INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 12, issue 11 (2025)

Embedding Security In Agile Cloud Environments: A Multi-Dimensional Devops Approach For Retail Systems

Artemis N. Kouroupi
University of Thessaloniki, Greece

Abstract: The rapid proliferation of cloud computing within the retail sector has created unparalleled opportunities for scalability, customer engagement, and operational agility. Yet this paradigm shift has simultaneously infused complex security and compliance challenges due to the distributed, dynamic, and externally managed nature of cloud infrastructures. Secure DevOps—or DevSecOps in practice—emerges as a transformative approach that seeks to integrate security practices directly into the software development lifecycle, thereby reducing vulnerabilities while supporting rapid delivery. This article delineates an interdisciplinary analysis of Secure DevOps frameworks with particular emphasis on cloud deployments in the retail domain. Drawing upon Gangula's foundational insights into compliance strategies and resilience mechanisms for retail cloud systems (Gangula, 2025), this research critically synthesizes theoretical foundations, historical developments, empirical evidence, and current scholarly debates surrounding the implementation of security in agile software pipelines. We explore the ontological distinctions between DevOps, SecDevOps, and DevSecOps, the tension between speed and security, regulatory imperatives such as PCI DSS, GDPR, and emerging international standards like IEC 62443, and the nuanced operationalization of security automation, cultural alignment, and risk management. The analysis extends to systemic challenges such as resistance to cultural change, the complexity of compliance verification within continuous deployment, and measurement barriers in security metrics. By juxtaposing theoretical frameworks with industry case studies—including historical cyber breaches affecting financial and retail institutions—the article illuminates the role of Secure DevOps in enhancing resilience and adaptive capacity. Conclusions advance a model for integrating security auditing, continuous monitoring, and resilience engineering, offering a roadmap for future empirical research and practice innovation in secure cloud-native retail systems.

Keywords: Secure DevOps, DevSecOps, Retail Cloud Security, Compliance, Resilience, Continuous Deployment, Security Automation

INTRODUCTION

The transformation of traditional retail systems into cloud-centric architectures has been one of the most consequential technological shifts of the 21st century. Driven by the promise of scalability, cost optimization, and omnichannel customer experiences, retailers have embraced cloud computing at an unprecedented pace. However, this transition has concomitantly introduced significant security and compliance challenges—especially in domains that handle highly sensitive consumer data, payment information, and supply chain intelligence. Indeed, the integration of cloud platforms amplifies vectors for exploitation, as evidenced by multiple high-profile breaches in financial and retail institutions where millions of records were compromised (CNN, 2019; Economic Times, 2025). The evolving threat landscape and the strictures of regulatory frameworks necessitate robust approaches that align rapid software delivery with proactive security safeguards.

Among the emergent paradigms designed to reconcile agility with security is Secure DevOps (often operationalized as DevSecOps), which infuses security practices into the development and operations lifecycle

rather than treating them as discrete stages or post-hoc checks. The foundational argument for Secure DevOps is that embedding security earlier in development cycles enhances compliance, reduces cumulative vulnerabilities, and promotes organizational resilience (Mohan & Othmane, 2016; Myrbakken & Colomo-Palacios, 2017). This repositioning of security from an impediment to an enabler aligns with wider imperatives in digital transformation strategies. Yet, the research landscape reveals both conceptual ambiguities and implementation difficulties that impede consistent adoption across industries—especially within highly regulated environments such as retail, healthcare, and finance (Cham Rajapakse et al., 2022; Yasar, 2017).

While recent studies, such as Gangula's analysis of Secure DevOps strategies for retail cloud systems, provide targeted insights into compliance and resilience mechanisms (Gangula, 2025), comprehensive frameworks that reconcile theoretical constructs with empirical and practice-based evidence remain underdeveloped. The question at the heart of this research is: How can Secure DevOps be systematically conceptualized and operationalized to meet stringent compliance requirements while preserving the agility and innovation promised by cloud computing in the retail sector?

This question sits at the intersection of multiple scholarly traditions: software engineering, cybersecurity, compliance theory, organizational studies, and cloud computing research. The concept of DevOps itself emerged in the late 2000s as a response to the bifurcation between software development and IT operations—seeking to collapse historical silos through cultural, technical, and process innovations. Yet, DevOps did not initially confront security concerns with the intensity now required in today's threat environment. As early as the mid-2010s, Mohan and Othmane questioned whether SecDevOps was a substantive paradigm shift or merely a marketing tag layered on DevOps practices (Mohan & Othmane, 2016). Myrbakken and Colomo-Palacios's multivocal literature review further revealed divergent interpretations of where security practices fit within DevOps pipelines, noting wide variability in practices ranging from ad hoc security checks to fully automated security gates within CI/CD workflows (Myrbakken & Colomo-Palacios, 2017).

Understanding the historical evolution of these frameworks is critical. Initially, DevOps sought to facilitate rapid release cycles through practices like infrastructure as code, continuous integration/continuous deployment (CI/CD), and microservices architectures. However, traditional security approaches were largely external to these accelerative practices, often resulting in bottlenecks, delayed releases, and increased operational risk. Incident analyses in other sectors underscore the cost of such disjunctions: for example, breaches in payment systems and banking infrastructures—such as the Capital One breach in 2019—illustrate how inadequate integration of security into velocity-oriented pipelines can lead to catastrophic data exposure (CNN, 2019). Similarly, massive debit card compromises in major Indian banks highlighted the systemic risks embedded within legacy and cloud-hybrid systems that lacked robust automated security flows (Economic Times, 2025).

The field responded by broadening DevOps to incorporate security considerations, leading to what is now commonly called DevSecOps. This approach emphasizes the automation of security testing, configuration management, identity and access controls, and compliance verification throughout the software lifecycle. Wilde et al. (2016) documented the need for embedding defenses directly within deployment processes, arguing that reactive approaches were insufficient for modern threat landscapes. Other researchers have highlighted the complexity of integrating security without undermining the efficiencies gained from DevOps practices (Cham Rajapakse et al., 2022; Yasar & Kontostathis, 2016). Some have even problematized the term itself, arguing that without substantive shifts in organizational culture and measurement systems, DevSecOps risks being a nominal label rather than a functional practice (Mohan & Othmane, 2016).

In addition to conceptual debates, regulatory frameworks exert considerable influence on how Secure DevOps must be implemented in retail. Standards such as the Payment Card Industry Data Security Standard (PCI DSS) require demonstrable controls for encryption, access management, audit logging, and vulnerability management—each of which must be embedded within cloud artifacts and development pipelines. International standards like IEC 62443, though originating in industrial control systems, offer insights into risk and requirement validation in secure software lifecycles (Göttel et al., 2023). Yet the translation of these

standards into automated compliance pipelines remains a formidable challenge, particularly as retail firms must adapt to both international and region-specific data protection laws. As retail ecosystems become more interconnected—with third-party vendors, supply chain partners, and customer-facing applications—the complexities of accountability and security assurance multiply.

A critical element in this landscape is organizational culture. The integration of security into DevOps is not merely a technological problem but an institutional transformation that requires reconciling operational, developmental, and compliance imperatives. Practices such as "shift-left security," where security testing occurs early in development cycles, have gained traction in this regard, yet they often require substantial retraining, tooling investments, and shifts in performance metrics. Without careful attention to human factors and governance models, security automation can become a point of friction rather than an accelerator.

Empirical studies of DevSecOps adoption further reveal barriers and facilitators that shape organizational outcomes. For instance, Rajapakse et al. (2022) synthesize challenges such as legacy system integration, skill gaps, and resistance to change, alongside solutions involving modular architectures, automated testing frameworks, and cross-functional training programs. Complementary research in regulated settings, such as automotive software and critical infrastructure, highlights bespoke integration models for security audits and resilience engineering (Achuthan & Alimohideen, 2024; Yu et al., 2024). However, these studies often lack comprehensive applicability to retail cloud contexts, which combine high throughput, consumer data sensitivity, and peak-demand variability.

In this light, the present research aims to construct an integrative theoretical and practical framework for Secure DevOps tailored to the retail cloud domain. By synthesizing extant literature, cross-sector insights, and compliance imperatives, we articulate a model that supports resilience, agility, and governance integrity.

The remainder of this article is organized as follows: the Methodology section outlines the analytical approach and theoretical lens employed; the Results section presents interpretive findings grounded in literature synthesis; the Discussion section offers deep theoretical engagement, comparative perspectives, and future research directions; and the Conclusion summarizes core insights while highlighting practical implications and research trajectories.

METHODOLOGY

This research employs a qualitative, integrative literature synthesis methodology to develop a comprehensive understanding of Secure DevOps frameworks in retail cloud environments. Unlike purely quantitative approaches that measure discrete outcomes, this methodology emphasizes conceptual development, theoretical elaboration, and the synthesis of empirical insights across multiple domains. The rationale for this approach lies in the interdisciplinary nature of Secure DevOps, which intersects software engineering, cybersecurity, organizational studies, compliance frameworks, and cloud infrastructure management. Given the complexity of these domains and the scarcity of standardized empirical datasets, a qualitative synthesis allows for the exploration of nuanced relationships, latent tensions, and emerging best practices.

The first step of the methodology involved systematic identification and collection of relevant scholarly and practitioner literature. Primary sources included peer-reviewed journal articles, conference proceedings, and industry white papers covering DevOps, DevSecOps, SecDevOps, cloud security, and compliance in regulated environments (Mohan & Othmane, 2016; Wilde et al., 2016; Cham Rajapakse et al., 2022). Additionally, domain-specific case studies and high-profile cyber incidents were analyzed to contextualize theoretical findings within real-world retail and financial environments (CNN, 2019; Economic Times, 2025). Gangula's (2025) work on retail cloud security provided the foundational framework for integrating compliance and resilience strategies, serving as the anchor point for the subsequent synthesis. Supplementary materials included technical standards and regulatory documents such as PCI DSS and IEC 62443, which informed discussions of governance, automated compliance, and risk management practices.

Once the corpus was identified, thematic coding was applied to extract key concepts, implementation strategies, and empirical findings. Codes included: "security integration points," "automation practices,"

"cultural barriers," "regulatory compliance," "resilience metrics," and "cloud-specific threats." This process allowed for a comparative mapping of approaches across diverse organizational contexts, identifying recurring patterns as well as anomalous cases that provided counterpoints to mainstream assumptions (Myrbakken & Colomo-Palacios, 2017; Yasar, 2017). The coding process was iterative, with multiple rounds of refinement to ensure both comprehensiveness and conceptual clarity. Particular attention was paid to distinguishing between superficial labeling of security practices (e.g., marketing-driven "SecDevOps") versus substantive, operationally embedded security mechanisms (Mohan & Othmane, 2016).

The second stage involved constructing a conceptual framework that aligns DevSecOps principles with the specific operational realities of retail cloud environments. This framework incorporates four interdependent dimensions: technical automation, process governance, regulatory compliance, and organizational culture. Within the technical dimension, CI/CD pipelines, automated testing, vulnerability scanning, infrastructure as code, and monitoring were analyzed for efficacy and limitations (Afifah et al., 2024; Aktas & Can, 2024). Process governance examines workflow standardization, auditability, and the embedding of risk assessment practices. Regulatory compliance integrates adherence to PCI DSS, GDPR, and emerging standards like IEC 62443, emphasizing automated verification, logging, and reporting mechanisms. Organizational culture addresses human factors, cross-functional collaboration, training, and incentive structures, acknowledging that technology adoption alone is insufficient without alignment with values and behaviors (Laukkarinen et al., 2018; Michener & Clager, 2016).

Limitations of this methodological approach are acknowledged. First, qualitative synthesis cannot provide generalizable predictive models in the way that large-scale quantitative analyses can. Second, the dynamic nature of both cloud technologies and cybersecurity threats introduces temporal variability; conclusions drawn may require continuous revision as novel attack vectors emerge. Third, the literature itself exhibits gaps, particularly in sector-specific studies of Secure DevOps in retail cloud infrastructures, necessitating cautious extrapolation from analogous domains such as automotive software or critical infrastructure (Achuthan & Alimohideen, 2024; Yu et al., 2024). Despite these limitations, the methodology is robust in generating a nuanced, theory-informed, and practically relevant understanding of Secure DevOps implementation.

Data interpretation follows a structured analytic protocol that integrates narrative synthesis with cross-case comparison. Key thematic relationships were evaluated based on frequency, contextual relevance, and interconnectivity with regulatory and technical considerations. Findings were iteratively refined to reconcile conflicting perspectives and identify latent tensions, such as the trade-offs between speed and security, or automation and human oversight. To ensure rigor, each thematic assertion was cross-referenced with multiple sources, reinforcing validity and reducing the risk of idiosyncratic conclusions. Finally, the methodology emphasizes translational value: the analytical outcomes are designed to inform both academic debate and practical application in retail cloud environments, bridging the gap between conceptual theory and operational execution.

RESULTS

The synthesis of literature and empirical observations reveals several critical insights regarding Secure DevOps implementation in retail cloud contexts. First, the integration of security practices directly within the DevOps pipeline substantially reduces vulnerability exposure and enhances resilience, supporting Gangula's (2025) assertion that compliance-oriented strategies are indispensable in cloud-based retail environments. Technical implementations such as automated vulnerability scanning, container image security, infrastructure as code verification, and continuous monitoring are central to this process. Afifah et al. (2024) and Aktas & Can (2024) highlight that these mechanisms not only detect threats proactively but also provide audit trails necessary for regulatory compliance, demonstrating the dual functional and governance value of embedded security.

Second, the literature underscores the importance of cultural transformation within organizations. DevSecOps adoption is frequently hindered by entrenched silos, resistance to change, and skill gaps (Rajapakse et al., 2022). Successful interventions often involve structured cross-functional collaboration, continuous security

education, and performance incentives aligned with security metrics. Such practices support the shift-left paradigm, where security considerations are addressed early in the development lifecycle rather than retrospectively (Myrbakken & Colomo-Palacios, 2017; Mohan & Othmane, 2016). This cultural dimension is particularly salient in retail, where rapid release cycles and seasonal demand spikes can otherwise undermine consistent security adherence.

Third, regulatory and compliance imperatives exert substantial influence on Secure DevOps strategies. Organizations in the retail sector must navigate a complex matrix of international and domestic regulations, including PCI DSS, GDPR, and emerging security standards. Automated compliance verification integrated within CI/CD pipelines reduces the likelihood of breaches and fines, while facilitating continuous reporting and auditability (Yasar, 2017; Göettel et al., 2023). Gangula (2025) emphasizes that these strategies not only ensure legal conformity but also enhance customer trust and brand resilience—a critical factor in competitive retail markets.

Fourth, the results illuminate trade-offs between operational speed and security rigor. While automation and CI/CD practices accelerate release cycles, they may also obscure vulnerabilities if not carefully configured. For instance, insufficiently monitored pipelines can allow misconfigurations, credential exposure, or container vulnerabilities to propagate rapidly, a phenomenon documented in financial breaches such as the Capital One case (CNN, 2019). Mitigation requires layered defense strategies, continuous monitoring, and integrated feedback loops that dynamically adjust risk thresholds in real-time. The literature suggests that such resilience-oriented approaches are most effective when combined with organizational policies that enforce accountability and cross-functional coordination (Laukkarinen et al., 2018; Michener & Clager, 2016).

Fifth, historical analyses of cyber incidents provide instructive counterexamples that reinforce the value of Secure DevOps. Notable events include the large-scale debit card compromises in Indian banks, the Bangladesh cyber heist, and ransomware attacks against Chilean banking institutions (Economic Times, 2025; Dhaka Tribune, 2025; Security Affairs, 2020). In each case, vulnerabilities often originated from inadequate integration of security practices within deployment pipelines, delayed patching, or insufficient monitoring. By contrast, organizations implementing holistic Secure DevOps frameworks, as described in Gangula (2025), demonstrate measurable reductions in incident frequency, faster recovery times, and enhanced compliance posture. These findings support the argument that Secure DevOps is not merely a conceptual ideal but an operationally effective strategy when systematically implemented.

Finally, emerging technologies such as AI-assisted monitoring, blockchain-based audit trails, and code obfuscation in CI/CD pipelines offer promising avenues to reinforce security and resilience (Afifah et al., 2024; Yu et al., 2024). These innovations facilitate predictive threat detection, automated anomaly response, and tamper-evident compliance verification, representing a forward-looking extension of traditional DevSecOps practices. The literature, however, cautions that these technologies must be contextually integrated and subject to human oversight to avoid overreliance on automated systems.

DISCUSSION

The theoretical interpretation of these findings emphasizes the multifaceted nature of Secure DevOps as both a technical and socio-organizational construct. By situating security within agile development practices, organizations effectively reconcile the historically conflicting imperatives of speed and protection. Gangula (2025) argues convincingly that in retail cloud systems, resilience and compliance are inseparable from operational success, as breaches can erode trust, reduce revenues, and provoke regulatory penalties. This perspective is reinforced by comparative analyses of financial and retail cyber incidents, which reveal consistent patterns of failure when security is treated as ancillary rather than integrative (CNN, 2019; Economic Times, 2025; Security Affairs, 2020).

A critical theoretical contribution is the delineation of four interdependent dimensions—technical automation, process governance, regulatory compliance, and organizational culture—that collectively define the efficacy of Secure DevOps implementations. Technical automation encompasses CI/CD security gates, vulnerability

scanning, and infrastructure as code verification, while process governance ensures standardized workflows, accountability, and traceable audit trails (Afifah et al., 2024; Aktas & Can, 2024). Regulatory compliance addresses the complex matrix of international and domestic standards, facilitating automated verification and reporting (Yasar, 2017; Göettel et al., 2023). Organizational culture remains the most variable and challenging dimension, requiring sustained investment in training, incentives, and cross-functional collaboration to enable a security-conscious mindset (Rajapakse et al., 2022; Laukkarinen et al., 2018).

Comparative scholarly perspectives reveal both consensus and contention. Mohan & Othmane (2016) critique SecDevOps as potentially a marketing buzzword, emphasizing the risk of superficial adoption without substantive process integration. This critique aligns with empirical observations of organizations that label pipelines as "Secure DevOps" without embedding automated checks, audit trails, or risk-based governance. In contrast, Myrbakken & Colomo-Palacios (2017) and Cham Rajapakse et al. (2022) present evidence of successful integration when technical, regulatory, and cultural dimensions are addressed concurrently. Gangula (2025) situates these findings within retail cloud contexts, demonstrating that adherence to automated compliance protocols and resilience frameworks materially reduces operational risk, highlighting the importance of sector-specific strategies.

The discussion further emphasizes the inherent tensions and trade-offs in Secure DevOps implementation. For example, the acceleration of release cycles can conflict with exhaustive security verification, while automated compliance mechanisms may encounter false positives that disrupt deployment schedules. Risk management frameworks, therefore, must incorporate adaptive feedback loops, context-sensitive thresholds, and human oversight to ensure that security measures do not inadvertently compromise operational agility (Wilde et al., 2016; Achuthan & Alimohideen, 2024). Moreover, as cloud infrastructures evolve toward hybrid and multi-cloud architectures, the complexity of security orchestration, inter-service trust, and cross-platform compliance verification intensifies. These challenges necessitate ongoing research into scalable, automated, and standards-compliant security frameworks that can operate across heterogeneous cloud environments.

Limitations identified in the literature point to gaps that future research must address. There is a relative paucity of longitudinal studies assessing Secure DevOps efficacy over extended deployment cycles in high-volume retail environments. Furthermore, cross-cultural organizational factors, especially in multinational retail operations, remain underexplored. Questions around measurement—such as defining appropriate security KPIs, resilience metrics, and risk-adjusted performance indicators—require systematic empirical investigation. The integration of emerging technologies such as AI, blockchain, and predictive analytics introduces both opportunities and uncertainties that necessitate rigorous evaluation in operational settings (Yu et al., 2024; Afifah et al., 2024).

The implications for practice are manifold. Retail organizations must recognize Secure DevOps as a holistic construct that encompasses not only technical mechanisms but also cultural alignment, process governance, and regulatory adherence. Investments in automation, continuous monitoring, and secure coding practices must be complemented by structured training, incentive structures, and leadership engagement. Sector-specific standards should be operationalized within automated pipelines to ensure consistent compliance. By integrating these dimensions, organizations can achieve both operational agility and security resilience—a combination increasingly recognized as a competitive differentiator in digital retail markets.

Finally, the synthesis of literature suggests a future research agenda focused on hybrid modeling approaches that combine qualitative assessments, simulation, and quantitative metrics to evaluate the efficacy of Secure DevOps frameworks. Experimental studies investigating cultural interventions, risk-adjusted compliance strategies, and adaptive automation protocols are particularly warranted. The integration of cross-sector insights—from automotive, critical infrastructure, and financial systems—can inform the development of robust, generalizable models applicable to retail cloud environments (Lazarus et al., 2024; Achuthan & Alimohideen, 2024). These directions underscore the ongoing evolution of Secure DevOps as both an applied and theoretical discipline, with implications for cybersecurity, organizational resilience, and regulatory governance.

CONCLUSION

In conclusion, Secure DevOps represents a pivotal paradigm for reconciling the competing imperatives of rapid software delivery, regulatory compliance, and operational resilience within retail cloud environments. The integration of security practices within DevOps pipelines—spanning automated testing, continuous monitoring, compliance verification, and cultural transformation—substantially enhances resilience against cyber threats while supporting agility and innovation. Gangula (2025) provides a compelling framework for aligning security and compliance in retail cloud contexts, demonstrating the operational and strategic value of holistic Secure DevOps adoption. While challenges remain—including cultural resistance, measurement complexities, and evolving threat landscapes—the evidence suggests that organizations adopting an integrative, multi-dimensional approach are better positioned to navigate the complexities of modern cloud-based retail systems. Future research should focus on longitudinal, cross-sector analyses, adaptive automation strategies, and empirically grounded metrics to refine both theory and practice. The sustained adoption of Secure DevOps thus emerges as a critical enabler for secure, resilient, and competitive digital retail operations in the 21st century.

REFERENCES

1. Yu, W.; Qian, J.; Xu, R.; Jin, C.; Fang, H.; Shi, X. Improving Substation Network Security with DevSecOps and AIOps. In Proceedings of the 2024 IEEE 10th Conference on Big Data Security on Cloud, BigDataSecurity, New York, NY, USA, 10–12 May 2024; pp. 113–118.

2. Göttel, C.; Kabir-Querrec, M.; Kozhaya, D.; Sivanthi, T.; Vuković, O. Qualitative Analysis for Validating IEC 62443-4-2 Requirements in DevSecOps. In Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Porto, Portugal, 9–12 September 2023.

3. Afifah, A.S.; Kabetta, H.; Setia Buana, I.K.; Setiawan, H. Code Obfuscation in CI/CD Pipelines for Enhanced DevOps Security. In Proceedings of the 2024 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics, ICoABCD, Bali, Indonesia, 20–21 August 2024; pp. 137–142.

4. Achuthan, B.; Alimohideen, M.A. Shifting Gears: Integrating Security Audits into Automotive DevSecOps. In Proceedings of the 2024 International Conference on Vehicular Technology and Transportation Systems (ICVTTS), Bangalore, India, 27–28 September 2024; pp. 1–6.

5. Lazarus, J.I.; Truett, L.; Fischer, B.; Kershner, C. DevSecOps Process Assessment Collaboration Tool: A Novel Method to Inject R&M Into Agile Development. In Proceedings of the Annual Reliability and Maintainability Symposium, Albuquerque, NM, USA, 22–25 January 2024.

6. Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A Multivocal Literature Review. In International Conference on Software Process Improvement and Capability Determination (pp. 17-29).

7. Mohan, V., & Othmane, L. B. (2016). SecDevOps: is it a marketing buzzword? -mapping research on security in DevOps. In Availability, Reliability and Security (ARES), 2016 11th International Conference on (pp. 542-547).

8. Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. Information and Software Technology, 141, 106700.

9. 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

10. IBM. What is DevSecOps? Available online: https://www.ibm.com/think/topics/devsecops (accessed on 5 October 2021).

11. Economic Times. 3.2 million Debit Cards Compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis Worst Hit. Available online: https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms (accessed on 12 July 2025).

12. Wilde, N., Eddy, B., Patel, K., Cooper, N., Gamboa, V., Mishra, B., & Shah, K. (2016). Security for DevOps Deployment Processes: Defences, Risks, Research Directions. International Journal of Software Engineering & Applications (IJSEA), 7(6).

13. Yasar, H. (2017). Implementing Secure DevOps assessment for highly regulated environments. In Proceedings of the 12th International Conference on Availability, Reliability and Security (p. 70).

14. CNN. A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts. Available online: https://www.cnn.com/2019/07/29/business/capital-one-data-breach (accessed on 29 July 2019).

15. Laukkarinen, T., Kuusinen, K., Mikkonen, T. Regulated software meets devops. Information and Software Technology 97 (2018).

16. IBM. What is DevSecOps and Why Is It So Important? Available online: https://developer.ibm.com/articles/devsecops-what-and-why/ (accessed on 10 March 2022).

17. Dhaka Tribune. The Great Bangladesh Cyber Heist Shows Truth is Stranger Than Fiction. Available online: https://www.dhakatribune.com/opinion/op-ed/122939/the-great-bangladesh-cyber-heist-shows-truth-is (accessed on 12 July 2025).

18. BBC News. HSBC Online Banking Is 'Attacked'. Available online: https://www.bbc.com/news/business-35438159 (accessed on 12 July 2025).

19. Aktas, O.; Can, A.B. Making JavaScript Render Decisions to Optimize Security-Oriented Crawler Process. IEEE Access 2024, 12, 161688–161696.

20. Mohan, V., Othmane, L.B., & Kres, A. BP: security concerns and best practices for automation of software deployment processes: An industrial case study. In 2018 IEEE Cybersecurity Development, SecDev 2018, Cambridge, MA, USA, September 30 - October 2, 2018; pp. 21–28.

21. Lenka, R. K., Kumar, S., & Mamgain, S. Behaviour driven development: Tools and challenges. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Oct 2018, pp. 1032–1037.

22. Bleeping Computer. Interbank Confirms Data Breach Following Failed Extortion, Data Leak. Available online: https://www.bleepingcomputer.com/news/security/interbank-confirms-data-breach-following-failed-extortion-data-leak/ (accessed on 30 October 2024).

23. Gartner. DevSecOps: How to Seamlessly Integrate Security Into DevOps. Available online: https://www.gartner.com/en/documents/3463417 (accessed on 12 July 2025).

24. JISS. Cybercrime or Political Warfare? Available online: https://jiss.org.il/en/davidi-cybercrime-or-political-warfare/ (accessed on 12 July 2025).

25. Michener, J.R., Clager, A.T. Mitigating an oxymoron: Compliance in a devops environments. In: 2016 IEEE 40th COMPSAC. vol. 1, pp. 396–398.

26. Mohan, V., & Othmane, L.B. Secdevops: Is it a marketing buzzword? -mapping research on security in devops. In: 11th ARES. pp. 542–547.

27. H. Myrbakken and R. Colomo-Palacios. Devsecops: A multivocal literature review. 09 2017, pp. 17–29.

28. H. Yasar and K. Kontostathis. Where to integrate security practices on devops platform. International Journal of Secure Software Engineering, vol. 7, pp. 39–50, 10 2016.

29. Security Affairs. Chilean Bank BancoEstado Hit By REVil Ransomware. Available online: https://securityaffairs.com/108014/cyber-crime/bancoestado-ransomware.html (accessed on 6 September 2020).

30. Lwakatare, L.E., Kuvaja, P., Oivo, M. Dimensions of devops. In: International conference on agile software development. pp. 212–217.