AI-Integrated Cyber Security Risk Management Framework for IT Projects

Haidar Jabbar
Faculty of Applied Science and Technology
Humber Polytechnic
Toronto, Canada
haidar.jabbar@humber.ca

Samir Al-Janabi
Department of Computing and Software
McMaster University
Hamilton, Canada
aljanasa@mcmaster.ca

Francis Syms
Faculty of Applied Science and Technology
Humber Polytechnic
Toronto, Canada
francis.syms@humber.ca

***Abstract*—Amid the rising complexity and frequency of cyber threats, integrating emerging technologies such as artificial intelligence (AI) within IT project management frameworks is crucial for fostering cyber resilience. This paper proposes an AI-enhanced Cyber-Resilient IT Project Management Framework that integrates predictive analytics and machine learning across the cybersecurity process. The proposed framework emphasizes governance and risk management through proactive risk assessment, real-time threat detection, and automated incident response, enhancing resilience against evolving threats. The framework's adaptability and effectiveness are illustrated through its potential applications in diverse domains such as forensics, healthcare, and other sectors requiring robust data protection and cybersecurity strategies.**

Keywords—AI, Cyber risk management, standards and frameworks, AI cyber security framework, Anomaly detection

I. Introduction

The cybersecurity landscape is marked by the continual emergence of sophisticated threats, compelling individuals and organizations to prioritize adaptive and robust IT security frameworks [1]. A study [2] highlights 2023's top strategic tech trends, focusing on IT's role in digital immune systems, observability, AI risk management, cloud platforms, platform engineering, wireless value, superapps, adaptive AI, the metaverse, and sustainable tech. Developing a vision for an IT-Security Management System is essential, as it significantly impacts holding companies and necessitates a robust cybersecurity risk management system [3][4]. Additionally, projects operate in dynamic environments with diverse risks, requiring informed decision-making and a structured approach.

In 2024, global IT spending rose to $4.5 trillion, reflecting substantial investments by organizations aiming to leverage technology for business value [5]. However, with this increase comes a heightened risk landscape, as evidenced by the 16,312 cybersecurity incidents and over 5,199 confirmed data breaches recorded in 2023, impacting sectors from healthcare to finance [6]. Such statistics underscore the urgent need for resilient IT project frameworks that prioritize security from inception to closure [7] [8].

An integrated Cyber Risk Management Framework, with proactive risk assessment, real-time threat detection, and automated responses, is essential to enhance resilience against evolving threats [7]. From an AI perspective, AI has emerged as a powerful tool in cybersecurity. The global AI market, valued at approximately $200 billion in 2023 and projected to exceed $1.8 trillion by 2030, showcases AI's transformative role in threat detection and risk assessment [9]. Models like GPT-4 and Google's Gemini Ultra require significant resources for training, estimated at $78 million and $191 million, respectively, highlighting the scale and investment involved in cutting-edge AI research [10]. Yet, AI governance has lagged, with a recent study showing that some leading AI laboratories scored as low as 0 out of 5 in risk management practices, raising concerns about responsible AI integration [11].

This research addresses the critical need for advancing cybersecurity by bridging existing gaps through an AI-driven framework, building on previous work that proposed a Cyber-Resilient IT Project Management Framework, which integrated cybersecurity into all facets of IT project management [12]. We summarize our contributions in this work as follows:

- The work improves adaptive threat detection and automated incident response. Integrating predictive analytics, the framework enables real-time monitoring, dynamic risk analysis, and optimized security management.
- A framework that provides organizations with a proactive, AI-integrated solution to manage present-day and emerging threats throughout the project lifecycle. By incorporating AI, it effectively meets the rising complexities of modern software products and processes [13] [14].
- We introduce a case study in diverse domains, including forensics and healthcare, to demonstrate its quality, adaptability, and contribution to a stronger cybersecurity posture.

This paper is organized as follows: Section II reviews related work and existing frameworks for IT project risk and cybersecurity management. Section III presents the proposed AI-integrated Cybersecurity Risk Management Framework, detailing its core principles and lifecycle integration. Section IV presents anomaly detection case studies across multiple domains to demonstrate the framework's application. Section V discusses the evaluation of key factors. Section VI concludes with insights and suggestions for future work.

II. Related Work

A. IT Risk Project Management

IT projects are inherently risky, with effective risk management crucial to their success. Unlike other fields, software project progress is difficult to measure due to its intangible nature, and each large project is often unique, limiting the usefulness of past experience [15] [16]. Rapid technological changes can make prior knowledge obsolete, and varied processes across companies further complicate predictability. Additionally, IT projects support diverse industries, requiring specialized knowledge that varies, for

2024 International Jordanian Cybersecurity Conference (IJCC) | 979-8-3315-1846-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/IJCC64742.2024.10847294

instance, between healthcare and real estate. Project teams also consist of diverse skill sets, adding complexity. Managing risks both positive (opportunities) and negative (threats) requires a structured risk management approach to make informed decisions and mitigate potential issues. [17] demonstrate how machine learning and deep learning models effectively monitor and predict cyber threats, thereby streamlining cybersecurity efforts. In the next section, we explore major frameworks, examining their applications and limitations.

B. Standards and Frameworks

A range of frameworks and standards offers valuable guidance for managing cybersecurity risks and implementing best practices in cybersecurity, governance, and project management. Despite the advancements, traditional frameworks like PMBOK [18] and COBIT [19] need enhancement to keep up with the rapid evolution of AI-driven threats. This paper expands upon these foundations by introducing a comprehensive AI-integrated framework that effectively balances proactive and adaptive cybersecurity within IT project management. The following section reviews several existing frameworks, while Table 1 provides a comparative analysis of selected frameworks and standards, detailing their main features, areas of applicability, and limitations.

In our review of the frameworks and standards presented in Table 1, we concluded that cybersecurity and AI are either partially integrated or overlooked, particularly in terms of AI incorporation. Most major frameworks and standards are in the process of drafting updated versions that incorporate AI and cybersecurity, reflecting the growing importance of these elements [20] [21] [22] [23].

C. Framework Evaluation Criteria

From various studies [12], we identified five key criteria for evaluating the effectiveness of our proposed research framework, as shown in Fig. 1. A comprehensive literature review allowed us to assess major frameworks and standards against these criteria. In the following sections, we apply these factors to evaluate our framework, with a table later illustrating how it integrates, meets, and improves upon existing work.

TABLE I. COMPARISON OF FRAMEWORKS AND STANDARDS

Frameworks/ Standards	Application	Limitations
NIST CSF [24]	Critical Infrastructure	Focuses on critical infrastructure withc with AI-driven IT project manager adaptive AI-driven risk assessment.
COBIT 2019 [19]	Enterprise IT	Primarily aimed at IT governance and aligning with business goals, but lacks specific cybersecurity and AI-driven risk focus within IT project management.
ISO/IEC 27000:2018 [25]	Information Security	Focuses on information security management but does not address AI-enhanced data processing or predictive capabilities in the IT project management lifecycle.
PMBOK Guide [18]	Project Management	Provides project management components but lacks integration with AI-driven cybersecurity tools and processes for predictive threat modeling.
NIST RMF [26]	Federal Cybersecurity	Designed for federal agencies with a focus on risk management; lacks adaptability for AI-powered real-time threat detection and predictive analytics outside federal contexts.
Microsoft SDL [27]	Software Development	Emphasizes secure software development but does not incorporate AI-driven vulnerability detection or broader IT project risk integration in cybersecurity.
NIST SSDF [28]	Software Development	Focuses on secure development practices but lacks a comprehensive AI-powered approach for proactive risk management in IT projects.
ISO 31000 [29]	Organizational Functions	Provides general risk management principles but lacks a specific focus on cybersecurity and AI-driven decision support within IT projects.
DevSecOps [30]	Software DevOps Process	Primarily addresses security in DevOps; it does not integrate well with traditional IT project management practices or leverage AI for dynamic threat prediction.

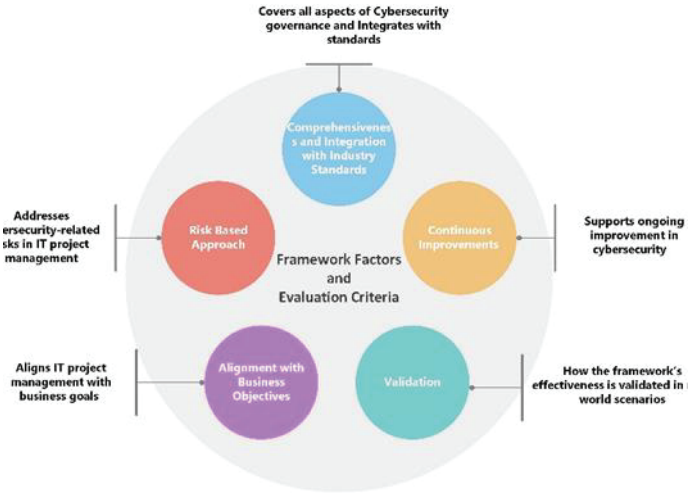

Fig. 1. Factors and Evaluation Criteria

III. THE PROPOSED FRAMEWORK

A. High-level Core Principles and Activities

IT projects are inherently risky, making effective risk management crucial to their success. The proposed AI-integrated Cyber Security Framework incorporates a cybersecurity risk management process seamlessly aligned with the standard IT project lifecycle. As illustrated in Fig. 2, this framework introduce high-level core principles, including an abstract view of AI integration and the alignment between cybersecurity risk management and IT project phases. Each component of the framework leverages AI-driven technologies to automate, optimize, and strengthen security processes, creating a proactive approach to managing cybersecurity risks. The core elements include:

- PCG (Project Cybersecurity-Based Governance)
- PTM (Project Threat Modeling)
- PAI (Project Asset Identification and Categorization)
- PRA (Project Risk Assessment)

- PRS (Project Risk Strategy)
- PSCS (Project Security Controls Selection)
- PRM (Project Risk Monitor)
- PRRE (Project Risk Response and Recovery Evaluation)

These core principles are built on the previously proposed framework [12], integrating AI for enhanced resilience in managing cybersecurity. The framework extends to digital crimes and forensic investigations, using predictive analytics to detect anomalies and generative AI to reconstruct attack pathways, aiding in evidence preservation and fraud detection. The following sections detail each component and its role in transforming traditional risk management into an adaptive, intelligent system.

B. *Mapping IT Project Life Cycle to the AI CyberSecurity Framework*

By integrating IT Project Management with AI-Enhanced Cybersecurity Risk Management, our proposed project lifecycle incorporates an AI-driven approach to address cybersecurity risks, effectively meeting the security requirements of both the project and its resulting product. Table 2 illustrates the alignment between the phases of a standard IT project lifecycle and the corresponding activities in AI-driven cybersecurity risk management within the proposed framework. This alignment strengthens the overall security posture of the system.

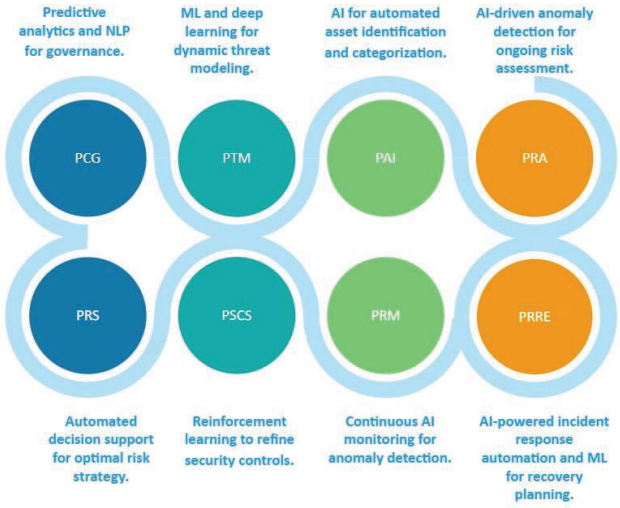

Fig. 2. Core Principles of the Proposed Framework at a High Level

IV. Application of the Framework

A. *Application of the Framework*

To demonstrate the applicability of the proposed framework, we conducted an experimental study focusing on an anomaly detection system during the "execute the plan" phase of Table 2. Anomaly detection is a crucial process that involves monitoring various areas within a computer or network to identify abnormal activity indicative of potential intrusions or incidents, providing timely warnings for mitigation. This case study emphasizes the practical integration of our framework into the interconnected context of anomaly detection across various domains such as forensics, healthcare, and IT operations. These areas require robust systems to maintain security and prevent breaches targeting the confidentiality, integrity, or availability of data and networks. Such violations can stem from unauthorized actors or legitimate users exceeding their access rights or engaging in unauthorized actions. As digital platforms and AI technologies become more pervasive in these fields, organizations face increasing susceptibility to cybersecurity threats.

The algorithm applied in this study was the Naive Bayes classifier, which utilizes Bayes' Theorem as its foundation. This theorem underpins the process of estimating the probability of a given outcome based on prior knowledge and observed evidence, making it well-suited for detecting anomalies in data. In this context, the Naive Bayes classifier helps determine the likelihood that a particular data instance indicates anomalous behavior, which is instrumental for real-time monitoring and response across diverse sectors requiring advanced cybersecurity measures.

B. *Machine Learning Algorithm and Dataset*

To evaluate the performance of the Naive Bayes classifier [31] within the proposed framework, we used a synthetic dataset. The dataset was carefully designed with key attributes such as Latency, Throughput, Port, and Anomalies (target class). Ensuring data integrity was a top priority, and we conducted rigorous duplicate checks using both automated tools and manual verification methods to guarantee the reliability and quality of the data. The evaluation of the Naive Bayes model was carried out using two primary performance metrics.

First, we calculated the classification accuracy, which measures the proportion of correctly predicted values to the total number of actual values. The classifier achieved an impressive accuracy of 98.36%, demonstrating its exceptional effectiveness in identifying anomalous activities.

Second, the quality of the model was assessed using the F-measure, which provides a balanced evaluation by combining two critical metrics: Precision and Recall. Precision reflects the proportion of correctly identified positive cases to all predicted positive cases, while Recall measures the proportion of actual positive cases that were correctly identified. In this study, a "true positive" scenario referred to an instance where an intrusion occurred and was accurately detected. By employing these metrics, we successfully validated the robustness and practicality of the Naive Bayes classifier in enhancing cybersecurity capabilities across domains such as forensics, healthcare, and IT operations.

Results are summarized in the F1 score, which was acceptable at 0.749%. This case study illustrates how AI can enhance the Cyber-Resilient IT Project Management Framework in securing critical points across various sectors requiring advanced anomaly detection and risk management systems. By integrating AI with cybersecurity practices, organizations can proactively detect and respond to threats, ensuring system integrity, confidentiality, and availability. This experimental study demonstrates the adaptability and effectiveness of the proposed framework in securing IT systems while offering valuable insights for its broader application across diverse domains such as forensics, healthcare, and other IT-driven fields.

TABLE II. ALIGNING IT PROJECT LIFECYCLE ACTIVITIES WITH THE AI-DRIVEN CYBERSECURITY RISK MANAGEMENT PROCESS

	Project Phases				
	AI-Driven Cybersecurity Risk Management Activities	**Start the Project**	**Plan the Project**	**Execute the Plan**	**Finish the Project**
Project Cybersecurity-Based Governance	-AI-Driven Threat Prediction -Automated Vulnerability Scanning -Intelligent Threat Awareness Training				
	-AI-Driven Risk Analysis - Predictive Modeling for Emerging Risks -Automated Defense Strategy Recommendation	-AI-Enhanced Feasibility Analysis -Predictive Stakeholder Analysis - Automated Initial Risk Scanning			
	-AI-Enhanced Decision Support -Automated Policy Review and Adjustment - Resource Optimization		-AI-Driven Scope and Risk Prediction - Resource Optimization with AI -AI-Based Budget Forecasting -Automated Risk control Prioritization -Risk Impact Analysis Using AI		
	-AI-Enhanced Control Matching -Adaptive Security Controls			-Real-Time Threat Detection and Response - Adaptive AI-Driven Quality Control -Automated Security Compliance Tracking - Endpoint Protection and Monitoring -Continuous Risk Reassessment and Adjustment	
	-Continuous AI-Based Threat Monitoring -Predictive Incident Reporting -Automated Incident Response -AI-Driven Recovery and Business Continuity Optimization - Continuous Learning from Incidents				-AI-Enhanced Deployment Strategy -Predictive Maintenance Planning -Post-Project AI-Driven Evaluation -Post-Project Threat Landscape Analysis -Security Metrics and Reporting -Continuous Improvement Recommendations

TABLE III. FACTORS EVALUATED ACCORDING TO THE CRITERIA OF THE PROPOSED AI-INTEGRATED FRAMEWORK

Factors	Evaluation Criteria	Indicators	Examples
Risk-based approach	Addresses cybersecurity-related risks in IT project management	Proactive risk identification with AI-driven analytics for efficient resource management	In the anomaly detection case study, AI algorithms analyzed data to detect potential disruptions early, allowing prioritized focus on high-risk areas across various domains such as supply chains, healthcare systems, and forensic investigations.
Comprehensiveness and Integration with Industry Standards	Covers all aspects of cybersecurity governance and integrates with standards like ISO/IEC 27001, COBIT, and NIST	AI-driven risk management is integrated across all project phases, aligning controls with industry compliance	In anomaly detection case studies, AI models performed threat modeling in the planning phase and monitored risks in real-time during operations, ensuring comprehensive risk coverage across different sectors. Automated control checks and anomaly detection upheld compliance with standards throughout the project lifecycle.
Alignment with business objectives	Aligns IT project management with business goals	Security risk management supports strategic objectives	In the anomaly detection case study, AI-powered insights identified critical points for resource allocation, ensuring resilience in components directly impacting operational timelines and aligning with organizational continuity goals across fields like logistics, healthcare, and IT infrastructure.
Continuous Improvement	Supports ongoing improvement in cybersecurity	Continuous adaptation with AI-driven monitoring and post-incident updates	In the anomaly detection case study, iterative model training and updates improved detection accuracy, ensuring the system adapted effectively to evolving threats across sectors like logistics, healthcare, and forensics.
Validation	Demonstrate effectiveness through real-world metrics	Case studies and quantitative metrics validate the framework	The testing of the anomaly detection in the case study showed a 23% increase in detection quality as per the F-measure score compared to a non-AI framework

V. Discussion and Factors Evalution

This section examines the evaluation of challenging factors and highlights the indicators identified by the proposed framework, with examples provided in Table 3 the proposed framework demonstrates and serves as an effective tool for organizations aiming to strengthen their AI-driven cybersecurity posture within IT project management. Its structured approach to risk management and AI enables organizations to prioritize cybersecurity efforts by addressing potential threats and vulnerabilities, creating a more secure and resilient IT environment.

The framework effectively integrates AI across all stages of development, ensuring comprehensive AI governance and addressing a range of IT-related challenges. By aligning AI and cybersecurity strategies with business objectives, it enhances organizational capabilities in achieving business goals. Its compatibility with other standards offers a unified approach to governance and management, while its focus on continuous improvement allows organizations to adapt to emerging threats and strengthen overall security defenses.

VI. Conclusion and Future work

The proposed AI-integrated Cybersecurity Risk Management Framework for IT projects addresses the increasing complexity of cybersecurity threats by integrating AI throughout the IT project lifecycle. This framework offers a structured approach to cybersecurity by incorporating predictive analytics and machine learning, enhancing real-time threat detection, risk assessment, and automated responses. The framework's adaptability and comprehensive approach make it suitable for various IT environments, particularly demonstrated through a case study in anomaly detection. This study underscores the effectiveness of AI in proactively identifying and mitigating security threats, ensuring the resilience and security of IT systems.

Future research will refine the framework's AI to boost scalability, quality, and adaptability across industries beyond anomaly detection systems. Further integration with evolving cybersecurity standards will enhance alignment with best practices. We also plan to develop advanced AI models for continuous learning, enabling sophisticated threat detection and response that adapts to emerging cybersecurity challenges.

References

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber Security: State of the Art, Challenges, and Future Directions," Cyber Security Applcation, vol. 2, p. 100031, 2024.

[2] Gartner, Inc., "Gartner Top 10 Strategic Technology Trends for 2023," Gartner, 2023. [Online]. Available: https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023.

[3] X. Xiong, Q. Yao, and Q. Ren, "Mission-Oriented Security Framework: An Approach to Embrace Cyber Resilience in Design and Action," in Proc. 2023 7th Int. Conf. Cryptography, Security and Privacy (CSP), Tianjin, China, 2023, pp. 54–58, doi: 10.1109/CSP58884.2023.00016.

[4] S. J. Aboud, M. A. AL-Fayoumi, M. Al-Fayoumi, and H. S. Jabbar, "An Efficient RSA Public Key Encryption Scheme," in Proc. 5th Int. Conf. Information Technology: New Generations (ITNG), Las Vegas, NV, USA, 2008, pp. 127–130.

[5] Gartner, Inc., "Gartner Forecasts Worldwide IT Spending to Grow 4.3% in 2023," Gartner, Jul. 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-07-19-gartner-forecasts-worldwide-it-spending-to-grow-4-percent-in-2023.

[6] Verizon Communications Inc., "2023 Data Breach Investigations Report," Verizon, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[7] J. Squillace, J. Cappella, and A. Sepp, "User Vulnerabilities in AI-Driven Systems: Current Cybersecurity Threat Dynamics and Malicious Exploits in Supply Chain Management and Project Management," in Proc. 2024 ASU Int. Conf. Emerging Technol. Sustain. Intell. Syst. (ICETSIS), Manama, Bahrain, 2024, pp. 1760–1765, doi: 10.1109/ICETSIS61505.2024.10459480.

[8] H. S. Jabbar, T. V. Gopal, and S. J. Aboud, "An Integrated Quantitative Assessment Model for Usability Engineering," ECOOP Doctoral Symp. PhD Workshop Organization, pp. 6, 2007.

[9] Statista, "Artificial Intelligence (AI) Market Size Worldwide 2023," Statista, 2023. [Online]. Available: https://www.statista.com/topics/3104/artificial-intelligence-ai-worldwide/.

[10] Stanford University, "AI Index Report 2024," AI Index Report, Stanford University, 2024. [Online]. Available: https://aiindex.stanford.edu/report/.

[11] E. Schoenberger, "New Study Reveals Leading AI Labs Weak in Risk Management," Time, Oct. 2024. [Online]. Available: https://time.com/7026972/saferai-study-xai-meta/.

[12] S. Al-Janabi, H. Jabbar, and F. Syms, "Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework," Digital, vol. 4, no. 4, pp. 866–897, Oct. 2024, doi: 10.3390/digital4040043.

[13] National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework," NIST, 2023. [Online]. Available: https://www.nist.gov/itl/ai-risk-management-framework.

[14] S. J. Aboud, M. Alnuaimi, and H. S. Jabbar, "Efficient Password Scheme Without Trusted Server," Int. J. Aviat. Technol. Eng. Manag. (IJATEM), vol. 1, no. 1, pp. 52–57, 2011.

[15] R. M. Boodai, H. A. Alessa, and A. H. Alanazi, "An Approach to Address Risk Management Challenges: Focused on IT Governance Framework," in Proc. 2022 IEEE Int. Conf. Cyber Security and Resilience (CSR), Rhodes, Greece, 2022, pp. 184–188, doi: 10.1109/CSR54599.2022.9850318.

[16] A. Chaturvedi et al., "A Comprehensive Vulnerability Tools Analysis for Security and Control in IT Environment and Organizations," in Proc. 2024 5th Int. Conf. Electron. Sustain. Commun. Syst. (ICESC), Coimbatore, India, 2024, pp. 612–618, doi: 10.1109/ICESC60852.2024.10689860.

[17] S. Kumar, B. P. Singh, and V. Kumar, "A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security," in Proc. 2021 3rd Int. Conf. Adv. Comput. Commun. Control Netw. (ICAC3N), Greater Noida, India, 2021, pp. 1963–1967, doi: 10.1109/ICAC3N53548.2021.9725596.

[18] Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), Project Management Institute Inc., USA, 2017.

[19] ISACA, COBIT 2019 Framework: Governance and Management Objectives, ISACA, 2018.

[20] N. M. Karie et al., "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," IEEE Access, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[21] J. Haidar and T. V. Gopal, "User Centered Design for Adaptive E-Learning Systems," Asian J. Technol., vol. 5, no. 4, pp. 429–436, 2006.

[22] S. Al-Janabi and R. Janicki, "Data Repair of Density-Based Data Cleaning Approach Using Conditional Functional Dependencies," Data Technol. Appl., vol. 56, no. 3, pp. 429–446, 2022.

[23] F. Syms and D. Smith, Cybersecurity in Canada: Operations, Investigations, and Protection. Canada: Emond Publishing, 2023.

[24] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," NIST, 2023. [Online]. Available: https://www.nist.gov/cyberframework.

[25] ISO/IEC, ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, Int. Org. Stand., Int. Electrotechnical Comm., Switzerland, 2018.

[26] NIST, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," NIST, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/37/r2/final.

[27] Microsoft, "Security Development Lifecycle (SDL)," Microsoft, 2023. [Online]. Available: https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle.

[28] NIST, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," NIST, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.

[29] ISO, ISO 31000:2018 Risk Management – Guidelines, Int. Org. Stand., 2018.

[30] H. Myrbakken and R. Colomo-Palacios, "DevSecOps: A Multivocal Literature Review," in Software Process Improvement and Capability Determination, A. Mas et al., Eds., SPICE 2017. Commun. Comput. Inf. Sci., vol. 770, Cham, Switzerland: Springer, 2017, pp. 17–29, doi: 10.1007/978-3-319-67383-7_2.

[31] I. As'ad, "Advancing Healthcare Diagnostics: A Study on Gaussian Naive Bayes Classification of Blood Samples," Int. J. Artif. Intell. Med. Issues, vol. 1, no. 2, pp. 1–15, Nov. 2023. [Online]. Available: https://doi.org/10.56705/ijaimi.v1i2.120.