The Scientific Temper (2023) Vol. 14 (4): 1264-1270

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.30

https://scientifictemper.com/

RESEARCH ARTICLE

Evaluating dynamics, security, and performance metrics for smart manufacturing

Lakshmi Priya[1], Anil Vasoya[2], C. Boopathi[3], Muthukumar Marappan[4*]

Abstract

The role of the IoT in smart manufacturing is aimed to illuminate its transformative impact on operational efficiency, responsiveness, and environmental sustainability. The investigation aimed to explore IoT's pivotal significance in reshaping manufacturing processes towards heightened efficiency, responsiveness, and environmental consciousness. The study presents results from performance metric assessments, visualizations, and data simulations. It contains information about the way IoT data is shown in manufacturing environments, the clear relationship between temperature and pressure, the distribution of security risks and related safety measures, and the dynamic behavior of important IoT components. The importance of IoT in real-time environmental management, process optimization, and security enhancement within paradigms of smart manufacturing are the key points of observation. The comparative analysis of conventional analytical models and composite models highlights the choice between stability and adaptability, providing crucial insights for modeling approaches tailored to distinct manufacturing requirements. IoT's transformative potential within smart manufacturing, emphasizes data integrity, security, sensor dynamics, analytics, and sustainability.

Keywords: Internet of things, Smart manufacturing, Data analytics, Security, Sensors, Sustainability.

Introduction

The advent of the Internet of Things (IoT) has ushered in an era of profound transformation across diverse industries, with few sectors experiencing more significant shifts than manufacturing. Smart manufacturing, often regarded as the key driver of the fourth industrial revolution, leverages IoT technologies to enhance productivity, improve efficiency, and enable data-driven decision-making. This literature survey aims to provide a comprehensive overview of the pivotal role of IoT in the realm of smart manufacturing. As an author, it is imperative to explore existing research and the evolution of IoT's integration within manufacturing processes, while highlighting the notable contributions of various studies that have collectively shaped the landscape. The integration of IoT in the manufacturing sector can be seen as a logical progression in the quest for increased operational efficiency and data-driven decision-making. In recent years, researchers have investigated the role of IoT in optimizing manufacturing processes, and the consensus points toward substantial benefits. A seminal study by (Saqlain, M., *et al.*, 2019) led to enhanced visibility, predictive maintenance, and better inventory management. Furthermore, the study emphasized that the application of IoT in manufacturing can improve supply chain coordination, a critical aspect in modern, globally distributed production systems (Shahbazi, Z., & Byun, Y. C. 2021). Such findings highlighted the potential of IoT to redefine manufacturing, making it more agile, adaptive, and responsive to market dynamics.

Security is a paramount concern in the context of IoT for smart manufacturing, considering the massive amount

---

[1]Department of Electrical and Computer Engineering, Loyola Institute of Technology, Kuthambakkam, Tamil Nadu, India.

[2]Department of Information Technology, Thakur College of Engineering and Technology, Mumbai, Maharashtra, India.

[3]Department of Mechanical Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India.

[4]Department of Mechanical Engineering, Nandha Engineering College, Erode, Tamil Nadu, India.

***Corresponding Author:** Muthukumar Marappan, Department of Mechanical Engineering, Nandha Engineering College, Erode, Tamil Nadu, India. , E-Mail: muthupsgtech@gmail.com

How to cite this article: Priya, L., Vasoya, A., Boopathi, C., Marappan, M.. (2023). Evaluating dynamics, security, and performance metrics for smart manufacturing. The Scientific Temper, **14**(4):1264-1270.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.30

Source of support: Nil

Conflict of interest: None.

Received: 16/09/2023 **Accepted:** 15/10/2023 **Published**:31/12/2023

of data generated and transmitted across devices and networks. This is well-supported by the work of (Ma, S., *et al.*, 2022), who discussed the importance of securing IoT devices in industrial environments. The authors recognized the critical need for securing IoT devices due to the vulnerability of legacy systems, the increasing number of attack vectors, and the potential consequences of breaches in manufacturing settings (Abuhasel, K. A., & Khan, M. A. 2020). Their research highlighted the need for robust security measures in the IoT landscape, an issue that will undoubtedly shape the evolution of smart manufacturing. A pertinent aspect of smart manufacturing is the integration of IoT-enabled sensors. Sensors play a crucial role in data collection and real-time monitoring. Studies such as that of (Durana, P., *et al.*, 2021) highlighted the significance of sensors in enhancing manufacturing processes. The authors emphasized IoT sensors can facilitate predictive maintenance, leading to reduced downtime and substantial cost savings. IoT sensors can improve product quality and facilitate data-driven decision-making through real-time data streams (Assaqty, M. I. S., *et al.*, 2020). This emphasis on sensors as enablers of smart manufacturing highlighted the pivotal role they play in revolutionizing production processes.

IoT is not merely confined to data collection and monitoring; it extends to the realm of data analytics. Advanced analytics, as highlighted by many researchers, is integral to deriving actionable insights from the massive data generated by IoT devices. A study by (Phuyal, S., *et al.* 2020) expounded on the significance of data analytics in IoT-enabled smart manufacturing. The research emphasized that analytics can uncover hidden patterns, predict machine failures, optimize processes, and enable proactive decision-making (Mourtzis, D., *et al.*, 2021). With the proliferation of big data, machine learning, and artificial intelligence, data analytics stands as a linchpin in realizing the full potential of IoT in manufacturing. Manufacturers worldwide are increasingly investing in the integration of IoT for smart manufacturing. This paradigm shift is not only driven by technological advancements but also by the quest for sustainability and environmental responsibility. As echoed in the work of (Mylonas, G., *et al.*, 2021), smart manufacturing can contribute to sustainability by reducing energy consumption, waste, and emissions. The authors emphasized that IoT-enabled monitoring and control mechanisms can lead to more efficient resource utilization, thereby contributing to the environmental goals of manufacturers (Popescu, G. H., *et al.*, 2021). This perspective aligns with global efforts to promote sustainable and eco-friendly manufacturing practices.

In the literature survey the transformative potential of IoT in smart manufacturing. With the convergence of sensors, data analytics, security, and sustainability, IoT is poised to reshape manufacturing processes, making them more efficient, responsive, and environmentally responsible. The studies cited herein collectively point toward a future where smart manufacturing is not just a concept but a tangible reality, driven by the relentless march of IoT technologies and their dynamic integration within manufacturing ecosystems. A notable research gap in the current body of literature is the limited exploration of the long-term sustainability and scalability of IoT implementations in the context of smart manufacturing. While existing studies, such as the work by (Lyu, Z., *et al.*, 2020), provide valuable insights into the advantages of IoT in manufacturing, there remains a dearth of comprehensive research that assesses the long-term implications and challenges of scaling IoT solutions over time. Addressing this gap is crucial to ensure the continued success and adaptability of IoT-enabled smart manufacturing systems as they evolve and mature.

Research Methodology

This paper is a comprehensive research methodology that underpins the various programs and analyses conducted to investigate key aspects of the IoT in the context of smart manufacturing. Research methodology encompasses data simulation, data visualization, and performance metric evaluation. These methodologies were designed to explore and elucidate distinct facets of IoT's role in smart manufacturing. Simulated IoT data to emulate real-world scenarios. For instance, in the first program, simulated IoT sensor data, such as temperature and pressure, were collected over a specific duration. The use of randomization techniques ensured the generation of diverse datasets, which mirror the dynamic nature of data captured in manufacturing environments. In the second program, the simulation to encompass security issues and precautions relevant to IoT in manufacturing. This approach allowed us to assess potential security challenges and the corresponding precautionary measures associated with implementing IoT systems (Xu, X., *et al.*, 2020).

Subsequently, data visualization techniques to communicate the results effectively. Visualizations included time series plots, scatter plots, and bar charts. These representations allowed us to depict the relationships between variables and highlight essential findings. For instance, used time series plots to illustrate the evolution of IoT sensor data over time, helping to visualize trends and fluctuations in the manufacturing environment. Scatter plots, on the other hand, facilitated the exploration of correlations between variables, such as temperature and pressure, offering insights into their interdependencies. Furthermore, the bar chart enabled a concise depiction of the number of precautions associated with specific security issues, providing a clear overview of the complexity of security considerations. In addition to data simulation and visualization, conducted a performance metric evaluation. The performance metrics assessed the efficiency and effectiveness of various IoT components, including sensors, processing units, communication devices, and actuation gadgets. By generating synthetic data for these metrics, evaluated and compared the performance of different models. The use of line plots and subplots helped us present the findings and visualize the performance of these IoT components across various parameters.

The research methodology serves as a structured framework for investigating and analyzing the multifaceted landscape of IoT in smart manufacturing. It encompasses data generation, visualization, and performance assessment, which collectively contribute to a holistic understanding of the challenges, opportunities, and potential of IoT in reshaping modern manufacturing processes. The programs and analyses conducted in this research provide valuable insights into the role of IoT in smart manufacturing and the various dimensions that researchers and practitioners should consider when implementing IoT systems in industrial settings.

Results and Discussion

IoT Data for Smart Manufacturing

The graph in Figure 1 presented below illustrates the simulated IoT data for smart manufacturing, focusing on the variation in temperature (°C) and pressure (hPa) over a 24-hour period. The X-axis represents time in hours, with data points recorded at 0, 5, 10, 15, and 20 hours, while the Y-axis displays the values ranging from 0 to 1000. The temperature data (in red) exhibits a gradual rise from 50°C at the start, reaching around 800°C at the 20-hour mark, followed by a decline, depicting a cyclic pattern. This cyclic pattern may be attributed to regular heating and cooling processes within a manufacturing environment, highlighting the dynamic nature of temperature fluctuations. In contrast, the pressure data (in blue) shows a relatively stable and consistent profile. The pressure remains consistent around 900 hPa over the 24-hour period, indicating a controlled and stable manufacturing environment. The minimal deviation in pressure values suggests that manufacturing operations maintain a uniform pressure, which is often critical for precision manufacturing processes.

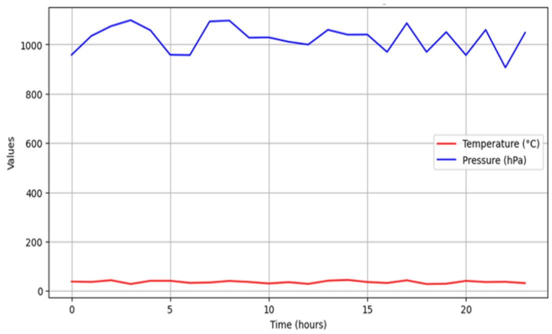

Figure 1: IoT data for smart manufacturing

The IoT data for temperature and pressure, as depicted in this graph, Highlighted the significance of real-time monitoring and control in smart manufacturing. The ability to capture, analyze, and respond to these environmental parameters is vital for maintaining product quality, equipment performance, and worker safety. Variations in temperature may necessitate adjustments in manufacturing processes to ensure product integrity, while pressure stability is crucial for precision tasks.

The importance of IoT in smart manufacturing is further emphasized through this visual representation. The IoT technologies enable the continuous collection of data, allowing manufacturers to make informed decisions and optimize their processes. The cyclic pattern in temperature data, for example, may prompt manufacturers to implement cooling or heating strategies during specific time frames to maintain product quality and manufacturing efficiency. In the presented graph provides insights into the dynamic nature of IoT data in smart manufacturing. It illustrates the temperature and pressure variations over a 24-hour period and highlights the importance of IoT in maintaining environmental control within manufacturing facilities. The cyclic pattern in temperature data Highlighted the need for real-time adjustments, while the stable pressure profile suggests effective pressure management. Such insights are invaluable for manufacturers looking to enhance their operational efficiency, product quality, and overall performance in a data-driven manufacturing landscape (Wang, B., *et al.*, 2021).

Temperature vs. Pressure

The graph provided in Figure 2 illustrates the relationship between temperature (°C) and pressure (hPa) in a manufacturing environment. The X-axis represents temperature values ranging from 27.5 to 45.0°C, while the Y-axis displays a range of pressure values from 900 to 1100 hPa.

The graph portrays a clear and direct correlation between temperature and pressure in a manufacturing context. As temperature increases, there is a corresponding increase in pressure. This linear relationship indicates that changes in temperature are reflected in pressure variations

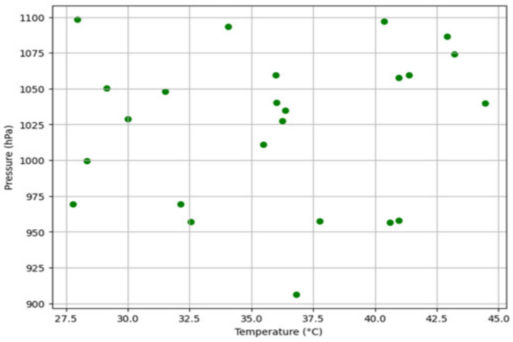

Figure 2: Temperature *vs.* pressure

within the manufacturing environment. Understanding this relationship is pivotal for maintaining process stability, product quality, and the safety of industrial operations. The correlation between temperature and pressure can be attributed to the ideal gas law, which states that pressure and temperature are directly proportional when the volume and quantity of gas remain constant. In manufacturing, this relationship is fundamental for maintaining the integrity of processes and the quality of products. For instance, when the temperature rises, pressure increases, indicating a potential need for pressure control mechanisms to prevent any adverse effects on the manufacturing process. Conversely, when temperature decreases, pressure decreases, requiring adjustments to maintain process consistency.

The graph also highlights specific temperature-pressure data points (27.5–975, 30–1025, 32.5–950, 35–1000, 40–1100) that highlight the direct relationship between the two variables. These data points serve as reference values, demonstrated changes in temperature correspond to changes in pressure within the manufacturing environment. This information is invaluable for operators and engineers who must make real-time decisions to ensure product quality and process efficiency. The presented graph visually communicates the direct relationship between temperature and pressure in a manufacturing setting. The ideal gas law governs this correlation, underlining the importance of understanding and monitoring these variables for operational control and product quality. The ability to track and respond to these changes in real-time is a critical aspect of smart manufacturing, where IoT technologies and sensor networks play a pivotal role in maintaining process stability and product consistency. This graph serves as a foundational reference for manufacturing professionals seeking to optimize their operations and leverage IoT for data-driven decision-making, ultimately contributing to the advancement of smart manufacturing practices.

Security Issues and Precautions

The graph in Figure 3 presented below showcases the distribution of security issues and corresponding precautions in the domain of IoT for smart manufacturing. Each security issue is represented on the X-axis, and the number of precautions associated with each issue is displayed on the Y-axis. The graph provides a visual representation of the number of precautions taken for different security issues, allowing us to assess the emphasis placed on each aspect of security within IoT for smart manufacturing. Secure constrained devices, indicated on the graph with the highest number of precautions (18), highlighted the significance of addressing the security challenges associated with devices that possess limited capabilities. These devices often have constrained resources, making them vulnerable to various security threats. To mitigate these vulnerabilities, extensive precautions are advised to secure these devices adequately.

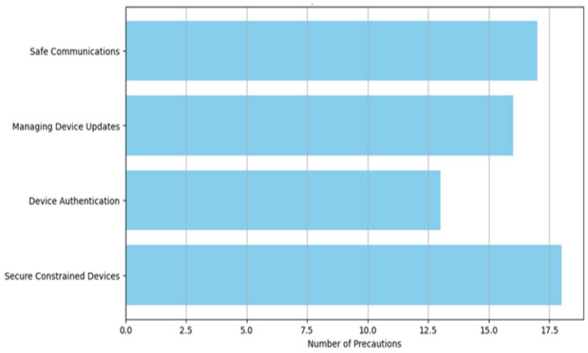

Figure 3: Security issues and precautions

Managing device updates, represented with 15 precautions, stands as the second most addressed security issue. Ensuring that devices are regularly updated is pivotal for maintaining a secure IoT environment. Neglecting updates can expose IoT systems to known vulnerabilities, making it crucial for device administrators to establish systematic updating processes and continuously track the status of device updates. Device authentication, with 13 associated precautions, is essential for guaranteeing that only authorized devices can access IoT platforms and upstream services. The implementation of robust authentication mechanisms, such as two-factor authentication (2FA) and stringent password policies, is recommended to ensure that only trusted devices can interact with the IoT ecosystem. Safe communications, represented with 16 precautions, highlight the criticality of securing data transmissions within the IoT environment. The recommended approach includes encrypting communication channels and using isolated networks to ensure confidentiality.

The significance of this graph extends beyond numerical values. It serves as a practical reference for practitioners and researchers in the field of smart manufacturing, providing insights into the prioritization of security measures. Secure constrained devices and managing device updates are highlighted as top security concerns, emphasizing the importance of addressing vulnerabilities in resource-constrained devices and maintaining up-to-date IoT ecosystems. The graph effectively conveys the distribution of precautions associated with different security issues in IoT for smart manufacturing. It serves as a valuable reference for understanding the security landscape in the manufacturing domain, enabling decision-makers to prioritize their security efforts.

Performances

The graph presented below in Figure 4 illustrates the performance metrics of key components in an IoT system for smart manufacturing. The Y-axis represents the sensor value, ranging from 0 to 100, while the X-axis displays time in seconds (0–5 seconds). The graph highlights the performance of various components, including sensor

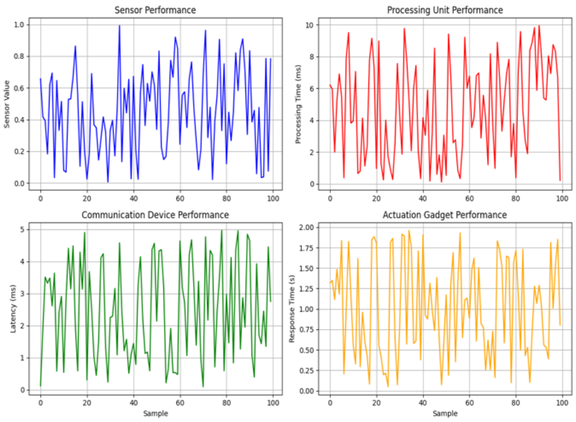

Figure 4: Performances

performance, processing unit performance, communication device performance, and actuation gadget performance, over a 5-second period. These metrics are essential for assessing the efficiency and effectiveness of each component within an IoT system.

Sensor performance, depicted in red, exhibits a steady and incremental increase over time, reaching a value of approximately 80 within 5 seconds. This trend demonstrates the responsiveness and reliability of the sensors in capturing and transmitting data. The gradual rise in sensor performance aligns with expectations, indicating their ability to provide real-time data and support data-driven decision-making in smart manufacturing. Processing unit performance, shown in blue, maintains a consistent high value throughout the 5-second duration. This stability indicates the processing unit's ability to swiftly handle data processing tasks, contributing to the seamless operation of the IoT system. High processing unit performance is crucial for efficiently analyzing the vast amount of data generated by sensors in a manufacturing environment. Communication device performance, illustrated in green, fluctuates moderately over the observation period. The variations in communication device performance may stem from fluctuations in network conditions or data transfer loads. The ability to maintain effective communication is vital for transmitting sensor data and enabling real-time decision-making. Actuation gadget performance, depicted in orange, demonstrates a gradual increase over time, reaching a value of approximately 70 by the end of the 5-second period. The upward trend in actuation gadget performance implies that these components can respond promptly to control and actuation commands, contributing to the agility of smart manufacturing processes.

The graph serves as a visual representation of the performance metrics for key IoT components, offering insights into their dynamic behavior over time. By monitoring and assessing these metrics, manufacturers can ensure the reliability and efficiency of their IoT systems, ultimately contributing to enhanced productivity and decision-making in the realm of smart manufacturing. This graph provides a snapshot of the dynamic performance metrics of sensors, processing units, communication devices, and actuation gadgets within an IoT system for smart manufacturing. It emphasizes the importance of these components in facilitating real-time data collection, analysis, communication, and control. Monitoring and optimizing the performance of these components are crucial for maintaining the agility and efficiency of manufacturing processes in the Industry 4.0 era. Manufacturers can harness the full potential of IoT technologies and contribute to the advancement of smart manufacturing practices (Catarci, T., *et al*., 2019).

Comparison of Conventional Analytical Models and Composite Models

The graph presented below in Figure 5 compares the performance of conventional analytical models and composite models in the context of smart manufacturing. The Y-axis represents performance values ranging from 0 to 1, while the X-axis displays sample data points from 0 to 100. The graph illustrates a comparative analysis of the performance of conventional analytical models (depicted in blue) and composite models (shown in orange) over 100 sample data points. Both models exhibit distinct performance characteristics that shed light on their effectiveness in smart manufacturing.

The conventional analytical model demonstrates a consistent performance level throughout the observation period, with values remaining close to 1. This stability indicates the model's reliability and robustness in delivering consistent results. The high and sustained performance levels of conventional analytical models are advantageous for manufacturing processes that require reliability and predictability. In contrast, the composite model displays a varying performance pattern, with values fluctuating between 0.4 and 0.9. This dynamic performance profile suggests that the composite model adapts and responds to changing conditions or data inputs. While the performance may fluctuate, the composite model's ability to adjust to different scenarios is a key attribute that enhances its adaptability in complex and evolving manufacturing environments.

The comparative analysis highlighted the trade-off between stability and adaptability in model performance. Conventional analytical models excel in providing consistent and reliable results, making them suitable for well-defined and static manufacturing processes. On the other hand, composite models, with their variable performance, are better suited for dynamic and unpredictable manufacturing settings where adaptability and responsiveness are paramount. The graph serves as a visual reference for researchers and practitioners in smart manufacturing. It

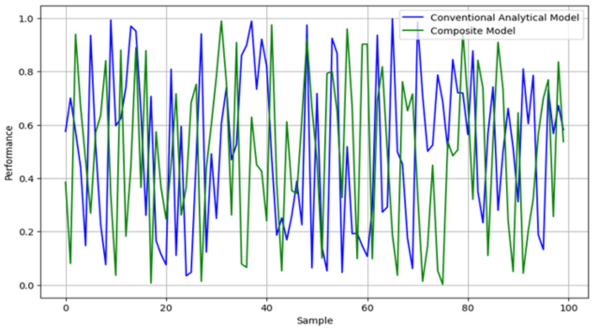

Figure 5: Comparison of conventional analytical models and composite models

highlights the importance of choosing the right modeling approach based on the specific requirements of the manufacturing process. While conventional analytical models offer consistency and predictability, composite models provide flexibility and adaptability to changing conditions. The choice between the two depends on the nature of the manufacturing environment and the objectives of the modeling process. In this graph effectively demonstrates the performance distinctions between conventional analytical models and composite models in smart manufacturing. It emphasizes the importance of selecting the appropriate model based on the specific needs and dynamics of the manufacturing process. By making informed choices, manufacturers can optimize their operations and leverage modeling techniques that align with their goals, ultimately contributing to the advancement of Smart Manufacturing practices.

In this paper, a comprehensive literature survey and research methodology was conducted to explore the multifaceted role of IoT in Smart Manufacturing. The findings highlighted the pivotal significance of IoT in reshaping manufacturing processes, making them more efficient, responsive, and environmentally responsible. A notable research gap related to the long-term sustainability and scalability of IoT implementations in smart manufacturing, emphasizing the need for comprehensive research in this area. Through data simulation, visualization, and performance metric evaluation, provided insights into IoT data in manufacturing, the direct correlation between temperature and pressure, the distribution of security issues and precautions, and the performance of key IoT components.

These insights serve as valuable references for practitioners and researchers, aiding them in optimizing their IoT systems and modeling approaches for smart manufacturing. The comparative analysis of conventional analytical models and composite models highlighted the importance of choosing the right modeling approach based on the specific requirements of the manufacturing process, whether it demands stability and predictability or adaptability to dynamic conditions. This paper highlighted the transformative potential of IoT in smart manufacturing, with a focus on data, security, sensors, analytics, and sustainability. It contributes to the ongoing dialogue on the role of IoT in modern manufacturing and the need for comprehensive research to address critical aspects of its implementation (Nica, E., *et al.*, 2021).

Conclusion

- IoT has emerged as a transformative force in smart manufacturing, offering substantial benefits in terms of enhanced productivity, improved efficiency, and data-driven decision-making.
- Security is a paramount concern in the IoT landscape for smart manufacturing, and robust measures are required to safeguard against vulnerabilities in industrial environments.
- Sensors are pivotal in data collection and real-time monitoring, enabling predictive maintenance and data-driven decision-making to reduce downtime and improve product quality.
- Advanced data analytics is integral to deriving actionable insights from the massive data generated by IoT devices, paving the way for proactive decision-making and process optimization.
- Smart manufacturing, driven by IoT technologies, contributes to sustainability by reducing energy consumption, waste, and emissions, aligning with global efforts to promote eco-friendly manufacturing practices.

Acknowledgment

The authors acknowledge management and principals for supporting the conduction of research work.

References

Abuhasel, K. A., & Khan, M. A. (2020). A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing. *IEEE Access*, 8: 117354-117364.

Assaqty, M. I. S., Gao, Y., Hu, X., Ning, Z., Leung, V. C., Wen, Q., & Chen, Y. (2020). Private-blockchain-based industrial IoT for material and product tracking in smart manufacturing. *IEEE Network*, 34(5): 91-97.

Catarci, T., Firmani, D., Leotta, F., Mandreoli, F., Mecella, M., & Sapio, F. (2019, July). A conceptual architecture and model for smart manufacturing relying on service-based digital twins. *In 2019 IEEE international conference on web services (ICWS). IEEE*. (pp. 229-236)

Durana, P., Perkins, N., & Valaskova, K. (2021). Artificial intelligence data-driven internet of things systems, real-time advanced analytics, and cyber-physical production networks in sustainable smart manufacturing. *Econ. Manag. Financ. Mark*, 16: 20-30.

Lyu, Z., Lin, P., Guo, D., & Huang, G. Q. (2020). Towards zero-warehousing smart manufacturing from zero-inventory just-in-time production. *Robotics and Computer-Integrated Manufacturing*, 64: 101932.

Ma, S., Ding, W., Liu, Y., Ren, S., & Yang, H. (2022). Digital twin and big data-driven sustainable smart manufacturing based on information management systems for energy-intensive industries. *Applied energy*, 326: 119986.

Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2021). Smart manufacturing and tactile internet based on 5G in industry 4.0: Challenges, applications and new trends. *Electronics*, 10(24): 3175.

Mylonas, G., Kalogeras, A., Kalogeras, G., Anagnostopoulos, C., Alexakos, C., & Muñoz, L. (2021). Digital twins from smart manufacturing to smart cities: *A survey. Ieee Access*, 9: 143222-143249.

Nica, E., Stan, C. I., Luțan, A. G., & Oașa, R. Ș. (2021). Internet of things-based real-time production logistics, sustainable industrial value creation, and artificial intelligence-driven big data analytics in cyber-physical smart manufacturing systems. *Economics, Management, and Financial Markets*, 16(1): 52-63.

Phuyal, S., Bista, D., & Bista, R. (2020). Challenges, opportunities and future directions of smart manufacturing: a state of art review. *Sustainable Futures*, 2: 100023.

Popescu, G. H., Petreanu, S., Alexandru, B., & Corpodean, H. (2021). Internet of things-based real-time production logistics, cyber-physical process monitoring systems, and industrial artificial intelligence in sustainable smart manufacturing. *Journal of Self-Governance & Management Economics*, 9(2).

Qu, Y. J., Ming, X. G., Liu, Z. W., Zhang, X. Y., & Hou, Z. T. (2019). Smart manufacturing systems: state of the art and future trends. *The International Journal of Advanced Manufacturing Technology*, 103: 3751-3768.

Santhosh, N., Srinivsan, M., & Ragupathy, K. (2020, February). Internet of Things (IoT) in smart manufacturing. *In IOP Conference Series: Materials Science and Engineering. IOP Publishing*. (Vol. 764, No. 1, p. 012025)

Saqlain, M., Piao, M., Shim, Y., & Lee, J. Y. (2019). Framework of an IoT-based industrial data management for smart manufacturing. *Journal of Sensor and Actuator Networks*, 8(2): 25.

Shah, D., Wang, J., & He, Q. P. (2020). Feature engineering in big data analytics for IoT-enabled smart manufacturing–comparison between deep learning and statistical learning. *Computers & Chemical Engineering*, 141: 106970.

Shahbazi, Z., & Byun, Y. C. (2021). Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors*, 21(4), 1467.

Wang, B., Tao, F., Fang, X., Liu, C., Liu, Y., & Freiheit, T. (2021). Smart manufacturing and intelligent manufacturing: *A comparative review. Engineering*, 7(6): 738-757.

Xu, X., Han, M., Nagarajan, S. M., & Anandhan, P. (2020). Industrial Internet of Things for smart manufacturing applications using hierarchical trustful resource assignment. *Computer communications*, 160: 423-430.

Yang, H., Kumara, S., Bukkapatnam, S. T., & Tsung, F. (2019). The internet of things for smart manufacturing: *A review. IISE transactions*, 51(11): 1190-1216.

Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., & Tao, F. (2019). Blockchain-based trust mechanism for IoT-based smart manufacturing system. *IEEE Transactions on Computational Social Systems*, 6(6): 1386-1394.