IT Infrastructure Vulnerability Assessment

Ștefan RĂILEANU and Ștefania Loredana NIȚĂ

***Abstract*—This paper presents the development of an integrated platform for automated vulnerability assessment in modern IT infrastructures. The proposed solution addresses current organizational challenges in identifying and managing cybersecurity risks by combining scanning tools with advanced machine learning technologies.**

The platform implements a distributed and containerized architecture that enables comprehensive security evaluation at both network infrastructure and web application levels. The system integrates machine learning capabilities for automatic vulnerability classification, reducing dependence on manual processes and improving security team efficiency.

The solution provides differentiated interfaces adapted to user responsibility levels and implements a hybrid data storage strategy for performance optimization. The modular architecture enables system scalability and extensibility, facilitating integration with diverse technological ecosystems.

Validation results demonstrate the viability of a competitive alternative to expensive commercial solutions, offering organizations the ability to implement advanced vulnerability assessment capabilities with reduced costs and increased flexibility. The research contributes to the democratization of cybersecurity technologies and accelerated adoption of proactive risk management practices.

***Index Terms*—containerization, integration, Internet of Things, open-source, virtual machine.**

I. Introduction

The acceleration of digital transformation and the proliferation of cybernetic threats have transformed vulnerability assessment from a recommended practice into a critical necessity for modern organizations. Contemporary IT infrastructures, characterized by increasing complexity and interconnectivity, present extensive attack surfaces that require systematic and integrated approaches for identifying and remedying security vulnerabilities.

A. The Importance of Cybersecurity Vulnerability Assessment

The accelerated digital transformation of recent years has placed IT (Information Technology) infrastructures at the center of modern organizational operations. This growing dependence on computer systems, coupled with their complex interconnectivity, has generated unprecedented challenges in the field of cybersecurity. Systematic vulnerability assessment no longer represents merely a recommended practice, but has become a critical necessity for organizational survival in the contemporary digital ecosystem [1].

The cyberthreat landscape is transforming at an alarming pace, with attackers constantly developing new complex techniques for exploiting IT system vulnerabilities. Current statistics reveal an exponential increase in cybersecurity incidents, with associated costs exceeding millions of dollars annually at a global level [2-3]. This concerning reality underscores the critical importance of proactive identification and remediation of vulnerabilities before they can be exploited by malicious actors.

Contemporary organizations face the complexity of managing security in heterogeneous IT infrastructures that encompass diverse networks, legacy computer systems, modern web applications, cloud services, and a varied range of IoT (Internet of Things) devices. This technological diversity creates an extensive and difficult-to-manage attack surface. The lack of a unified vision regarding security status and challenges in prioritizing identified vulnerabilities constitute major obstacles in implementing an efficient cybernetic protection strategy [4].

Traditional vulnerability assessment solutions frequently present significant limitations regarding integration with diverse security ecosystems, capabilities for generating personalized reports, and providing actionable recommendations for remediation. This situation has created an urgent need for developing an integrated and comprehensive solution that combines the power of specialized scanning tools with modern technologies for analysis, reporting, and machine learning.

B. Research Objectives and Proposed System

This work aims to respond to the identified challenges through designing and developing an advanced system for evaluating IT infrastructure vulnerabilities. The proposed solution is not limited to simple aggregation of existing tools, but creates a unified and intelligent platform that transforms how organizations approach the identification, analysis, and management of security vulnerabilities.

The main objective of this work consists in developing a platform that organically integrates specialized tools Open Vulnerability Assessment Scanner[2] (OpenVAS) and Open Web Application Security Project Zed Attack Proxy[3] (OWASP ZAP) into a modern architecture based on contemporary web technologies and containerization principles. This integration is not merely technical, but represents a reconceptualization of the vulnerability assessment process, making it more accessible, more efficient, and more actionable for security teams.

The proposed system has several specific objectives that address gaps identified in existing solutions: Technology Integration for Scanning, Machine Learning Implementation for Enhanced, Scalable Architecture Development, Differentiated User Interface, Hybrid Data Management.

The developed system is characterized by several

Ș. RĂILEANU is with the Military Technical Academy "Ferdinand I", Bucharest, Romania (e-mail: stefan.raileanu@mta.ro).

Ș. L. NIȚĂ is with the Military Technical Academy "Ferdinand I", Bucharest, Romania (e-mail: stefania.nita@mta.ro).

[2] OpenVAS, https://www.openvas.org

[3] OWASP ZAP, https://www.zaproxy.org/

distinctive elements that differentiate it from existing solutions. The distributed architecture, implemented across two virtual machines, ensures clear separation of responsibilities and improved overall performance. Complete containerization of all components using Docker facilitates implementation and maintenance, while native integration with specialized vulnerability scanning utilities using specialized Application Programming Interface (API) eliminates the need for manual interventions in the scanning process.

The source code of the proposed platform can be found at https://gitlab.fsisc.ro/stefan.raileanu/Licenta.

C. Research Methodology

The methodological approach adopted in this work reflects the complexity of the proposed objectives and the necessity of combining a solid theoretical foundation with practical implementation and rigorous experimental validation. The selected mixed methodology allows detailed exploration of the studied domain, from specialized literature analysis to functional system development and testing.

The initial implementation stage was dedicated to exhaustive study of specialized literature, focusing on analysis of existing solutions for vulnerability assessment. This process included detailed examination of commercial and open-source platforms, identification of main challenges and limitations of current solutions, as well as exploration of emerging trends in cybersecurity. The comparative study of available tools provided the foundation for subsequent architectural and technological decisions.

Analysis of available technologies constituted an essential component of the research methodology. Evaluation of tools and frameworks concentrated on multiple criteria, including compatibility, performance, scalability, security, and ease of integration. This comparative analysis guided the selection of technologies used in system implementation, ensuring optimization for specific project objectives.

The design and architecture process was structured according to modern software engineering principles and industry standards. Utilization of service-oriented design methodologies and modern architectural principles ensured creation of a robust, scalable, and easily maintainable solution. Detailed software design documentation facilitated efficient development throughout all project stages.

System implementation followed the Agile Scrum methodology, with well-defined development sprints and continuous testing practices. This iterative approach allowed rapid adaptation to technical challenges encountered during development and continuous improvement of the solution based on results obtained from intermediate tests.

The testing and validation methodology was structured across multiple levels to ensure quality and reliability of the developed system. Unit testing validated the functionality of individual components, while integration testing verified the correct interaction between system modules. Performance testing evaluated the system's capacity to support the specified load of 100 concurrent users, confirming fulfillment of non-functional requirements. Security testing validated implemented protection mechanisms and identified potential vulnerabilities of the system itself.

D. Presentation of Obtained Results

Implementation of the vulnerability assessment system generated significant results that demonstrate the viability and efficiency of the proposed solution. The technical achievements exceed simple fulfillment of initial requirements, representing innovative contributions in the field of cybersecurity and integrated system development.

Complete integration of OpenVAS and OWASP ZAP scanning tools into the platform was achieved through the development of native API interfaces that facilitate scanning and allow intelligent aggregation of results in a unified interface. This integration eliminates the necessity of separate tool management and offers a consistent experience for users, regardless of the technical complexity of background operations.

Implementation of the machine learning system based on the Random Forest algorithm obtained impressive results in automatic vulnerability classification. The developed model achieves classification accuracy of over 80% for categorizing vulnerabilities according to severity and risk type, demonstrating the system's capacity to automate the analysis and prioritization process. This performance significantly reduces time required for manual evaluation and improves consistency in decision-making processes.

Performance and scalability tests confirmed the system's capacity to support 100 concurrent users, with response times maintained below the 3-second threshold for standard operations. This performance is remarkable for a system that integrates multiple complex components and processes significant volumes of data in real time.

Implementation of security mechanisms was achieved at high industry standards, including secure authentication for user session management and a robust role-based access control system. These security measures ensure that the system itself does not introduce vulnerabilities into the organizational infrastructure.

II. State of the Art

The landscape of vulnerability assessment technologies presents a complex ecosystem dominated by commercial enterprise solutions that, while technically sophisticated, pose significant challenges for military and government adoption. Contemporary cybersecurity markets are characterized by high-cost proprietary platforms that create vendor dependencies incompatible with the strategic autonomy requirements of defense organizations.

A. Commercial Solutions and Their Military Limitations

Leading commercial platforms such as Tenable Nessus[4] and Qualys VMDR[5] have established themselves as industry standards through comprehensive vulnerability databases and enterprise-grade management capabilities. However, their deployment in military environments encounters fundamental obstacles that extend beyond mere budgetary constraints. These solutions typically require continuous internet connectivity for updates and cloud-based management, creating unacceptable risks for classified and air-gapped networks that form the backbone of defense IT

[4] Tenable Nessus, https://www.tenable.com/products/nessus

[5] Qualys VMDR, https://www.qualys.com/apps/vulnerability-management-detection-response/

 Digital Object Identifier 10.32754/JMT.2026.1.04

infrastructure. The subscription-based pricing models, often exceeding several thousand dollars annually per scanner, strain government procurement processes designed around capital expenditures rather than recurring operational costs [5].

Moreover, the proprietary nature of these platforms introduces strategic vulnerabilities through vendor dependency. Military organizations require the ability to validate, modify, and maintain critical security tools independently, capabilities that commercial solutions inherently restrict through closed-source architectures and licensing constraints. The recent geopolitical tensions have further highlighted the risks of relying on commercial vendors whose business priorities may conflict with national security interests [5].

B. Open-Source Alternatives and Integration Challenges

The open-source security community has developed robust alternatives that address many commercial solution limitations. OpenVAS represents a mature, community-driven vulnerability assessment platform offering comprehensive scanning capabilities without licensing restrictions. Its transparent development model allows security professionals to examine, validate, and modify the underlying code, addressing the trust and independence requirements critical for military applications. Similarly, OWASP ZAP provides specialized web application security testing capabilities that have become indispensable for modern application security assessment.

Despite these advantages, current open-source tools present their own operational challenges. They typically exist as isolated solutions requiring significant integration effort to create comprehensive security assessment workflows. The technical expertise required for deployment and maintenance often exceeds the resources available in many government IT environments, where staff must balance multiple responsibilities beyond specialized security tool management. Furthermore, the lack of unified management interfaces forces security teams to context-switch between different tools, reducing operational efficiency and increasing the likelihood of overlooking critical vulnerabilities.

C. Government-Specific Initiatives and Their Limitations

Federal cybersecurity initiatives have attempted to address these gaps through programs like Assured Compliance Assessment Solution [6] (ACAS) and the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program [7]. While these initiatives provide standardized approaches to vulnerability assessment within government networks, they essentially repackage commercial solutions with government-specific configurations rather than fundamentally addressing the underlying dependency and cost issues [8].

For example, ACAS utilizes Tenable's technology with specific configurations to meet Department of Defense needs, but it still retains the main vendor relationship and its strategic risks. Meanwhile, the CDM program, despite its wider scope, has led to a fragmented landscape of various vendor solutions, which adds to, rather than lessens, complexity and costs for the involved agencies.

D. Machine Learning Integration Gaps

The cybersecurity research community has increasingly explored machine learning applications for automated threat detection and vulnerability analysis. Academic studies demonstrate promising results in using natural language processing for CVE (Common Vulnerabilities and Exposures) classification and ensemble learning methods for reducing false positives in vulnerability scanning [9]. However, these research advances remain largely confined to laboratory environments with minimal translation into operational security tools.

Current commercial and open-source platforms incorporate limited machine learning capabilities, typically restricted to basic anomaly detection or rudimentary risk scoring. The absence of complex automated classification systems forces security analysts to manually review and prioritize large volumes of vulnerability data, a process that scales poorly with the expanding attack surfaces of modern military IT infrastructure.

E. Containerization and Modern Deployment Paradigms

The broader IT industry has embraced containerization and microservices architectures for their scalability, portability, and operational efficiency benefits. However, security assessment platforms have lagged in adopting these modern deployment paradigms. While some commercial vendors offer containerized versions of their tools, these implementations typically maintain the same licensing restrictions and vendor dependencies that limit their utility in government environments.

The security community has not fully leveraged containerization's potential for creating integrated, scalable vulnerability assessment platforms that combine multiple specialized tools within unified orchestration frameworks [10]. This represents a significant opportunity for developing next-generation security assessment capabilities that align with modern IT operational practices while addressing the specific requirements of government and military organizations.

F. Strategic Gap Analysis

This analysis reveals fundamental gaps between available vulnerability assessment technologies and the operational requirements of military cybersecurity programs [11-13]. Commercial solutions, while feature-rich, introduce unacceptable strategic dependencies and cost structures. Open-source alternatives provide technical capabilities and independence but lack the integration and usability required for efficient operations. Government-specific programs have not successfully addressed these core challenges, essentially redistributing rather than resolving the underlying issues [11-13].

The convergence of these limitations creates a clear requirement for developing integrated, open-source vulnerability assessment platforms that leverage modern deployment technologies and automated analysis capabilities while maintaining the independence, transparency, and cost-effectiveness essential for sustainable military cybersecurity operations.

III. PROPOSED SOLUTION

The proposed integrated vulnerability assessment platform addresses identified gaps through a containerized, machine learning-enhanced architecture that unifies infrastructure and web application security testing within a single operational framework.

A. System Architecture Overview

The architecture of the proposed system is presented in Fig. 1. The solution implements a distributed two-tier virtual machine (VM) architecture optimized for military deployment scenarios. The primary VM hosts the application core, including Python Flask backend services, React frontend interfaces, and hybrid data storage infrastructure combining PostgreSQL for structured data and Elasticsearch for vulnerability indexing. The secondary VM isolates security scanning tools (OpenVAS and OWASP ZAP) to ensure system stability and enable independent scaling of scanning capabilities.

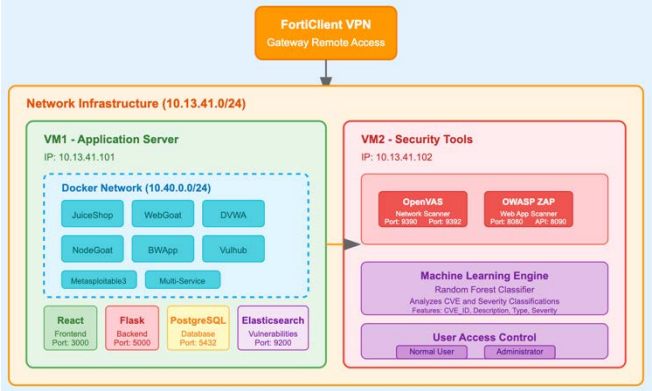

Figure 1. System architecture diagram

Network segmentation employs a dual-layer architecture: a management network (10.13.41.0/24) for administrative access via FortiClient VPN, and an isolated testing network (172.28.0.0/24) for containerized vulnerable applications. This design ensures operational security while providing comprehensive testing environments for validation.

B. Integrated Scanner Orchestration

The platform eliminates tool fragmentation through unified API orchestration of heterogeneous security tools. OpenVAS integration utilizes Greenbone Management Protocol[6] (GMP) for comprehensive infrastructure assessment, supporting both authenticated and unauthenticated scanning modes with real-time progress monitoring. OWASP ZAP integration leverages REST APIs for web application security testing, enabling both passive spidering and active penetration testing with configurable intensity levels.

Asynchronous task management through Celery[7] and RabbitMQ[8] enables parallel execution of multiple scan types while maintaining system responsiveness. The orchestration layer abstracts tool-specific complexities, presenting users with unified interfaces regardless of underlying scanner technologies.

C. Machine Learning Classification Engine

Automated vulnerability classification employs Random Forest [14] algorithms trained on comprehensive CVE and National Vulnerability Database [15] (NVD) datasets comprising 38,311 vulnerability records. The ML pipeline includes a multi-stage text preprocessing module comprising HTML tag removal, special character normalization, and TF-IDF vectorization with a 10,000-feature limit.

The classification system achieved 83.2% overall accuracy in categorizing vulnerabilities across 13 distinct types, including SQL Injection, Cross-Site Scripting, Buffer Overflow, and Remote Code Execution. Feature extraction combines textual analysis through n-gram patterns (1-2 word combinations) with categorical attributes, including vulnerability type patterns, severity indicators, and technical keyword presence.

D. Containerized Deployment Strategy

Complete containerization through Docker ensures deployment consistency across diverse military IT environments while eliminating dependency conflicts. The container orchestration strategy separates compute-intensive scanning operations from interactive user services, enabling independent resource allocation and scaling.

Container security implements the principle of least privilege with minimal attack surfaces, isolated network namespaces, and secure secrets management for scanner credentials. This approach facilitates deployment in air-gapped environments common in military networks while maintaining operational security requirements.

E. Role-Based Access Control

The platform implements differentiated user interfaces aligned with military organizational structures. Junior Security Engineers receive streamlined interfaces for scan execution, vulnerability analysis, and remediation tracking within their areas of responsibility. Senior Security Engineers access comprehensive administrative capabilities, including user management, system-wide reporting, and strategic vulnerability trend analysis.

Authentication employs JWT tokens with configurable expiration and automatic rotation, while authorization granularity extends to individual vulnerability records and scanning targets based on organizational hierarchy and clearance levels.

F. Hybrid Data Architecture

Strategic data partitioning optimizes performance through specialized storage technologies. PostgreSQL manages structured operational data, including user accounts, scan configurations, and audit trails, leveraging ACID compliance for critical security operations. Elasticsearch handles high-volume vulnerability data with full-text search capabilities, real-time aggregations, and horizontal scaling to accommodate growing datasets.

This hybrid approach enables sub-3-second response times for standard operations while supporting complex analytical queries across large vulnerability datasets without performance degradation.

[6] Greenbone Management Protocol, https://docs.greenbone.net/GSM-Manual/gos-22.04/en/gmp.html
[7] Celery, https://docs.celeryq.dev/en/stable/
[8] RabbitMQ, https://www.rabbitmq.com/

 Digital Object Identifier 10.32754/JMT.2026.1.04

G. Cost-Effectiveness and Strategic Independence

The open-source foundation eliminates recurring licensing costs while providing complete source code transparency essential for military security validation. Modular architecture enables incremental capability expansion without vendor dependencies, supporting long-term strategic autonomy in cybersecurity operations.

Platform design prioritizes air-gapped deployment scenarios common in classified environments, with offline operation capabilities and local vulnerability database management eliminating external connectivity requirements during security assessments.

IV. Results and Discussion

This section presents comprehensive validation results demonstrating the effectiveness of the integrated vulnerability assessment platform in military operational scenarios. Testing was conducted across multiple dimensions, including functional capabilities, machine learning performance, system scalability, and operational integration, to verify compliance with defense cybersecurity requirements. The evaluation methodology employed controlled testing environments with deliberately vulnerable applications alongside performance benchmarking under simulated operational loads representative of military IT infrastructure assessments.

A. Functional Validation

System validation was conducted using deliberately vulnerable applications, including JuiceShop[9], DVWA[10], and WebGoat[11] deployed in containerized testing environments. The integrated platform successfully demonstrated unified vulnerability assessment capabilities across both infrastructure and web application domains.

Scanner integration testing confirmed reliable orchestration of OpenVAS and OWASP ZAP through native API interfaces. Comprehensive vulnerability detection results are summarized in Table I, demonstrating the system's capability to identify diverse security issues ranging from configuration weaknesses to code-level vulnerabilities.

Table I. Vulnerability Detection Results from JuiceShop Assessment

Severity Category	Vulnerabilities Detected	Percentage of Total	Primary Vulnerability Types
Informational	52	18.5%	Information disclosure, missing headers
Low	100	35.6%	Configuration issues, weak policies
Medium	129	45.9%	Authentication bypass, injection flaws
Total	281	100%	Cross-domain security assessment

The detection profile aligns with expected vulnerability distributions in modern web applications while confirming the platform's effectiveness across multiple security domains. The predominance of medium-severity vulnerabilities reflects the comprehensive nature of the assessment, capturing both surface-level configuration issues and deeper application logic flaws typical of complex web applications.

B. Machine Learning Classification Performance

The Random Forest classification engine achieved solid performance metrics on vulnerability categorization tasks. Training on 38,311 CVE and NVD vulnerability records with an 80/20 training-testing split demonstrated effective automated classification capabilities for military cybersecurity applications.

Performance results are presented in Table II, showing balanced classification metrics across key performance indicators essential for operational vulnerability assessment.

Table II. Machine Learning Classification Performance Metrics

Performance Metric	Value	Operational Significance
Overall Accuracy	83.2%	Reliable automated classification
Precision	70.0%	Reduced false positive burden
Recall	87.0%	High vulnerability detection rate
F1-Score	75.0%	Balanced precision-recall performance
False Positive Rate (FPR)	0.98%	Minimal false alarm generation
False Negative Rate (FNR)	13.18%	Acceptable miss rate for screening

V. Conclusion

This research addressed a critical challenge in military cybersecurity by developing an integrated vulnerability assessment platform that unifies open-source security tools within a machine learning-enhanced framework. The solution demonstrates that sophisticated cybersecurity capabilities can be achieved through strategic integration of established tools with modern deployment technologies.

A. Technical Achievements

The platform successfully integrates OpenVAS infrastructure scanning with OWASP ZAP web application testing through unified API orchestration, eliminating traditional tool fragmentation that complicates military security operations. Machine learning classification achieved 83.2% overall accuracy across vulnerability categories, with balanced performance metrics including 70% precision and 87% recall rates. The system demonstrates exceptional performance for critical threats, including SQL Injection and Cross-Site Scripting detection. The containerized architecture supports concurrent operations for 100+ users while maintaining sub-3-second response times for standard operations.

B. Strategic Value for Military Organizations

Using the proposed solution, vendor dependencies that compromise strategic autonomy are eliminated. Complete source code transparency enables security validation essential for military deployments, while modular architecture supports customization for mission-specific requirements without licensing constraints.

The dual-VM architecture with network segmentation aligns with military operational security requirements, supporting both air-gapped environments and secure

[9] OWASP JuiceShop, https://juice-shop.herokuapp.com/
[10] DVWA, https://github.com/digininja/DVWA
[11] OWASP WebGoat, https://owasp.org/www-project-webgoat/

management access through VPN channels. Role-based access control accommodates military organizational structures through differentiated interfaces for junior and senior security personnel.

C. Operational Impact

Automated vulnerability classification significantly reduces manual analysis workload while improving assessment consistency across military IT infrastructures. Contextual remediation recommendations transform raw vulnerability data into actionable guidance suitable for implementation by technical staff with varying expertise levels. The unified interface eliminates context-switching between separate security tools, streamlining workflows for resource-constrained military cybersecurity teams.

D. Future Research Directions

The platform's modular architecture supports expansion through additional security tool integration (Nmap, Nuclei, Nikto) and SIEM connectivity for enhanced threat correlation. Advanced machine learning models, including deep learning approaches, could further improve classification accuracy and enable predictive vulnerability analysis. Mobile and IoT security assessment capabilities would address emerging threat vectors in modern military technology environments.

The successful implementation validates that strategic integration of open-source tools with machine learning and containerization technologies can produce competitive vulnerability assessment solutions for military cybersecurity operations. This research contributes to democratizing advanced cybersecurity technologies while providing defense organizations with cost-effective, strategically independent alternatives to expensive commercial solutions.

REFERENCES

[1] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, Jul. 2023. doi:10.3390/s23156666

[2] C. Odo, "Strengthening cybersecurity resilience: The importance of education, training, and risk management," *SSRN Electron. J.*, 2024. doi:10.2139/ssrn.4779289

[3] A. K. D. Kazim and N. R. Shanshul, "The impact of cyber-attacks on companies and organisations in developed countries," *Edelweiss Applied Science and Technology*, vol. 8, no. 6, pp. 9245–9252, Dec. 2024. doi:10.55214/25768484.v8i6.3980

[4] D. P. F. Möller, "Cybersecurity in digital transformation," in *Advances in Information Security*, Cham: Springer Nature Switzerland, 2023, pp. 1–70. doi:10.1007/978-3-031-26845-8_1

[5] M. Rodban, "Political risk and the geopolitics of cybersecurity," in *The Routledge Handbook of Political Risk*, London: Routledge, 2025, pp. 156–171. doi:10.4324/9781003456117-15

[6] J. Galliani, "What is Assured Compliance Assessment Solution (ACAS)?," *Seguetech.com*, May 2015. [Online]. Available: https://www.seguetech.com/assured-compliance-assessment-solution-acas/.

[7] "Continuous diagnostics and mitigation (CDM) program," *Cybersecurity and Infrastructure Security Agency CISA*. [Online]. Available: https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program.

[8] U.S. Government Accountability Office, "Cybersecurity: Agencies need to fully establish risk management programs and address challenges," Rep. GAO-19-384, Jul. 2019.

[9] M. A. Alsoufi, S. Razak, M. M. Siraj, A. Ali, M. Nasser, and S. Abdo, "Anomaly intrusion detection systems in IoT using deep learning techniques: A survey," in *Innovative Systems for Intelligent Health Informatics (IRICT 2020)*, Cham: Springer International Publishing, 2021, pp. 659–675. doi:10.1007/978-3-030-70713-2_60

[10] Z. Moric, V. Dakic, and M. Kulic, "Implementing a security framework for container orchestration," in *2024 IEEE 11th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2024, pp. 200–206. doi:10.1109/CSCloud62866.2024.00042

[11] J. Correnti, J. Lospinoso, M. Weigand, and K. Kramer, "Hidden vulnerabilities: Operational technology cybersecurity shortfalls," in *SAE Technical Paper Series*, Aug. 2020. doi:10.4271/2024-01-3863

[12] B. Erickson, "Cybersecurity figure of merit," *Dtic.mil*, Apr. 2016. [Online]. Available: https://apps.dtic.mil/sti/html/tr/AD1016749/.

[13] U.S. Government Accountability Office, "Weapon systems cybersecurity: DOD just beginning to grapple with scale of vulnerabilities," Rep. GAO-19-128, Oct. 2018.

[14] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, Oct. 2001. doi:10.1023/A:1010933404324

[15] National Institute of Standards and Technology, "National Vulnerability Database," *NIST*. [Online]. Available: https://nvd.nist.gov/.