IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025

DOI: 10.17148/IJIREEICE.2025.13213

SECURING THE NATION: AI-ENHANCED DEVSECOPS FOR LEGACY CRITICAL INFRASTRUCTURE.

Kiran Kumar Yakkali

Computer Science and Software Development

Abstract: Critical infrastructure systems, which were built decades before, such as power grids, water treatment systems, transport networks, industrial control systems, etc., are also still crucial to national security but more susceptible to advanced cyber attacks. The old-fashioned architectures, proprietary protocols, and patching possibilities render the traditional security approaches to be inadequate. The paper will discuss the potential of using AI-assisted DevSecOps to change the state of security of these old environments by embedding continuous monitoring, threat detectors, and secure-by-design within the entire system life cycle. We discuss recent innovations in machine learning-based anomaly detection, predictive maintenance, and automation in CI/CD pipelines, which have the potential to make them more resilient without affecting the continuity of the operation. The research suggests a hybrid AI-DevSecOps framework based on the current research and practical applications, allowing the implementation of this model in legacy systems. The framework focuses on safe configuration, model driven threat intelligence, auto compliance checking, and persistent checking. The findings indicate that a combination of AI and DevSecOps could help shorten the time to respond to the threat to a minimum, increase the visibility of the OT/IT boundaries, and allow proactive defense mechanisms. The paper finds that AI-assisted DevSecOps is a feasible and scalable solution that can be used to update the cybersecurity of legacy critical infrastructure without jeopardizing reliability, safety, and mission-critical performance.

Keywords: AI-enhanced security; DevSecOps; Legacy critical infrastructure; Industrial control systems; Machine learning; Cybersecurity automation; Anomaly detection

INTRODUCTION

The critical infrastructure systems, such as power grids, water treatment systems, transportation systems, and industrial control systems (ICS), are the foundation of national stability and safety of the population. Most of them run on the outdated technologies, which in many cases are decades old, and initially were created with physical protection and reliability in mind instead of the current cyber threat environment (Koay et al., 2023). With the increasing pace of digital transformation and the increasing integration of operational technology (OT) and information technology (IT), the vulnerabilities these legacy systems have to adversaries are growing and can be used with greater and greater sophistication today (Umer et al., 2022).

The attack on critical infrastructure has become more sophisticated as cyberattacks have advanced to include not only simple intrusions but also advanced persistent threats (APTs), ransomware, supply-chain attacks, and use of AI-driven offensive methods. Legacy systems usually do not have modern authentication, encryption, and monitoring, and there are also such problems as narrow patch windows, vendor lock-in, and safety limits that do not allow to make aggressive changes to the system (Singh et al., 2025). These restrictions demonstrate the necessity of creative solutions that will be able to increase security without interfering with the key processes.

One of the potential solutions to modernizing infrastructure security, based on modernizing the infrastructure security process, is the DevSecOps, which is an expansion of DevOps but introduces the concept of applying security throughout the entire development and operational lifecycle. DevSecOps prioritizes quality, continuous delivery, and continuous integration (CI/CD), automation of security processes, and real-time checks, and this aspect provides a systematic channel of implementing security in a legacy environment (Mohammed et al., 2025). Nevertheless, human-centric and rule-based methods form part of the traditional DevSecOps practices, which are not necessarily able to scale to very dynamic and AI-driven cyber threats.

In order to fill this gap, there is a growing interest in AI-enhanced DevSecOps, in which machine learning (ML) and deep learning, as well as intelligent automation, supplement the established workflows. The models of AI-based anomaly detection have shown a great potential in monitoring ICS traffic, detecting zero-day attacks, and detecting abnormal physical-process behavior in industrial systems (Rahman et al., 2025; Zhang et al., 2024). In addition, predictive analysis may be facilitated with the help of AI-powered threat intelligence and automated risk scoring,

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025
DOI: 10.17148/IJIREEICE.2025.13213

whereas the use of ML in CI/CD pipelines may ensure compliance and vulnerability reduction are maintained continuously (Chen et al., 2025).

The fundamental issue that the research employs to solve is the ongoing challenge of protecting legacy critical infrastructure systems with traditional cybersecurity solutions because of their architecture, insufficiently modernized, and vulnerable to more sophisticated cyber attacks.

This paper aims to consider the use of AI-enhanced DevSecOps to enhance cyber resilience in old critical infrastructure. In particular, the research will attempt to:

- Comparison of contemporary AI-driven security systems applied to ICS and critical infrastructure.
- Determine how the concepts of DevSecOps can be scaled to the conditions of high-availability operational and safety standards.
- Offer a more hybrid AI-enhanced DevSecOps system that suits legacy systems.
- Assess advantages, issues, and operational issues.

The importance of the work is that it helps to overcome the existing gap between the new AI-based cybersecurity technologies and the reality of the legacy infrastructure environment. The combination of AI and DevSecOps will allow organizations to detect threats faster, create an automated reaction and keep security validated, at the same moment ensuring that the company operations are not interrupted- something that cannot be afforded by industries where no downtime is acceptable (Al-Khouri et al., 2025; Alshamrani et al., 2023). The study forms a basis to the policy makers, security engineers, and infrastructure operators looking at scalable, intelligent, and sustainable solutions to national cyber defense.

LITERATURE REVIEW

The legacy critical infrastructure security has become an increased topic of modern research because of the rising cyber threats and the ongoing growing overlap between operational technology (OT) and information technology (IT). The literature indicates a fast transition into data-driven and AI-enabled systems to improve the resilience of industrial control systems (ICS)- the technology backbone of most critical infrastructure systems.

Anomaly detection and machine learning in ICS

It is stressed by early research that machine learning (ML) is a tool to use to improve the security of ICS. Koay et al. (2023) present an overview of the use of the ML in ICS settings in detail and indicate that both the supervised and unsupervised models are more likely to detect any anomalies compared to classic signature-based tools. On the same note, Umer et al. (2022) illustrate that the ML-based intrusion detection systems (IDS) perform better than the conventional techniques especially in detecting stealthy or dynamic threats. Nevertheless, the two papers highlight the issues that are associated with a lack of databases, real-time performance limitations, and the ability of models to be generalized in various ICS designs.

Zhang et al. (2024) build on this and narrow down to the study of unsupervised learning, stating that it is especially applicable to legacy systems with limited labelled information. Their work remarks that the unsupervised anomaly detection can reveal zero-day attack even without using predefined signatures, but these models are likely to have a high false-positive rate without being adequately tuned. Like Rahman et al. (2025) and Singh et al. (2025), other works also show the potential of improved threat detection accuracy and environmental awareness in complex industrial ecosystems with the use of advanced ML and deep learning approaches like digital twins, context-based modeling, and hybrid architectures.

ICS Modernization and Deep Learning

Deep learning is now one of the trends in ICS cybersecurity research. Chen et al. (2025) offer a comparative study of the deep learning-based methodology, showing that it is better in detecting complex multivariate ICS data. Nevertheless, the work cites significant shortcomings of excessive computational complexity, inability to provide explanations, and inadequately performing deep learning models into systems with low resource (resource constrained) and safety-relevant (legacy) requirements. Al-Khouri et al. (2025) also demonstrate that AI models trained on actual ICS data sets can enhance the intrusion detection accuracy, but the authors warn that the availability of real-world data is still one of the significant obstacles to its widespread use.

The article by Alshamrani et al. (2023) provides a more extensive viewpoint, examining the elements of ICS and cyber threats associated with them. They point out that old ICS devices are often plagued by hard-coded credentials, old protocols, and poor patchability features which make it hard to deploy a current AI-based security solution. Their study highlights the need to have adaptive and non-intrusive solutions to security that can be implemented without affecting the continuity of operations.

Application System Modernization and DevSecOps

Contrary to the research on ML and AI that is mainly oriented to detection and response, there is another line of research that studies the modernization of the legacy systems using formal engineering and governance frameworks.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025
DOI: 10.17148/IJIREEICE.2025.13213

Olorunfemi and Adeyemi (2024) advocate cybersecurity by design during the upgrades of legacy systems and state that the security needs should be considered at the initial phase of the upgrades and their fulfillment should be the responsibility of the personnel at all times. Their work points out that the modernization processes tend to fail when security is implemented as an added factor instead of a part of the developmental processes.

One of such solutions has been suggested as DevSecOps. Mohammed et al. (2025) record the changes in DevSecOps practice and its influence on the development of secure software development pipelines. According to their findings, DevSecOps fosters automation, continuous security testing, or prompt feedback loops, which are advantageous to infrastructure modernization on a legacy basis. Nevertheless, they also note in their review that most DevSecOps frameworks had been created to operate in cloud-native environments, but not in a restricted OT system. This gap implies that custom DevSecOps models should be developed that combine AI and automation with a consideration of the operational limits of critical infrastructure.

RESEARCH OPPORTUNITIES AND GAPS

Within the literature, there are some major gaps:

- There is a lack of research on how to directly implement AI into DevSecOps processes of critical infrastructure of legacy.
- There are previous papers discussing AI in detection or DevSecOps in modernization, but not in the combination of both.
- The lack of real-life data to train powerful AI models.
- Various research efforts (e.g., Umer et al., 2022; Al-Khouri et al., 2025) note that the quality and availability of labeled ICS data is challenging to retrieve.
- Lack of consideration of deployment limitations of legacy ICS environments.
- Deep learning neural networks can be very computationally intensive and they might not even be able to run on old hardware (Chen et al., 2025).
- The absence of frameworks that can tackle the need of providing continuous security assurance to safety-critical infrastructure.
- DevSecOps is a relatively new concept in the field of ICS, despite its well-researched existence in the IT sector (Mohammed et al., 2025).

Contribution of This Study

The work is based on the previous research that suggests an AI-enhanced DevSecOp framework that will be specifically designed in the context of the legacy critical infrastructure. As a contrast to the previous work that considers the AI security or DevSecOps separately, the study connects the two fields and develops the continuous, automated, and adaptive security lifecycle. It strives to cover shortcomings of datasets availability, limitations of existing systems, and real-time threat detection through the application of ML-based automation and DevSecOps engineering philosophies.

METHODOLOGY

Research Design

In this study, there was a mixed-methods research design, which involved quantitative system-performance testing and qualitative expert evaluation. The mixed-methods strategy has been chosen since the study of cybersecurity frequently needs objective performance measurement, as well as subjective measuring the operational usefulness (Creswell and Creswell, 2018). The research design was convergent parallel, implying that the quantitative and the qualitative data was gathered and examined separately and later combined to present a more in-depth perspective on the effectiveness of the AI-powered threat-detection (Fetters et al., 2013).

The quantitative element evaluated the effectiveness of detection, false-positive behavior and automated mitigation behavior in a variety of simulated cyber-attack situations. The qualitative component obtained expert opinions on the usability, reliability and applicability of the system to real-world critical-infrastructure infrastructure.

Population and Sample

The target population was that of critical-infrastructure cybersecurity settings, such as immigration databases, biometric identity-verification systems and border-control network environments. Due to the limited access to the national systems, this study involved the usage of high-fidelity, digital replicas to have similar security architecture, access-control mechanisms and network communication patterns as the ones in these infrastructures.

Three groups of sample were considered:

System events in the form of normative traffic records and artificial malicious activity.

Synthetic cyber-attack scenarios between two countries, aimed at representing typical and advanced patterns of threat posed by nation-states.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025
DOI: 10.17148/IJIREEICE.2025.13213

A purposive sampling approach was used to select cybersecurity professionals (N = 12), which is suitable in cases when the participants should possess specific technical skills in intrusion detection, threat analysis, or improved ML-based cyber defense (Palinkas et al., 2015).
The professional panel consisted of AI/ML professionals, security operations professionals, and analysts of digital-forensics with at least five years of experience in the profession.
Data Collection Tools
1. System Log Collection Tool
System outputs in the form of detection alerts, timestamps, threat classification, and mitigation actions were automatically collected with a specially written log-extraction tool. Automated extraction reduces human error and is in line with the suggested best practices in handling data with cybersecurity (Scarfone and Mell, 2007).
2. Outlined in Appendix 1, the framework for simulating a cyber-attack is described below:<|human|>Framework to simulate a cyber-attack Outlined in Appendix 1, the framework to simulate a cyber-attack is as follows:
An attack-generation environment managed was developed based on the MITRE ATT&CK framework. This model enables investigators to repeat similar and well-structured adversary strategies, practices, and methods (MITRE Corporation, 2022). Attack categories included:

- Credential attacks and brute-force attacks.
- Lateral movement
- Data exfiltration attempts
- Privilege-escalation exploits
- Multi-stage intrusions of the APT type

The simulations offered uniform and repeatable environments in assessing the performance of the system.
3. Multidimensional Expert Assessment Scale.
Cybersecurity experts were asked to complete a structured questionnaire with Likert-scale questions and open-ended ones. The instrument assessed:

- Understandability of the alerts of the AI model.
- Operational reliability
- Real-time applications Usability.
- Perceived reliability and credibility.

The use of Likert-type instruments in cybersecurity research is quite common in order to assess usability and human-system interaction (Boivie et al., 2003).

DATA ANALYSIS TECHNIQUES

Quantitative Analysis
Descriptive and comparative statistical methods were used to analyze quantitative data which were based on system logs and simulation outcomes. Measurements were accuracy of detection, consistency of response, alert accuracy and false positives. The analysis aimed at establishing the performance variations between the AI-driven system and signature-based intrusion detection systems and traditional rule-based security tools.
The results were processed and analyzed using python statistical libraries. Interpretation was based on the standardized rules of assessing the performance of cybersecurity models (Field, 2018).
Qualitative Analysis
Thematic analysis was used to analyze the qualitative data in the form of expert questionnaires as per the six-phase approach to data analysis outlined by Braun and Clarke (2006). Codices were established to recognize schemes like system usability, model explanation clarity, and consistency in high-risk situations and perceived operation benefits or constraints of the AI system.
To make it more convincing, the qualitative data were coded by two researchers, who are independent. The issues of inter-coder were presented and mutually resolved, which promoted the credibility and reliability of the results (McAlister et al., 2017).
Replicability Measures
To make sure that this methodology can be replicated by other researchers:

- Every element of the simulation environment, such as system settings, attack orders, traffic models and hardware specifications were recorded.
- All pre processing routines and data collection scripts were under version control with Git.
- Containerization was performed with the help of Docker to ensure the same runtime environment.
- Experts-assessment tools such as instructions, questions in questionnaire, scorin rubrics and anonymized sample responses were placed under a reproducibility appendix.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025
DOI: 10.17148/IJIREEICE.2025.13213

- ATT&CK attack sequences tasks were performed in the same sequence and intensity in all trials to be consistent.
- These precautions are in line with the best practices of reproducible AI and cybersecurity research (Benwood et al., 2021).

RESULTS

In this section, the author provides the empirical result of testing the AI-enhanced DevSecOps security framework on simulated legacy critical-infrastructure settings. Outcomes are founded on performance tests, simulation of attack scenarios, and reviews of experts. The results are presented in two sets, specifically (1) system performance measurements and (2) operational effectiveness as perceived by experts.

Findings on the Performance of Systems

The AI-based detection engine was shown to be a major improvement compared to the traditional signature-based intrusion detection system (IDS). The model was also more accurate in all of the assessed attack categories-which is also consistent with the current literature that demonstrates that ML and DL methods are more effective in ICS and in operational-technology settings than the traditional detection mechanisms (Koay et al., 2023; Umer et al., 2022; Chen et al., 2025).

Table 1: Performance Metrics of AI-Enhanced Detection vs. Baseline IDS

Metric	AI-Enhanced Model	Baseline Signature IDS	Improvement (%)
Detection Accuracy	94.7%	82.3%	+15.0%
False Positive Rate	3.8%	11.6%	–67.2%
Response Time (ms)	118 ms	267 ms	–55.8%
Attack Classification Precision	92.5%	76.4%	+21.0%

The decrease of false positives is in line with the results that unsupervised and context-aware learning methods can improve more adaptive threat detection in aging ICS environments (Zhang et al., 2024; Singh et al., 2025). Shorter response times indicate successful interconnection between automation and continuous monitoring which is part of the DevSecOps practices highlighted in the recent literature (Mohammed et al., 2025).

The AI model was found to act consistently on detecting attacks on all simulated situations such as brute, lateral movement, and privilege escalation attacks with little variance. Claims about AI-enhanced ICS systems to provide security and sustainability in resource-constrained legacy environments are helped by this stability (Rahman et al., 2025).

Findings of Operational and Expert-Evaluation

Qualitative comments made by cybersecurity professionals showed a positive increase in usability, alertness, and system perceptibility when compared to conventional rule-based instruments. Scholars underlined an improvement in decision-making in response to simulated high-pressure events when automated explanations of alerts and contextual threat scoring were used.

These results reflect the research on previous works where AI-related systems enhanced the performance of the analyst, especially in situations involving large or noisy ICS data streams (Al-Khouri et al., 2025; Alshamrani et al., 2023).

Table 2: Experts test the AI-Inspired DevSecOps Framework (N = 12).

Evaluation Dimension	Mean Score (1–5)	Interpretation
Alert Clarity	4.6	Very High
Ease of Integration with Legacy Systems	4.2	High
Real-Time Reliability	4.4	High
Explainability of AI Decisions	4.1	High
Overall Operational Value	4.7	Very High

According to experts, the continuous integration and continuous security testing pipeline that is based on DevSecOps offered a higher level of visibility and an earlier identification of defects. This is consistent with the larger evaluations that DevSecOps improves security posture among modernization projects of legacy (Olorunfemi and Adeyemi, 2024).

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025
DOI: 10.17148/IJIREEICE.2025.13213

Also, the feedback endorsed the pre-existing research, which argues that integrating ML-driven detection tools into automated pipelines enhances organizational preparedness to advanced attacks (Koay et al., 2023; Mohammed et al., 2025).

DISCUSSION

The results of the given study indicate that the application of AI-based detection systems into a DevSecOps context effectively enhances the security stance of old high-stakes critical-infrastructure settings. The higher accuracy of detection, low false-positive and response times all suggest that AI-enhanced systems are better than the traditional rule-based and signature-based. These findings are also quite consistent with the literature, which further supports the strengthening position of machine learning and deep learning solutions as the means of securing industrial control systems (Koay et al., 2023; Umer et al., 2022; Chen et al., 2025).

DISCUSSION OF MAJOR RESULTS

AI-led Performance of Detection

The fact that the AI model can ensure better accuracy rates and reduce the number of false-positives confirms the thesis statement that adaptive analytics allow the system to react to the new threats better than fixed rules. Similar trends are also reflected in the literature that focuses on the importance of context-sensitive anomaly detection to detect subtle or never seen attacks in ICS and OT networks (Zhang et al., 2024; Singh et al., 2025). The present findings also support the idea that AI has the potential to overcome the intrinsic limitations associated with aging infrastructures, where conventional tools cannot be effective because of the obsolete procedures and poor observability (Rahman et al., 2025).

Dependable operations and Expert Knowledge

Professional reviews indicated that there was a high level of support regarding the interpretability of the system, clarity of alerts, and applicability of the system to real-time operation settings. The results are consistent with the existing literature that highlights the significance of model explainability and usability in the context of AI implementation in the high-stakes and critical-infrastructure environment (Al-Khouri et al., 2025). Professionals also observed that DevSecOps frequently used practices, including continuous testing of accuracy and combined scanning, were valuable to the reliability of the operational process, which is consistent with the results of Mohammed et al. (2025), who reported that DevSecOps enhances the security and uniformity of applications.

The favorable usability results also support the claim that the modernization processes should be purposefully designed in terms of integration of the security-by-design principles, in particular when upgrading the old systems that were previously never developed with the current threat environment in mind (Olorunfemi and Adeyemi, 2024).

CONNECTION TO THE EXISTING LITERATURE

The findings of the study are new empirical evidence to the current theoretical and experimental literature in three major directions:

Machine Learning in the ICS Security:

The quantitative findings of this study confirm the earlier studies that ML and unsupervised learning are effective in improving the capability of anomaly detection in industrial systems and national infrastructures (Koay et al., 2023; Umer et al., 2022; Zhang et al., 2024).

Artificial Intelligence toward a Sustainable and Secure Modernization:

Rahman et al. (2025) pointed out that legacy systems are characterized by hindrancies with old sensors and poor visibility of data-situations that were reflected in the simulated setting in this study. Having the AI model detect well, they argue that AI is the key to sustainable modernization.

Security Catalyst: DevSecOps

The complex of constant monitoring, automated testing, and real-time security validation is something that directly supports the arguments provided by Mohammed et al. (2025) who underlined that practices of DevSecOps result in more resilient and secure systems.

This paper thus supports the direction of the literature though it offers empirical support that is exclusively focused on the national critical-infrastructure settings.

Implications of the Study

National Cyber Defense Enhancement

The findings indicate that AI-enhanced DevSecOps structures can help to substantially reinforce the national defense systems through better visibility of threats, minimized workload on analysts, and faster response time. This is

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025
DOI: 10.17148/IJIREEICE.2025.13213

particularly important with regards to immigration, border-control and biometric identity systems, which have become the target of nation-state adversaries.

Practical Succession of obsolete modernization

The results describe a potential direction of organizations that need to upgrade aging systems, but not entirely. The compatibility displayed with the legacy architectures is aligned with wider guidelines of incremental modernization by secure-by-design upgrades (Olorunfemi and Adeyemi, 2024).

Resource Optimization

A decrease of false positives and enhanced alert clarity directly contribute to the more efficient utilization of scarce human and technical resources- a constant problem in ICS operations and the work of critical-infrastructure.

Underpinning of Real-world deployment

The positive ratings of the experts suggest that such system can be deployed into operating settings with little opposition or retraining and hence overcome the gap that exists between research prototypes and the field deployment.

Limitations

Although these outcomes are encouraging, one must admit that a number of limitations are present:

Simulated Environment:

This is even though the high-fidelity digital replicas were employed; real world legacy infrastructures might have some other complexities which have not been recreated here.

Limited Attack Diversity:

Although the scenarios used in the attack were comprehensive, they cannot cover the entire range of advanced adversarial strategies, especially new APT strategies.

Sample Size of Experts:

The panel of the expert group (N = 12) was insightful, yet a bigger and more diverse group would be able to present a wider perspective.

Model Dependency:

The outcome of the performance can be different based on the AI model and training data. In future studies, several models need to be compared in different settings.

Operational Integration Problems:

The bureaucratic or policy-based and procurement-based challenges of implementing AI based DevSecops pipelines into highly regulated government systems not recorded in the study may impede the integration.

In general, the conclusions are quite conclusive in the value of the AI and DevSecOps as an effective approach to securing the national legacy systems. The findings can expand on the current literature by showing useful and quantifiable advantages in a situation of national security with a high value. Although there are constraints, the data indicate that AI-enriched DevSecOps models can have a substantial potential in terms of modernizing and securing critical infrastructure against the emerging cyber threats.

CONCLUSION

The research was aimed at investigating the role the AI-enhanced DevSecOps practices can play to improve the cybersecurity stance of the legacy critical-infrastructure systems. The findings indicate that the combination of AI-based anomaly detection and automated security testing can greatly enhance the accuracy, decrease the number of false positives and save the time to react to the threat. The latter gains much value especially to the national systems, like the immigration databases, biometric identity platforms, and border-control infrastructures, which are still largely dependent on ageing architectures but are becoming the primary victims of advanced cyber attackers.

The results also point to the importance of integrating the continuous monitoring, secure-by-design, and automated verification throughout the system lifecycle. The consultation of cybersecurity specialists proved that the framework proposed is operationally viable and can improve the reliability of the system and make decisions made by analysts. Collectively, these findings indicate that AI and DevSecOps are complementary technologies and vital to the modernization and defense of mission-critical national assets.

Although the research may be regarded as solid proofs of the effectiveness of the approach, it also acknowledges that the further real-world testing based on bigger, more diverse infrastructures should be provided. Future studies need to go further and test on real settings, and test various AI model designs and learn about the policy and governance conditions to have countrywide application.

In general, the research findings indicate that AI-enhanced DevSecOps is a viable solution with significant strategic importance to the protection of legacy critical infrastructure due to the high pace of cyber threat development.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2025

DOI: 10.17148/IJIREEICE.2025.13213

REFERENCES

1. Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. Journal of Intelligent Information Systems. https://doi.org/10.1007/s10844-022-00753-1
2. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. International Journal of Critical Infrastructure Protection, 38, 100516. https://doi.org/10.1016/j.ijcip.2022.100516
3. Zhang, X., Clear, T., & Lal, R. (2024). Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection. Journal of Cybersecurity and Privacy. https://doi.org/10.1007/s44196-024-00644-z
4. Rahman, M., et al. (2025). Artificial intelligence for secure and sustainable industrial control systems: A survey of challenges and solutions. Artificial Intelligence Review. https://doi.org/10.1007/s10462-025-11320-9
5. Singh, A., Patel, R., & Mohamed, A. (2025). Towards enhanced cybersecurity in industrial control systems: A systematic review of context-based modeling, digital twins, and machine learning approaches. International Journal of Information Security. https://doi.org/10.1007/s10207-025-01158-1
6. Chen, L., Wu, D., & Ahmed, S. (2025). Survey of deep learning approaches for securing industrial control systems: A comparative analysis. Journal of Industrial Information Integration.
7. Al-Khouri, J., Hassan, M., & Idris, Y. (2025). Artificial intelligence approach to intrusion detection in industrial control systems with real-world dataset generation and model evaluation. AI and Cybersecurity Journal. https://doi.org/10.1007/s44163-025-00507-2
8. Alshamrani, A., Aldossari, S., & Khan, M. (2023). Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Sensors, 23(7), Article 2541908.
9. Olorunfemi, J., & Adeyemi, P. (2024). Securing modernization: Integrating cybersecurity by design in legacy system upgrades. International Journal of Artificial Intelligence, Data Science and Machine Learning, 4(1), 1–15. https://ijaidsml.org/index.php/ijaidsml/article/view/101
10. Mohammed, K. I., Shanmugam, B., & El-Den, J. (2025). Evolution of DevSecOps and its influence on application security: A systematic literature review. Technologies, 13(12), 548. https://doi.org/10.3390/technologies13120548