World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

The emergence and importance of DevSecOps: Integrating and reviewing security practices within the DevOps pipeline

Oluwatosin Oluwatimileyin Abiona [1,*], Oluwatayo Jacob Oladapo [2], Oluwole Temidayo Modupe [3], Oyekunle Claudius Oyeniran [4], Adebunmi Okechukwu Adewusi [5] and Abiola Moshood Komolafe [6]

[1] *Independent Researcher, Nebraska, USA.*
[2] *Independent Researcher, Canada.*
[3] *Independent Researcher, New York, USA.*
[4] *Independent Researcher, North Dakota, USA.*
[5] *Independent Researcher, Ohio, USA.*
[6] *Independent Researcher, Kentucky, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2024, 11(02), 127–133

Publication history: Received on 31 January 2024; revised on 09 March 2024; accepted on 11 March 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.11.2.0093

Abstract

The emergence of DevSecOps marks a significant paradigm shift in software development, focusing on integrating security practices seamlessly into the DevOps pipeline. This paper explores the evolution, principles, and importance of DevSecOps in contemporary software engineering. DevSecOps arises from the recognition that traditional security measures often lag behind the rapid pace of DevOps development cycles, leading to vulnerabilities and breaches. By integrating security early and continuously throughout the software development lifecycle, DevSecOps aims to proactively identify and mitigate risks without impeding the agility and speed of DevOps practices. This paper delves into the core principles of DevSecOps, emphasizing automation, collaboration, and cultural transformation. Automation streamlines security processes, enabling the automated testing and validation of code for vulnerabilities. Collaboration fosters communication and shared responsibility among developers, operations, and security teams, breaking down silos and promoting a collective approach to security. Cultural transformation involves cultivating a security-first mindset across the organization, where security is not an afterthought but an inherent part of the development process. The importance of DevSecOps cannot be overstated in today's digital landscape, where cyber threats are omnipresent and the cost of security breaches is staggering. By integrating security into every stage of the DevOps pipeline, organizations can enhance their resilience to cyber attacks, comply with regulatory requirements, and build trust with customers. DevSecOps represents a holistic approach to software development that prioritizes security without compromising speed or innovation. Embracing DevSecOps principles is imperative for organizations seeking to stay ahead in an increasingly complex and hostile digital environment.

Keyword: DevSecOps; Security; Practices; Emergence; DevOps; Review

1. Introduction

DevSecOps is a methodology that integrates security practices into the DevOps process, ensuring that security measures are implemented and maintained throughout the entire software development lifecycle (Desai and Nisha, 2021). It emphasizes collaboration, automation, and cultural transformation to enable faster delivery of secure and reliable software. The DevOps pipeline is a set of practices and tools used to automate the software delivery process, from code development to deployment and operations (Karamitsos *et al.*, 2020). It typically includes stages such as coding, building, testing, deployment, monitoring, and feedback. The goal of the DevOps pipeline is to streamline and accelerate

* Corresponding author: Oluwatosin Oluwatimileyin Abiona

the delivery of high-quality software by breaking down silos between development and operations teams and promoting continuous integration and continuous delivery (CI/CD) practices (Mowad *et al*., 2022). Traditionally, security has been treated as a separate phase in the software development lifecycle, often added as an afterthought or handled by a separate security team (Khan *et al*., 2022). This approach can lead to security vulnerabilities and risks being overlooked or addressed too late in the development process, resulting in costly and time-consuming security breaches. With the increasing frequency and sophistication of cyber threats, organizations can no longer afford to treat security as an isolated concern. DevSecOps acknowledges the critical importance of security in software development and seeks to address vulnerabilities and security risks early and continuously throughout the DevOps pipeline (Battina, 2021). By integrating security into every stage of the development process, DevSecOps helps organizations mitigate security threats, comply with regulatory requirements, and build trust with customers (Rangaraju *et al*., 2023).

2. Evolution of DevSecOps

DevSecOps emerged as a response to the limitations of traditional security approaches in fast-paced DevOps environments. It draws inspiration from DevOps principles and practices, as well as the growing recognition of the need for a more holistic and proactive approach to security in software development (Amaro *et al*., 2022). The evolution of DevSecOps can be traced back to early efforts to integrate security into the DevOps pipeline, such as the introduction of security-focused DevOps tools and practices (Ramaj *et al*., 2022). Key milestones include the publication of influential papers and frameworks advocating for DevSecOps principles, as well as the development of specialized security tools and technologies designed to support DevSecOps practices. In recent years, there has been a significant increase in the adoption of DevSecOps practices across industries, driven by factors such as the rise of cloud computing, the proliferation of cyber threats, and the growing regulatory pressure to ensure the security of software systems (Mao *et al*., 2020; Battina, 2021). Organizations are increasingly recognizing the benefits of DevSecOps in terms of improved security posture, faster time-to-market, and greater operational efficiency. As a result, DevSecOps is becoming increasingly mainstream, with more organizations integrating security into their DevOps pipelines and embracing a culture of security-first development (Jha *et al*., 2023).

3. Core Principles of DevSecOps

Automation plays a crucial role in DevSecOps by enabling the rapid and consistent testing and validation of security measures throughout the development process (Zaydi and Nassereddine, 2020). Automated security tests help identify vulnerabilities early in the development lifecycle, allowing teams to address them promptly and reduce the risk of security breaches. Various tools and technologies are available to support automated security checks in DevSecOps pipelines (Rangnau *et al*., 2020). These include static code analysis tools for scanning code for potential security issues, dynamic application security testing (DAST) tools for simulating real-world attacks, and container security tools for scanning container images for vulnerabilities.

DevSecOps promotes collaboration and communication between traditionally siloed development, operations, and security teams (Sánchez-Gordón and Colomo-Palacios, 2020). By breaking down these silos, teams can share insights, expertise, and responsibilities, leading to better alignment and coordination in addressing security concerns. Cross-functional collaboration involves bringing together individuals from different disciplines, such as development, operations, security, and quality assurance, to work together towards common security goals (Dyson, 2020; Kalabina and Belyak, 2021). This collaboration fosters a deeper understanding of security requirements and challenges across teams, leading to more effective security measures.

DevSecOps requires a cultural shift towards prioritizing security throughout the software development lifecycle (Akbar *et al*., 2022). This involves instilling a mindset where security is considered a fundamental aspect of software development, rather than an afterthought or separate concern. In DevSecOps, security is everyone's responsibility, not just the responsibility of the security team (Lombardi and Fanton, 2023). Fostering a culture of shared responsibility involves empowering developers, operators, and other stakeholders to take ownership of security tasks and make security-conscious decisions in their respective roles (Habbal *et al*., 2024).

3.1. Integrating Security Practices into the DevOps Pipeline

Providing developers with training and resources on secure coding practices helps them write code that is resilient to security threats (Vyas, 2023). This includes educating developers on common vulnerabilities, secure coding guidelines, and best practices for writing secure code. Establishing and enforcing secure coding guidelines and standards ensures consistency and adherence to security best practices across development teams (De Cremer *et al*., 2020). These guidelines may cover areas such as input validation, authentication, authorization, and data encryption.

Integrating security testing into CI/CD pipelines allows for automated and continuous validation of security controls throughout the software delivery process (Putra and Kabetta, 2022). This includes running security tests such as static code analysis, dynamic application security testing (DAST), and dependency scanning as part of the automated build and deployment process. Static analysis, dynamic analysis, penetration testing, etc.:

Security testing encompasses various techniques and methodologies for identifying and assessing security vulnerabilities in software applications (Dissanayake *et al*., 2022). This includes static analysis, which examines the code for security flaws without executing it, dynamic analysis, which tests the application in a runtime environment, and penetration testing, which simulates real-world attacks to uncover vulnerabilities.

Infrastructure as Code (IaC) involves managing and provisioning infrastructure using code and automation tools (Hasan *et al*., 2020). By implementing security controls directly in infrastructure code, such as configuration files and scripts, organizations can ensure that security measures are consistently applied across their environments. IaC enables organizations to define and deploy infrastructure configurations in a repeatable and consistent manner, reducing the risk of configuration drift and misconfigurations that could lead to security vulnerabilities (Bhatia and Gabhane, 2023, Oguejiofor *et al*., 2023). By treating infrastructure as code, organizations can apply the same versioning, testing, and review processes to infrastructure changes as they do to application code.

4. Importance of DevSecOps

DevSecOps emphasizes the integration of security practices throughout the software development lifecycle, enabling teams to detect and address security vulnerabilities early on (Zaydi and Nassereddine, 2020). By incorporating automated security testing and continuous monitoring into the development pipeline, DevSecOps facilitates the proactive identification of vulnerabilities, allowing organizations to fix issues before they can be exploited by attackers. This proactive approach helps to bolster the overall security posture of software systems, reducing the risk of potential security breaches (Adekanmbi and Wolf, 2024).

5. Reduced attack surface and likelihood of breaches:

Through the implementation of DevSecOps practices, organizations can minimize their attack surface—the potential points of entry for cyber threats. By integrating security measures such as secure coding practices, vulnerability scanning, and access controls into the development process, DevSecOps reduces the likelihood of successful attacks (Onoyere and Adekanmbi, 2012; Kumar and Goyal, 2020). This reduction in the attack surface area, coupled with the proactive identification and mitigation of vulnerabilities, significantly lowers the risk of security breaches and data compromises. DevSecOps assists organizations in meeting regulatory standards and compliance mandates by embedding security into the development process (Ramaj *et al*., 2022). Regulations such as GDPR, HIPAA, PCI DSS, and others require organizations to implement specific security measures to protect sensitive data and ensure privacy and confidentiality (Belmabrouk, 2023). DevSecOps facilitates compliance with these regulations by automating security controls, conducting regular security assessments, and documenting security measures, thereby reducing the risk of non-compliance and associated penalties (Fabian *et al*., 2023; Tatineni, 2023).

By incorporating security into every stage of the software development lifecycle, DevSecOps enables organizations to demonstrate their commitment to security best practices (Ashenden and Ollis, 2020). This includes following industry-recognized security frameworks such as NIST Cybersecurity Framework or CIS Controls and adhering to established security guidelines and standards. By demonstrating adherence to these best practices, organizations can build trust with customers, partners, and regulatory bodies, showcasing their dedication to protecting sensitive information and mitigating security risks. DevSecOps plays a crucial role in building trust with customers and stakeholders by ensuring the security and reliability of software products and services (Uchechukwu *et al*., 2023). By prioritizing security throughout the development process, organizations demonstrate their commitment to protecting customer data and sensitive information. This fosters trust and confidence in the organization's ability to deliver secure and dependable solutions, enhancing customer satisfaction and loyalty (Adeleke *et al*., 2019). In the event of a security incident, organizations that have implemented DevSecOps practices are better equipped to respond effectively, minimizing the impact on their reputation and brand. By proactively identifying and addressing vulnerabilities, organizations can reduce the likelihood and severity of security incidents. Additionally, by maintaining transparent communication and demonstrating a commitment to remediation and improvement, organizations can mitigate reputational damage and rebuild trust with customers and stakeholders, ultimately preserving their reputation and credibility in the market (Ilugbusi *et al.,* 2020; Pool *et al*., 2024).

6. Future Directions and Trends

With the widespread adoption of containerization technologies like Docker and Kubernetes, there is a growing need for enhanced container security solutions (Vincent *et al*., 2021). Emerging tools such as container vulnerability scanners, runtime protection platforms, and image signing and verification tools aim to mitigate risks associated with containerized environments. These tools automate security checks, enforce security policies, and protect containerized applications from vulnerabilities, malware, and unauthorized access (Abrahams *et al*., 2023). As organizations increasingly leverage cloud computing services, ensuring the security of cloud-based environments becomes paramount. Emerging cloud security solutions focus on providing visibility, control, and compliance in cloud environments (Adaga *et al*., 2024). Tools such as cloud security posture management (CSPM) platforms, cloud workload protection platforms (CWPP), and cloud access security brokers (CASB) help organizations secure their cloud infrastructure and applications (Haber *et* al., 2022; Abrahams *et al*., 2024). These tools enable organizations to identify misconfigurations, enforce security policies, monitor user activity, and detect and respond to security threats in real-time. AI and machine learning technologies are being integrated into DevSecOps practices to enhance security analytics, threat detection, and incident response capabilities (Sen, 2021). Machine learning algorithms analyze large volumes of security data to identify patterns, anomalies, and potential threats. AI-driven security solutions automate threat detection, prioritize security alerts, and recommend remediation actions based on historical data and contextual information (Sarker *et al*., 2024). These technologies enable organizations to improve their ability to detect and respond to security incidents promptly, reducing the impact of cyber attacks and minimizing the risk of data breaches.

There is a growing trend towards shifting security practices to the left—integrating security into the early stages of the software development lifecycle. DevSecOps practices will continue to evolve to facilitate security testing and validation at every stage of the development process, from code commit to deployment (Pendyala, 2020). Developers will be empowered with tools and automation capabilities to identify and remediate security issues during the development phase, reducing the likelihood of vulnerabilities making their way into production environments.

DevSecOps practices will evolve to automate compliance management and reporting, addressing the challenges associated with maintaining regulatory compliance in dynamic and fast-paced development environments (Dupont *et al*., 2021). Automation tools will streamline compliance assessments, audits, and reporting processes, enabling organizations to demonstrate adherence to regulatory standards more efficiently. These tools will provide visibility into compliance status, identify non-compliance issues, and generate compliance reports automatically, reducing the manual effort and administrative overhead associated with compliance management (Hidayat and Defitri, 2024). There will be a greater emphasis on fostering a culture of security within organizations, with a focus on security awareness, education, and training. DevSecOps practices will evolve to empower developers, operations teams, and security professionals to collaborate effectively and take ownership of security responsibilities (Anjaria and Kulkarni, 2022). Organizations will invest in security training programs, workshops, and awareness campaigns to educate employees about security best practices, threats, and mitigation strategies. By promoting a security-first mindset and culture of shared responsibility, organizations can strengthen their security posture and resilience to cyber threats (Willie, 2023).

7. Recommendation and Conclusion

DevSecOps represents a holistic approach to software development that integrates security practices seamlessly into the DevOps pipeline. By prioritizing security, fostering collaboration across teams, and embracing automation and cultural transformation, organizations can enhance their security posture and resilience to cyber threats. In today's digital landscape, where cyber threats are increasingly sophisticated and regulatory requirements are becoming more stringent, embracing DevSecOps principles and practices is essential for organizations to protect sensitive data, ensure regulatory compliance, and maintain trust and credibility with customers and stakeholders.

Organizations are encouraged to invest in training, tools, and technologies to effectively implement DevSecOps and stay ahead of emerging threats and regulatory requirements. By integrating security into every aspect of the software development lifecycle and fostering a culture of security awareness and collaboration, organizations can build robust and secure software solutions that meet the demands of today's dynamic and evolving threat landscape.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2023. Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security.

[2] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. MASTERING COMPLIANCE: A Comprehensive Review Of Regulatory Frameworks In Accounting And Cybersecurity. *Computer Science & IT Research Journal*, *5*(1), pp.120-140.

[3] Adaga, E.M., Egieya, Z.E., Ewuga, S.K., Abdul, A.A. and Abrahams, T.O., 2024. Philosophy In Business Analytics: A Review Of Sustainable And Ethical Approaches. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.69-86.

[4] Adekanmbi, A.O. and Wolf, D., 2024. Solid Mineral Resources Extraction and Processing Using Innovative Technology in Nigeria. *ATBU Journal of Science, Technology and Education*, *12*(1), pp.1-16.

[5] Adeleke, O.K., Segun, I.B. and Olaoye, A.I.C., 2019. Impact of internal control on fraud prevention in deposit money banks in Nigeria. *Nigerian Studies in Economics and Management Sciences*, *2*(1), pp.42-51.

[6] Akbar, M.A., Smolander, K., Mahmood, S. and Alsanad, A., 2022. Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology*, *147*, p.106894.

[7] Amaro, R., Pereira, R. and da Silva, M.M., 2022. Capabilities and practices in DevOps: a multivocal literature review. *IEEE Transactions on Software Engineering*, *49*(2), pp.883-901.

[8] Anjaria, D. and Kulkarni, M., 2022. Effective DevSecOps Implementation: A Systematic Literature Review. *Cardiometry*, (24), pp.410-417.

[9] Ashenden, D. and Ollis, G., 2020, October. Putting the sec in devsecops: Using social practice theory to improve secure software development. In *New Security Paradigms Workshop 2020* (pp. 34-44).

[10] Battina, D.S., 2021. The Challenges and Mitigation Strategies of Using DevOps during Software Development. *International Journal of Creative Research Thoughts (IJCRT), ISSN*, pp.2320-2882.

[11] Belmabrouk, K., 2023. Cyber Criminals and Data Privacy Measures. In *Contemporary Challenges for Cyber Security and Data Privacy* (pp. 198-226). IGI Global.

[12] Bhatia, S. and Gabhane, C., 2023. Terraform: Infrastructure as Code. In *Reverse Engineering with Terraform: An Introduction to Infrastructure Automation, Integration, and Scalability using Terraform* (pp. 1-36). Berkeley, CA: Apress.

[13] De Cremer, P., Desmet, N., Madou, M. and De Sutter, B., 2020. Sensei: Enforcing secure coding guidelines in the integrated development environment. *Software: Practice and Experience*, *50*(9), pp.1682-1718.

[14] Desai, R. and Nisha, T.N., 2021, July. Best practices for ensuring security in devops: A case study approach. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042045). IOP Publishing.

[15] Dissanayake, N., Jayatilaka, A., Zahedi, M. and Babar, M.A., 2022. Software security patch management-A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*, p.106771.

[16] Dupont, S., Ginis, G., Malacario, M., Porretti, C., Maunero, N., Ponsard, C. and Massonet, P., 2021, September. Incremental common criteria certification processes using DeVSecOps practices. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 12-23). IEEE.

[17] Dyson, T., 2020. A revolution in military learning? Cross-functional teams and knowledge transformation by lessons-learned processes. *European Security*, *29*(4), pp.483-505.

[18] Fabian, A.A., Uchechukwu, E.S., Okoye, C.C. and Okeke, N.M., (2023). Corporate Outsourcing and Organizational Performance in Nigerian Investment Banks. *Sch J Econ Bus Manag, 2023Apr*, *10*(3), pp.46-57.

[19] Habbal, A., Ali, M.K. and Abuzaraida, M.A., 2024. Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*, p.122442.

[20] Haber, M.J., Chappell, B. and Hills, C., 2022. Mitigation Strategies. In *Cloud Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Cloud Resources* (pp. 221-296). Berkeley, CA: Apress.

[21] Hasan, M.M., Bhuiyan, F.A. and Rahman, A., 2020, November. Testing practices for infrastructure as code. In *Proceedings of the 1st ACM SIGSOFT International Workshop on Languages and Tools for Next-Generation Testing* (pp. 7-12).

[22] Hidayat, M. and Defitri, S.Y., 2024. Digitalization and the Changing Landscape of Tax Compliance (Challenges and Opportunities). *Accounting Studies and Tax Journal (COUNT)*, *1*(1), pp.131-139.

[23] Ilugbusi, S., Akindejoye, J.A., Ajala, R.B. and Ogundele, A., 2020. Financial liberalization and economic growth in Nigeria (1986-2018). *International Journal of Innovative Science and Research Technology*, *5*(4), pp.1-9.

[24] Jha, A.V., Teri, R., Verma, S., Tarafder, S., Bhowmik, W., Kumar Mishra, S., Appasani, B., Srinivasulu, A. and Philibert, N., 2023. From theory to practice: Understanding DevOps culture and mindset. *Cogent Engineering*, *10*(1), p.2251758.

[25] Kalabina, E. and Belyak, O., 2021. The influence of cross-functional teams on the development of the companies' absorption ability in the conditions of work 4.0. In *Digital Transformation and New Challenges: Changes in Business and Society in the Digital Era* (pp. 183-199). Cham: Springer International Publishing.

[26] Karamitsos, I., Albarhami, S. and Apostolopoulos, C., 2020. Applying DevOps practices of continuous automation for machine learning. *Information*, *11*(7), p.363.

[27] Khan, R.A., Khan, S.U., Khan, H.U. and Ilyas, M., 2022. Systematic literature review on security risks and its practices in secure software development. *ieee Access*, *10*, pp.5456-5481.

[28] Kumar, R. and Goyal, R., 2020. Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). *Computers & Security*, *97*, p.101967.

[29] Lombardi, F. and Fanton, A., 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*, pp.1-36.

[30] Mao, R., Zhang, H., Dai, Q., Huang, H., Rong, G., Shen, H., Chen, L. and Lu, K., 2020, December. Preliminary findings about devsecops from grey literature. In *2020 IEEE 20th international conference on software quality, reliability and security (QRS)* (pp. 450-457). IEEE.

[31] Mowad, A.M., Fawareh, H. and Hassan, M.A., 2022, November. Effect of Using Continuous Integration (CI) and Continuous Delivery (CD) Deployment in DevOps to reduce the Gap between Developer and Operation. In *2022 International Arab Conference on Information Technology (ACIT)* (pp. 1-8). IEEE.

[32] Oguejiofor, B.B., Omotosho, A., Abioye, K.M., Alabi, A.M., Oguntoyinbo, F.N., Daraojimba, A.I. and Daraojimba, C., 2023. A review on data-driven regulatory compliance in Nigeria. *International Journal of applied research in social sciences*, *5*(8), pp.231-243.

[33] Onoyere, I.O and Adekanmbi A. O. O., 2012. Sustainable Energy Development In a Developing Economy: The Nigerian Experience. *ATBU Journal of Science, Technology and Education*, 1, pp 142 – 150.

[34] Pendyala, V., 2020. Evolution of integration, build, test, and release engineering into devops and to DevSecOps. In *Tools and Techniques for Software Development in Large Organizations: Emerging Research and Opportunities* (pp. 1-20). IGI Global.

[35] Pool, J., Akhlaghpour, S., Fatehi, F. and Burton-Jones, A., 2024. A systematic analysis of failures in protecting personal health data: a scoping review. *International Journal of Information Management*, *74*, p.102719.

[36] Putra, A.M. and Kabetta, H., 2022, October. Implementation of DevSecOps by Integrating Static and Dynamic Security Testing in CI/CD Pipelines. In *2022 IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM)* (pp. 1-6). IEEE.

[37] Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., Chockalingam, S. and Colomo-Palacios, R., 2022. Holding on to Compliance While Adopting DevSecOps: An SLR. *Electronics*, *11*(22), p.3707.

[38] Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., Chockalingam, S. and Colomo-Palacios, R., 2022. Holding on to Compliance While Adopting DevSecOps: An SLR. *Electronics*, *11*(22), p.3707.

[39] Rangaraju, S., Ness, S. and Dharmalingam, R., 2023. Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security. *International Journal of Innovative Science and Research Technology*, *8*(23592365), pp.10-5281.

[40] Rangnau, T., Buijtenen, R.V., Fransen, F. and Turkmen, F., 2020, October. Continuous security testing: A case study on integrating dynamic security testing tools in ci/cd pipelines. In *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)* (pp. 145-154). IEEE.

[41] Sánchez-Gordón, M. and Colomo-Palacios, R., 2020, June. Security as culture: a systematic literature review of DevSecOps. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops* (pp. 266-269).

[42] Sarker, I.H., Janicke, H., Ferrag, M.A. and Abuadbba, A., 2024. Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, p.101110.

[43] Sen, A., 2021. DevOps, DevSecOps, AIOPS-paradigms to IT operations. In *Evolving Technologies for Computing, Communication and Smart World: Proceedings of ETCCS 2020* (pp. 211-221). Springer Singapore.

[44] Tatineni, S., 2023. Compliance and Audit Challenges in DevOps: A Security Perspective. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(10), pp.1306-1316.

[45] Uchechukwu, E.S., Amechi, A.F., Okoye, C.C. and Okeke, N.M., 2023. Youth Unemployment and Security Challenges in Anambra State, Nigeria. *Sch J Arts Humanit Soc Sci*, *4*, pp.81-91.

[46] Vincent, A.A., Segun, I.B., Loretta, N.N. and Abiola, A., 2021. Entrepreneurship, agricultural value-chain and exports in Nigeria. *United International Journal for Research and Technology*, *2*(08), pp.1-8.

[47] Vyas, B., 2023. Security Challenges and Solutions in Java Application Development. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *12*(2), pp.268-275.

[48] Willie, M.M., 2023. The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. *Journal of Research, Innovation and Technologies*, *2*(2 (4)), pp.179-198.

[49] Zaydi, M. and Nassereddine, B., 2020. DevSecOps PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT. *Journal of Management Information & Decision Sciences*, *23*(2).

[50] Zaydi, M. and Nassereddine, B., 2020. DevSecOps PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT. *Journal of Management Information & Decision Sciences*, *23*(2).