023). These tools are particularly valuable in complex cloud architectures where manual inspection is infeasible due to scale and velocity.

Artificial intelligence and machine learning have emerged as transformative forces within DevSecOps automation. Research indicates that machine learning models can …analyze extensive logs, trace microservice communications, and detect anomalous behaviors that traditional rule-based systems might miss (Kohyarnejadfard et al., 2022; Guzman Camacho, 2024). Such AI-enhanced monitoring supports predictive security, allowing teams to proactively mitigate potential breaches before they escalate. However, the integration of AI/ML also introduces challenges, including model interpretability, false positives, and bias, which must be carefully managed to avoid undermining security objectives (Fu et al., 2024; Pakalapati et al., 2023). The findings underscore that technological sophistication alone is insufficient; the human, organizational, and procedural dimensions remain critical.

Methodologically, model-based approaches to secure software development and quantitative Security-by-Design frameworks have shown promise in providing structured guidance for implementing DevSecOps in cloud-native retail systems (Casola et al., 2024; Casola et al., 2020). These frameworks not only codify best practices for vulnerability assessment but also embed compliance monitoring directly into development processes, ensuring that regulatory requirements are consistently met. For instance, Gangula (2025) emphasizes that in retail cloud environments, DevSecOps strategies must align with both PCI DSS and local privacy regulations, requiring a continuous loop of verification, audit, and remediation. Integrating compliance metrics into the development lifecycle enhances accountability and provides measurable assurance to stakeholders.

The literature further highlights the significance of microservice-oriented security. With retail systems increasingly adopting containerized microservices, the attack surface expands, necessitating specialized detection mechanisms (Flora et al., 2023; Dong & Kotenko, 2025). Automated tools capable of inspecting container configurations, tracking API communications, and performing anomaly detection have proven effective in maintaining operational security. Research by Petrović et al. (2022) demonstrates that Python-based DevSecOps tools can automate Infrastructure-as-Code (IaC) inspections, significantly reducing configuration-related vulnerabilities. These findings suggest that

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

comprehensive DevSecOps adoption in retail clouds requires a multi-layered approach: combining automated technical safeguards with governance, process discipline, and continuous monitoring.

Organizational culture emerges as a decisive factor in the successful implementation of DevSecOps. Studies reveal that cultural adoption—where development, security, and operations teams share responsibility for security—is essential for embedding security as a default practice rather than an afterthought (Sánchez-Gordón & Colomo-Palacios, 2020; Tomas et al., 2019). Cultural misalignment, by contrast, can impede the adoption of automated tools and compromise the integrity of security processes. Furthermore, metrics-driven oversight provides essential feedback loops, enabling continuous improvement of security practices while ensuring compliance objectives are met (Prates et al., 2019).

Critical gaps persist despite advancements. Automated tools, while effective in monitoring and anomaly detection, are challenged by the dynamic nature of cloud-native retail environments. Microservices can scale rapidly, and complex service meshes introduce unpredictability in communication patterns, potentially leading to undetected vulnerabilities (Ibrahim et al., 2022; Okubo & Kaiya, 2022). Moreover, regulatory frameworks evolve constantly, creating the need for adaptive compliance mechanisms capable of integrating into DevSecOps pipelines without introducing friction. Addressing these limitations requires ongoing research into adaptive AI models, cross-domain security orchestration, and standardized metrics for evaluating DevSecOps effectiveness in retail contexts.

DISCUSSION

The findings from the literature synthesis indicate a deeply interwoven relationship between technological, procedural, and cultural dimensions of DevSecOps in cloud-native retail systems. Conceptually, DevSecOps embodies the principle of “security as code,” where security is embedded into every stage of software development rather than treated as a discrete, post-development activity (Lombardi & Fanton, 2023). This paradigm shift aligns with the broader movement toward proactive cybersecurity strategies, emphasizing resilience, predictability, and compliance. Gangula (2025) articulates that for retail cloud infrastructures, the stakes are particularly high: sensitive customer data, financial transactions, and regulatory obligations converge to create an environment in which any security lapse can have profound operational and reputational consequences.

From a theoretical standpoint, the integration of AI and machine learning into DevSecOps pipelines represents a critical innovation. By enabling predictive threat modeling and automated anomaly detection, AI augments human capacity to manage complex and dynamic cloud environments (Fu et al., 2024; Guzman Camacho, 2024). However, the literature stresses that the introduction of AI is not a panacea. Model interpretability, the risk of false positives, and potential biases must be carefully addressed to ensure that AI-driven insights are both reliable and actionable (Dong & Kotenko, 2025).

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

Scholars argue that interpretability frameworks and continuous retraining mechanisms are necessary to maintain trust and operational efficacy.

The discussion also underscores the necessity of cultural alignment and process governance. Successful DevSecOps adoption is contingent upon the breakdown of traditional silos between development, operations, and security teams (Sánchez-Gordón & Colomo-Palacios, 2020; Tomas et al., 2019). Establishing shared accountability and fostering a culture of continuous security awareness ensures that automated tools are effectively utilized and that vulnerabilities are addressed promptly. Moreover, the integration of compliance metrics and audit-ready reporting into the development lifecycle ensures that regulatory obligations are consistently met, mitigating legal and financial risk (Gangula, 2025; Casola et al., 2024).

Comparative analysis reveals that while automated and AI-enhanced tools are increasingly sophisticated, human oversight remains indispensable. Literature on secure software development methodologies demonstrates that model-based and Security-by-Design approaches complement technological solutions by providing structured guidance for risk assessment, vulnerability management, and compliance verification (Casola et al., 2020; Casola et al., 2024). These frameworks act as scaffolding for AI-driven automation, ensuring that rapid development cycles do not compromise security integrity.

Notably, gaps remain in current research. Despite advancements in automated detection, the scalability and adaptability of these solutions in highly dynamic microservices architectures require further exploration (Kohyarnejadfard et al., 2022; Petrović et al., 2022). Moreover, the alignment of AI-enhanced DevSecOps practices with evolving regulatory frameworks, particularly in multi-jurisdictional retail operations, remains an underdeveloped area. Future research should prioritize adaptive compliance mechanisms capable of incorporating real-time regulatory changes, as well as cross-domain security orchestration that harmonizes AI predictions with human oversight.

The discussion further explores the implications of integrating DevSecOps into the strategic planning of retail enterprises. Beyond operational security, DevSecOps practices can foster trust among stakeholders, including customers, partners, and regulators. By demonstrating proactive risk management and compliance adherence, organizations can differentiate themselves competitively while mitigating the financial and reputational impact of potential security incidents (Rajapakse et al., 2021; Alouffi et al., 2021). Moreover, the deployment of metrics-driven governance frameworks allows enterprises to quantify the effectiveness of security initiatives, identify areas for improvement, and guide investment in infrastructure, tools, and personnel.

From a methodological lens, the article emphasizes that DevSecOps adoption is not a one-size-fits-all endeavor. Variability in organizational scale, system complexity, regulatory context, and technological infrastructure necessitates tailored approaches. Case studies suggest that enterprises that integrate model-based security, AI-driven monitoring, and cultural alignment tend to achieve superior outcomes

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

in both compliance and resilience (Okubo & Kaiya, 2022; Cankar et al., 2023). Conversely, organizations that rely solely on automation without cultivating a security-conscious culture or structured methodologies often experience limited effectiveness, illustrating the interdependency of technology, process, and people.

The discussion also critically engages with the interplay between regulatory compliance and technological innovation. In retail cloud systems, compliance requirements such as PCI DSS, GDPR, and other regional mandates impose constraints that can conflict with rapid development practices. DevSecOps frameworks, particularly when augmented with AI and machine learning, offer mechanisms to reconcile these competing demands by embedding continuous compliance checks into the CI/CD pipeline (Gangula, 2025; Ibrahim et al., 2022). Nevertheless, research indicates that the dynamic nature of cloud environments, coupled with frequent regulatory updates, poses ongoing challenges, underscoring the need for adaptive security frameworks capable of evolving alongside technological and legal landscapes.

Finally, theoretical interpretation of the literature suggests that the convergence of AI-enhanced automation, structured security methodologies, and cultural alignment represents the future trajectory of DevSecOps in retail cloud contexts. Scholars advocate for hybrid frameworks that combine predictive analytics with human oversight, standardized metrics with continuous feedback, and security-by-design principles with agile development practices (Casola et al., 2024; Guzman Camacho, 2024). This integrated approach not only enhances operational resilience but also ensures that security, compliance, and business objectives are mutually reinforcing rather than competing priorities.

The limitations highlighted in the discussion emphasize areas for future research. While automated tools and AI offer significant promise, empirical validation in large-scale, real-world retail cloud deployments remains limited. Longitudinal studies examining the effectiveness of integrated DevSecOps frameworks across diverse organizational contexts are necessary to establish best practices. Additionally, ethical considerations surrounding AI-driven decision-making in security, including bias mitigation, transparency, and accountability, warrant deeper investigation. Finally, exploring cross-industry applications and standardizing metrics for evaluating DevSecOps efficacy could provide a foundation for global best practices in secure cloud-native development.

CONCLUSION

In conclusion, the integration of DevSecOps practices in cloud-native retail environments offers a transformative pathway for achieving both operational resilience and regulatory compliance. By embedding security into the continuous development lifecycle, leveraging AI and machine learning for predictive threat detection, and fostering a culture of shared accountability, retail enterprises can navigate the complex landscape of cyber threats while maintaining agility and scalability. The literature underscores that technological tools, while indispensable, must be complemented by structured

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

methodologies and cultural alignment to ensure robust security outcomes. Gangula (2025) reinforces this imperative by highlighting strategies tailored to retail cloud infrastructures, emphasizing compliance and resilience as core objectives. Despite notable advancements, gaps remain in scalability, adaptive compliance, and empirical validation, presenting fertile ground for future research. As the digital landscape continues to evolve, the synergistic integration of automation, human oversight, and regulatory alignment will define the next generation of secure, resilient, and compliant retail cloud systems.

REFERENCES

1. Ahmed Bahaa, Ahmed Abdelaziz, Abdalla Sayed, Laila Elfangary, and Hanan Fahmy. 2021. Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review. Information 12, 4 (2021), 154.
2. José Flora, Miguel Teixeira, and Nuno Antunes. 2023. µDetector: Automated Intrusion Detection for Microservices. In 2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). 748–752.
3. Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. 2020. A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. Journal of Systems and Software 163 (2020), 110537.
4. Rupesh Raj Karn, Prabhakar Kudva, and Ibrahim Abe M. Elfadel. 2019. Dynamic Autoselection and Autotuning of Machine Learning Models for Cloud Network Analytics. IEEE Transactions on Parallel and Distributed Systems 30, 5 (2019), 1052–1064.
5. Gangula, S. 2025. Secure DevOps in retail cloud: Strategies for compliance and resilience. The American Journal of Engineering and Technology, 7(05), 109-122. https://doi.org/10.37547/tajet/Volume07Issue05-09
6. Valentina Casola, Alessandra De Benedictis, Carlo Mazzocca, and Vittorio Orbinato. 2024. Secure software development and testing: A model-based methodology. Comput. Secur. 137, C (Feb. 2024), 16 pages.
7. Amr Ibrahim, Ahmed H. Yousef, and Walaa Medhat. 2022. DevSecOps: A Security Model for Infrastructure as Code Over the Cloud. In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC). 284–288.
8. Tsakani Mboweni, Themba Masombuka, and Cyrille Dongmo. 2022. A systematic review of machine learning devops. In 2022 international conference on electrical, computer and energy technologies (ICECET). IEEE, 1–6.
9. Michael Fu, Jirat Pasuksmit, and Chakkrit Tantithamthavorn. 2024. Ai for devsecops: A landscape and future opportunities. ACM Transactions on Software Engineering and Methodology (2024).
10. Matija Cankar, Nenad Petrovic, Joao Pita Costa, Ales Cernivec, Jan Antic, Tomaz Martincic, and Dejan Stepec. 2023. Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps. In Companion of the 2023 ACM/SPEC International Conference on Performance

Volume11 Issue02, Febuary-2026, pg. 01-10

Published Date: - 01-02-2026

E-ISSN: 2536-7919
P-ISSN: 2536-7900

Engineering (Coimbra, Portugal) (ICPE '23 Companion). Association for Computing Machinery, New York, NY, USA, 201–205.

11. Nenad Petrović, Matija Cankar, and Anže Luzar. 2022. Automated Approach to IaC Code Inspection Using Python-Based DevSecOps Tool. In 2022 30th Telecommunications Forum (TELFOR). 1–4.

12. Luis Prates, João Faustino, Miguel Silva, and Rúben Pereira. 2019. Devsecops metrics. In Information Systems: Research, Development, Applications, Education: 12th SIGSAND/PLAIS EuroSymposium 2019, Gdansk, Poland, September 19, 2019, Proceedings 12. Springer, 77–90.

13. Huiyao Dong and Igor Kotenko. 2025. Cybersecurity in the AI era: analyzing the impact of machine learning on intrusion detection. Knowledge and Information Systems (2025), 1–52.

14. Yérom-David Bromberg and Louison Gitzinger. 2020. DroidAutoML: A Microservice Architecture to Automate the Evaluation of Android Machine Learning Detection Systems. In Distributed Applications and Interoperable Systems: 20th IFIP WG 6.1 International Conference, DAIS 2020, Held as Part of the 15th International Federated Conference on Distributed Computing Techniques, DisCoTec 2020, Valletta, Malta, June 15–19, 2020, Proceedings (Valletta, Malta). Springer-Verlag, Berlin, Heidelberg, 148–165.

15. R. Kumar, R. Goyal, Modeling Continuous Security: A Conceptual Model for Automated DevSecOps using Open-Source Software over Cloud, Comput. Secur. 97 (2020) 101967.

16. Federico Lombardi and Alberto Fanton. 2023. From DevOps to DevSecOps is not enough. CyberDevOps: an extreme shifting-left architecture to bring cybersecurity within software security lifecycle pipeline. Software Quality Journal 31, 2 (April 2023), 619–654.

17. Ahmed Bahaa, et al. 2021. Monitoring real-time security attacks for IoT systems using DevSecOps: a systematic literature review.