International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 10212-10219
http://www.ijcesen.com

ISSN: 2149-9144

Copyright © IJCESEN

Research Article

Adaptive Edge Intelligence: Integrating AI and DevSecOps for Real-Time Threat Mitigation

Vinod Kumar Thottempudi*

New England College and Henniker, New Hampshire
* **Corresponding Author Email:** vinod.thottempudi@gmail.com - **ORCID:** 0009-0007-4995-092X

Article Info:

DOI: 10.22399/ijcesen.4799
Received : 02 March 2025
Revised : 29 March 2025
Accepted : 30 March 2025

Keywords

AI-driven cybersecurity,
DevSecOps integration,
edge intelligence,
real-time threat mitigation

Abstract:

Since edge computing is a more viable functionality of real-time processing and decision-making, the traditional models of security are grotesquely incapacitated in their ability to respond to the emerging cyber menaces. The integrated application of Artificial Intelligence (AI) and DevSecOps can provide a breakthrough network in the adaptive response to threats on a decentralized platform, which requires low latency, high scalability, and enhanced responsiveness. The present paper is an edge computing system AI and DevSecOps convergence review that constitutes what is otherwise referred to as Adaptive Edge Intelligence. It discusses the most prominent mechanism of adding AI-assisted threat detection, policy enforcement, and other security inspections to the DevSecOps chain. It also takes care of the MLOps functions of the model lifecycle management, compares the models of the AI-based security, and outlines the new practices to eliminate the operational discontinuity between the DevOps and the SecOps workgroups. To establish how such integration improves the resiliency of cybersecurity, the paper discusses the current strategies and frameworks and provides compliance and allows prompt response to dynamic and distributed computing environments.

1. Introduction

The continuous enlarging of the scale and the sophistication of cyber threats have established the paradigm shift of incorporating security in the life cycles of the software development and edge computing networks. The new digital world, which is more decentralized, with data generation and processing performed at the edge, has come along with the high demand for intelligent, automated, and dynamic security models. These structures must operate dynamically and be capable of detecting and responding to attacks within rapid development cycles. The Adaptive Edge Intelligence based on the combined application of Artificial Intelligence (AI) and DevSecOps can be considered as a disruptive approach to the emerging problems. This integration is not only providing the system strength but also decreasing the lag time in responding to the threat since it is providing power to the security at the source of the data.

As far as pipelines are concerned in software development, it concerns the union of AI and DevSecOps automation of security activities, enhanced understanding of dangers, and lifelong learning. Concurrently, convergence to the edge computing infrastructures provides its near real-time response times required in industries that need to define and respond to cyber attacks, e.g., healthcare, finance, and other critical infrastructure, in a short period of time. The paper provides an overview of the existing methodology, framework, and technologies as far as the interface of AI, DevSecOps, and edge intelligence. It is provided that they will evolve to reduce threat in the real-time setting.

2. The Role of AI in Adaptive DevSecOps

The DevSecOps introduction has changed the conventional software engineering system to incorporate security as a component in the whole development process. Organizations can use security checks, compliance, and vulnerability scanning to detect and eliminate the threats during the early stages of the Continuous Integration/Continuous Delivery (CI/CD) cycle. Nevertheless, the pace and amount of developing and establishing the modern applications will not permit the acceptance of manual security practices. To manage these dynamic

requirements, AI can automate, streamline, and broaden the DevSecOps practices.

DevSecOps AI models imply the use of machine learning models to discover and process hazards and monitor anomalies in the software processes in real-time using behavior. Such models can scan code repositories, system logs, and network traffic in real time, compute deviations from normal behavior, and trigger automatic remediation actions. Excessive reliance on manual intervention undermines the scalability and efficiency that AI adoption offers, thereby minimizing the chances of false alarms in high-throughput environments [1].

Also, the model is constantly being improved, since the adaptive AI systems that are the components of the DevSecOps pipelines are constantly undergoing changes due to the reinforcement of the learning and feedback loops that are carried out. The smart systems superimpose the conventional reactive cybersecurity on the more offensive and proactive one, and the threat dwell time is minimized to a great extent. The automation and accuracy are not achievable in the fields that are hard to automate, as in the health care and financial fields, where edge computing is relevant [2].

3. Adaptive Program Management in Edge-Based AI Security

Effective threat mitigation depends on timely responses and proximity to the data source, especially in edge computing setups where AI and DevSecOps play a critical role. The adapted model of the program in this domain is the integrated deployment of the AI models, resource distribution, and activity policy, which is set to stimulate resilience within the edge infrastructures. This is majorly required in the control of distributed resources within the industrial system, remote medical system, and smart grid system.

These adaptive systems are controlled via a decentralized control, i.e., the AI models are uploaded to edge devices and autonomously act to mitigate and identify the threat without always communicating with the central servers. Response time is also very low in this decentralized form, as well as the bandwidth and latency that are eliminated. DevSecOps practices, in turn, are to be distributed beyond the cloud so that the former are facilitated to accommodate containerized deployment, live monitoring, and defensive update operations of edge nodes [2].

The two adaptive strategies - versioning of models, monitoring capabilities, and rollback capabilities - are also essential to adapt to the evolving landscape of threats. As soon as implemented in the operations of the CI/CD that will be made to adapt to the edge deployments, the organizations will be able to make sure the security patches and the changes to the models are provided without interrupting the flow of the work. Moreover, AI can be applied to provide contextual policy implementation, and, in this scenario, the policy implementation enables systems to dynamically provide access control, recording and encryption policy, and the risk assessment is unequal [3].

4. Real-Time Threat Detection and Decision-Making in Connected Environments

The number of associated equipment and cloud-edge frameworks has only increased the degree of assault in the online dimension. The previously working security measures do not work in the current times, as cybercriminals have developed better methods like polymorphic malware, phishing attacks that utilize artificial intelligence, etc. The real-time threat detection should then be responsive and predictive in nature. The feature is provided in different forms of deep learning, natural language processing (NLP), and graph-based threat modelling on the DevSecOps pipelines AI algorithms.

Artificial intelligence-driven threat intelligence engines are constantly being fed with telemetry data on applications, APIs, and user activity on such ecosystems and accumulate profile risk data. Depending on the signal correspondence across layers involving the network, application, and infrastructure, these engines enable the detection of zero-day security vulnerabilities and Advanced Persistent Threats (APTs). This also includes real-time alerting integrated with automated incident response, where an incident is repaired automatically in real time without the necessity of pressing a button [3].

Another aspect that adds to the paradigm is the edge intelligence since the AI capability can be deployed on the endpoint, and hence it can micro-segment and make a local decision. An example would be AI, which can be used to guard the integrity of the equipment, identify the intentions to add a command, and automatically deploy security baselines within the industry IoT environment. They can greatly decrease Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), whose metrics are the most appropriate indicators of cybersecurity resilience [4].

5. AI-Driven Cloud Security and Infrastructure Scalability

The problem of security of the cloud-native applications and infrastructure becomes vital due to the influx of workloads into the clouds within organizations. Data compliance and access control

are also complicated in cloud environments due to their elastic and dynamic nature. One of the trends created to fight all such complexities is intelligent automation by applying predictive analytics, policy orchestration, and live compliance validation, which is among the trends.

The AI-based cloud security systems verify the foundations of the behavior in virtual machines (VMs), containers, and serverless functions to identify the breakages that can be described as suspicious. Such learners are trained on mass data, signatures of known threats, and patterns of anomalies and can therefore be employed in a predictive manner to prevent threats. The DevSecOps process is also supported by AI and includes security baseline enforcement, patch validation, and compliance reporting [4] [20].

Scalability is the concept of cloud infrastructure enabled and dynamically delegated by the AI orchestration tools according to the sensitivity of the workload and security position. It is possible to consider an example of the suggested network segmentation policies that are dynamic according to the identified traffic pattern and the threat or no-threat level of the AI algorithms. All these flexibility features mean that even in such a case whereby scaling a system either horizontally or vertically could occur, there is no security loss realized. The DevSecOps are developed in such a way that the adaptations are configured in a way that is sufficient as a part of the pipelines of its implementation, which provides the security that is continuously available without the participation of human beings [5] [18] .

6. AI for DevSecOps: Challenges and Future Opportunities

Along with a vast array of positive features of AI, there are certain issues that can be specific to the process of implementing AI into the pipelines of DevSecOps. The quality of the training data required to generate realistic and accurate AI models and its quantity are two of the most important concerns. The data related to cybersecurity is usually very sensitive and, thus, requires a high level of privacy and anonymity. What is more, the fact that the threats posed by cyber activities are dynamic requires the models to be updated at any particular time, and thus model drift and concept drift are urgent issues that are operating in character.In addition, transparency and clarity of the application of AI in the security context should also follow. The stakeholders need to be told how and why a model will lead to such definite decisions with reference to automated access control or threat blocking. A notable concern with black-box models, including those developed through deep learning, is that in regulated industries, they must be accountable and verifiable. Methods like Explainable AI (XAI) [5] are viewed as the means of overcoming such restrictions.

The other significant issue is interoperability, that is, with non-homogeneous systems, i.e., multi-cloud, on-premise, and edge computing systems. The APIs, data formats, and governance protocols need to be united to ensure that it is easy to introduce the AI tools to other platforms and languages. It provides a new benchmark for additional research undertakings on the development of universal DevSecOps models that can be applicable to numerous computing settings yet without the necessity of altering security postures of the systems [6] [17] .Figure 1 illustrates the architecture of Adaptive Edge Intelligence, where AI-driven DevSecOps pipelines interface with edge devices for real-time security enforcement.

7. MLOps and AI Model Lifecycle Management at the Edge

MLOps operations plus machine learning are gaining relevance as a problem related to the implementation of AI in DevSecOps environments and, specifically, at the edges. To implement machine learning in production, it must be trained continuously, tested continuously, deployed continuously, and monitored in the form of automated pipelines. This is made worse when taken to the extreme, where hardware is never homogeneous, connection is discontinuous, and resources are limited.

The development of the MLOps lifecycle is required to implement AI models at the edge and utilize them as the basis of security intelligence in real-time. The models of this versioned lifecycle are performance degradation and rollback models of performance monitoring. The deployment of newly trained models and their redeployment in response to evolving threats should be performed on updated datasets with minimal or no service disruption to edge nodes. This is made possible through MLOps that offers resiliency, traceability, and reproducibility throughout the model pipeline [6].

In addition to that, the process of introducing MLOps with security should be conducted as well to avoid the manipulation of AI adversarially. Hackers can corrupt the training data, block model output, or compromise holes in the inference pipeline. At this, AI security should be controlled through DevSecOps, i.e., threat modeling. This will make sure that safety is one of the natural features of the AI-controlled pipelines and not a side effect [7] [19] .

The edge environment monitoring models also facilitate adaptive mitigation. Taking an example, if a deployed model begins to indicate incorrect network behavior classification with stale information, then the systems to identify abnormalities will take action, and the question would be that the model is not right and a new update of the model is needed. This kind of feedback loop brings in resilience and responsiveness of systems such that the latency and reliability of these systems are of utmost interest to the integrity of the operation.

8. DevSecOps for Cloud-Native and Microservice Architectures

Microservices, containerization, and serverless computing have gained popularity in the development of cloud-native models. Such paradigms can be adopted to implement agility and scalability, and the increase in the number of attack surfaces, workloads, and vulnerability of the inter-service can also be viewed as a complex security issue. The challenges can be overcome with the assistance of DevSecOps that may offer observability and automation of security throughout all the stages of the application lifecycle through the implementation of AI.

The microservice architecture can be leveraged by deploying AI-based applications to track inter-service calls, real-time logs, and patterns of lateral movement to identify breaches. DevSecOps pipelines are proactively pumped with such lessons to ensure that security baselines are enforced, remediation scripts are automatically executed, and audit-ready logs are produced. Since the tools are launched at the orchestration tier of containers, e.g., Kubernetes, systems can obtain insight into the behavior of workloads at an exceptionally detailed tier [7].

Besides that, the cloud-native systems can also host DevSecOps, whose infrastructure settings are defined in Infrastructure as Code (IaC). The IaC scripts represented as misconfigurations, policy violations, and access aberrations can also be detected by trained AI models that are based on historic configuration weaknesses. These tests comprise the pipelines of the CI/CD, and this implies that insecure releases are not under production at all.The microservices are dynamic as well and need dynamism in the enforcement of policy. AI allows adjusting the policies until the time of their enforcement depending on the dynamics of behavior and automatic opening and closing of restrictive features. It is an active process where an individual does not need to reset it manually, hence the convenience of making it functional even as reconfiguring services or the addition of new services is done. In addition to that, canary deployments and feature tortures as a subset of DevSecOps would also potentially help to ensure that the new feature could be tested in the real world with a minimal number of risks.

9. Comparative Perspectives on AI-Driven DevSecOps Models

Probably, the comparison of other AI-based security solutions in DevSecOps shows that their solutions are at different maturity, scalability, and complexity levels. Other models have interest in pattern recognition, where AI is used as signature-based detection, but others involve behavior-based analysis, where unsupervised learning algorithms are used. One of them is a trade-off in terms of accuracy, explainability, and computation requirements.

In both instances, hybrid methods suggesting supervised and unsupervised learning have huge performance in the recognition of unidentified threats. These models are trained using labeled data while also enabling the detection of anomalies that fall outside the training distribution. They are implemented to advantage, especially in edge environments in which a zero-day threat can spread without detection. On the other hand, rule-based AI systems lack flexibility and may fail to adapt to new threat vectors [8] [21].

Integration effort and the necessity to establish data-based models, including building domain-related data, can be listed among the challenges that AI-driven DevSecOps adoption will need to address. The security models (Enterprise IT trained) are not perfect tools that can be applied in operational technology (OT) and IoT networks. In this respect, retraining and customization of the model, which is founded on the concrete situation, is the main determinant in ensuring that detection rates are similar.

Another consideration that should be taken in comparative consideration is scalability. Although the list of AI security systems that can be deployed on a cloud-native infrastructure is not zero, not all of them will be able to run on edge computing resource limits. Model pruning is also used in optimization methods, as is federated learning, and they are currently under investigation to further optimize on smaller hardware.

Moreover, organizational preparation may prove to be relevant when it comes to the establishment of the efficacy of such models. Only a cross-functional approach can make the collaboration between data scientists, security engineers, and DevOps practitioners successful. Another prevalent

DevSecOps maturity model that is being widely propagated is AI-readiness to establish the potential of an organization to bring intelligent security tools into practice [9] [16] .

10. Policy Enforcement and Vulnerability Management

The speed, accuracy, and compliance that are attained due to the use of AI are another factor that makes the implementation of policies significant. Old-fashioned engine policy relies on existing regulations, which are most likely to be overtaken in a dynamic threat environment. To improve such engines, AI gets acquainted with real-time work, and the policies are automatically modified regarding the existing risk.

The policy enforcement AI access contextual control can be implemented with the use of AI-based policy enforcement systems with dynamic variables, including user behavior, location, the nature of the device, and system vulnerabilities. The degree of trust is calculated on a continuous basis, and revoked or delegated privileges are granted, respectively, using these systems, also referred to as identity and access management systems (IAMS). Security is also fine-tuned, scalable, and restricted on the policy layer, which is specifically useful in distributed and hybrid environments with the assistance of AI [9].

Vulnerability management is one of the weak points of traditional security operations that can be enhanced with the assistance of AI-based automation. AI-based vulnerability scanners assist in identifying known vulnerabilities, and it will also be identified according to the possibility of zero-day vulnerability presence because the frequency of patterns and settings of the code is established. According to this, issues are prioritized on the principle of which issues can be exploited and which assets are of utmost importance, and the results are automatically pumped into remediation pipelines.This feedback loop supports the 'Secure by Design' principle in CI/CD environments. Real-time code fix alerts and proposed developments are provided to development teams and patch management and rollback to operations teams. Such continuous change will make it possible to ensure that by the time vulnerabilities are tapped, they will have been patched, and therefore quicker recovery and overall resiliency will be achieved [10] [15] .

11. Bridging the Gap Between DevOps and SecOps Through AI

The orthodox dilemma concerning the establishment of modern software is the disparity between culture and development teams (DevOps) and security teams (SecOps). The impact of AI is that it is a negotiator since it offers similar and standardized tools, measurements, and insights that can incorporate both functions with a single goal of safe and sound software delivery.

The process of such convergence can be made possible with the help of AI that creates a single layer of threat visibility and is perceived by every stakeholder. It is a layer that is utilized to draw together information in the application stack, correlate security incidents, and act with the assistance of dashboards and notifications. This intelligence can be used by development teams to optimize application code and dependencies, and security teams can use it to optimize detection rules and incident response plans.In addition, AI can also be implemented in the automation of security governance in order to authorize alignment of policies within the environment. To take a case in point, AI engines can be utilized to make sure that regulations of encryption, identity checks, and firewall settings are introduced at any time irrespective of the residence location. This minimizes compliance drift and creates audit preparedness during the lifecycle of software [11] [14].

The integration of AI also fosters a culture of continuous security learning across development and operations teams. AI provides security data, which is used operationally in response, and developers and engineers are trained. It leads to improved coding, minimization of security debt, and cross-team work.

Figure 2 shows how AI-driven DevSecOps significantly reduces response times compared to traditional security methods in key operational metrics.

12. Real-Time Security Beyond Zero Trust at the Edge

The trend is also developing toward a less Zero Trust architecture-oriented and more responsive, context-based security model. Another aspect that is of great concern in edge environments is real-time access control and threat monitoring, wherein latency and autonomy are the utmost priority. AI augments this idea by researching indefinitely on edge activities and revising control mechanisms on the threats under consideration.

These systems offer dynamic risk scoring to evaluate access requests based on device identity, network context, and user behavior history. AI can either create or delete access controls in a few milliseconds and thus allow Just-in-Time (JIT) security posture. Such a fine level of control is needed in high-risk systems such as industrial control or networked

healthcare systems, where a slow response may result in fatality [12] [13] .

In addition to access control, operational integrity on the edge is also seen with the help of AI. These are process whitelisting, sensor behavior control, and device fingerprinting. These systems ensure that legitimate processes are applied and hardware settings are not ad hoc baselines. Deviation reporting and treatment are also covered and handled separately and do not need the involvement of central security departments.

Moreover, federated learning and distributed model training can be used to provide edge devices with the opportunity to train detection capacity without disclosing sensitive data. This would meet privacy requirements and increase risk consciousness towards decentralized infrastructures.

AI is applied in different fields and reported in the literature [22-33].

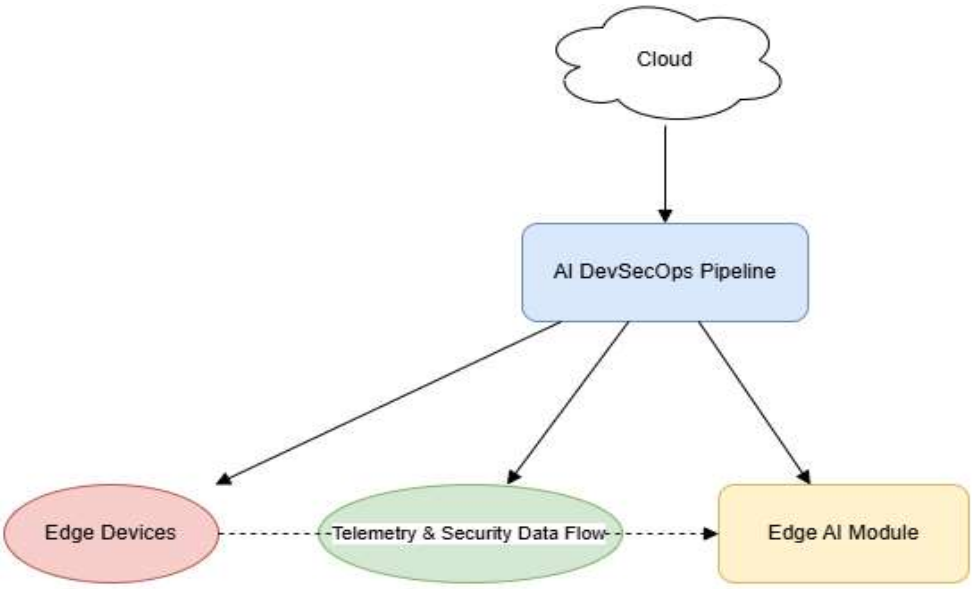


Figure 1*: Diagram of Adaptive Edge Intelligence Architecture [1][4][6][11]*

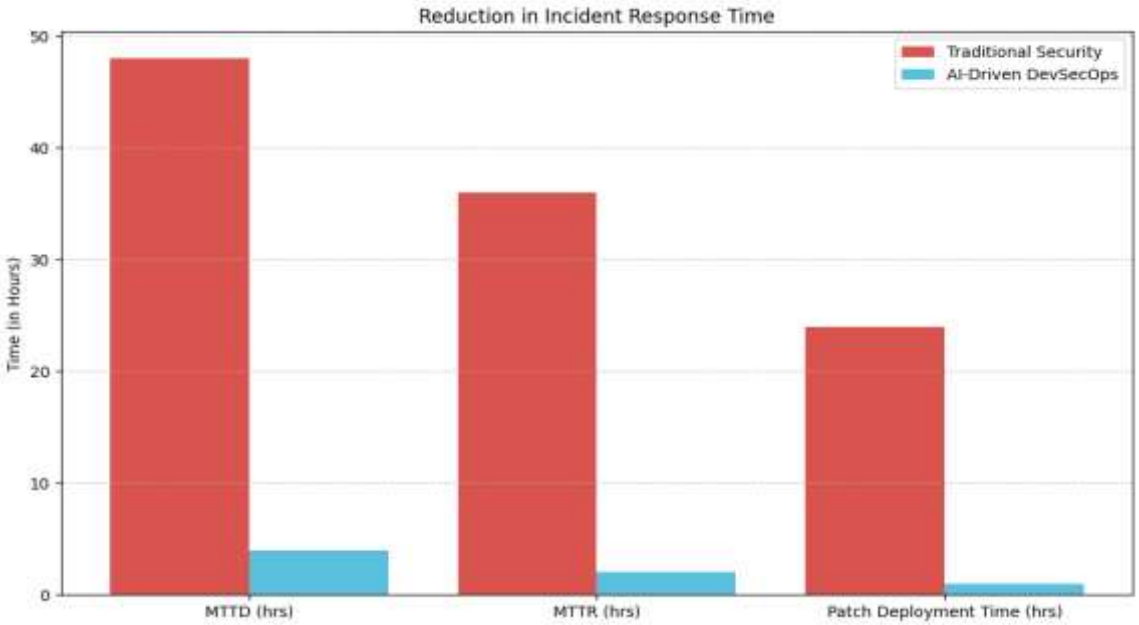


Figure 2: *Reduction in Response Time with AI-Driven DevSecOps [1][5][8][9]*

Table 1: *Key Capabilities of AI-Driven DevSecOps for Edge Environments*

Capability	Functionality	Impact
Threat Intelligence Automation	Real-time threat analysis from telemetry data	Reduced response time
Behavior-based Anomaly Detection	Identification of deviations from baseline behavior	Early threat detection

Continuous Compliance Enforcement	Automated checks for regulatory alignment	Improved audit readiness
Edge Model Deployment	On-device AI for localized decision-making	Lower latency and bandwidth consumption
Context-Aware Policy Management	Dynamic access and security configurations	Adaptive risk-based controls

13. Conclusions

It is possible to regard adaptive edge intelligence as one of the most essential innovations within the realm of real-time cybersecurity, and this objective is attained with the help of the tactical partnership between AI and DevSecOps. Convergence empowers organizations to gain operational distributed infrastructures, which take into account intelligence and mechanization throughout growth levels and the pipeline lifecycle of operation. AI-driven DevSecOps models are dynamic, precise, and valid since they provide solutions to threat detection, policy implementation, and edge deployment, among other cloud-native solutions.

The transformation of traditional security systems into adaptive and predictive models will continue as AI advances and edge computing evolves. It can be anticipated that future work will be engaged in further openness of models, expertise of MLOps approaches, and similarity of DevSecOps implementation in other locations. The cyber environment is becoming multifaceted, and hence smart solutions are the only ones that can offer speed and responsiveness of proactive reaction to threats.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Yulianto, S., & Ngo, G. N. C. (2024, September). Enhancing DevSecOps Pipelines with AI-Driven Threat Detection and Response. In 2024 International Conference on ICT for Smart Society (ICISS) (pp. 1-8). IEEE.

[2] Muthusamy, M. (2022). AI-Enhanced DevSecOps architecture for cloud-native banking secure distributed systems with deep neural networks and automated risk analytics. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(6), 7807-7813.

[3] Kyler, T. (2024). AI-Driven DevSecOps: Integrating Security into Continuous Integration and Deployment Pipelines.

[4] Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research, 13(8), 11-27.

[5] Gandhi, S. T. (2024). Enhancing Software Security with AI-Powered SDKs: A Framework for Proactive Threat Mitigation. International Journal of Computer Technology and Electronics Communication, 7(2), 8507-8514.

[6] Kummarapurugu, C. S. (2022). A Framework for Real-Time AI-Driven Secure Code Analysis Integrated with DevSecOps in Cloud-Native CI/CD Pipelines.

[7] Al-Nuaimi, Y. A. S. (2022). A Federated Cloud Security Framework for Financial Networks Multi-Source Threat Correlation, Adaptive Caching, DevSecOps Automation, and ERP Strategy Planning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(6), 7814-7821.

[8] Rangaraju, S., Ness, S., & Dharmalingam, R. (2023). Incorporating AI-driven strategies in DevSecOps for robust cloud security. International Journal of Innovative Science and Research Technology, 8(23592365), 10-5281.

[9] Parasaram, V. K. B. (2024). Real-Time Risk Forecasting in Serverless DevOps: A Meta-Learning Approach. International Journal of Humanities and Information Technology, 6(02), 26-29.

[10] 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.

[11] Kumar, M., & Kaushik, D. (2024). Current trends in it. Pranjana: The Journal of Management Awareness, 27(1and2), 127-134.

[12] Cui, J. (2024). The enhancement of software delivery performance through enterprise devsecops and generative artificial intelligence in chinese technology firms. arXiv preprint arXiv:2411.02255.

[13] Prabakaran, M. J. (2024). Autonomous DevOps-Driven Zero-Trust AI Governance for Rural Healthcare and Financial Cloud Environments with SAP Optimization. International Journal of Research and Applied Innovations, 7(6), 11802-11806.

[14] Olabowale, B. (2024). SCALABLE TEST INTELLIGENCE FRAMEWORKS FOR HIGH-RELIABILITY SOFTWARE SYSTEMS.

[15] Sotiropoulos, J. (2024). Adversarial AI Attacks, Mitigations, and Defense Strategies: A cybersecurity professional's guide to AI attacks, threat modeling, and securing AI with MLSecOps. Packt Publishing Ltd.

[16] Neha, R., Jonathan, M., & Ali Hassan, A. T. (2024). Predictive Maintenance in Software Systems: Leveraging AI and Data Science to Reduce Failures in Continuous Deployment Environments. International Journal of Informatics and Data Science Research, 1(9), 72-89.

[17] Hussain, A., & Shabir, G. (2024). AI-Powered DevSecOps: Elevating Security Practices with Machine Learning.

[18] Thota, R. C. (2024). Cloud-Native DevSecOps: Integrating Security Automation into CI/CD Pipelines. INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH AND CREATIVE TECHNOLOGY, 10(6), 1-19.

[19] Zaydi, M., Khourdifi, Y., Nassereddine, B., & Zhang, J. (Eds.). (2024). Agile Security in the Digital Era: Challenges and Cybersecurity Trends. CRC Press.

[20] Sadovykh, A., Truscan, D., Ahmad, T., Schneider, M. A., Mallouli, W., Cavalli, A., & Seceleanu, C. (2024). Smart Assistants for Enhancing System Security and Resilience.

[21] Chatterjee, P., & Das, A. (2024). Enhancing Software Security: A Research-Driven Automation Framework. International Journal of Scientific Research and Management (IJSRM), 12(12), 10-18535.

[22]Hafez, I. Y., & El-Mageed, A. A. A. (2025). Enhancing Digital Finance Security: AI-Based Approaches for Credit Card and Cryptocurrency Fraud Detection. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.21

[23]Attia Hussien Gomaa. (2025). Value Engineering in the Era of Industry 4.0 (VE 4.0): A Comprehensive Review, Gap Analysis, and Strategic Framework. *International Journal of Natural-Applied Sciences and Engineering*, *3*(1). https://doi.org/10.22399/ijnasen.22

[24]Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.19

[25]Nadya Vázquez Segura, Cruz García Lirios, Isabel Cristina Rincón Rodríguez, Vivian Vannesa Vargas Mazuela, Jorge E. Chaparro Medina, Rosa María Rincón Ornelas, … Josefina Haydeé Guitiérrez Hernández. (2025). The Declaration of Helsinki and the Evolution of Ethics in Medical Research. *International Journal of Natural-Applied Sciences and Engineering*, *3*(1). https://doi.org/10.22399/ijnasen.25

[26]Nadya Vázquez Segura, Felipe de Jesús Vilchis Mora, García Lirios, C., Enrique Martínez Muñoz, Paulette Valenzuela Rincón, Jorge Hernández Valdés, … Oscar Igor Carreón Valencia. (2025). The Declaration of Helsinki: Advancing the Evolution of Ethics in Medical Research within the Framework of the Sustainable Development Goals. *International Journal of Natural-Applied Sciences and Engineering*, *3*(1). https://doi.org/10.22399/ijnasen.26

[27]García, R. (2025). Optimization in the Geometric Design of Solar Collectors Using Generative AI Models (GANs). *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.32

[28]Attia Hussien Gomaa. (2025). From TQM to TQM 4.0: A Digital Framework for Advancing Quality Excellence through Industry 4.0 Technologies. *International Journal of Natural-Applied Sciences and Engineering*, *3*(1). https://doi.org/10.22399/ijnasen.21

[29]Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.18

[30]Chui, K. T. (2025). Artificial Intelligence in Energy Sustainability: Predicting, Analyzing, and Optimizing Consumption Trends. *International Journal of Sustainable Science and Technology*, *3*(1). https://doi.org/10.22399/ijsusat.1

[31]García, R., Carlos Garzon, & Juan Estrella. (2025). Generative Artificial Intelligence to Optimize Lifting Lugs: Weight Reduction and Sustainability in AISI 304 Steel. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.22

[32]Fabiano de Abreu Agrela Rodrigues. (2025). DWRI as a New Neurobiological Perspective of Global Intelligence: From Synaptic Connectivity to Subjective Creativity. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.24

[33]Fabiano de Abreu Agrela Rodrigues, Flavio Henrique dos Santos Nascimento, André Di Francesco Longo, & Adriel Pereira da Silva. (2025). Genetic study of gifted individuals reveals individual variation in genetic contribution to intelligence. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.25