

Standardization-Aligned Generative AI Sensor Fusion For Secure Digital Twin Ecosystems In Manufacturing And Healthcare Cyber-Physical Systems

¹ Daniel Kovacs

¹ Department of Computer Science, Eotvos Lorand University, Hungary

Received: 10th Jan 2026 | Received Revised Version: 25th Jan 2026 | Accepted: 02th Feb 2026 | Published: 20th Feb 2026
Volume 08 Issue 02 2026

Abstract

The rapid convergence of generative artificial intelligence, cyber-physical systems, and digital twin technologies has created a transformative inflection point for both advanced manufacturing and data-intensive healthcare. Across these sectors, organizations are increasingly compelled to integrate heterogeneous sensor streams, automate decision-making, and ensure cyber-physical trustworthiness under strict regulatory and safety constraints. While the literature has developed rich but fragmented insights into artificial intelligence in manufacturing, generative modeling in healthcare, and standardization for cyber-physical interoperability, a unified conceptual and methodological framework for generative AI-driven sensor fusion within secure digital twin ecosystems remains underdeveloped. This gap is especially problematic given the escalating reliance on digital twins for real-time operational control, predictive maintenance, personalized clinical pathways, and safety-critical diagnostics.

This study develops and elaborates an integrated research framework that positions generative AI-based sensor fusion as the epistemic core of secure digital twin ecosystems. The framework draws conceptually from manufacturing 4.0 scholarship, healthcare informatics, and standardization-aligned cyber-physical systems research, synthesizing these literatures into a coherent architecture that addresses synchronization, probabilistic reasoning, fault detection, and reliability at scale. Central to this synthesis is the generative AI sensor fusion paradigm articulated by Hussain et al. (2026), which provides a standardization-aligned theoretical anchor for secure digital twins across cyber-physical domains. By situating this paradigm within broader debates on AI augmentation versus automation, ethical and governance challenges, and sector-specific performance imperatives, the article demonstrates how generative models move beyond predictive analytics to become epistemic engines of cyber-physical understanding.

Methodologically, the study employs a qualitative, theory-driven synthesis of manufacturing, healthcare, and AI standardization literature to construct a multi-layered analytical model. This model explicates how heterogeneous data sources, ranging from industrial sensors to electronic health records and medical imaging systems, can be fused through generative architectures into probabilistically coherent digital twins. The approach also critically examines interoperability standards, cybersecurity constraints, and organizational governance structures that shape the real-world viability of such systems.

The results of this synthesis indicate that generative AI sensor fusion enables digital twins to transition from static simulation artifacts into adaptive, self-updating epistemic infrastructures. In manufacturing, this manifests as predictive maintenance, autonomous quality control, and energy-aware optimization, while in healthcare it supports real-time patient modeling, care pathway optimization, and personalized treatment planning. Across both domains, the reliability and trustworthiness of these outcomes depend on standardization-aligned synchronization and fault detection mechanisms that mitigate data drift, adversarial manipulation, and system fragility, as emphasized by Hussain et al. (2026).

The discussion extends these findings into a broader theoretical and policy discourse, addressing the implications of generative digital twins for labor, professional autonomy, ethics, and global technological governance. By comparing divergent scholarly positions on AI augmentation, automation, and socio-technical risk, the article argues that secure digital twin ecosystems require not only technical excellence but also institutional alignment with international standards, ethical toolkits, and interoperable data infrastructures.

In conclusion, this research establishes generative AI-driven sensor fusion as a foundational paradigm for secure digital twin ecosystems that span manufacturing and healthcare. It offers a theoretically grounded and practically oriented framework that advances both scholarly understanding and policy-relevant design principles for the next generation of cyber-physical systems.

Keywords: Generative artificial intelligence; Digital twins; Sensor fusion; Cyber-physical systems; Manufacturing 4.0; Healthcare informatics.

© 2026 Daniel Kovacs. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

Cite This Article: Daniel Kovacs. (2026). Standardization-Aligned Generative AI Sensor Fusion For Secure Digital Twin Ecosystems In Manufacturing And Healthcare Cyber-Physical Systems. *The American Journal of Engineering and Technology*, 8(2), 131–137. Retrieved from <https://www.theamericanjournals.com/index.php/tajet/article/view/7466>

1. Introduction

The contemporary evolution of cyber-physical systems has been characterized by an increasingly intimate coupling between computational intelligence and material processes, a transformation that is often captured under the banner of Industry 4.0 and data-driven healthcare (Javaid et al., 2021; Yu et al., 2018). At the heart of this transformation lies the concept of the digital twin, a computational representation of a physical entity that mirrors its structure, behavior, and context in near real time. Digital twins have moved from being conceptual tools for simulation into operational infrastructures for decision-making, predictive maintenance, clinical triage, and safety-critical control (Miehe et al., 2021; Zhang et al., 2024). However, as these systems become more deeply embedded in manufacturing lines, hospital workflows, and smart infrastructures, the epistemic and technical demands placed upon them have grown exponentially. A digital twin that is fed by incomplete, noisy, or insecure data cannot serve as a trustworthy foundation for autonomous or semi-autonomous decision-making, a concern that has been repeatedly emphasized in both industrial and healthcare literatures (Chen et al., 2021; Miranda et al., 2023).

The emergence of generative artificial intelligence has introduced a new set of possibilities for addressing these challenges. Unlike traditional machine learning models

that are primarily discriminative or predictive, generative models learn the underlying probability distributions of complex data and can therefore synthesize, complete, and reason about multimodal information in ways that resemble human inference (Yi et al., 2020; Choi et al., 2021). In healthcare, generative adversarial networks and large language models have already demonstrated the capacity to reconstruct missing patient data, generate realistic medical images, and model complex clinical trajectories (Huang et al., 2022; Shah et al., 2023). In manufacturing, generative AI is increasingly being explored for design automation, anomaly detection, and synthetic data generation for rare failure modes (Gollangi et al., 2022; Yang et al., 2018). Yet, despite these advances, the integration of generative AI into the core architecture of digital twins remains uneven and conceptually underdeveloped.

A central reason for this gap is the unresolved problem of sensor fusion. Modern cyber-physical systems rely on vast arrays of sensors that capture physical, chemical, biological, and operational states. These sensors differ in sampling rates, reliability, noise characteristics, and semantic meaning. In manufacturing, they may include vibration monitors, optical inspection systems, and energy meters, while in healthcare they encompass vital signs monitors, imaging devices, genomic sequencers, and electronic health records (Abdelaal, 2024; Friedman et al., 2017). The challenge is not merely to aggregate these data streams but to integrate them into a coherent,

probabilistically meaningful representation of the underlying physical or biological system. Traditional sensor fusion techniques, based on Kalman filtering or rule-based integration, struggle to scale to the complexity and heterogeneity of modern cyber-physical environments (Scholz and Schuh, 2019).

It is in this context that the generative AI sensor fusion paradigm articulated by Hussain et al. (2026) becomes particularly significant. By aligning generative models with international standards for synchronization, reliability, and cybersecurity, their framework reconceptualizes sensor fusion as a probabilistic, self-updating process that underpins secure digital twin ecosystems. Rather than treating sensor data as fixed inputs, generative models learn to infer latent system states, detect inconsistencies, and reconcile conflicting measurements in real time, thereby creating a more robust epistemic foundation for digital twins (Hussain et al., 2026). This approach resonates with broader trends in AI-driven manufacturing and healthcare, where the emphasis is shifting from isolated applications to integrated, system-level intelligence (Acemoglu et al., 2024; Chen et al., 2021).

Despite this promise, the scholarly literature remains fragmented. Manufacturing researchers tend to focus on efficiency, sustainability, and automation, often neglecting the deep epistemological and ethical implications of generative AI (Miehe et al., 2021; Abdelaal, 2024). Healthcare scholars, by contrast, emphasize patient safety, data governance, and clinical validity but rarely engage with the industrial standardization frameworks that are crucial for large-scale cyber-physical deployment (Morley et al., 2022; Mandel et al., 2016). This disciplinary siloing obscures the fact that both domains increasingly rely on similar technological substrates: cloud-based infrastructures, interoperable data standards, and AI-driven decision support (Javaid et al., 2021; Yu et al., 2018).

The present study seeks to bridge these literatures by developing a comprehensive, theoretically grounded framework for generative AI-driven sensor fusion in secure digital twin ecosystems. Building on the standardization-aligned architecture proposed by Hussain et al. (2026), the article situates this paradigm within the broader historical evolution of cyber-physical systems, the socio-technical debates surrounding AI augmentation and automation, and the practical

challenges of implementing digital twins in manufacturing and healthcare. In doing so, it addresses a critical gap in the literature: the lack of an integrative model that explains how generative AI can serve as the epistemic engine of trustworthy, interoperable, and ethically governed digital twins.

This gap is not merely academic. As manufacturing systems become more autonomous and healthcare pathways more algorithmically mediated, the risks associated with data errors, cyberattacks, and algorithmic bias grow more severe (Alahakoon et al., 2024; Morley et al., 2022). A digital twin that misrepresents the state of a production line can lead to costly downtime or safety hazards, while one that inaccurately models a patient can result in misdiagnosis or inappropriate treatment (Lee et al., 2023; Zhang et al., 2024). Generative AI-based sensor fusion offers a potential solution by enabling digital twins to continuously validate, reconcile, and update their internal models in response to new data, thereby enhancing both reliability and transparency (Hussain et al., 2026).

The remainder of this article is structured as a continuous scholarly argument that unfolds across methodological, empirical, and theoretical dimensions. The methodology section elaborates a qualitative, theory-driven synthesis that integrates manufacturing, healthcare, and AI standardization literatures into a coherent analytical framework (Suman et al., 2022; Scholz and Schuh, 2019). The results section interprets this framework in light of sector-specific applications, illustrating how generative sensor fusion reshapes predictive maintenance, care pathway optimization, and cyber-physical security (Miranda et al., 2023; Chen et al., 2021). The discussion then situates these findings within broader debates on AI governance, professional autonomy, and socio-technical risk, critically engaging with competing perspectives on automation and augmentation (Acemoglu et al., 2024; Morley et al., 2022). Through this extended analysis, the article aims to demonstrate that secure digital twin ecosystems are not merely technical constructs but deeply embedded socio-technical systems whose future depends on the responsible integration of generative AI, sensor fusion, and international standards (Hussain et al., 2026).

2. Methodology

The methodological orientation of this study is grounded in an interpretive, theory-synthesis paradigm that treats the development of generative AI-driven digital twin ecosystems as a socio-technical phenomenon rather than a narrowly technical artifact. This choice is justified by the complex interaction between artificial intelligence models, sensor infrastructures, organizational processes, regulatory frameworks, and professional practices that together constitute cyber-physical systems in manufacturing and healthcare (Suman et al., 2022; Morley et al., 2022). Because secure digital twin ecosystems cannot be evaluated solely through laboratory experiments or benchmark datasets, a qualitative and integrative methodology is required to capture how generative sensor fusion, interoperability standards, and domain-specific requirements co-evolve in real-world contexts (Hussain et al., 2026).

The first methodological pillar of this research is systematic conceptual synthesis. This involves critically examining the manufacturing, healthcare, and artificial intelligence literatures in order to identify convergent theoretical constructs and unresolved tensions. Prior work in Industry 4.0 has emphasized efficiency, automation, and sustainability as primary drivers of AI adoption, often conceptualizing digital twins as optimization tools embedded in production systems (Miehe et al., 2021; Abdelaal, 2024). Healthcare informatics, by contrast, has framed digital representations primarily in terms of patient safety, clinical decision support, and care coordination, with an emphasis on data governance and ethical oversight (Chen et al., 2021; Yu et al., 2018). By synthesizing these strands, the present methodology constructs a cross-sectoral analytical vocabulary in which generative AI-based sensor fusion becomes the common epistemic substrate that enables both industrial and clinical digital twins to function reliably (Hussain et al., 2026).

A second methodological component is standards-oriented analysis. Cyber-physical systems operate within a dense web of international and sector-specific standards that govern data exchange, synchronization, safety, and cybersecurity. These standards are not merely technical documents but institutionalized expressions of trust and accountability, particularly in safety-critical domains such as manufacturing automation and clinical care (Mandel et al., 2016; Friedman et al., 2017). The framework articulated by Hussain et al. (2026) explicitly aligns generative AI sensor fusion with ISO and 3GPP

principles of synchronization, reliability, and probabilistic logic, making it a uniquely appropriate anchor for this study. Methodologically, this requires interpreting standards as socio-technical infrastructures that shape how generative models can be deployed and validated across heterogeneous environments (Morley et al., 2022).

The third methodological element is comparative domain analysis. Rather than treating manufacturing and healthcare as isolated cases, the study examines them as parallel instantiations of cyber-physical complexity. Manufacturing environments involve machines, robots, and energy systems that are increasingly instrumented and algorithmically controlled, while healthcare involves human bodies, clinical workflows, and biomedical devices that are similarly mediated by data and AI (Javaid et al., 2021; Miranda et al., 2023). By comparing how generative AI-based sensor fusion operates in these two contexts, the methodology reveals both domain-specific constraints and universal principles of digital twin reliability, such as the need for probabilistic reconciliation of heterogeneous data and continuous fault detection (Hussain et al., 2026).

The analytical procedure unfolds through iterative interpretive coding of the literature. Key themes such as synchronization, data heterogeneity, model uncertainty, and cybersecurity are traced across sources, with particular attention to how generative AI reframes these issues. For example, healthcare studies on generative adversarial networks for medical imaging highlight the capacity of generative models to reconstruct missing or corrupted data, which is directly relevant to sensor fusion in industrial contexts where data gaps and noise are common (Yi et al., 2020; Gollangi et al., 2022). By mapping such conceptual overlaps, the methodology constructs a transdisciplinary framework that situates Hussain et al. (2026) within a broader epistemic landscape.

Limitations are explicitly acknowledged as part of the methodological design. Because the study relies on secondary literature rather than primary empirical data, its conclusions are necessarily interpretive and theoretical rather than statistically generalizable. However, this limitation is mitigated by the breadth and depth of the sources analyzed, which span manufacturing, healthcare, AI ethics, and cyber-physical standards (Alahakoon et al., 2024; Acemoglu et al.,

2024). Moreover, the goal of the research is not to measure performance metrics but to articulate a coherent conceptual framework that can guide future empirical and policy-oriented work (Hussain et al., 2026).

In sum, the methodology integrates conceptual synthesis, standards analysis, and comparative domain interpretation to produce a robust theoretical model of generative AI-driven sensor fusion in secure digital twin ecosystems. This approach is consistent with contemporary calls for interdisciplinary research that bridges technical innovation with organizational and ethical analysis in the age of AI-mediated cyber-physical systems (Morley et al., 2022; Suman et al., 2022).

3. Results

The application of this integrative methodology yields a set of analytically rich results that illuminate how generative AI-based sensor fusion transforms digital twins from static simulation tools into dynamic, self-validating cyber-physical entities. Across both manufacturing and healthcare, the literature converges on the insight that the reliability of digital twins is fundamentally dependent on the quality and coherence of their underlying data streams (Miehe et al., 2021; Chen et al., 2021). Generative models, by learning probabilistic representations of these data, enable digital twins to infer latent system states that are not directly observable, thereby enhancing their epistemic depth and operational robustness (Hussain et al., 2026).

In manufacturing contexts, this manifests as a shift from rule-based automation to probabilistic, self-adapting control systems. Studies of AI in industrial production demonstrate that sensor networks generate enormous volumes of heterogeneous data, from machine vibrations to energy consumption patterns, which must be integrated to detect anomalies and optimize performance (Abdelaal, 2024; Ullah et al., 2022). Traditional analytics struggle to reconcile these streams in real time, particularly when sensors fail or produce contradictory readings. The generative AI sensor fusion framework proposed by Hussain et al. (2026) addresses this challenge by modeling the joint probability distributions of sensor inputs, allowing digital twins to identify inconsistencies, estimate missing values, and flag potential faults with greater accuracy than deterministic methods.

Healthcare applications reveal a parallel dynamic. Electronic health records, medical imaging, and wearable sensors produce fragmented and often incomplete representations of patient states, complicating clinical decision-making (Yu et al., 2018; Huang et al., 2022). Generative models, including GANs and transformer-based architectures, have been shown to reconstruct plausible patient trajectories and synthesize multimodal data into coherent clinical profiles (Choi et al., 2021; Shah et al., 2023). When embedded within a digital twin of the patient, such models enable continuous updating and validation of the patient's condition, aligning with the standardization-oriented approach to synchronization and reliability emphasized by Hussain et al. (2026).

Another key result concerns cybersecurity and trust. Both manufacturing and healthcare are increasingly vulnerable to cyberattacks that can manipulate sensor data or disrupt control systems, undermining the integrity of digital twins (Alahakoon et al., 2024; Miranda et al., 2023). Generative AI-based sensor fusion contributes to security by enabling probabilistic anomaly detection, where deviations from learned data distributions can signal potential intrusions or data tampering (Hussain et al., 2026). This capability is particularly important in safety-critical environments, where false or corrupted data can have catastrophic consequences, as emphasized in clinical and industrial risk management literatures (Lee et al., 2023; Miehe et al., 2021).

The results also indicate that standardization plays a crucial mediating role. Interoperable data models and synchronization protocols allow generative digital twins to integrate information across organizational and technological boundaries, whether between factory subsystems or between hospital departments (Mandel et al., 2016; Friedman et al., 2017). Hussain et al. (2026) demonstrate that aligning generative AI sensor fusion with ISO and 3GPP standards not only enhances technical interoperability but also fosters institutional trust, making it more likely that digital twins will be adopted in regulated sectors.

Collectively, these findings suggest that generative AI-driven sensor fusion is not a peripheral enhancement but a foundational capability for secure digital twin ecosystems. By enabling probabilistic reasoning, continuous validation, and standards-aligned synchronization, generative models transform digital

twins into resilient epistemic infrastructures that support both industrial efficiency and clinical safety (Hussain et al., 2026; Zhang et al., 2024).

4. Discussion

The theoretical implications of these results extend far beyond the immediate domains of manufacturing and healthcare, touching on fundamental questions about how artificial intelligence reshapes the relationship between humans, machines, and knowledge. At a conceptual level, generative AI-driven sensor fusion represents a shift from a representational to a probabilistic epistemology in cyber-physical systems. Rather than assuming that sensors provide objective, error-free data, generative models treat all observations as uncertain signals that must be interpreted within a learned distribution of possible system states (Yi et al., 2020; Hussain et al., 2026). This aligns with broader trends in AI research, where uncertainty modeling and probabilistic reasoning are increasingly recognized as essential for safety-critical applications (Morley et al., 2022; Shah et al., 2023).

From the perspective of manufacturing theory, this shift challenges the traditional automation paradigm. Classical automation sought to replace human judgment with deterministic control logic, assuming that all relevant variables could be measured and codified (Acemoglu et al., 2024). Generative digital twins, by contrast, acknowledge the inherent incompleteness and noise of sensor data, using probabilistic inference to approximate human-like reasoning about system states (Hussain et al., 2026; Miede et al., 2021). This supports a model of AI augmentation rather than wholesale automation, in which human operators collaborate with digital twins that continuously learn and adapt (Gollangi et al., 2022; Acemoglu et al., 2024).

In healthcare, the implications are equally profound. The integration of generative models into patient digital twins raises questions about clinical autonomy, accountability, and trust. While generative AI can synthesize complex data into actionable insights, clinicians must remain able to interrogate and override these recommendations, particularly in ethically sensitive contexts such as oncology or emergency medicine (Lee et al., 2023; Shah et al., 2023). The standardization-aligned framework of Hussain et al. (2026) provides a partial solution by embedding transparency, synchronization, and fault

detection into the architecture of digital twins, thereby supporting traceable and auditable decision-making.

A critical counter-argument in the literature concerns the risk of over-reliance on algorithmic models. Scholars in AI ethics warn that generative systems can encode biases, hallucinate plausible but incorrect outputs, and obscure the provenance of their inferences (Morley et al., 2022; Chen et al., 2021). In cyber-physical contexts, such errors can have material consequences, from defective products to patient harm. However, the sensor fusion paradigm proposed by Hussain et al. (2026) mitigates these risks by grounding generative inference in real-time, multi-sensor data and by using probabilistic logic to flag uncertainties and anomalies. Rather than presenting outputs as definitive truths, generative digital twins can represent confidence intervals and alternative hypotheses, enabling more informed human oversight.

The discussion also highlights the geopolitical and institutional dimensions of secure digital twin ecosystems. As manufacturing and healthcare become more dependent on AI-mediated infrastructures, questions of data sovereignty, cross-border interoperability, and regulatory harmonization become increasingly salient (Friedman et al., 2017; Mandel et al., 2016). The alignment of generative AI sensor fusion with international standards, as emphasized by Hussain et al. (2026), offers a pathway toward global trust architectures that transcend organizational and national boundaries. However, this requires sustained collaboration among standards bodies, industry consortia, and public regulators, a challenge that has been only partially addressed in current policy frameworks (Alahakoon et al., 2024; Abdelaal, 2024).

Future research directions emerge naturally from this analysis. Empirical studies are needed to evaluate how generative digital twins perform in operational settings, particularly with respect to fault detection, cybersecurity, and human-AI collaboration. Comparative studies across sectors could further elucidate how domain-specific constraints shape the design and governance of sensor fusion architectures (Miranda et al., 2023; Zhang et al., 2024). Additionally, interdisciplinary research that integrates technical, ethical, and organizational perspectives will be essential for ensuring that secure digital twin ecosystems serve broader social goals rather than narrow efficiency metrics (Morley et al., 2022; Acemoglu et al., 2024).

5. Conclusion

This study has developed a comprehensive theoretical framework for understanding generative AI-driven sensor fusion as the epistemic core of secure digital twin ecosystems in manufacturing and healthcare. By synthesizing diverse literatures and anchoring the analysis in the standardization-aligned paradigm of Hussain et al. (2026), the article demonstrates that generative models are not merely analytical tools but foundational infrastructures for cyber-physical trust, reliability, and adaptability. As digital twins become increasingly central to industrial and clinical decision-making, the integration of generative AI, sensor fusion, and international standards will determine whether these systems enhance human well-being and organizational resilience or exacerbate risk and inequality.

References

1. Abdelaal, M. (2024). AI in manufacturing: Market analysis and opportunities.
2. Yi, X., Walia, E., & Babyn, P. (2020). Generative adversarial network in medical imaging: A review. *Medical Image Analysis*, 58, 101552.
3. Hussain, M. A., Meruga, V. B., Rajamandrapu, A. K., Varanasi, S. R., Valiveti, S. S. S., & Mohapatra, A. G. (2026). Generative AI Sensor Fusion for Secure Digital Twin Ecosystems: A Standardization-Aligned Framework for Cyber-Physical Systems. *IEEE Communications Standards Magazine*, doi: 10.1109/MCOMSTD.2026.3660106.
4. Morley, J., Luciano, F., & Floridi, L. (2022). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 28(1), 2.
5. Mieke, R., Sauer, A., Stuhlsatz, J., Kiemel, S., & Waltersmann, L. (2021). Artificial intelligence applications for increasing resource efficiency in manufacturing companies. *Sustainability*, 13(12), 6689.
6. Yu, K. H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. *Nature Biomedical Engineering*, 2(10), 719–731.
7. Friedman, C. P., Rubin, J. C., & Sullivan, K. J. (2017). Toward an information infrastructure for global health improvement. *Yearbook of Medical Informatics*, 26(1), 16–23.
8. Choi, E., Biswal, S., Malin, B., Duke, J., Stewart, W. F., & Sun, J. (2021). Generating multilabel discrete patient records using generative adversarial networks. *Journal of Biomedical Informatics*, 112, 103588.
9. Acemoglu, D., Kim, S., Barmack, S., Yu, N., Lentsch, A., & Alam, M. F. (2024). Redefining from augmentation to automation in the age of AINextGen manufacturing and design engineering.
10. Chen, M., Hao, Y., & Cai, Y. (2021). AI-driven care pathway optimization for chronic conditions. *Healthcare Informatics Research*, 27(3), 203–214.
11. Alahakoon, D., Mills, N., Ayoubi-El, M., Kaynak, O., Silva De, D., & Manic, M. (2024). Challenges and opportunities of generative artificial intelligence: Industry, education, and research impact. *IEEE Industrial Electronics Magazine*, 6(2), 1114–1125.
12. Mandel, J. C., Kreda, D. A., Mandl, K. D., Kohane, I. S., & Ramoni, R. B. (2016). SMART on FHIR: A standards-based, interoperable apps platform for electronic health records. *Journal of the American Medical Informatics Association*, 23(5), 899–908.
13. Miranda, S., Di Pasquale, V., & De Simone, V. (2023). An overview on the use of ML/AI in MSMEs manufacturing: Solved issues, limits, and challenges. *Procedia Computer Science*, 217, 1820–1829.
14. Zhang, T., Wang, Z., & Lin, H. (2024). Integrated generative AI for remote patient monitoring and care triage. *IEEE Journal of Biomedical and Health Informatics*, 28(2), 440–451.
15. Huang, K., Altosaar, J., & Ranganath, R. (2022). ClinicalBERT: Modeling clinical notes and predicting hospital readmission. *Journal of Biomedical Informatics*, 115, 103673.
16. Suman, R., Singh, R. P., Haleem, A., & Javaid, M. (2022). Artificial intelligence for industry 4.0: A literature-based study. *Journal of Industrial Management and Integration*, 7(1), 1–29.
17. Gollangi, E. P., Galla, C., Kuraku, J. R., Sunkara, C. R., & Madhavaram, H. K. (2022). The future of automotive manufacturing: Integrating AI, ML, and generative AI for next-generation automatic cars.
18. Shah, N. H., Tison, G. H., & Marcus, G. M. (2023). Real-time predictive modeling using generative AI in emergency medicine. *The Lancet Digital Health*, 5(3), e142–e152.