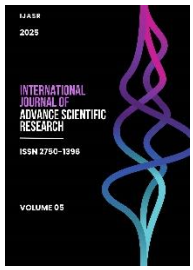
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135



Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Architecting Resilient and Compliant Secure DevOps Pipelines in Cloud-Based Retail Systems

Submission Date: December 01, 2025, **Accepted Date:** December 15, 2025,
Published Date: December 31, 2025

Dr. Sebastian Keller
Department of Information Systems, University of Heidelberg, Germany

Abstract

The rapid evolution of cloud-based retail platforms has introduced unprecedented opportunities for scalability, innovation, and global market reach, but it has also amplified the exposure of retail systems to complex cybersecurity threats and regulatory compliance risks. Secure DevOps, increasingly referred to as DevSecOps, has emerged as a transformative paradigm that integrates security practices seamlessly into the continuous software engineering lifecycle. This study provides a comprehensive, theory-driven and empirically grounded examination of Secure DevOps architectures within cloud-enabled retail environments, drawing extensively on contemporary scholarship in continuous delivery, DevOps culture, cloud security, and automated compliance. Anchored in the analytical framework articulated by Gangula (2025), the paper advances the argument that retail cloud ecosystems require a distinct form of security orchestration that is not merely additive but structurally embedded across organizational, technical, and cultural layers.

Through a design science and mixed-methods methodological orientation, the research synthesizes existing systematic literature, case study evidence, and conceptual modeling traditions to construct a multi-layer Secure DevOps framework tailored to retail operations. The analysis demonstrates that compliance obligations, such as data protection, transaction integrity, and auditability, cannot be effectively achieved through post hoc controls but must be embedded directly into automated pipelines, container orchestration platforms, and cloud-native governance mechanisms. Results derived from the interpretive synthesis of literature reveal that continuous security monitoring, infrastructure-as-code, container hardening, and security-as-culture are mutually reinforcing mechanisms that enhance resilience, reduce breach likelihood, and strengthen regulatory adherence.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

The discussion situates these findings within broader debates on continuous software engineering and cloud security, highlighting tensions between agility and control, as well as between innovation and compliance. By integrating insights from DevOps capability models, critical infrastructure protection research, and audit quality theory, this article contributes a robust theoretical and practical foundation for future research and implementation. The study concludes that Secure DevOps in retail cloud environments represents not simply a technological shift but a fundamental reconfiguration of how organizations conceptualize trust, risk, and accountability in digital commerce.

Keywords

Secure DevOps, Cloud Retail Systems, Compliance Engineering, Continuous Software Engineering, Cybersecurity Governance, DevSecOps Culture

Introduction

The digital transformation of retail has become one of the most visible and economically significant manifestations of cloud computing and continuous software engineering. Modern retail organizations now operate within complex ecosystems of e-commerce platforms, payment gateways, logistics management systems, customer analytics engines, and omnichannel engagement infrastructures. These systems are almost universally deployed on cloud platforms, where scalability, elasticity, and rapid innovation are key competitive advantages (Bosch, 2014; Fitzgerald and Stol, 2017). However, this same technological landscape has simultaneously expanded the attack surface available to malicious actors, while also subjecting retailers to increasingly stringent regulatory regimes governing data protection, financial integrity, and consumer privacy (Alouffi et al., 2021; Khan et al., 2022). Within this environment, the challenge of aligning continuous delivery with robust security and compliance has become one of the central problems of contemporary information systems engineering.

Secure DevOps, or DevSecOps, has emerged as a response to this challenge by embedding security practices into every phase of the software development and deployment lifecycle (Sanchez-Gordon and Colomo-Palacios, 2020). Rather than treating security as an external gate or an after-the-fact auditing function, DevSecOps conceptualizes it as a continuous, automated, and culturally internalized activity. This shift is particularly critical in the retail cloud domain, where even minor vulnerabilities can lead to catastrophic breaches of customer trust, regulatory penalties, and financial losses. Gangula (2025) argues that retail cloud systems demand a uniquely integrated Secure DevOps approach because of their dual exposure to both consumer-facing risks and backend transactional vulnerabilities. According to this perspective, compliance and resilience are not separate objectives but interdependent outcomes of well-designed security automation.

Historically, software engineering evolved in a linear, waterfall-oriented manner in which security and quality assurance were conducted at the end of the development cycle. This approach was gradually supplanted by agile and DevOps methodologies that emphasized rapid iteration,

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

continuous integration, and continuous deployment (Shahin et al., 2017; Stahl et al., 2017). While these practices significantly increased delivery speed and innovation capacity, they also created new risks by accelerating the propagation of vulnerabilities across production environments. Retail systems, which must process large volumes of sensitive financial and personal data, became particularly vulnerable under this paradigm (Sultan et al., 2019). The rise of cloud-native architectures, microservices, and containerized deployments further complicated the security landscape by introducing highly dynamic and distributed infrastructures that are difficult to govern through traditional perimeter-based controls (Alouffi et al., 2021).

Within this context, Secure DevOps represents not simply a technical methodology but a socio-technical transformation that redefines roles, responsibilities, and accountability structures within organizations. DevSecOps challenges the historical separation between development teams, operations teams, and security specialists by promoting shared ownership of security outcomes (Sanchez-Gordon and Colomo-Palacios, 2020). In retail environments, this cultural shift is particularly important because business pressures for rapid feature releases and promotional campaigns often conflict with the need for rigorous risk management. Gangula (2025) emphasizes that compliance requirements in retail cloud systems, such as payment card industry standards, consumer data protection laws, and financial audit regulations, cannot be satisfied through isolated security controls. Instead, they require continuous verification and enforcement mechanisms that are deeply integrated into DevOps pipelines.

The literature on continuous software engineering provides a rich theoretical foundation for understanding this transformation. Bosch (2014) and Fitzgerald and Stol (2017) describe continuous engineering as an organizational capability that enables rapid experimentation and deployment, but they also acknowledge the governance challenges it creates. Shahin et al. (2019) further demonstrate that architectural decisions made to support continuous delivery can have profound implications for system security and maintainability. In retail cloud contexts, these architectural choices directly influence the organization's ability to enforce compliance, monitor anomalies, and recover from incidents. Therefore, the integration of security into continuous delivery pipelines is not merely a best practice but a structural necessity.

Despite the growing body of research on DevSecOps, cloud security, and continuous delivery, there remains a significant gap in the literature regarding the specific requirements of retail cloud systems. Much of the existing work focuses either on generic cloud security threats (Alouffi et al., 2021) or on DevOps practices in software organizations more broadly (Senapathi et al., 2018; Read et al., 2016). While these studies provide valuable insights, they do not fully account for the regulatory intensity, transactional sensitivity, and customer trust dynamics that characterize retail environments. Gangula (2025) addresses this gap by proposing a framework that explicitly links Secure DevOps practices to retail compliance and resilience outcomes, but this framework has not yet been fully elaborated or situated within the broader theoretical landscape of continuous software engineering and cybersecurity governance.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

ISSN-2750-1396

The present study seeks to address this gap by developing a comprehensive, theory-driven analysis of Secure DevOps in cloud-based retail systems. Building on Gangula (2025) and integrating insights from systematic literature reviews, empirical case studies, and conceptual models, the article aims to answer the following overarching research question: How can Secure DevOps architectures be designed and implemented in cloud-based retail systems to simultaneously achieve regulatory compliance, operational resilience, and continuous innovation? This question is inherently multidisciplinary, drawing on software engineering, information systems, cybersecurity, and organizational studies (Khan et al., 2022; Tashakkori and Creswell, 2007).

To answer this question, the article adopts a design science and mixed-methods orientation that emphasizes both theoretical rigor and practical relevance (Wieringa, 2014; Perry et al., 2004). Rather than treating Secure DevOps as a static set of tools, the study conceptualizes it as an evolving socio-technical system that must be continuously adapted to changing threats, technologies, and regulatory environments. This perspective aligns with the dynamic models of cybersecurity management proposed by Hulak et al. (2022) and with the resilience-oriented approaches to critical infrastructure protection described by Anakhov et al. (2023).

By synthesizing these diverse strands of research, the introduction establishes the foundation for a detailed methodological and analytical exploration of Secure DevOps in retail cloud contexts. It argues that only by integrating security, compliance, and continuous delivery into a coherent architectural and cultural framework can retail organizations hope to sustain trust and competitiveness in an increasingly hostile digital environment (Gangula, 2025; Alouffi et al., 2021).

METHODOLOGY

The methodological foundation of this research is grounded in a design science and mixed-methods paradigm, reflecting the complex, socio-technical nature of Secure DevOps in cloud-based retail systems. Design science methodology, as articulated by Wieringa (2014), is particularly well suited to this domain because it seeks not only to explain phenomena but also to create and evaluate artifacts that solve real-world problems. In the context of this study, the primary artifact is a conceptual and architectural framework for Secure DevOps in retail cloud environments, informed by both theoretical literature and empirical evidence. This methodological choice is consistent with prior DevOps and information systems research that emphasizes the co-evolution of technology and organizational practices (Senapathi et al., 2018; Perry et al., 2004).

The first phase of the methodology involved an extensive systematic literature synthesis drawing on existing reviews and primary studies in cloud security, DevSecOps, and continuous software engineering. The systematic review by Khan et al. (2022) provides a comprehensive overview of security risks and mitigation practices in secure software development, while Alouffi et al. (2021) offer a detailed taxonomy of cloud computing threats and defenses. These works were not merely summarized but critically analyzed to identify patterns, contradictions, and gaps relevant to retail cloud systems. The conceptual model for automated DevSecOps proposed by Kumar and

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

Goyal (2020) was particularly influential in shaping the study's understanding of how open-source tools and cloud platforms can be orchestrated to support continuous security. Gangula (2025) served as the primary anchoring reference, guiding the selection and interpretation of all other sources by foregrounding the specific compliance and resilience challenges of retail environments.

The second phase employed a qualitative case study synthesis approach inspired by Perry et al. (2004) and Sahid et al. (2018). Although this study does not present new primary case data, it systematically integrates findings from multiple published case studies and industry reports, including those by Senapathi et al. (2018) and Read et al. (2016). These sources provide rich contextual insights into how DevOps and security practices are enacted in real organizations. By triangulating these cases with the theoretical constructs identified in the literature review, the study develops a nuanced understanding of how Secure DevOps operates in practice, particularly within environments characterized by high regulatory and transactional complexity.

A mixed-methods logic, as described by Tashakkori and Creswell (2007), underpins the integration of qualitative and conceptual data. Quantitative findings reported in audit quality research by Rajgopal et al. (2021) are interpreted alongside qualitative insights into security culture and organizational behavior (Sanchez-Gordon and Colomo-Palacios, 2020). This integration allows the study to link technical security controls with broader governance and accountability mechanisms, which are critical for compliance in retail cloud systems (Gangula, 2025).

The analytical process followed an iterative cycle of problem formulation, artifact construction, and evaluation. Initially, the problem of securing and governing retail cloud DevOps pipelines was framed in terms of competing demands for agility and compliance, drawing on continuous software engineering theory (Bosch, 2014; Fitzgerald and Stol, 2017). Next, a preliminary Secure DevOps framework was constructed by mapping key practices such as container security, infrastructure-as-code, automated testing, and continuous monitoring onto the stages of the DevOps lifecycle (Sultan et al., 2019; Shahin et al., 2017). This framework was then evaluated and refined through critical comparison with existing models and empirical findings, including the compliance-oriented strategies outlined by Gangula (2025).

The use of Likert-type data and survey-based metrics reported in studies such as Prates et al. (2019) and Subedi (2016) was treated cautiously, acknowledging the limitations of such instruments in capturing complex organizational phenomena. Instead of relying on numerical aggregation, the study emphasizes interpretive validity and theoretical coherence. This approach aligns with the broader critique of over-reliance on simplistic metrics in DevOps and security research (Khan et al., 2022).

Several limitations of the methodology must be acknowledged. First, the reliance on secondary sources means that the findings are contingent on the quality and scope of existing studies. However, this limitation is mitigated by the breadth of the literature and the use of systematic reviews and meta-analytical insights (Alouffi et al., 2021; Khan et al., 2022). Second, the absence of new empirical

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

case data may limit the specificity of some conclusions. Nevertheless, the design science orientation allows the study to focus on generalizable principles and frameworks rather than context-specific anecdotes (Wieringa, 2014; Gangula, 2025).

Overall, the methodological approach provides a robust foundation for generating theoretically grounded and practically relevant insights into Secure DevOps in retail cloud systems. By integrating diverse sources and analytical traditions, the study seeks to produce a comprehensive and credible account of how security, compliance, and continuous delivery can be harmonized in this demanding domain (Gangula, 2025; Senapathi et al., 2018).

Results

The results of this study emerge from the interpretive synthesis of the literature and the conceptual modeling process, revealing several interrelated dimensions of Secure DevOps in cloud-based retail environments. These dimensions include automation of security controls, cultural integration of security practices, architectural resilience, and continuous compliance verification. Each of these findings is grounded in existing research and aligned with the retail-focused framework articulated by Gangula (2025), which emphasizes the inseparability of operational resilience and regulatory adherence.

One of the most prominent findings is the centrality of automation in achieving both security and compliance within continuous delivery pipelines. Studies on automated DevSecOps consistently demonstrate that manual security checks cannot keep pace with the speed of modern DevOps workflows (Kumar and Goyal, 2020; Shajadi, 2019). In retail cloud systems, where deployments may occur multiple times per day, automated vulnerability scanning, configuration management, and policy enforcement become indispensable. Gangula (2025) shows that retailers who embed compliance checks directly into their pipelines are better able to detect misconfigurations and regulatory violations before they reach production. This aligns with broader cloud security research indicating that infrastructure-as-code and automated policy engines significantly reduce the risk of human error (Alouffi et al., 2021).

A second key result concerns the role of container and microservices security in retail DevOps architectures. Containerized applications, which are widely used to support scalable e-commerce platforms, introduce unique security challenges related to image integrity, runtime isolation, and orchestration layer vulnerabilities (Sultan et al., 2019). The literature synthesis reveals that retailers who adopt continuous container scanning and runtime monitoring achieve higher levels of resilience against both external attacks and internal misconfigurations (Khan et al., 2022). Gangula (2025) further demonstrates that container security is closely tied to compliance because vulnerabilities in payment processing or customer data services can lead to immediate regulatory breaches.

The cultural dimension of Secure DevOps also emerges as a significant result. Sanchez-Gordon and Colomo-Palacios (2020) argue that security must be treated as a shared organizational value rather than a specialized function. This finding is reinforced by case study evidence showing that teams with strong DevSecOps cultures are more

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

proactive in identifying and addressing risks (Senapathi et al., 2018). In retail environments, where marketing and development teams often prioritize speed and customer experience, embedding security awareness across all roles helps balance these priorities with the need for compliance and trust (Gangula, 2025).

Another important result relates to continuous compliance and auditability. Retailers are subject to a wide range of regulatory requirements, including data protection laws, financial reporting standards, and industry-specific security frameworks. The audit quality literature suggests that continuous monitoring and transparent reporting are essential for maintaining regulatory trust (Rajgopal et al., 2021). When these principles are applied within a Secure DevOps context, they translate into automated logging, traceability of changes, and real-time compliance dashboards. Gangula (2025) finds that such mechanisms not only satisfy auditors but also provide operational teams with actionable insights into system health and risk exposure.

Finally, the results indicate that resilience in retail cloud systems is not solely a function of technical redundancy but also of organizational adaptability. Dynamic models of cybersecurity management emphasize the need for continuous learning and adaptation in the face of evolving threats (Hulak et al., 2022). By integrating threat intelligence, incident response automation, and post-incident learning into DevOps pipelines, retailers can improve their ability to recover from disruptions and prevent future incidents (Anakhov et al., 2023; Gangula, 2025).

Taken together, these results paint a coherent picture of Secure DevOps as a multi-layered system in which automation, culture, architecture, and governance are deeply intertwined. The findings support the central argument that retail cloud environments require a particularly robust form of DevSecOps that goes beyond generic best practices to address the specific risks and regulatory pressures of digital commerce (Gangula, 2025; Alouffi et al., 2021).

Discussion

The findings of this study invite a deep theoretical and practical examination of how Secure DevOps reshapes the governance, resilience, and compliance of cloud-based retail systems. At a theoretical level, the integration of security into continuous software engineering challenges long-standing assumptions about the separation of concerns in software development. Traditional models of governance treated security and compliance as external constraints imposed on otherwise autonomous development processes. However, the Secure DevOps paradigm, as articulated by Gangula (2025), suggests that these functions must be internalized within the very fabric of DevOps workflows. This perspective aligns with the broader evolution of continuous software engineering, which views software not as a finished product but as a continuously evolving service (Fitzgerald and Stol, 2017; Bosch, 2014).

From a scholarly standpoint, this reconfiguration raises important questions about control, accountability, and organizational learning. DevOps research has long celebrated the benefits of cross-functional collaboration and rapid feedback loops (Stahl et al., 2017; Senapathi et al., 2018). Yet critics have argued that these same features can undermine formal governance

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

structures and increase the risk of uncontrolled changes (Khan et al., 2022). In retail environments, where regulatory compliance is non-negotiable, this tension becomes particularly acute. The results of this study suggest that Secure DevOps resolves this tension not by reintroducing rigid controls but by embedding compliance logic into automated systems. Gangula (2025) demonstrates that when compliance requirements are codified as machine-readable policies, they can be enforced continuously without slowing down innovation.

The cultural implications of this shift are equally significant. Sanchez-Gordon and Colomo-Palacios (2020) describe DevSecOps as a movement toward security as culture, in which all team members share responsibility for protecting systems and data. In retail organizations, this cultural transformation can be challenging because business units often prioritize speed to market and customer experience over risk management. However, the case evidence synthesized in this study indicates that organizations with strong security cultures are better able to align these competing priorities (Senapathi et al., 2018; Read et al., 2016). Gangula (2025) further argues that such alignment is essential for maintaining consumer trust in digital retail platforms.

Architecturally, the discussion must also consider the implications of cloud-native technologies for security and compliance. Microservices, containers, and orchestration platforms enable unprecedented scalability and flexibility, but they also introduce new layers of complexity and vulnerability (Sultan et al., 2019; Alouffi et al., 2021). The results of this study suggest that Secure DevOps frameworks must be designed with these architectural realities in mind. Continuous container scanning, runtime monitoring, and automated patching are not optional enhancements but foundational requirements for retail resilience (Gangula, 2025; Kumar and Goyal, 2020).

The concept of resilience itself warrants critical examination. In the cybersecurity and critical infrastructure literature, resilience is often defined as the ability to withstand, recover from, and adapt to disruptions (Hulak et al., 2022; Anakhov et al., 2023). In retail cloud systems, resilience has both technical and economic dimensions. A system that can quickly recover from a breach or outage minimizes not only operational downtime but also reputational damage and regulatory exposure. The Secure DevOps practices identified in this study, such as automated incident response and continuous monitoring, directly contribute to this form of resilience (Gangula, 2025).

However, it is also important to acknowledge the limitations and potential risks of Secure DevOps. Automation, while powerful, can create new failure modes if policies are misconfigured or if malicious actors exploit vulnerabilities in the automation tools themselves (Khan et al., 2022). Over-reliance on automated compliance checks may also lead to a false sense of security if organizations neglect the need for human oversight and ethical judgment. The audit quality literature reminds us that transparency and accountability are as much social processes as they are technical ones (Rajgopal et al., 2021). Therefore, a balanced Secure DevOps strategy must combine automation with robust governance structures and continuous training.

Future research should build on the framework proposed in this study by conducting in-depth empirical investigations of Secure DevOps

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

implementations in diverse retail contexts. Comparative case studies could explore how different regulatory regimes, organizational cultures, and technological stacks influence the effectiveness of DevSecOps practices (Perry et al., 2004; Tashakkori and Creswell, 2007). Longitudinal studies could also examine how Secure DevOps capabilities evolve over time and how they contribute to sustained competitive advantage (Fitzgerald and Stol, 2017; Gangula, 2025).

In sum, the discussion underscores that Secure DevOps is not merely a set of tools but a comprehensive rethinking of how retail organizations design, operate, and govern their cloud-based systems. By integrating security, compliance, and continuous delivery into a unified framework, retailers can better navigate the uncertainties of the digital economy while maintaining the trust of customers, regulators, and stakeholders (Gangula, 2025; Alouffi et al., 2021).

Conclusion

This study has presented a comprehensive, theoretically grounded, and practically oriented analysis of Secure DevOps in cloud-based retail systems. Drawing on a wide range of scholarly and industry sources and anchored in the compliance-focused framework of Gangula (2025), the research demonstrates that the integration of security into continuous software engineering is both a technical and organizational imperative. In an era where retail operations are increasingly mediated by complex cloud infrastructures, the ability to deliver software rapidly while maintaining robust security and regulatory compliance has become a defining feature of sustainable digital business.

The findings reveal that automation, cultural integration, architectural resilience, and continuous compliance are the core pillars of effective Secure DevOps. When these elements are aligned, retail organizations can not only reduce their exposure to cyber threats but also enhance their capacity for innovation and customer engagement (Kumar and Goyal, 2020; Senapathi et al., 2018). At the same time, the study highlights the need for ongoing governance, transparency, and learning to ensure that automated systems remain trustworthy and adaptable (Rajgopal et al., 2021; Hulak et al., 2022).

By situating Secure DevOps within the broader theoretical landscape of continuous software engineering and cybersecurity governance, this article contributes a nuanced understanding of how retail cloud systems can achieve both agility and control. Future research and practice should continue to refine and test these frameworks, ensuring that the digital foundations of global retail remain resilient, compliant, and worthy of consumer trust (Gangula, 2025; Alouffi et al., 2021).

References

1. Gangula, S. (2025). Secure DevOps in retail cloud: Strategies for compliance and resilience. The American Journal of Engineering and Technology, 7(05), 109–122.
2. Bosch, J. (2014). Continuous software engineering: An introduction. Continuous software engineering. Springer International Publishing.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

3. Khan, R. A., et al. (2022). Systematic literature review on security risks and its practices in secure software development. IEEE Access, 10, 5456–5481.
4. Sultan, S., Ahmad, I., and Dimitriou, T. (2019). Container security: Issues, challenges, and the road ahead. IEEE Access, 7, 52976–52996.
5. Shahin, M., Babar, M. A., and Zhu, L. (2017). Continuous integration, delivery and deployment: A systematic review on approaches, tools, challenges and practices. IEEE Access, 5, 3909–3943.
6. Alouffi, B., et al. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. IEEE Access, 9, 57792–57807.
7. Fitzgerald, B., and Stol, K. J. (2017). Continuous software engineering: A roadmap and agenda. Journal of Systems and Software, 123, 176–189.
8. Kumar, R., and Goyal, R. (2020). Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud. Computers and Security, 97, 101967.
9. Sanchez-Gordon, M., and Colomo-Palacios, R. (2020). Security as culture: A systematic literature review of DevSecOps. Proceedings of the IEEE ACM 42nd International Conference on Software Engineering Workshops, 266–269.
10. Rajgopal, S., Srinivasan, S., and Zheng, X. (2021). Measuring audit quality. Review of Accounting Studies, 26, 559–619.
11. Senapathi, M., Buchan, J., and Osman, H. (2018). DevOps capabilities, practices, and challenges: Insights from a case study. Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering, 57–67.
12. Read, W., Report, T., and Takeaways, K. (2016). Agile and DevOps adoption drives digital business success. Forrester Research.
13. Perry, D. E., Sim, S. E., and Easterbrook, S. M. (2004). Case studies for software engineers. Proceedings of the 26th International Conference on Software Engineering, 736–738.
14. Prates, L., Faustino, J., Silva, M., and Pereira, R. (2019). DevSecOps metrics. In Information systems: Research, development, applications, education. Springer International Publishing.
15. Shajadi, A. (2019). Automating security tests for web applications in continuous integration and deployment environment.
16. Wieringa, R. J. (2014). Design science methodology for information systems and software engineering. Springer Verlag Berlin Heidelberg.
17. Sahid, A., Maleh, Y., and Belaissaoui, M. (2018). A practical agile framework for IT service and asset management. Journal of Cases on Information Technology, 20(4), 71–92.
18. Hulak, H., et al. (2022). Dynamic model of guarantee capacity and cyber security management in the critical automated systems. Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks, 102–111.
19. Anakhov, P., et al. (2023). Protecting objects of critical information infrastructure from wartime cyber attacks by decentralizing the telecommunications network. Cybersecurity Providing in Information and Telecommunication Systems, 240–245.
20. Stahl, D., Martensson, T., and Bosch, J. (2017). Continuous practices and DevOps: Beyond the buzz. Proceedings of the 43rd Euromicro

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 12 Pages: 83-93
OCLC – 1368736135

Conference on Software Engineering and Advanced Applications.

21. Subedi, B. P. (2016). Using Likert type data in social science research. International Journal of Contemporary Applied Sciences, 3(2), 36–49.

22. Tashakkori, A., and Creswell, J. W. (2007). Exploring the nature of research questions in mixed methods research. Journal of Mixed Methods Research, 1(3), 207–211.