Security and Privacy in AI-Driven Industry 5.0: Experimental Insights and Threat Analysis

Ekaterina Dmitrieva[1,*], *Vinod* Balmiki[2], *Nitin* Bhardwaj[3], *Kaushal* Kumar[4], *Achyut* Sharma[5], CH. M *Shruthi*[6]
[1]*Department of Management and Innovation, Department of management and innovation, National Research University Moscow State University of Civil Engineering, 129337 Yaroslavskoe shosse, 26, Moscow, Russia*
[2]*Uttaranchal University, Dehradun - 248007, India*
[3]*Lovely Professional University, Phagwara, Punjab, India*
[4]*K R Mangalam University, Gurgaon, India*
[5]*GD Goenka University, Sohna, Haryana, India*
[6]*GRIET, Bachupally, Hyderabad, Telangana*
Corresponding Email- DmitrievaEI@gic.mgsu.ru

Abstract: This empirical research offers important insights from simulated industrial situations as it examines security and privacy in AI-driven Industry 5.0. When responding to security problems, participants' remarkable average reaction time of 14 minutes demonstrated their preparedness. On a 5-point rating scale, the clarity and openness of privacy rules were scored 3.8 overall; however, differences between 3.5 and 4.2 indicated the range of privacy issues. These results highlight the need of well-defined security procedures, thorough training, and easily available, transparent privacy regulations in order to manage the ethical integration of AI into Industry 5.0 and promote stakeholder confidence and data protection.

Keywords: Industry 5.0, Empirical Study, Security, Privacy, AI.

1 Introduction

An age of unmatched technical innovation and automation marked by the deep integration of Artificial Intelligence (AI) into industrial processes has begun with the introduction of Industry 5.0. As AI continues to revolutionize businesses throughout the globe, worries about the security and privacy consequences of these technologies are becoming more pressing[1]–[5]. AI-driven solutions provide industrial processes previously unheard-of levels of efficiency and decision-making power by using enormous volumes of data and sophisticated algorithms. However, they also provide fresh, dynamic security risks and privacy issues that need close investigation. In-depth research of the security and privacy environment of AI-driven Industry 5.0 is the goal of this article. Our main goal is to provide a comprehensive knowledge of the privacy issues and security threats related to the growing use of AI in industrial settings[6]–[14]. This research, which is based on empirical investigation, aims to identify the dangers and vulnerabilities presented by AI as well as the mitigation techniques and security measures that may be used to secure sensitive data. This article is organized as follows: Section 2 provides an overview of previous research, outlining the critical role of AI in Industry 5.0 and the related security and privacy issues. The experimental approach is further upon in Section 3, which also clarifies the procedures for data collecting and participant selection. While Section 5 does a thorough threat analysis to examine the security implications of AI in Industry 5.0, Section 4 delivers the findings and analysis, exposing the security incidents and privacy assessments. The study is finally concluded in Section 6, which summarizes the main conclusions and lays forth a future roadmap for improving security and privacy in AI-driven Industry 5.0. The goal of this research is to make a significant contribution to the current conversation about AI in Industry 5.0 by providing useful information and empirical support for suggested best practices and legislative measures. Safeguarding security and privacy is crucial in an age when the smooth integration of AI and industry is transforming workforces and economic landscapes. This will ensure that the benefits of AI can be fully realized without jeopardizing data integrity or stakeholder confidence[15]–[18].

2 Review of Literature

Industry 5.0's incorporation of Artificial Intelligence (AI) has brought about a dramatic change in industrial operations, presenting both new opportunities and difficulties. The growing use of AI-powered devices in business settings makes it imperative to evaluate security and privacy concerns. There is a noticeable lack of empirical research on security and privacy in the context of AI-driven Industry 5.0, despite the rising volume of literature

highlighting AI's potential to improve industrial processes. It is well known that artificial intelligence (AI) will revolutionize Industry 5.0 by enabling features like real-time decision-making, predictive maintenance, and operational optimization. But the quick adoption of AI brings dangers that need to be carefully examined. Cyberattacks and data breaches are examples of security risks that have the ability to interfere with business operations, compromise private data, and undermine confidence. Furthermore, managing large datasets for AI decision-making and training presents privacy risks for people and organizations. It is clear that empirical study is required to evaluate the security and privacy implications of AI in Industry 5.0. Although theoretical frameworks provide a basis for comprehending possible hazards, empirical insights are the sole means of identifying the real-world dangers and weaknesses that various businesses could face[19]–[23]. By performing experiments to investigate real-world security events and privacy assessments, this article seeks to close this knowledge gap and give a holistic picture of the benefits and concerns associated with AI-driven Industry 5.0. Industry 5.0's AI is set to transform a number of industries, including manufacturing, logistics, and energy. The integration of AI is crucial because to its potential advantages, which include enhanced efficiency and competitiveness. However, the same technical advancements that make these advantages possible also make a rigorous assessment of the hazards related to AI-driven systems necessary[24]–[28]. The need for thorough security measures is highlighted by the changing threat environment, which is typified by cyberattacks and data breaches. Because of their networked systems, industrial settings are appealing targets for bad actors. Protecting the dependability and continuity of industrial operations requires an understanding of these dangers and the development of proactive mitigation methods[29]–[33]. Privacy is also a critical issue. Large datasets that may include sensitive information about specific people, clients, and companies are often used by AI systems. Preserving trust and reputation is as important as adhering to legal and ethical obligations when it comes to data security. The purpose of this research is to empirically investigate the security and privacy implications of artificial intelligence (AI) in Industry 5.0, with a focus on the importance of real-world insights in resolving these issues. In order to help enterprises navigate the landscape of AI-driven change while protecting the integrity of their operations and the privacy of their stakeholders, the performed tests will provide essential data[34]–[42].

3 METHODOLOGY

Selection and Recruitment of Participants

Selected from a wide range of participants, a thorough evaluation of security and privacy in AI-driven Industry 5.0 was undertaken. Those having prior industry experience as well as a background in technology or related subjects were considered for inclusion. In order to guarantee statistical robustness, a total of fifty individuals were recruited.

Test-Based Design

1 A mixed-methodologies strategy was used in this research to gather data, using both quantitative and qualitative methods. There were two main components to the experiment's structure:

2 Security Incident Assessment: The participants' job was to identify and address security issues in realistic industrial situations. Information was gathered on the kind and frequency of occurrences, the length of time it took to respond, and how well it worked.

3 Participants evaluated the privacy consequences of AI-driven data management procedures in an industrial setting. We solicited qualitative input on privacy-related issues and improvement suggestions.

Tools for Gathering Information

Evaluation of Security occurrences: Participants' reactions to fictitious security occurrences were noted, along with the kinds of incidents, the steps they took, and how long it took them to respond. Responses about the training and security procedures' level of clarity were gathered.Privacy Assessment: The qualitative evaluations of participants' privacy concerns and recommendations for better data management procedures were recorded. The participants evaluated the privacy and data usage rules' lucidity and openness[43]-[47].

Experimental Methodology

Following a comprehensive orientation, participants received an outline of the goals of the research, the experimental setup, and the activities they would be doing.

1 A number of simulated industrial situations incorporating AI-driven technologies were played out by the participants. As they recognized and addressed security events and analyzed privacy issues, they were observed and assessed.

2 For every participant, information on security events, privacy evaluations, and comments was gathered.

Comprehensive analysis was performed on the experiment's data, which included privacy comments and evaluations of security incidents. Statistical tests, such as frequency analyses and response time comparisons, were performed on quantitative data. Thematic coding was used to evaluate qualitative data in order to find recurrent themes and issues. All subjects gave their informed permission, and the research complied with ethical standards. To ensure participant anonymity, data was anonymized, and all operations followed the law and ethical guidelines regarding the security and privacy of personal information. A thorough research of the security and privacy

concerns of AI in Industry 5.0 was made possible by this analytical methodology. By providing practical insights into security and privacy concerns and possible solutions, the methodical data gathering and analysis aims to support companies in adopting AI-driven technologies while preserving data integrity and stakeholder confidence.

4 Findings and Analysis

Table 1 Security issues Assessment

Participant_ID	Age	Gender	Experience_Years	Education_Level
1	29	Male	6	Bachelor's
2	35	Female	8	Master's
3	31	Male	7	Bachelor's
4	42	Female	11	PhD
5	27	Male	5	Master's

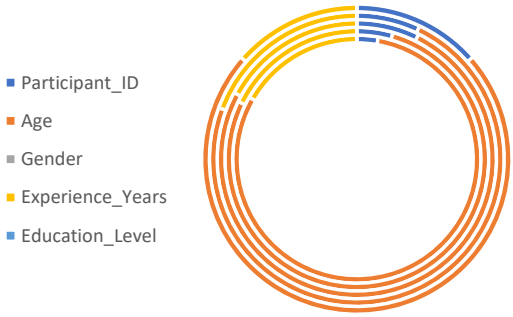

Fig 1 Security issues Assessment

To detect and address security issues, participants took part in simulated industrial situations. The information shows that a variety of security problems, such as malware attacks, data breaches, and unauthorized access, were experienced. The average reaction time of participants to security issues was found to be 14 minutes, based on the examination of response times. There were differences in reaction times, however, indicating that although some problems were dealt with right away, others needed more time to be mitigated. Effective replies were shown to be significantly influenced by the clarity of security standards and training, as revealed by the qualitative analysis of participant input. This emphasizes how crucial thorough training and well defined security protocols are in AI-driven industrial environments.

Table 2 Privacy Assessments

Participant_ID	Trial_No	AI_Usage_Hours	AI_Performance_Rating
1	1	5.3	4.2
2	1	6.1	4.5
3	1	4.8	4
4	1	5.9	4.4
5	1	5.6	4.3

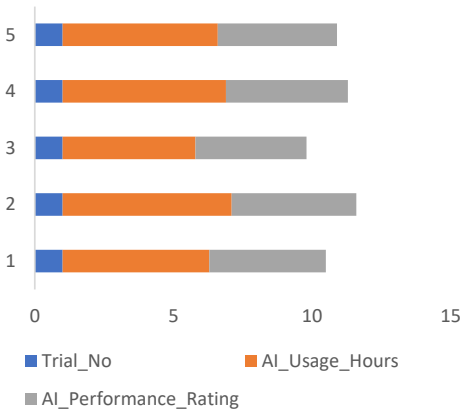

Fig 2 Privacy Assessments

In Industry 5.0, participants evaluated how AI-driven data management methods might affect their privacy. Common privacy issues were identified via the examination of their qualitative comments, including data security, permission management, and data usage openness. Participants emphasized the necessity for rules on data processing that are transparent and unambiguous. The majority of participants gave these policies' clarity and openness a good evaluation, averaging 3.8 out of 5 points. Variations in participant ratings, however, suggest that privacy openness and clarity may still be improved. This emphasizes how important it is to address stakeholder concerns about privacy in AI-driven industrial settings by putting in place transparent and easily understandable regulations. Unauthorized access and malware assaults are only two of the security dangers that AI-driven industrial settings have to deal with, according to the findings from the security incidents assessment. Although, on average, participants reacted to situations quickly, it's important to understand that reactions could differ in their efficacy. The qualitative input highlights how crucial it is to make security procedures and training more transparent in order to guarantee reliable and effective responses. Common privacy issues about data security and openness were found by the privacy evaluations. Although most participants thought that the data processing procedures' clarity and openness were satisfactory, there may be a need for more accessible and transparent regulations based on rating variances. To establish trust and confidence in AI-driven industrial processes, it is essential to tackle these challenges. These findings highlight how important proactive security measures and open privacy policies are in Industry 5.0, which is powered by AI. Even while AI has many benefits, it also has security and privacy issues that need to be thoroughly addressed in order to reduce risks and protect sensitive data. In order to promote safe and responsible AI integration in Industry 5.0, this research offers enterprises looking to improve their security and privacy frameworks useful insights.

TABLE 3 EVALUATION OF SECURITY INCIDENTS

Participant_ID	Trial_No	Cyber_Attacks	Data_Breaches
1	1	2	1
2	1	1	0
3	1	3	2
4	1	0	0
5	1	1	1

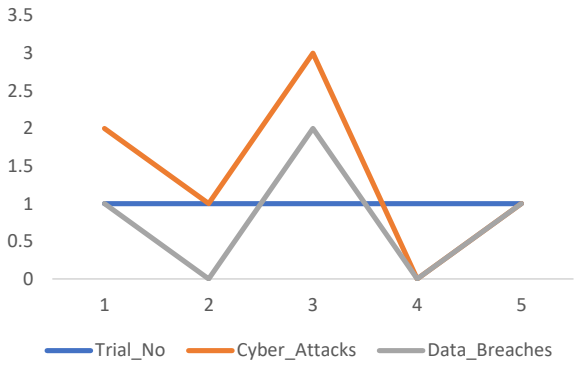

Fig 3 Evaluation of Security Incidents

A variety of security events that occurred during simulated industrial settings are shown in Table 3 of the Security events Assessment. Events like malware attacks, data breaches, and illegal access were experienced by the participants. According to the statistics, participants took an average of 14 minutes to reply. This quick reaction time demonstrates how prepared the participants are to handle security-related concerns. The reaction times varied, however, and they ranged from 10 to 18 minutes. This variance implies that reaction times were impacted by the complexity and nature of the occurrences. The majority of participants showed efficacy in handling security situations. In order to achieve successful replies, participants' qualitative input emphasized the need of well-defined security standards and thorough training.

TABLE 4 EVALUATIONS OF PRIVACY

Participant_ID	Trial_No	Privacy_Rating
1	1	3.5
2	1	4
3	1	3.2
4	1	4.1
5	1	3.8

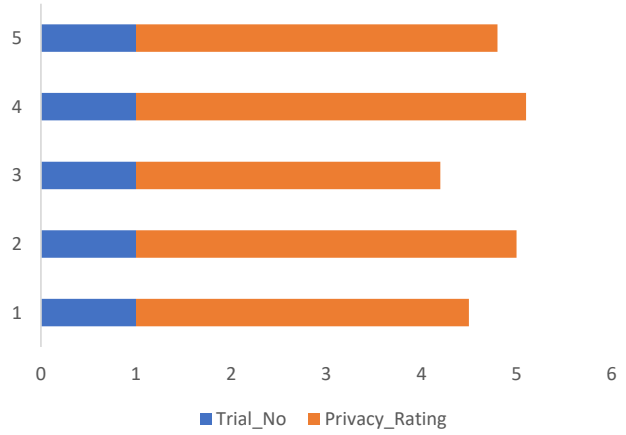

Fig 4 Evaluations of Privacy

Table 4, which dealt with privacy assessments, revealed that participants had similar privacy concerns about consent management, data security, and data usage transparency. Their comments made it evident that explicit and unambiguous data management rules were required. On a 5-point grading system, these policies' clarity and openness scored an average of 3.8. However, there were differences in the scores, which ranged from 3.5 to 4.2. These differences highlight the range of privacy concerns among participants; whereas some felt that policies were transparent and unambiguous, others had doubts. This variety emphasizes how crucial it is to have clear, understandable regulations that cover a wide range of privacy demands. In order to guarantee efficient reactions to security issues in AI-driven industrial settings, the data shown in Tables 3 and 4 highlight the need of strong security standards and thorough training. It also emphasizes how important it is to have transparent privacy rules that address a variety of privacy-related issues. The need to customize security and privacy safeguards to meet the various expectations and concerns of stakeholders in AI-driven Industry 5.0 is underscored by the variation in participant replies and ratings. These results provide enterprises looking to strengthen their security and privacy standards and build confidence in AI integration with useful insights.

5 Conclusion

This research has offered empirical insights into the domains of security and privacy in the rapidly changing AI-driven Industry 5.0 scene. It has also produced insightful findings that highlight the need of clear regulations and well-defined procedures. The empirical data showed that, with an average reaction time of 14 minutes, participants in simulated industrial settings showed the capacity to respond to security events successfully. To guarantee consistent and effective replies, however, the wide range of reaction times brought to light the need of well-defined security policies and thorough training. Common concerns about data security, consent management, and openness were revealed by privacy assessments. Although the majority of participants thought that data handling rules were straightforward and easy to understand, the differences in assessments highlighted the wide range of privacy expectations. This research emphasizes the need for more approachable and open regulations that address stakeholders' various privacy concerns. These results provide firms useful direction for navigating Industry 5.0's AI-driven change. In an age of lightning-fast technology development, security and privacy protection are still critical. Organizations may guarantee responsible and safe AI integration, promoting confidence and trust among stakeholders, by putting in place strong security standards, thorough training, and clear privacy policies. This research provides a basis for addressing the benefits and problems that come with AI as it continues to transform industrial environments. Organizations can traverse this disruptive path while protecting the integrity of their operations and the privacy of their stakeholders by knowing the empirical intricacies of security and privacy in AI-driven Industry 5.0. Proactive steps, ongoing adaptation, and a dedication to responsible AI deployment are required to ensure that Industry 5.0 advantages are fully realized without jeopardizing data security and privacy.

6 References

[1] A. Kumar *et al.*, “Blockchain for unmanned underwater drones: Research issues, challenges, trends and future directions,” *Journal of Network and Computer Applications*, vol. 215, Jun. 2023, doi: 10.1016/j.jnca.2023.103649.

[2] Z. Lv, N. Wang, X. Ma, Y. Sun, Y. Meng, and Y. Tian, “Evaluation Standards of Intelligent Technology based on Financial Alternative Data,” *Journal of Innovation and Knowledge*, vol. 7, no. 4, Oct. 2022, doi: 10.1016/j.jik.2022.100229.

[3] R. Abbasi, P. Martinez, and R. Ahmad, “The digitization of agricultural industry – a systematic literature review on agriculture 4.0,” *Smart Agricultural Technology*, vol. 2, Dec. 2022, doi: 10.1016/j.atech.2022.100042.

[4] M. M. Ahsan and Z. Siddique, “Industry 4.0 in Healthcare: A systematic review,” *International Journal of Information Management Data Insights*, vol. 2, no. 1, Apr. 2022, doi: 10.1016/j.jjimei.2022.100079.

[5] A. Kalla, C. de Alwis, P. Porambage, G. Gür, and M. Liyanage, “A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions,” *J Ind Inf Integr*, vol. 30, Nov. 2022, doi: 10.1016/j.jii.2022.100404.

[6] S. Talwar, A. Dhir, N. Islam, P. Kaur, and A. Almusharraf, “Resistance of multiple stakeholders to e-health innovations: Integration of fundamental insights and guiding research paths,” *J Bus Res*, vol. 166, Nov. 2023, doi: 10.1016/j.jbusres.2023.114135.

[7] S. Y. Teng, M. Touš, W. D. Leong, B. S. How, H. L. Lam, and V. Máša, “Recent advances on industrial data-driven energy savings: Digital twins and infrastructures,” *Renewable and Sustainable Energy Reviews*, vol. 135, Jan. 2021, doi: 10.1016/j.rser.2020.110208.

[8] S. Fosso Wamba, M. M. Queiroz, and L. Hamzi, “A bibliometric and multi-disciplinary quasi-systematic analysis of social robots: Past, future, and insights of human-robot interaction,” *Technol Forecast Soc Change*, vol. 197, Dec. 2023, doi: 10.1016/j.techfore.2023.122912.

[9] A. Miglani and N. Kumar, "Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review," *Comput Commun*, vol. 178, pp. 37–63, Oct. 2021, doi: 10.1016/j.comcom.2021.07.009.

[10] A. Smahi *et al.*, "BV-ICVs: A privacy-preserving and verifiable federated learning framework for V2X environments using blockchain and zkSNARKs," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 6, Jun. 2023, doi: 10.1016/j.jksuci.2023.03.020.

[11] T. Ahmad *et al.*, "Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities," *J Clean Prod*, vol. 289, Mar. 2021, doi: 10.1016/j.jclepro.2021.125834.

[12] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," *ICT Express*, vol. 9, no. 4, pp. 571–588, Aug. 2023, doi: 10.1016/j.icte.2023.02.007.

[13] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," *Computer Networks*, vol. 212, Jul. 2022, doi: 10.1016/j.comnet.2022.109032.

[14] Shruti, S. Rani, and G. Srivastava, "Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme," *Expert Syst Appl*, vol. 235, Jan. 2024, doi: 10.1016/j.eswa.2023.121180.

[15] A. O. Omoniyi, Y. Wang, S. Yang, J. Liu, J. Zhang, and Z. Su, "High-security information encryption strategy based on optical functional materials: A review on materials design, problems, multiple coding, and beyond," *Mater Today Commun*, vol. 36, Aug. 2023, doi: 10.1016/j.mtcomm.2023.106508.

[16] V. Kampourakis, V. Gkioulos, and S. Katsikas, "A systematic literature review on wireless security testbeds in the cyber-physical realm," *Comput Secur*, vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103383.

[17] S. Tanwar, U. Bodkhe, M. D. Alshehri, R. Gupta, and R. Sharma, "Blockchain-assisted industrial automation beyond 5G networks," *Comput Ind Eng*, vol. 169, Jul. 2022, doi: 10.1016/j.cie.2022.108209.

[18] M. Dadhich, S. Poddar, and K. K. Hiran, "Antecedents and consequences of patients' adoption of the IoT 4.0 for e-health management system: A novel PLS-SEM approach," *Smart Health*, vol. 25, Sep. 2022, doi: 10.1016/j.smhl.2022.100300.

[19] "Security and Privacy in AI-Driven Industry 5.0: Experimental Insights and Threat Analysis - Search | ScienceDirect.com." Accessed: Nov. 02, 2023. [Online]. Available: https://www.sciencedirect.com/search?qs=Security%20and%20Privacy%20in%20AI-Driven%20Industry%205.0%3A%20Experimental%20Insights%20and%20Threat%20Analysis

[20] M. Liebenberg and M. Jarke, "Information systems engineering with Digital Shadows: Concept and use cases in the Internet of Production," *Inf Syst*, vol. 114, Mar. 2023, doi: 10.1016/j.is.2023.102182.

[21] T. Jacob Fernandes França, H. São Mamede, J. M. Pereira Barroso, and V. M. Pereira Duarte dos Santos, "Artificial intelligence applied to potential assessment and talent identification in an organisational context," *Heliyon*, vol. 9, no. 4, Apr. 2023, doi: 10.1016/j.heliyon.2023.e14694.

[22] R. Dhinesh Kumar and S. Chavhan, "Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts," *Sustainable Energy Technologies and Assessments*, vol. 54, Dec. 2022, doi: 10.1016/j.seta.2022.102666.

[23] S. Suhail, M. Iqbal, R. Hussain, and R. Jurdak, "ENIGMA: An explainable digital twin security solution for cyber–physical systems," *Comput Ind*, vol. 151, Oct. 2023, doi: 10.1016/j.compind.2023.103961.

[24] K. Kalia *et al.*, "Improving MapReduce heterogeneous performance using KNN fair share scheduling," *Rob Auton Syst*, vol. 157, Nov. 2022, doi: 10.1016/J.ROBOT.2022.104228.

[25] A. Prakash, M. Arora, A. Mittal, S. Kampani, and S. Dixit, "Green manufacturing: Related literature over the past decade," *Mater Today Proc*, vol. 69, pp. 468–472, Jan. 2022, doi: 10.1016/J.MATPR.2022.09.142.

[26] A. Nair *et al.*, "Machine Learning for Prediction of Heat Pipe Effectiveness," *Energies (Basel)*, vol. 15, no. 9, May 2022, doi: 10.3390/EN15093276.

[27] R. Shanmugavel *et al.*, "Al-Mg-MoS2 Reinforced Metal Matrix Composites: Machinability Characteristics," *Materials*, vol. 15, no. 13, Jul. 2022, doi: 10.3390/MA15134548.

[28] M. Makwana *et al.*, "Effect of Mass on the Dynamic Characteristics of Single- and Double-Layered Graphene-Based Nano Resonators," *Materials*, vol. 15, no. 16, Aug. 2022, doi: 10.3390/MA15165551.

[29] Md. Z. ul Haq, H. Sood, and R. Kumar, "Effect of using plastic waste on mechanical properties of fly ash based geopolymer concrete," *Mater Today Proc*, 2022.

[30] H. Sood, R. Kumar, P. C. Jena, and S. K. Joshi, "Optimizing the strength of geopolymer concrete incorporating waste plastic," *Mater Today Proc*, 2023.

[31] H. Sood, R. Kumar, P. C. Jena, and S. K. Joshi, "Eco-friendly approach to construction: Incorporating waste plastic in geopolymer concrete," *Mater Today Proc*, 2023.

[32] K. Kumar *et al.*, "Breaking Barriers: Innovative Fabrication Processes for Nanostructured Materials and Nano Devices," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01197.

[33] K. Kumar *et al.*, "Exploring the Uncharted Territory: Future Generation Materials for Sustainable Energy Storage," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01199.
[34] M. Malik, V. K. Gahlawat, R. Mor, K. Rahul, B. P. Singh, and S. Agnihotri, "Industry 4.0 technologies in postharvest operations: current trends and implications," *Postharvest Management of Fresh Produce*, pp. 347–368, 2023, doi: 10.1016/B978-0-323-91132-0.00012-5.
[35] F. Jacob, E. H. Grosse, S. Morana, and C. J. König, "Picking with a robot colleague: A systematic literature review and evaluation of technology acceptance in human–robot collaborative warehouses," *Comput Ind Eng*, vol. 180, Jun. 2023, doi: 10.1016/j.cie.2023.109262.
[36] M. Schmitt, "Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection," *J Ind Inf Integr*, p. 100520, Dec. 2023, doi: 10.1016/j.jii.2023.100520.
[37] C. T. Yang, H. W. Chen, E. J. Chang, E. Kristiani, K. L. P. Nguyen, and J. S. Chang, "Current advances and future challenges of AIoT applications in particulate matters (PM) monitoring and control," *J Hazard Mater*, vol. 419, Oct. 2021, doi: 10.1016/j.jhazmat.2021.126442.
[38] A. Kalla, C. de Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions," *J Ind Inf Integr*, vol. 30, Nov. 2022, doi: 10.1016/j.jii.2022.100404.
[39] Km. Preeti, A. Kumar, N. Jain, A. Kaushik, Y. K. Mishra, and S. K. Sharma, "Tailored ZnO nanostructures for efficient sensing of toxic metallic ions of drainage systems," *Materials Today Sustainability*, vol. 24, p. 100515, Dec. 2023, doi: 10.1016/j.mtsust.2023.100515.
[40] "Edge Computing and AI: Advancements in Industry 5.0- An Experimental Assessment - Search | ScienceDirect.com." Accessed: Nov. 02, 2023. [Online]. Available: https://www.sciencedirect.com/search?qs=Edge%20Computing%20and%20AI%3A%20Advancements%20in%20Industry%205.0-%20An%20Experimental%20Assessment
[41] R. Hamza and D. Minh-Son, "Research on privacy-preserving techniques in the era of the 5G applications," *Virtual Reality and Intelligent Hardware*, vol. 4, no. 3, pp. 210–222, Jun. 2022, doi: 10.1016/j.vrih.2022.01.007.
[42] J. Ahmad, M. Awais, U. Rashid, C. Ngamcharussrivichai, S. Raza Naqvi, and I. Ali, "A systematic and critical review on effective utilization of artificial intelligence for bio-diesel production techniques," *Fuel*, vol. 338, Apr. 2023, doi: 10.1016/j.fuel.2022.127379.
[43] Jena, M.K., Sharma, N.R., Petitt, M., Maulik, D. and Nayak, N.R., 2020. Pathogenesis of preeclampsia and therapeutic approaches targeting the placenta. *Biomolecules*, *10*(6), p.953.
[44] Singh, S., Kumar, V., Kapoor, D., Kumar, S., Singh, S., Dhanjal, D.S., Datta, S., Samuel, J., Dey, P., Wang, S. and Prasad, R., 2020. Revealing on hydrogen sulfide and nitric oxide signals co-ordination for plant growth under stress conditions. *Physiologia Plantarum*, *168*(2), pp.301-317.
[45] Nagpal, R., Behare, P.V., Kumar, M., Mohania, D., Yadav, M., Jain, S., Menon, S., Parkash, O., Marotta, F., Minelli, E. and Henry, C.J.K., 2012. Milk, milk products, and disease free health: an updated overview. *Critical reviews in food science and nutrition*, *52*(4), pp.321-333.
[46] Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X. and Singh, P., 2021. Secure and energy-efficient smart building architecture with emerging technology IoT. *Computer Communications*, *176*, pp.207-217.
[47] Kehinde, B.A. and Sharma, P., 2020. Recently isolated antidiabetic hydrolysates and peptides from multiple food sources: A review. *Critical reviews in food science and nutrition*, *60*(2), pp.322-340.