ISSN: 2756-2638
Transactions on Engineering and Computing Sciences; Vol. 14 No. 03 (2026) (09-17)
https://doi.org/10.14738/tmlai.1403.10823

AI-Driven Cybersecurity in Human-Centric Industry 5.0

Mohammed Ketel & Hari Joshi

1. Applied Information Technology Department, University of Baltimore, Baltimore, MD 21201, USA

Abstract: Industry 5.0 represents a transformation of the industrial competitive framework toward a human-oriented, sustainable, and resilient ecosystem built on human–machine collaboration. Artificial Intelligence (AI) plays a key role in this development, as, when combined with the Industrial Internet of Things (IIoT), it enables higher levels of personalization, operational efficiency, and predictive capability. However, this shift also introduces significant cybersecurity challenges due to expanded attack surfaces and the unique vulnerabilities associated with AI systems. This paper explores the integration of AI in Industry 5.0, examines its implications for cybersecurity, and discusses the strategies required to ensure a secure, ethical, and trustworthy digital industrial future.

Keywords: Industry 5.0, AI, Cybersecurity, Human-Centric, Internet of Things (IoT), Ethics

INTRODUCTION

Industry 5.0 represents a significant advancement in the technological evolution that began with Industry 4.0. While Industry 4.0 primarily focused on automation and efficiency, Industry 5.0 emphasizes human needs and sustainability within industrial transformation. This new paradigm acknowledges not only economic and technical requirements but also ethical and social considerations. A key aspect of this shift is the symbiotic relationship between humans and AI-driven systems, which enhances creativity, productivity, and personalization in the production environment [1], [6], [12]. However, the integration of advanced technologies also increases cybersecurity risks, raising concerns about data quality, system stability, and the ethical use of AI in critical infrastructures [3].

Industry 5.0 is not merely a continuation of its predecessor but a redefinition of industrial development priorities. It focuses on value creation through ethical AI, social inclusion, and environmental sustainability. Governments and industries worldwide are recognizing the need to design systems that not only optimize production but also improve the quality of life [8], [10]. This shift requires redefining technological innovation in alignment with human values, necessitating robust frameworks for secure, adaptable, and responsible use of digital technologies.

Recent studies indicate a significant rise in research on sustainability, human–machine collaboration, and the ethical implementation of AI, suggesting that Industry 5.0 is a global transformation rather than a localized trend [7], [8]. This evolution aligns with the development of emerging socio-technical systems.

Furthermore, recent literature identifies AI maturity, workforce adaptability, and organizational innovation capability as critical drivers for successfully transitioning to Industry 5.0. Organizations that effectively align AI innovation strategies with human

intelligence and ethical principles demonstrate greater resilience and a stronger capacity for sustainable growth [9].

This paper reviews key insights at the intersection of AI, cybersecurity, and Industry 5.0. It extends previous conceptual models by incorporating ethical, organizational, and regulatory dimensions, thereby reflecting the interdisciplinary nature of Industry 5.0.

INDUSTRY 5.0: OVERVIEW AND COMPARISON WITH INDUSTRY 4.0

Overview of Industry 5.0

The proponents of Industry 5.0 emphasize three core principles: human-centricity, sustainability, and resilience. This new paradigm builds upon Industry 4.0 by reintroducing human values and creativity into the production environment, fostering closer collaboration between humans and intelligent machines. Industry 5.0 leverages enabling technologies such as AI, IoT, collaborative robots, edge and cloud computing, and digital twins to create responsive, personalized, and efficient systems [2], [6].

Human-centricity ensures that technological advancements do not replace or disadvantage workers but instead empower them. For example, wearable sensors and intelligent interfaces can enhance workplace safety, ergonomics, and productivity. Sustainability is achieved through AI-based optimization that reduces waste and emissions, while resilience refers to a system's ability to adapt to external disruptions such as economic shifts, environmental challenges, or cyberattacks [8].

Applications of Industry 5.0 include personalized healthcare, where AI enables tailored diagnostics and treatments; adaptive manufacturing systems that respond to real-time human input; and sustainable energy networks optimized through intelligent monitoring systems. These examples demonstrate how Industry 5.0 transforms industrial operations while prioritizing human and environmental values [5].

Recent research further expands this perspective by highlighting the importance of Human–Robot Collaboration (HRC), smart manufacturing architectures, and advanced sensing technologies [8], [9], [11]. Collaborative robots equipped with multimodal sensing, predictive algorithms, and force-limiting capabilities create safer, more adaptive, and human-centered workplaces.

Additionally, Industry 5.0 involves the integration of extended reality (XR), immersive training systems, and value-sensitive design frameworks. These innovations enhance worker skills, support ethical adaptation to automation, and help organizations transition from technology-driven models to human-centered approaches [8], [11].

Comparison: Industry 4.0 vs Industry 5.0

The transition from Industry 4.0 to Industry 5.0 represents a significant shift in manufacturing priorities. Industry 4.0 focuses on automation, efficiency, and data-driven processes, whereas Industry 5.0 emphasizes collaboration between humans and machines, sustainability, and system resilience. This evolution reflects the growing need to combine human creativity and decision-making with advanced technologies to create more flexible, personalized, and environmentally friendly production systems [4], [6], [13]. Below is a

concise comparison table of Industry 4.0 vs Industry 5.0, focusing on objectives without listing detailed components (Table 1).

Table 1: Comparison Between Industry 4.0 and Industry 5.0

Aspect	Industry 4.0	Industry 5.0
Focus	Automation and efficiency	Human-centric, sustainable, and resilient production
Objective	Maximize productivity and reduce costs	Enhance human-machine collaboration and personalization
Human Role	Supervisory, limited involvement	Central, creative, and decision-making role
Technology Role	Drives automation and speed	Supports collaboration and sustainable practices
End Goal	High efficiency and throughput	Customization, sustainability, and resilience

ARTIFICIAL INTELLIGENCE ROLE IN INDUSTRY 5.0

AI has become a key enabler in realizing the promise of Industry 5.0. Human–AI collaboration supports the execution of intricate and highly individualized production tasks. AI-powered robots and digital twins assist in real-time simulation and optimization of production processes. Additionally, predictive analytics enable AI systems to proactively manage maintenance, enhance decision-making, reduce waste, and improve reliability [1], [9].

AI also enables real-time adjustments to manufacturing processes, allowing customization without compromising efficiency or speed. This aligns with market trends that increasingly demand personalized products. Furthermore, integrating AI into production lines facilitates decentralized decision-making, improving system agility and reducing dependence on centralized control [8, 9].

Intelligent platforms such as Siemens MindSphere and IBM Watson [20], [21] demonstrate real-world applications of AI in monitoring, diagnostics, and automated decision-making. These systems create intelligent feedback loops, where machines learn from human input to improve output quality and enhance customization capabilities [2]. AI also contributes to seamless coordination across value chains, improving supply chain visibility and enabling the prediction of disruptions.

Recent studies show that explainable AI (XAI), active learning, and simulated environments can support human decision-making in factories by making AI systems more transparent and trustworthy [8], [9], [11]. These tools allow workers to understand how AI systems make decisions, provide feedback, and actively participate in decision-making loops, fostering trust and innovation.

Researchers further emphasize that AI is no longer limited to automation it now influences business innovation, strategic direction, and long-term competitiveness. Organizations with higher AI maturity tend to achieve better product designs, more efficient processes, greener production, and greater adaptability to market changes [9].

CYBERSECURITY IN INDUSTRY 5.0

While the technological convergence of Industry 5.0 creates value, it also expands the digital attack surface. AI systems and cloud-edge infrastructures rely on interconnected devices,

increasing vulnerabilities such as data poisoning in AI models, ransomware attacks on critical manufacturing systems, and privacy breaches caused by pervasive IoT sensors [3], [4], [7].

Many emerging technologies still lack mature security measures, making them susceptible to attacks. For example, collaborative robots and digital twins depend on real-time data flows, which can be exploited to manipulate performance parameters. Additionally, decentralized operations make it more challenging to maintain secure communication between system nodes.

Although human-in-the-loop designs are essential for human-centric systems, they introduce new vulnerabilities, including social engineering attacks and unintended misuse of interfaces. Traditional cybersecurity approaches are no longer sufficient to protect dynamic, hybrid Industry 5.0 environments [3].

Recent cybersecurity reviews highlight that integrating humans and AI increases system risks [3], [7], [8]. These include misuse of smart systems, invasion of privacy, and the expansion of attack layers, making systems more vulnerable overall [7]. Threats such as adversarial machine learning, cyber-physical sabotage, and errors in human–robot interaction require a fundamental rethinking of defense strategies.

Experts emphasize the need for proactive, adaptive, and context-aware security solutions. Continuous monitoring, threat intelligence, user behavior simulation, and fault-tolerant architectures are essential to securing next-generation factories and human–machine ecosystems. Relying solely on traditional security models is no longer sufficient [7], [11].

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

AI serves as both a target and a powerful tool in cybersecurity. In Industry 5.0, AI-based threat detection systems use machine learning and deep learning to identify anomalies, detect malware, and predict potential breaches. These self-learning systems adapt to evolving threats, enabling faster response and mitigation [4].

AI also helps prioritize alerts and correlate incidents across large datasets, reducing the workload on human analysts. AI-driven deception technologies, such as honeypots, are used to lure attackers and analyze emerging threat patterns. Additionally, reinforcement learning models can dynamically adjust defense strategies in response to changing threat environments.

For example, deep learning models can classify behavioral anomalies in IoT networks, while AI-based Security Information and Event Management (SIEM) systems correlate security events in real time and provide actionable insights [22]. These capabilities are essential for proactive defense in highly distributed and sensor-dense environments [3], [22].

Researchers stress that Industry 5.0 requires not just automated security, but intelligent, explainable, and ethical security systems [2], [3], [5], [8], [9]. Integrating explainable AI into cybersecurity tools allows human operators to better understand and collaborate with AI systems.

Moreover, AI-driven cybersecurity must address vulnerabilities specific to collaborative robotics, digital twins, and cyber-physical systems where breaches can directly impact human safety. Adaptive defense models that incorporate human feedback are increasingly seen as critical for building secure and resilient Industry 5.0 ecosystems [7], [11].

ANTHROPOCENTRIC SECURITY CONCERNS

The shift toward human-centric security models is essential for achieving Industry 5.0. AI systems should be developed with careful consideration of usability, transparency, and trust. Human–AI interfaces must be user-friendly, ethically grounded, and supported by well-defined accountability mechanisms. Failures in security technologies can lead to reduced adoption and the improper use of these systems [5].

Designers must also consider the psychological comfort of end users. For example, XAI techniques enable users to understand why specific decisions are made, thereby fostering trust. However, ethical concerns such as bias in AI models, lack of transparency in decision-making, and issues related to surveillance remain significant challenges. A human-centered security model encourages stakeholder involvement in the design process and promotes principles such as explainability, fairness, and respect for user autonomy [2], [8].

In addition, privacy-by-design principles, data minimization, and informed consent are critical when implementing technologies that handle personal and sensitive information. Integrating these principles not only ensures regulatory compliance but also enhances societal acceptance of Industry 5.0 technologies [2], [11].

Scholars emphasize that human-centered cybersecurity must incorporate ethical AI governance, value-sensitive design, and robust frameworks to ensure that digital systems align with human dignity, autonomy, and workplace well-being [7], [8], [10]. These elements help create an environment of trust, reduce resistance to automation, and empower workers in increasingly cyber-intensive environments.

Furthermore, human-centric systems require strong safety measures for human–robot collaboration, protection against sensor tampering, and intuitive interfaces that allow workers to understand and monitor system actions—particularly in scenarios where AI directly assists with physical tasks [11], [12].

SECURITY STRATEGIES FOR INDUSTRY 5.0 ENVIRONMENTS

To ensure the security of cyber-physical environments in Industry 5.0, several strategies are indispensable. One of the most critical approaches is Zero Trust Architecture (ZTA), which eliminates the assumption of implicit trust within networks and systems. Instead, all users, devices, and endpoints must be continuously verified. This approach significantly limits the lateral spread of threats and strengthens overall system security [3].

Another essential strategy is the development of secure-by-design AI systems. Security must be embedded into AI systems from the initial design phase rather than added later. This includes ensuring adversarial robustness, implementing strong data protection mechanisms, conducting rigorous dataset validation, and maintaining continuous model

monitoring. Additionally, systems must be equipped to defend against adversarial inputs, ensuring resilience against evolving cyber threats [4].

Edge security and IoT protocols also play a vital role in protecting distributed cyber-physical systems. Strong security measures at the edge include the use of lightweight encryption techniques, robust authentication for edge devices, and real-time intrusion detection capabilities. Furthermore, physical tamper protection and secure firmware update mechanisms are necessary to safeguard edge nodes and IoT ecosystems from potential vulnerabilities and attacks [2].

Equally important are ethics and governance structures that guide the responsible implementation of AI technologies. Regulatory frameworks such as the EU AI Act and the NIST [14], [15], [16]. AI Risk Management Framework provides essential guidelines for ethical and secure AI deployment. These frameworks help organizations balance innovation with responsibility while addressing legal, ethical, and societal considerations, thereby ensuring accountability in AI systems [2], [5], [8].

Continuous education and training programs are also crucial for maintaining cybersecurity resilience. Organizations must invest in ongoing workforce development through simulation-based cybersecurity training, education in AI management and governance, and upskilling initiatives that promote secure human–machine interaction. Such efforts enhance awareness, preparedness, and the ability to respond effectively to emerging threats [1], [11].

A holistic approach to cybersecurity in Industry 5.0 requires the integration of technical controls, organizational culture, and regulatory alignment. Collaboration among key stakeholders, including developers, policymakers, users, and regulators. It is essential to ensure that cybersecurity measures support rather than hinder innovation [14], [15], [16].

Contemporary frameworks further recommend incorporating advanced security considerations such as human–robot collaboration safety protocols, digital twin security guidelines, and behavioral analytics for threat detection into enterprise security strategies. The growing use of collaborative robots (cobots) and cyber-physical systems underscores the need for comprehensive security models that address physical safety, sensor integrity, and real-time validation of AI-driven decisions [11].

Organizations should adopt forward-looking strategies that align cybersecurity with sustainability. These include data-driven sustainability security practices, Green IoT models, and resilient supply chain security mechanisms. Recent research in Industry 5.0 highlights these areas as key directions for future development, emphasizing the importance of harmonizing environmental responsibility with robust cybersecurity practices [7], [10].

A CONCEPTUAL FRAMEWORK FOR SECURE INDUSTRY 5.0

Industry 5.0 represents a paradigm shift in industrial systems, emphasizing human-centric, resilient, and secure production environments. Unlike Industry 4.0, which prioritized automation and efficiency, Industry 5.0 integrates human intelligence with advanced technologies, such as AI, robotics, and IoT, while embedding ethical, cybersecurity, and governance principles throughout operations [14], [15], [16]. Effective adoption of Industry

5.0 requires a clear framework that aligns human, technological, and data elements in a secure and manageable structure. The framework is organized into three essential layers:

1. Human-Centric Governance: Focused on workforce safety, training, ethical AI deployment, and human-machine collaboration [12], [17]
2. Cybersecurity & IT/OT Security: Ensures robust protection of information technology (IT) and operational technology (OT) systems using Zero Trust Architecture (ZTA), multi-factor authentication (MFA), identity and access management (IAM), and industrial control systems (ICS) security [18].
3. Data & AI Security: Covers secure data management, encryption, regulatory compliance (e.g., GDPR), XAI, and continuous AI model validation to prevent adversarial attacks or misuse [19].

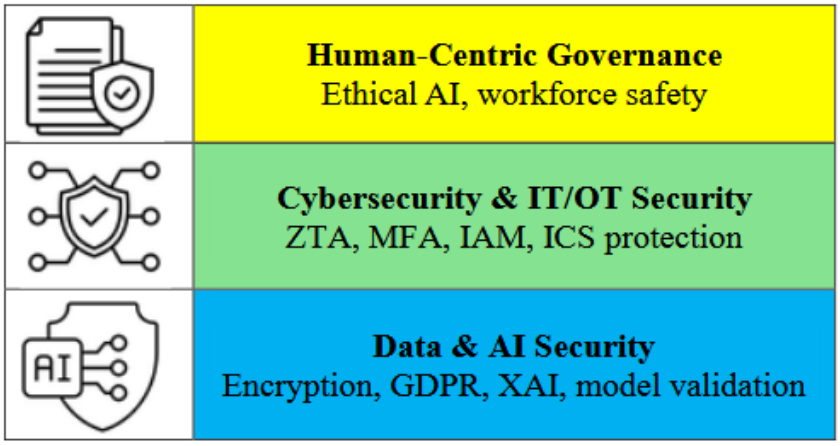

Figure 1: Core Industry 5.0 Security Framework (3 Layers)

Note: Security principles are embedded across all three layers, with governance at the top, technical cybersecurity in the middle, and data/AI security as the foundation for safe operations.

CONCLUSION

Industry 5.0 marks a new era that unites human values, intelligent systems, and sustainability. AI acts as both an enabler and a challenge, offering unprecedented levels of personalization and efficiency, while also introducing new cybersecurity risks. Addressing these challenges requires an interdisciplinary approach that combines technological advances with anthropocentric design and robust security controls.

This new industrial paradigm demands not only technical solutions for security but also cultural change, ethical development, and policy creation. Organizations must adopt forward-looking security practices that accommodate change, foster trust, and promote inclusiveness. By integrating concepts such as resiliency, transparency, and ethics into design and implementation, they can better navigate the complexities of Industry 5.0.

Future studies emphasize the importance of incorporating innovation capacity and human-centric AI design into cybersecurity strategies. This integration ensures that Industry 5.0 systems remain flexible, sustainable, and ethical. By aligning technological progress with human welfare, organizations can maximize the benefits of secure, trusted, and collaborative human–machine ecosystems.

REFERENCES

[1] A. Adel. (2022). The future of Industry 5.0 in society: Human-centered solutions, challenges and possible research perspectives. Journal of Cloud Computing, vol. 11, no. 40, Springer Nature, https://doi.org/10.1186/s13677-022-00314-5

[2] A. S. George and A. S. H. George. (2023). Revolutionizing manufacturing: The promise and problems of Industry 5.0. Partners Universal International Innovation Journal, vol. 1, no. 2, https://doi.org/10.5281/zenodo.7852124

[3] B. Santos, R. L. C. Costa, and L. Santos. (2024). "Cybersecurity in Industry 5.0: Open challenges and future directions," arXiv preprint, https://arxiv.org/pdf/2410.09538

[4] G. Czeczot, I. Rojek, D. Mikolajewski, and B. Sangho. (2023). AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes. MDPI Electronics, vol. 12, https://doi.org/10.3390/electronics12183800

[5] B. Martini, D. Bellisario, and P. Coletti. (2024). Human-Centered and Sustainable Artificial Intelligence in Industry 5.0: Challenges and Perspectives. MDPI Sustainability, vol. 16, p. 5448, https://doi.org/10.3390/su16135448.

[6] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. Journal of Manufacturing Systems, vol. 61, pp. 530–535, Elsevier, https://doi.org/10.1016/j.jmsy.2021.10.006

[7] R. W. Anwar, Y. Souissi, and S. Ali. (2025). Cyber Threats and Vulnerabilities in Industry 5.0: A Review. Arab Journal of Administrative Sciences, vol. 32, no. 2, pp. 435–454. https://doi.org/10.34120/ajas.v32i2.1289

[8] J. M. Rozanec et al. (2023). Human-centric artificial intelligence architecture for industry 5.0 applications. International Journal of Production Research, vol. 61, no. 20, pp. 6847–6872, https://doi.org/10.1080/00207543.2022.2138611

[9] A. Becue, J. Gama, and P. Q. Brito. (2024). AI's effect on innovation capacity in the context of industry 5.0: a scoping review. Artificial Intelligence Review, vol. 57, no. 215, Springer Nature, https://doi.org/10.1007/s10462-024-10864-6

[10] M. Hammad et al. (2025). From Industry 4.0 to 5.0: leveraging AI and IoT for sustainable and human-centric operations," International Journal of Industrial Engineering and Operations Management, https://doi.org/10.1108/IJIEOM-04-2025-0070

[11] M. L. Memon, M. N. Khan, and A. A. Shaikh. (2025). Industry 5.0: Human & robot interaction, smart manufacturing & integration of AI/ML-A comprehensive review for next generation manufacturing systems," Spectrum of Engineering Sciences, vol. 3, no. 10, pp. 1889–1928, https://doi.org/10.5281/zenodo.17645867

[12] J. Alves, T. M. Lima, and P. D. Gaspar. (2023). Is Industry 5.0 a human-centered approach? A systematic review. MDPI Processes, https://doi.org/10.3390/pr11010193

[13] Infor, "What is Industry 4.0 vs. Industry 5.0," URL: [Online]. Available: https://www.infor.com/industries/industrial-manufacturing/industry-4-0-vs-5-0 [Accessed: January 16, 2026].

[14] National Institute of Standards and Technology. (2025). Cybersecurity framework profile for artificial intelligence. NIST IR 8596, https://csrc.nist.gov/pubs/ir/8596/iprd

[15] European Union. (2024). Regulation (EU) 2024/1689 (AI Data Protection Regulation). https://zivilrecht.univie.ac.at/fileadmin/user_upload/i_zivilrecht/Wendehorst/Workshop_Datenschutz/Draft_AI_Data_Protection_Regulation_WENDEHORST_24-12-20.pdf

[16] ENISA. (2023). Artificial Intelligence and Cybersecurity Research. June 7, 2023, https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research [Accessed: November 7, 2025].

[17] E. Papagiannidis, P. Mikalef, and K. Conboy. (2025). Responsible artificial intelligence governance: A review and research framework. The Journal of Strategic Information Systems, Elsevier, https://doi.org/10.1016/j.jsis.2024.101885

[18] P. Papadopoulos, S. Katsikas, and N. Pitropakis. (2025). Cybersecurity and artificial intelligence: Advances, challenges, opportunities, threats. Frontiers in Big Data, Cybersecurity and Privacy, https://doi.org/10.3389/fdata.2024.1537878

[19] C. Nott. (2025). Organizational adaptation to generative AI in cybersecurity: A systematic review," arXiv preprint, https://doi.org/10.48550/arXiv.2506.12060

[20] Maya Derrick. (2025). Top 10: IoT Infrastructure Platforms. Technology Magazine, [Online]. Available: URL: https://technologymagazine.com/top10/top-10-iot-infrastructure-platforms [Accessed: January 16, 2026].

[21] Unity Tech Connect. (2025). 8 Best Industrial IoT Platforms for Business ROI in 2025. [Online]. Available: URL: https://unitytech-connect.com/resources/blog/industrial-iot-platforms-for-business/ [Accessed: December 5, 2025].

[22] Chrissy Kidd. (2025). SIEM: Security Information & Event Management Explained. [Online]. Available: URL: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html [Accessed: December 12, 2025].