International Journal of Applied Mathematics

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

SECURING ENTERPRISE CLOUD APPLICATIONS WITH DEVSECOPS AND ZERO TRUST

Anaswara Thekkan Rajan[1]

Ponnaiyah Ramajayam Institute of Science & Technology University, Thanjavur, Tamil Nadu, India

Abstract

The use of cloud-native applications in the telecommunications industry has drastically increased the attack surface of the enterprise systems, subjecting them to advanced cyberattacks. Conventional security frameworks tend to fail on dynamic, distributed, and multitenant clouds. The paper provides a review of the adoption of Zero Trust Architecture and DevSecOps to strengthen the security of cloud applications in the telecommunications industry. The most popular types of threats, including insider attacks, API vulnerabilities, and misconfigurations, can be resolved with the help of automated security testing, ongoing compliance, and identity-based access controls. The paper combines the knowledge of the literature, industry knowledge, and case studies to provide a holistic approach to attain an effective security posture that facilitates agile development and resilient operations, and discusses the future challenges and directions, such as AI-driven security solutions.

Keywords: Cloud Security, DevSecOps, Zero Trust, Telecommunications, Enterprise Applications

I. Introduction

Cloud-native idols have completely revolutionized the telecommunication industry, as operators have altered their approach to service implementation and management. Telecom operators have the opportunity to provide their services faster, more flexibly, and with increased scale, thanks to 5G networks, virtualization technologies, and power. These innovations make it possible to support the innovative paradigm, such as IoT and edge computing, to provide data processing as it is nearer to end-users and has lower latency. This will enable the operators to address the changing needs more efficiently, provide the services in a highly efficient manner, and innovate at a fast pace, enhancing customer experience and business adaptability. Nonetheless, as much as they come with such advantages, they also create a complicated virtual plane that is prone to cybersecurity risks like data breaches, insider attacks, and supply chain risks [1-4].

The former models of conventional perimeter security used to provide a sufficient level of defense, but cannot be applied anymore to the high dynamism and distributed characteristics of the cloud-native and 5G infrastructure. In this sense, the telecom operators have been adopting new security systems like DevSecOps and Zero Trust Architecture to meet the existing security needs. DevSecOps makes security an inherent and ongoing aspect of the software development lifecycle in such a manner that any vulnerability is discovered and

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

handled early on rather than after it is released. Zero Trust Architecture involves a shift in the attitude of implicit trust that is substituted by strict checks of the identity, the tightest of tight access controls, and constant monitoring of the system activity that uncovers anomalies. By so doing, the telecom operators can build sturdy, reactive, and regulatory-sensitive cloud-native and 5G frameworks that are more resilient to meet the ever-evolving threat environment and deliver an assured provision of important services [2-8]. The VNFs, microservices, automated DevSecOps, Zero Trust Access Control with multi-factor authentication, continuous threat monitoring, and Identity and Access Management (IAM) are the main security components of a cloud-native telecom setting, as shown in Figure 1.

Figure 1 – Cloud-Native Telecom Infrastuture Security Framework

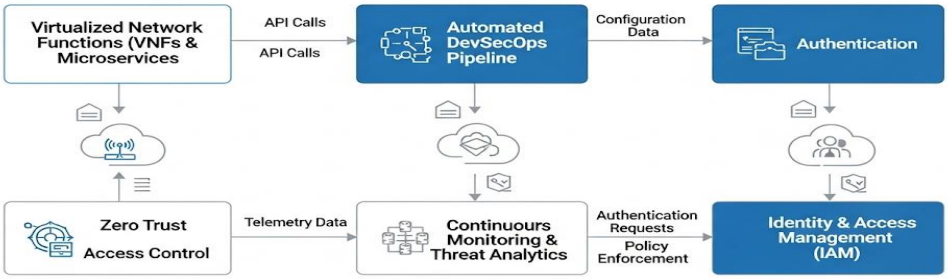

Figure 1: Security Strategy in Cloud-Native Telecom Infrastructure

1.1 Background

The use of cloud computing has transformed the ways in which telecom companies can offer their services, and they are versatile, scalable, and reasonably priced. However, there are also some special security issues [6] that come along with this change. Multi-tenant designs, dynamism of multi-service and distributed data flows, expose them to cyber threats. DevSecOps (a type of DevOps) is one in which pipelines in CI/CD are enhanced with security controls, in which vulnerabilities are detected and blocked during the initial phases [7]. This plan is complemented by Zero Trust Architecture (ZTA), whereby verification of identity and continuous monitoring of the network and fine-grained access controls are enforced on the network without any implicit trusting to the network boundaries [8]. The combination of these strategies provides an active framework of cloud application protection in complex telecommunication environments [9].

1.2 Objective of the Paper

The key goal of this paper is to present an overview of the means of ensuring the security of the enterprise cloud applications within the telecommunications industry based on the DevSecOps and Zero Trust integration. This study aims to:

Discuss the security threats specific to telecom cloud applications, such as insider threats, API threats, and regulatory compliance threats.

Research the application of Zero Trust Architecture to telecom businesses, especially identifying-based access controls, micro-segmentation, and constant monitoring.

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Integrate DevSecOps and Zero Trust: suggest a unified model that maintains a better level of security posture and promotes agility and business efficiency in the in-house cloud infrastructure.

II. Literature Review

A comprehensive literature review is essential to understand the current state of research and industry practices in securing cloud applications within the telecommunications sector. By examining existing studies, frameworks, and case analyses, this review identifies prevailing challenges, highlights best practices, and uncovers gaps where integrating DevSecOps and Zero Trust can significantly enhance security. The literature also reveals trends in automation, identity-centric controls, and compliance strategies, providing a foundation for developing a robust and research-informed framework tailored to telecom enterprises [8-17]. Table 1 summarizes key studies on DevSecOps and Zero Trust practices relevant to enterprise cloud applications in telecom.

Table 1. Summary of key literature on DevSecOps and Zero Trust in telecom cloud applications.

Focus Area	Telecom Relevance	Security Approach	Key Findings / Contribution
DevSecOps in Cloud	High	CI/CD integration, automated security testing	Emphasizes the importance of integrating security seamlessly into the entire software development lifecycle, automating security testing and compliance checks, and fostering a culture of shared responsibility among development, operations, and security teams.
Zero Trust Architecture	High	Identity-based access, least privilege	Provides an abstract definition of Zero Trust Architecture (ZTA) and general deployment models and use cases where ZTA could improve an enterprise's overall IT security posture.
Cybersecurity Resilience	High	DevSecOps, Zero Trust, AI-based automation	Highlights the integration of DevSecOps and Zero Trust with AI-based automation to enhance cybersecurity resilience and compliance with regulations.
DevSecOps Security Model	High	CI/CD pipelines, automated security testing	Analyzes the necessity of using the DevSecOps approach and its advantages and disadvantages, emphasizing its role in securing cloud applications.
Zero Trust in 5G/6G Networks	High	AI-driven Zero Trust, O-RAN	Discusses the integration of Zero Trust principles into next-generation communication networks (5G/6G), introducing the concept of an intelligent Zero Trust Architecture (i-ZTA) as a security framework.

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cloud Security Best Practices	High	Zero Trust, API security, automated tools	Proposes best practices for cloud security in telecom, including implementing Zero Trust architectures, securing APIs, and adopting automated security tools to enhance efficiency and accuracy in threat management.
Resilient Cloud Cluster with DevSecOps	High	DevSecOps security model	Explores DevSecOps implementation for cloud-native applications, focusing on automation in CI/CD pipelines and risk mitigation strategies.
Zero Trust in Cloud Networks	High	Zero Trust Architecture	Explores the implementation and effectiveness of Zero Trust Architecture (ZTA) in addressing security challenges within cloud networks, particularly in sensitive and mission-critical environments.

III. Methodologies and Approaches

Telecommunications can protect enterprise cloud applications by doing more than traditional perimeter protection through a multi-layered method. DevSecOps + Zero Trust provides a sound framework: DevSecOps is applied to ensure protection throughout the software development life cycle with automated checks, vulnerability detection, and compliance tests with no human error and fast and secure delivery. Zero Trust is a concept of strong identity checks, continuous authentication, and least-privilege access, reduction of attack surface, and prevention of further circulation. Together, the strategies have the potential to make telecom businesses agile, ensure compliance with regulations, and mitigate the evolving cyber threats with the assistance of specific tools, techniques, and best practices associated with the management of cloud-native applications.

3.1 DevSecOps Integration

DevSecOps extends traditional DevOps by embedding security at every stage of the CI/CD pipeline. Automated security testing, code analysis, and compliance verification reduce vulnerabilities early in the development lifecycle. Key steps include:

Continuous Integration (CI): Incorporate automated code scanning and static application security testing (SAST) into CI pipelines.

Continuous Deployment (CD): Deploy microservices with automated security validation and configuration checks.

Monitoring and Feedback: Continuous monitoring of application behavior, logging, and alerting for anomalous activities.

Table 2 provides an overview of commonly used DevSecOps tools and their functions in telecom cloud environments.

Table 2: Overview of commonly used DevSecOps tools

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

DevSecOps Tool	Function	Telecom Application	Security Benefit
Jenkins / GitLab CI	CI/CD automation	Cloud app deployment	Integrates automated testing and security checks into pipelines
SonarQube	Static code analysis	Telecom microservices	Detects vulnerabilities early in development
OWASP ZAP	Dynamic application security testing	API services	Identifies runtime security flaws and misconfigurations
Terraform / Ansible	Infrastructure as code	Cloud provisioning	Ensures secure configuration and consistent deployments
Prometheus / Grafana	Monitoring & alerting	Network functions, cloud apps	Detects anomalies, performance bottlenecks, and potential attacks

3.2 Zero Trust Implementation

The Zero Trust Architecture (ZTA) removes implicit trust in telecom cloud environments by imposing strict identity verification, least privileged access, and ongoing monitoring. Notable features of ZTA are Identity and Access Management (IAM), which centralizes authentication and introduces multi-factor verification so that only authorized users can access the network; micro-segmentation, which isolates workloads and prevents the further spread of threats over the network; continuous monitoring and analytics, allowing real-time analysis of user and network traffic behavior to identify an irregularity; and dynamic policy enforcement, which implements security policies in light of the current risk assessment and thus grants adaptive protection against any emergent threats. Figure 2 illustrates an integrated framework combining DevSecOps and Zero Trust to secure telecom applications in the enterprise cloud.

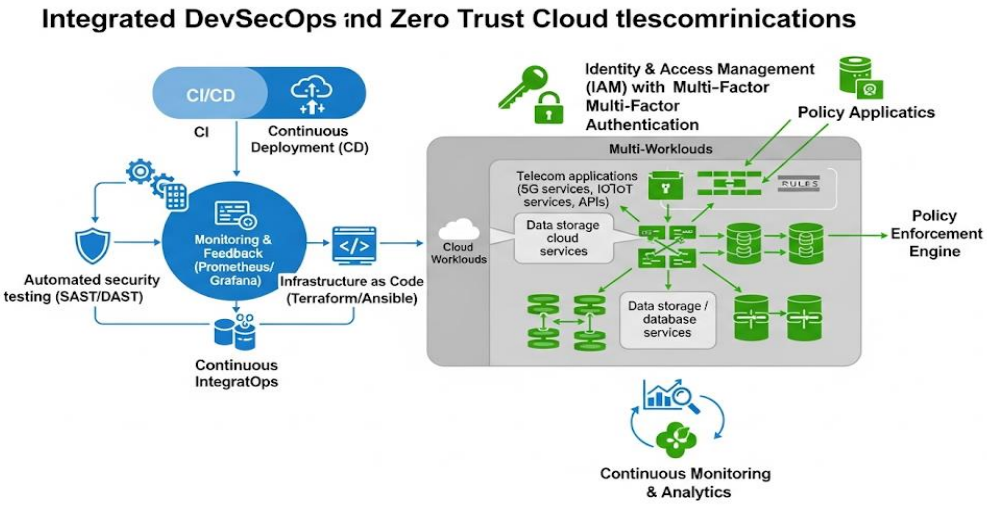

Figure 2: DevSecOps and Zero Trust Application in Telecommunications

As depicted in Figure 2, the integration of DevSecOps and Zero Trust principles enables a continuous, automated, and identity-centric approach to securing telecom cloud applications.

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IV. Case Studies

The telecommunications industry is moving towards the use of DevSecOps and Zero Trust to ensure the security of cloud-native applications. Case studies show a quantifiable decrease in the level of threat mitigation, compliance, and operational efficiency, which shows the significance of automated security pipelines, identity-based access controls, and continuous monitoring. These examples help understand the best practices and the practical effect of the integration of DevSecOps and Zero Trust in complicated cloud systems. Table 3 provides a summary of 6 case studies of companies.

Table 3: Case studies implementing DevSecOps and Zero Trust

Telecom Application	Security Approach	Key Implementation	Outcomes / Benefits
Multi-cloud enterprise apps	DevSecOps + Zero Trust	Automated CI/CD pipelines, IAM, micro-segmentation	Reduced breach incidents, faster incident response, improved compliance
5G network functions	Zero Trust	Continuous authentication, network micro-segmentation	Strengthened access control, prevented lateral threat movement
Cloud-native customer platforms	DevSecOps	Integrated SAST/DAST, CI/CD security automation	Detected vulnerabilities early, reduced deployment delays, improved resilience
IoT and edge services	DevSecOps + Zero Trust	Policy-driven IAM, automated monitoring	Minimized insider threats, enhanced visibility, streamlined security operations
5G core and cloud apps	Zero Trust	AI-based monitoring, least-privilege access	Real-time threat detection, reduced misconfigurations, improved compliance
Cloud-based enterprise services	DevSecOps	Automated testing, code scanning, secure deployment	Faster vulnerability remediation, secure multi-tenant applications, improved audit readiness

V. Challenges and Limitations

The use of DevSecOps and Zero Trust principles in telecom cloud applications has a number of technical, organizational, and regulatory issues. While these frameworks enhance security and compliance, they necessitate significant modifications to culture, procedures, and technology. Companies tend to struggle with the concept of introducing security tools into the already existing CI/CD workflow, policy enforcement on a large scale, and compliance with industry rules like GDPR, CCPA, and telecom-specific standards. Also, the dynamism of cloud-natives, such as microservices and multi-cloud systems, makes it more challenging to apply the concepts of Zero Trust on a regular basis. In a nutshell of these challenges, Table 4

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

identifies the main constraints that telecom enterprises experience when implementing DevSecOps and Zero Trust solutions.

Table 4: Challenges and limitations in implementing DevSecOps and Zero Trust in telecom cloud applications.

Challenge	Description	Impact on Telecom Cloud Applications	Mitigation Strategies
Toolchain Integration	Difficulty integrating security tools into CI/CD pipelines	Slower deployment, potential security gaps	Standardized APIs, automation scripts, centralized management
Cultural Resistance	Resistance from teams to adopt security-first practices	Low adoption of security policies, fragmented responsibility	Training, awareness programs, executive support
Policy Enforcement at Scale	Complexity in applying ZTA across large, distributed networks	Inconsistent access controls, increased risk of breaches	Automated policy management, centralized monitoring
Regulatory Compliance	Compliance with GDPR, CCPA, and telecom standards	Risk of fines and reputational damage	Continuous auditing, compliance-as-code, automated reporting
Multi-cloud Complexity	Managing security across multiple cloud providers	Inconsistent configurations, increased vulnerability surface	Unified security platform, cross-cloud policies, standardization
AI/Automation Limitations	Dependence on AI-driven monitoring may yield false positives/negatives	Potential for missed threats or unnecessary alerts	Hybrid approach combining AI and human oversight, regular tuning

VI. Discussion and Future Directions

The adoption of DevSecOps and Zero Trust frameworks in telecom cloud applications offers significant improvements in security, compliance, and operational efficiency [18–23]. However, the challenges highlighted in the previous section, including toolchain integration, cultural resistance, policy enforcement at scale, and regulatory compliance, underscore the complexities of implementation [24-30]. Addressing these challenges requires not only technical solutions but also organizational change and strategic planning [31]. The following subsections explore these aspects in detail, providing insights and potential future directions for telecom enterprises seeking to strengthen their cloud security posture. As illustrated in Figure 3, successful implementation involves coordinated efforts across multiple dimensions: adopting automated and standardized security tools, fostering a culture of shared security responsibility, aligning policies with cloud-native practices, and establishing compliance as code practices.

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

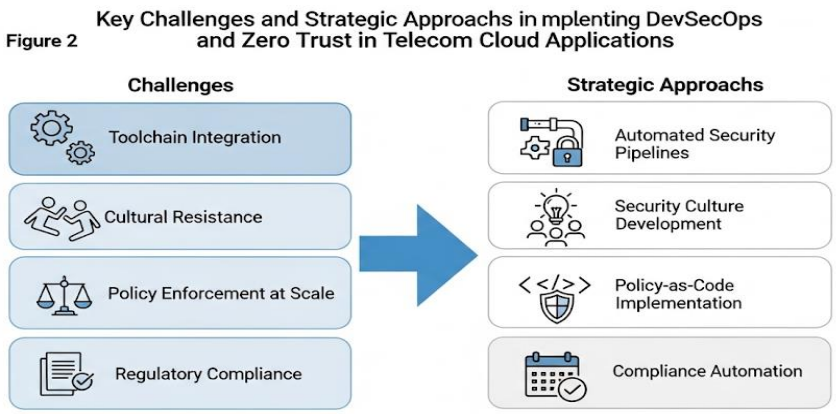

Figure 3: Key Challenges and Strategic Approaches in Implementing DevSecOps and Zero Trust in Telecom Cloud Applications

6.1 Toolchain Integration Challenges

Integrating security tools into existing CI/CD pipelines can be complex due to incompatible technologies, legacy systems, and varying vendor standards [24, 30]. Telecom enterprises often operate multi-cloud and hybrid environments, making consistent tool deployment difficult [28]. Future research and practice should focus on standardized APIs, cross-platform automation, and centralized tool management to streamline integration [30]. Advanced DevSecOps platforms that offer end-to-end security automation may further reduce deployment friction while ensuring continuous monitoring and compliance [18, 20].

6.2 Cultural and Organizational Resistance

Cultural resistance remains a significant barrier to adopting security-first practices [25, 31]. Development, operations, and security teams may perceive additional security tasks as slowing down innovation. Addressing this requires training, awareness programs, executive sponsorship, and fostering a shared responsibility culture [25, 29]. Future directions include leveraging gamification, AI-driven alerts, and dashboards that demonstrate real-time security impact to encourage adoption and collaboration across teams [29, 30].

6.3 Policy Enforcement at Scale

Applying Zero Trust principles consistently across large, distributed telecom networks is challenging [26, 31]. Ensuring dynamic access control, micro-segmentation, and continuous verification requires automation and robust governance [19]. Future frameworks should emphasize policy-as-code, automated monitoring, and adaptive risk-based access control, allowing scalable and reliable policy enforcement across multiple cloud environments and applications.

6.4 Regulatory Compliance and Multi-Cloud Complexity

Telecom enterprises must comply with global regulations such as GDPR, CCPA, and industry-specific standards [27, 31]. Multi-cloud deployments further complicate compliance due to inconsistent configurations and policy enforcement. Future strategies include continuous

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

auditing, compliance-as-code, AI-assisted monitoring, and unified multi-cloud security platforms [22, 27]. Such approaches can help maintain regulatory alignment, reduce fines, and ensure consistent security across diverse cloud infrastructures.

VII. Conclusion

Securing cloud-native applications in telecommunications requires more than traditional perimeter-based approaches. This review shows that integrating DevSecOps with Zero Trust Architecture offers a proactive framework to reduce vulnerabilities, enforce continuous monitoring, and ensure compliance. DevSecOps automates security throughout CI/CD pipelines, while Zero Trust enforces identity-centric access and micro-segmentation. Despite challenges like toolchain integration, cultural resistance, and multi-cloud complexity, this combined approach enhances security, operational efficiency, and resilience. Future efforts should focus on AI-assisted automation, policy-as-code, and unified multi-cloud governance. Adopting DevSecOps and Zero Trust is therefore a strategic imperative for telecom enterprises aiming to secure cloud applications while maintaining agility and innovation.

References:

[1] Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity, 8*(1), 12.

[2] Prates, L., & Pereira, R. (2025). DevSecOps practices and tools. *International Journal of Information Security, 24*(1), 11.

[3] Alghawli, A. S. A., & Radivilova, T. (2024). Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation. *Alexandria Engineering Journal, 107*, 136-149.

[4] Zhao, X., Clear, T., & Lal, R. (2024). Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *Journal of Systems and Software, 214*, 112063.

[5] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing, 76*(12), 9493-9532.

[6] Manda, J. K. (2020). Cloud Security Best Practices for Telecom Providers: Developing comprehensive cloud security frameworks and best practices for telecom service delivery and operations. Available at SSRN 5003526.

[7] Zhang, J. Y., & Zhang, Y. (2024). Quantitative DevSecOps Metrics for Cloud-Based Web Microservices. *IEEE Access*.

[8] Jin, Q., & Wang, L. (2021). Zero-Trust Based Distributed Collaborative Dynamic Access Control Scheme with Deep Multi-Agent Reinforcement Learning. *EAI Endorsed Transactions on Security and Safety, 8*(27), e2.

[9] Leshchenko, B., Snisar, B., Stupak, A., & Osadchyi, V. (2024). Integrating DevSecOps into the software development lifecycle: A comprehensive model for securing containerized and cloud-native environments. *CPITS II 2024-Cybersecurity Providing in Information and Telecommunication Systems, (3826)*, 153-161.

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[10] Stafford, V. (2020). Zero trust architecture. *NIST Special Publication, 800*(207), 800-207.

[11] Karthick, R. (2025). A Comprehensive Survey on AI-Enabled Cloud Security, DevSecOps, and Scalable Digital Infrastructure.

[12] Manchana, R. (2024). DevSecOps in Cloud Native CyberSecurity: Shifting Left for Early Security, Securing Right with Continuous Protection. *International Journal of Science and Research (IJSR), 13*(8), 1374-1382.

[13] Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks, 217*, 109358.

[14] Vadisetty, R., & Polamarasetti, A. (2025, July). IP Protection Strategies for AI Models. In *Proceedings of International Conference on Next-Generation Communication and Computing: NGCCOM 2024, Volume 2 (Vol. 1306, p. 115)*. Springer Nature.

[15] Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security, 133*, 103412.

[16] Amachaghi, E. N., Shojafar, M., Foh, C. H., & Moessner, K. (2024). A survey for intrusion detection systems in open RAN. *IEEE Access, 12*, 88146-88173.

[17] Joshi, H. (2024). Emerging technologies driving zero trust maturity across industries. *IEEE Open Journal of the Computer Society.*

[18] Friman, O. (2024). Agile and DevSecOps oriented vulnerability detection and mitigation on public cloud.

[19] Massoud, A. (2021). Threat Simulations of Cloud-Native Telecom Applications.

[20] Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., ... & Akan, Ö. B. (2025). Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. *IEEE Internet of Things Journal.*

[21] SIGOPS, A. International Workshop on MetaOS for the Cloud-Edge-IoT Continuum.

[22] Babar, Z. (2024). A study of business process automation with DevOps: A data-driven approach to agile technical support. *American Journal of Advanced Technology and Engineering Solutions, 4*(04), 01-32.

[23] Owoko, W. (2024). Exploring the technological advancements and security issues of 5G. *World Journal of Advanced Research and Reviews, 23*, 812-846.

[24] Alquwayzani, A. A., & Albuali, A. A. (2024). A systematic literature review of zero trust architecture for military UAV security systems. *IEEE Access.*

[25] Storey, V. C., Lukyanenko, R., & Castellanos, A. Supplementary materials for Conceptual Modeling: Topics, Themes, and Technology Trends.

[26] Gebrealif, Y., & Altmann, J. (2022, September). Effect of Trust and Institutional Quality on Cloud Federation Formation Using Agent-Based Modeling. In International Conference on the Economics of Grids, Clouds, Systems, and Services (pp. 50-61). Cham: Springer Nature Switzerland.

Received: August 09, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[27] Hossain, E., & Vera-Rivera, A. 6G Cellular Networks: Mapping the Landscape for the IMT-2030 Framework.

[28] Koneru, N. M. K. (2025). Optimizing CI/CD Pipelines for Multi-Cloud Environments: Strategies for AWS and Azure Integration. *The Eastasouth Journal of Information System and Computer Science, 2*(03), 288-310.

[29] Orisakwe, C. A. (2025). Effective Public Sector Information System Enterprise Cybersecurity Leadership Strategies (Doctoral dissertation, Walden University).

[30] Vakhula, O., Opirskyy, I., Vorobets, P., Bobko, O., & Kulinich, O. (2025). Research on Policy-as-Code for Implementation of Role-based and Attribute-based Access Control.

[31] Mohammad, N. (2021). Enhancing security and privacy in multi-cloud environments: A comprehensive study on encryption techniques and access control mechanisms. *International Journal of Computer Engineering and Technology (IJCET), 12*(2), 51-63.

Received: August 09, 2025