On the Comparative Analysis of Trends in Cybersecurity Risk Assessment, Governance, and Compliance Frameworks

Sami Jamil Aljarrah
SMS Inc
Amman, Jordan
sami.jarrah@sms.com.jo

Sarra Cherbal
University of Setif 1
Setif, Algeria
sarra_cherbal@univ-setif.dz

Ashraf Mashaleh
Balqa Applied University
Salt, Jordan
mashaleh@bau.edu.jo

Jamal Al Karaki
Zayed University
Abu Dhabi, United Arab Emirates
Jamal.Al-Karaki@zu.ac.ae

Amjad Gawanmeh
University of Dubai
Dubai, United Arab Emirates
amjad.gawanmeh@ieee.org

2024 International Jordanian Cybersecurity Conference (IJCC) | 979-8-3315-1846-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/IJCC64742.2024.10847280

***Abstract*—This paper proposes an evaluation framework and systematic review of recent trends for cybersecurity risk assessment governance and compliance. The proposed framework incorporates several metrics for assessing model effectiveness. The findings highlight research opportunities in scalable privacy-preservation techniques, cross-domain validation, and standardized performance benchmarks. Federated learning models achieve the highest privacy rating while maintaining strong performance in precision and automation, suggesting distributed learning architectures as a promising direction for future governance, risk, and compliance framework development. Based on these findings, we recommend for future frameworks supported by regulatory considerations that balance privacy, performance, and ethical requirements, and combine quantum-resistant architectures with privacy-preserving features.**

***Index Terms*—Cybersecurity Risk Assessment; Adaptive Governance; Privacy-Preserving Frameworks; Regulatory Compliance**

I. Introduction

With the increasingly complex and rapidly emerging cybersecurity threats, organizations face significant challenges in implementing effective risk assessment, governance, and compliance frameworks. Despite the emergence of innovative approaches and technologies, such as AI-driven solutions [1], blockchain-based frameworks [2], and quantum-resistant methods [3], there remain several gaps and practical implementation that need to be addressed. This paper is intended to provide a comprehensive analysis of the current state of the art in cybersecurity risk assessment, governance, and compliance, and propose a framework to evaluate and compare various models using several metrics, and hence identify potential emerging trends.

Recent developments in cybersecurity risk assessment, governance, and compliance demonstrate a growing focus on real-time, adaptive frameworks that can dynamically respond to changing risk profiles. While AI-driven solutions show superior detection rates, there is still a lack of incorporating models that are understandable and explainable to the users and stakeholders, highlighting a critical gap. Similarly, blockchain-based approaches excel in maintaining audit trails but face significant scalability challenges in high-throughput environments.

On the other hand, the integration of advanced technologies, such as digital twins and explainable AI (XAI), is enabling more transparent risk assessment, governance, and compliance processes [4], [5]. Moreover, the increasing importance of compliance with regulatory standards, such as GDPR and industry-specific guidelines, is driving

the development of comprehensive, and integrated risk assessment solutions [6], [7]. However, despite these advancements, significant challenges remain in implementing effective risk assessment, governance, and compliance frameworks across organizational contexts and governance bodies.

Cybersecurity risk assessment, governance, and compliance frameworks must be adaptable to the diverse needs of various organizations, ranging from researchers, developers, and technical enterprises, to governments and regulators. In addition, the complexity of the threats, the rapid pace of technology advancement, and the emergence of several new tools, dictate the urgent need for the development of scalable, adaptable, and practical solutions for risk assessment, governance, and compliance. This paper provides a comprehensive analysis of current approaches in this domain, comparing various models using several key metrics, which will help in providing standardization and governance practices.

The remainder of this paper is organized as follows: Section II presents a literature review, Section III introduces our comparative analysis framework, Section IV presents the results based on the evaluation framework, Section V discusses the implications and provides recommendations, and Section VI concludes the paper.

II. Background and literature

In order to summarize state of the art approaches, this paper uses five parameters: primary domain, assessment methodology, technological focus, compliance framework adherence, and key innovations. These parameters can identify how key contributions in terms of infrastructure and emerging technology addressed in the literature. The authors in [8] introduced risk-based premium calculations for smart technology integration in power systems, while authors in [9] developed dynamic quantification methods for industrial control systems.

Healthcare and privacy-sensitive sectors demonstrate significant advancement in compliance-focused solutions. Authors in [11] introduced the integration of GDPR and HIPAA requirements into governance frameworks, while authors in [15] developed specialized privacy-centric approaches for health informatics. Authors in [14] provided unified assessment approach for Industry 4.0 SCADA environments, incorporating multiple compliance standards.

Artificial intelligence and machine learning applications are revolutionizing risk assessment methodologies. Authors in [1] developed AI-driven risk prediction models for insurance applications, while authors in [23] introduced ML-based detection for zero-day vulnerabilities. The integration of quantum computing technologies, as demonstrated by authors in [24], represents forward-thinking approaches to post-quantum cryptography challenges.

Recent developments show a clear trend toward more sophisticated assessment methodologies. Authors in [12] introduced real-time assessment capabilities with adaptive response mechanisms, while authors in [13] developed multi-criteria decision frameworks for comprehensive risk evaluation. The emergence of explainable AI, as implemented by authors in [5], addresses the critical need for transparency in AI-driven risk assessments.

Distributed systems and edge computing represent another frontier in risk assessment. Authors in [19] used federated learning approaches for privacy-preserving risk assessment, while authors in [20] developed real-time monitoring solutions for IoT environments using blockchain and edge computing. Supply chain security has been enhanced through the work in [21] graph analytics approach, enabling better understanding of risk propagation across complex networks. Table I illustrates the summary of cybersecurity risk assessment, governance, and compliance state of the art Approaches.

III. Comparison of various models

Table II compares various cybersecurity risk assessment models across several key dimensions. The first parameter is Model type, which indicates the used approach or methodology, such as quantitative, AI-driven, blockchain-based, etc. The second, Risk Quantification, describes how the model quantifies cybersecurity risk, which can be done quantitatively, qualitatively, probabilistically, or using a hybrid approach. Next, is Compliance Scope, which refers to the regulatory standards or frameworks that the model aims to comply with,

TABLE I
SUMMARY OF CYBERSECURITY RISK ASSESSMENT, GOVERNANCE, AND COMPLIANCE APPROACHES

Ref.	Primary Domain	Assessment Method	Technology Focus	Compliance Framework	Key Innovation
[1]	Insurance	Predictive Analysis	AI/ML	Insurance Standards	AI Risk Prediction
[2]	IoT	Traceability Analysis	Blockchain, IoT	GDPR	Regulatory Track
[3]	Cryptography	Hybrid Assessment	Quantum Computing	PQC Standards	PQC Framework
[4]	Industrial Systems	Digital Twin Analysis	Simulation	IEC 62443	Digital Twin Sim
[5]	AI Security	Explainable Assessment	XAI	AI Act, GDPR	XAI Risk Logic
[6]	Data Protection	Threat Modeling	–	GDPR	STRIDE-LINDDUN
[7]	Infrastructure	Zero-Trust Modeling	Network Security	NIST 800-207	Zero-Trust Arch
[8]	Power Systems	Risk Evaluation	Smart Technology	Industry Standards	Risk-based Premium
[9]	Industrial Control	Dynamic Quantification	Data Integration	ICS Standards	Adaptive Assessment
[10]	General Security	Quantitative Metrics	Attack Graphs	CVSS	Asset-Vuln Metrics
[11]	Healthcare	Governance-Based	Risk Management	GDPR, HIPAA	Compliance Integration
[12]	General Security	Real-time Assessment	Threat Intelligence	–	Adaptive Response
[13]	General Security	Multi-criteria Decision	–	–	Risk Hierarchy
[14]	SCADA	Unified Assessment	Industry 4.0	Multiple Standards	Standards Unification
[15]	Healthcare	Privacy-focused	–	HIPAA	Privacy-Security
[16]	Organizational	Adaptive Evaluation	–	Multiple Standards	Custom Governance
[17]	Cloud Computing	Quantitative Analysis	Cloud Technology	GDPR	Cloud Metrics
[18]	Cross-sector	Probabilistic Modeling	Bayesian Analysis	–	Risk Probability
[19]	Distributed Systems	Collaborative Learning	Privacy-Preserving AI	GDPR, CCPA	Federated Risk
[20]	Edge Computing	Real-time Monitoring	IoT Security	ISA/IEC 62443	Edge Detection
[21]	Supply Chain	Graph Analytics	Network Analysis	ISO 28000	Chain Propagation
[22]	Software Development	Continuous Assessment	CI/CD Pipeline	Multiple	DevSecOps Auto
[23]	Vulnerability Management	ML-based Detection	AI/ML	CWE, CVE	Zero-day Predict
[24]	Quantum Security	Probabilistic Analysis	Quantum Algorithms	NIST PQC	Quantum-Safe Risk

such as GDPR, HIPAA, NIST, ISO 27001, etc. The Real-Time Adaptability parameter specifies whether the model is static or can adapt in real-time to changing risk landscapes. Finally, Validation parameter indicates how the model was validated, either through simulation, real-world application, or theoretical analysis.

The models span a wide range of approaches, from traditional quantitative methods [10], [13], [17] to cutting-edge techniques like AI [1], blockchain [2], quantum computing [3], [24], and digital twins [4]. There is an increasing focus on real-time, continuous monitoring [7], [12], [20], [22] and adaptive models that can evolve with the threat landscape [1], [9], [14], [16], [23]. From a compliance perspective, GDPR is the most commonly targeted regulation [5], [6], [11], [14], [17], [19], followed by HIPAA [11], [15]. Industry-specific standards like NIST [7], ISO 27001 [21], IEC 62443 [4] and post-quantum cryptography (PQC) guidelines [3], [24] are also represented. Various validation approaches were used, for example, simulation was adopted in [4], [8], [9], [11], [14], [16], [18], [20], [23], in addition, by real-world applications were adopted in [1], [2], [5], [7], [15], [19], [21], [22] and theoretical

analysis [3], [6], [10], [13], [24].

Many proposed methods have a narrow compliance scope, focusing on one or two regulations. A more comprehensive approach covering multiple standards would be valuable. Real-world validation is less common than simulation. More case studies demonstrating practical application would strengthen the body of research. Integration of multiple techniques (e.g. AI, blockchain, quantum, and federated learning) is limited. Therefore, exploring synergies between various methods could yield a powerful new risk assessment, governance, and compliance paradigms.

Developing integrated models that leverage the strengths of multiple emerging technologies is needed to provide more robust, adaptive risk assessment [9], [14]. Expanding compliance scope to create unified frameworks that help organizations efficiently navigate the complex web of security regulations is another key priority [5], [22]. Real-world validation through industry partnerships and case studies should be prioritized to demonstrate practical value and accelerate adoption [1], [2], [19]. Investigating applications of quantum computing and post-quantum cryptography in risk assessment is crucial for future-proofing models against evolving threats [3], [24]. Finally, leveraging explainable AI techniques can improve transparency and build trust in AI-driven risk assessment [5].

IV. Evaluation Framework

The evaluation framework (shown in Figure 1) is based on nine essential metrics that collectively provide a comprehensive assessment of cybersecurity risk assessment, governance, and compliance models. Privacy measurement focuses on a model's ability to protect sensitive data and maintain confidentiality during risk assessment processes, with ratings ranging from N/A to Very High. The evaluation adopted in this work considers the model's efficiency and effectiveness in conducting risk assessments, governance, and compliance, while precision indicates the accuracy and reliability of results. The ethics metric is evaluated based on of fairness and bias mitigation. On the other hand, customization evaluates the model's flexibility across different organizational contexts. Integration capabilities are measured based on interoperability with existing security infrastructure, while resilience indicates the model's effectiveness under varying conditions. Automation levels are assessed for workflow efficiency, and cost evaluations consider both resource requirements and implementation expenses. Table III shows the summary of the evaluation.

The summary in the above table shows a growing emphasis on real-time assessment and automated response capabilities. Recent models show remarkable progress in technology integration, with digital twin implementations and explainable AI solutions achieving exceptional ratings across multiple metrics. The [4] model, for instance, demonstrates Very High ratings in performance, precision, and automation. However, these improvements often come with higher implementation costs. This indicates a market trend towards adopting more advanced solutions that require more resources, even if they are more complex and costly to implement.

Privacy and ethical considerations have become increasingly central to modern risk assessment, governance, and compliance models. The emergence of federated learning approaches represents a significant advancement in privacy protection, while XAI-based solutions demonstrate strong ethical standards. This evolution reflects growing awareness of data protection requirements and ethical implications in cybersecurity risk assessment, governance, and compliance.

Despite significant advances, several critical aspects remain inadequately addressed in current models. Scalability metrics across different organizational sizes are notably absent from most evaluation frameworks. User experience considerations, including usability and learning curves for security professionals, receive limited attention. The cross-domain applicability of models across different industry sectors lacks thorough assessment, and long-term effectiveness evaluation remains insufficient. Additionally, the ability to adapt to evolving regulatory requirements needs more comprehensive consideration.

The evaluation framework, depicted in the flowchart (Figure 1), provides a simplified overview of the key stages involved in assessing cybersecurity models. While the process includes nine detailed steps, the flowchart out-

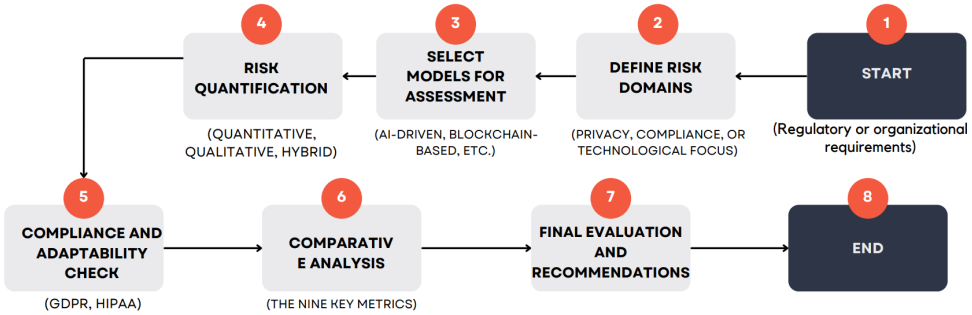

Fig. 1. Cybersecurity Model Evaluation Framework.

TABLE II
COMPARISON OF MODEL TYPES AND KEY FEATURES ACROSS STUDIES.
NOTE: RQ = RISK QUANTIFICATION, RTA = REAL-TIME ADAPTABILITY

No.	Model Type	RQ	Domain	RTA	Validation
[1]	AI-driven	Predictive	Cyber insurance	Adaptive	Real-World
[2]	Blockchain	Distributed	IoT ecosystems	Static	Real-World
[3]	Quantum-resistant	Hybrid	Autonomous vehicles	Adaptive	Theory
[4]	Digital Twin	Real-time	Critical infrastructure	Continuous	Simulation
[5]	XAI-based	Explainable	Anti-phishing defenses	Adaptive	Real-World
[6]	Threat Modeling	Qualitative	Privacy policy assessment	Static	Theory
[7]	Zero-Trust	Continuous	Critical infrastructure	Adaptive	Real-World
[8]	Insurance, Probabilistic	Quantitative	Power systems	Static	Simulation
[9]	Hybrid, Data-driven	Hybrid	Large-scale ICS	Adaptive	Simulation
[10]	Quantitative	Scoring	Enterprise IT systems	Static	Theory
[11]	Compliance	Qualitative	Healthcare data governance	Static	Simulation
[12]	Dynamic	Real-time	Adaptive environments	Adaptive	Simulation
[13]	Multi-criteria	Quantitative	Decision models	Static	Theory
[14]	Integrated	Quantitative	SCADA and Industry 4.0	Adaptive	Simulation
[15]	Privacy-centric	Quantitative	Medical informatics	Static	Real-World
[16]	Maturity Model	Hybrid	SMEs	Adaptive	Simulation
[17]	Quantitative	Quantitative	Cloud platforms	Static	Theory
[18]	Bayesian	Probabilistic	Network security assessments	Static	Simulation
[19]	Federated Learning	Distributed	Federated networks	Adaptive	Real-World
[20]	Edge Computing	Real-time	Agriculture 4.0	Adaptive	Simulation
[21]	Supply Chain	Graph-based	Supply chains	Continuous	Real-World
[22]	DevSecOps	Continuous	integration systems	Adaptive	Real-World
[23]	Zero-Day Defense	Predictive	Vulnerability mitigation	Adaptive	Simulation
[24]	Quantum Computing	Probabilistic	Infrastructure security	Static	Theory

lines the major stages—beginning with **Defining Risk Domains** and **Model Selection** and continuing through **Risk Quantification**, a **Compliance Check**, and **Key Metric Evaluation**. A **Comparative Analysis** then highlights optimal models, with final **Recommendations** based on the comprehensive assessment. This summary offers a structured approach to selecting effective cybersecurity models.

V. DISCUSSION AND RECOMMENDATIONS

Analysis of the evaluation metrics reveals that privacy-preserving federated approaches consistently outperform traditional frameworks across multiple dimensions. Federated learning models achieves the highest privacy rating (Very High) while maintaining strong performance in precision and automation. Organizations must carefully weigh tradeoffs between cost and efficiency against their security requirements. Medium-cost

TABLE III
PERFORMANCE, PRIVACY, COST, AND OTHER METRICS COMPARISON ACROSS MODELS

No.	Privacy	Performance	Precision	Ethics	Customization	Integration	Resilience	Automation	Cost
[1]	N/A	High	High	N/A	Yes	Limited	Medium	High	High
[2]	High	Medium	Medium	High	Medium	Medium	Medium	High	High
[3]	High	Medium	High	Medium	Limited	Medium	High	Medium	High
[4]	Medium	Very High	Very High	High	Yes	Very High	High	Very High	High
[5]	High	High	Very High	Very High	Yes	High	Medium	High	High
[6]	High	Medium	High	High	Yes	Medium	Medium	Medium	Medium
[7]	High	High	High	High	Yes	High	High	High	High
[8]	N/A	Medium	High	N/A	Limited	Limited	Medium	Low	Medium
[9]	N/A	High	Medium	N/A	Medium	Medium	Low	Medium	High
[10]	N/A	Medium	High	N/A	Limited	High	Medium	Low	Medium
[11]	High	Medium	Medium	High	Yes	High	Medium	Medium	Medium
[12]	High	High	High	Medium	High	High	High	High	High
[13]	N/A	Medium	Medium	N/A	Medium	High	Low	Low	Medium
[14]	Medium	High	High	Medium	High	High	High	High	High
[15]	High	High	High	High	Yes	Limited	Medium	Medium	High
[16]	Medium	High	High	Medium	Yes	High	High	High	High
[17]	Medium	High	Medium	N/A	Limited	Limited	Low	Low	Medium
[18]	N/A	Medium	High	N/A	Limited	High	Low	Low	Medium
[19]	Very High	High	High	High	Yes	High	High	High	High
[20]	Medium	Very High	High	Medium	Yes	High	High	Very High	Medium
[21]	High	High	High	High	Yes	High	High	High	High
[22]	Medium	Very High	High	High	Yes	Very High	High	Very High	Medium
[23]	Medium	High	High	Medium	Yes	High	High	High	High
[24]	High	Medium	High	High	Limited	Medium	Very High	Medium	Very High

solutions, particularly edge computing frameworks, offer an attractive middle ground, achieving Very High performance while maintaining moderate implementation expenses. Integration capabilities emerge as a critical differentiator among frameworks. Models incorporating DevSecOps principles and digital twin technologies demonstrate superior integration ratings. However, the data reveals a concerning gap in quantum-resistant frameworks, where integration capabilities often rate as Limited or Medium, despite high resilience scores.

Ethics considerations show significant variation across frameworks, with XAI-based approaches achieving the highest ratings. Organizations should prioritize frameworks that balance ethical considerations with technical performance, particularly in regulated industries. The customization dimension reveals a clear divide between traditional and emerging approaches. Newer frameworks incorporating AI and federated learning typically offer more flexible deployment options, crucial for organizations operating across multiple regulatory organizations. Moving forward, prioritizing development of frameworks that combine privacy-preserving architectures with quantum-resistant capabilities is needed. Additionally, organizations should invest in frameworks that demonstrate strong integration capabilities, as the data suggests this correlates with successful long-term deployment.

Implementation costs need to be reduced for high-performing solutions, particularly in digital twin and DevSecOps approaches. Furthermore, standardization efforts should prioritize integration capabilities and ethics considerations, as these emerge as key factors in framework effectiveness. Regulatory bodies should consider the strong performance of federated and XAI-based approaches when developing compliance requirements. Future regulations should encourage adoption of such balanced approaches while remaining flexible enough to accommodate technological advancement and also consider national frameworks for smart auditing and ranking of organizations security [25].

VI. CONCLUSION

The provided comprehensive analysis of cybersecurity risk assessment, governance, and compliance frameworks shows a significant transition toward privacy-preserving and ethically-aware approaches. The evaluation metrics demonstrate that

federated learning architectures and AI solutions can provide a good balance between security effectiveness with privacy protection. The identified gaps between theoretical capabilities and practical implementation highlights the need for continued innovation in scalability and cross-domain validation. The findings suggest that future framework development should focus on reducing the cost barriers associated with advanced implementations while maintaining high performance standards. The strong correlation between integration capabilities and successful deployment indicates that interoperability should be a key consideration in framework design.

REFERENCES

[1] S. Jawhar, C. E. Kimble, J. R. Miller, and Z. Bitar, "Enhancing cyber resilience with ai-powered cyber insurance risk assessment," in *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2024, pp. 0435–0438.

[2] I. Ullah and P. J. Havinga, "Governance of a blockchain-enabled iot ecosystem: A variable geometry approach," *Sensors*, vol. 23, no. 22, p. 9031, 2023.

[3] R. Soundarapandiyan, P. Sivathapandi, and A. Selvaraj, "Quantum-resistant cryptography for automotive cybersecurity: Implementing post-quantum algorithms to secure next-generation autonomous and connected vehicles," *Cybersecurity and Network Defense Research*, vol. 3, no. 2, pp. 177–218, 2023.

[4] M. Masi, G. P. Sellitto, H. Aranha, and T. Pavleska, "Securing critical infrastructures with a cybersecurity digital twin," *Software and Systems Modeling*, vol. 22, no. 2, pp. 689–707, 2023.

[5] B. Biswas, A. Mukhopadhyay, A. Kumar, and D. Delen, "A hybrid framework using explainable ai (xai) in cyber-risk management for defence and recovery against phishing attacks," *Decision Support Systems*, vol. 177, p. 114102, 2024.

[6] A. R. Alshamsan and S. A. Chaudhry, "A gdpr compliant approach to assign risk levels to privacy policies." *Computers, Materials & Continua*, vol. 74, no. 3, 2023.

[7] A. Akinsanya, "Securing the future: Implementing a zero-trust framework in us critical infrastructure cybersecurity," *Int. Journal of Advance Research, Ideas and Innovations in Technology*, vol. 10, no. 3, pp. V10I3–1221, 2024.

[8] P. Lau, L. Wang, W. Wei, Z. Liu, and C.-W. Ten, "A novel mutual insurance model for hedging against cyber risks in power systems deploying smart technologies," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 630–642, 2022.

[9] Y. Peng, K. Huang, W. Tu, and C. Zhou, "A model-data integrated cyber security risk assessment method for industrial control systems," in *2018 IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS)*. IEEE, 2018, pp. 344–349.

[10] M. U. Aksu, M. H. Dilek, E. İ. Tatlı, K. Bicakci, H. I. Dirik, M. U. Demirezen, and T. Aykır, "A quantitative cvss-based cyber security risk assessment methodology for it systems," in *International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2017, pp. 1–8.

[11] A. Faridoon and M. T. Kechadi, "Healthcare data governance, privacy, and security-a conceptual framework," *arXiv preprint arXiv:2403.17648*, 2024.

[12] S. Naumov and I. Kabanov, "Dynamic framework for assessing cyber security risks in a changing environment," in *International Conference on Information Science and Communications Technologies*. IEEE, 2016, pp. 1–4.

[13] V. Petrova, "The hierarchical decision model of cybersecurity risk assessment," in *2021 12th National Conference with International Participation (ELECTRONICA)*. IEEE, 2021, pp. 1–4.

[14] E. Wai and C. Lee, "Seamless industry 4.0 integration: A multilayered cyber-security framework for resilient scada deployments in cpps," *Applied Sciences*, vol. 13, no. 21, p. 12008, 2023.

[15] V. S. Naresh, M. Thamarai, and V. D. Allavarpu, "Privacy-preserving deep learning in medical informatics: applications, challenges, and solutions," *Artificial Intelligence Review*, vol. 56, no. Suppl 1, pp. 1199–1241, 2023.

[16] B. Yigit Ozkan and M. Spruit, "Adaptable security maturity assessment and standardization for digital smes," *Journal of Computer Information Systems*, vol. 63, no. 4, pp. 965–987, 2023.

[17] O. Awodele, C. Ogbonna, E. Ogu, J. Hinmikaiye, and J. Akinsola, "Characterization and risk assessment of cybersecurity threats in cloud computing: A comparative evaluation of mitigation techniques," *Acadlore Trans. Mach. Learn*, vol. 3, no. 2, pp. 106–118, 2024.

[18] J. Xie, S. Zhang, H. Wang, and M. Chen, "Multiobjective network security dynamic assessment method based on bayesian network attack graph," *International Journal of Intelligent Computing and Cybernetics*, vol. 17, no. 1, pp. 38–60, 2024.

[19] H. J. Alyamani, "Cyber security for federated learning environment using ai technique," *Expert Systems*, vol. 40, no. 5, p. e13080, 2023.

[20] S. Padhy, M. Alowaidi, S. Dash, M. Alshehri, P. P. Malla, S. Routray, and H. Alhumyani, "Agrisecure: A fog computing-based security framework for agriculture 4.0 via blockchain," *Processes*, vol. 11, no. 3, p. 757, 2023.

[21] Y. Yang, C. Peng, E.-Z. Cao, and W. Zou, "Building resilience in supply chains: A knowledge graph-based risk management framework," *IEEE Transactions on Computational Social Systems*, 2023.

[22] C. Feio, N. Santos, N. Escravana, and B. Pacheco, "An empirical study of devsecops focused on continuous security testing," in *IEEE European Symposium on Security and Privacy Workshops*. IEEE, 2024, pp. 610–617.

[23] I. O. Ibraheem and A. U. Tosho, "Zero day attack vulnerabilities: mitigation using machine learning for performance evaluation," *Journal of Computers for Society*, vol. 5, no. 1, pp. 43–58, 2024.

[24] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," *arXiv preprint arXiv:2404.10659*, 2024.

[25] J. N. Al-Karaki, A. Gawanmeh, and S. El-Yassami, "Gosafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp. 3079–3095, 2022.