International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(Review Article)

Check for updates

Industry 4.0 moving towards smart manufacturing: A comprehensive review

Swapnil Deokar [1,*], Vaibhav Bansode [1], Sachin Wankhede [2] and Prashant Kharche [1]

[1] Department of Mechanical Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India.
[2] Department of Master in Business Administrative, Shreeyash Pratishthan, Sambhajinagar, Maharashtra, India.

International Journal of Science and Research Archive, 2025, 16(03), 630–642

Publication history: Received on 02August 2025; revised on 11 September 2025; accepted on 13 September 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2596

Abstract

Industry 4.0, also known as the Fourth Industrial Revolution, represents a transformative shift in manufacturing, driven by the integration of digital technologies, automation, data exchange, and the Internet of Things (IoT). This paradigm shift is reshaping traditional manufacturing processes by fostering interconnected, smart systems that enable real-time monitoring, predictive analytics, and enhanced operational efficiency. Through the adoption of cyber-physical systems, cloud computing, advanced robotics, artificial intelligence (AI), and big data analytics, manufacturers can optimize production processes, reduce costs, improve quality, and create flexible, agile production environments. The concept of smart manufacturing, a core component of Industry 4.0, revolves around the seamless interaction between machines, systems, and human operators to enhance decision-making and drive innovation. This paper explores the key technologies, benefits, and challenges associated with Industry 4.0, highlighting its potential to revolutionize the manufacturing landscape and pave the way for more sustainable, efficient, and customized production. The shift toward smart manufacturing presents an opportunity for manufacturers to not only enhance competitiveness but also to address the challenges of an increasingly complex global market.

Keywords: Internet of Things; Smart Factories; Augmented Reality; Cognitive Computing; Artificial Intelligence

1. Introduction

Industry 4.0, also known as the Fourth Industrial Revolution, represents a transformative paradigm in manufacturing that has fundamentally reshaped production processes through the integration of digital technologies and smart automation [1]. This revolutionary approach combines cyber-physical systems, the Internet of Things (IoT), cloud computing, and artificial intelligence to create intelligent manufacturing environments known as smart factories [2]. The concept emerged as a response to increasing market demands for customization, efficiency, and sustainability in manufacturing operations. Smart factories, as demonstrated by facilities like Rittal's plant in Haiger, represent the practical implementation of Industry 4.0 principles, where interconnected systems and real-time data analytics drive production decisions and optimize operations [2]. The significance of this technological transformation extends beyond mere automation, as it enables predictive maintenance, adaptive manufacturing, and unprecedented levels of production flexibility. According to recent studies by MIT Technology Review, these advancements have led to substantial improvements in manufacturing efficiency, with some facilities reporting productivity gains of up to 25% after implementing Industry 4.0 technologies [3]. The purpose of this literature review is to comprehensively analyze the technological integration within smart factories and evaluate their impact on manufacturing processes, workforce dynamics, and economic outcomes. This analysis will examine various case studies, including successful implementations across different industries, challenges encountered during digital transformation, and the evolving relationship between human workers and automated systems. Furthermore, this review aims to identify current research gaps and emerging trends in smart manufacturing, providing valuable insights for future technological developments and implementation strategies.

*Corresponding author: Swapnil Deokar

1.1. Industry 4.0 and the Fourth Industrial Revolution

- **Industrial revolution is continuous process.** Figure 1 represents industrial revolution journey
- **First Industrial Revolution (late 18th to early 19th century) -** The first industrial revolution was a true turning point, driven by the invention of steam engines, the use of water and steam power, and various other machines. This transformation revolutionized industries with the advent of trains, factory mechanization, and, unfortunately, heavy pollution.
- **Second Industrial Revolution (late 19th to early 20th century) -** The second industrial revolution is typically marked by the widespread use of electricity and the innovations it spurred, such as the assembly line, which enabled mass production and some degree of automation.
- **Third Industrial Revolution (mid-20th century to early 21st century) -** The third industrial revolution centered around the rise of computers, computer networks (like WAN, LAN, and MAN), and robotics in manufacturing. It also saw the birth of the Internet, drastically changing how information was shared and processed. This era also shifted traditional brick-and-mortar environments toward more automated and connected systems.
- **Fourth Industrial Revolution (present and future) -** The fourth industrial revolution goes beyond the internet and client-server models to an era of ubiquitous mobility, where digital and physical worlds merge (especially in manufacturing, known as Cyber-Physical Systems). This phase is defined by the convergence of IT and OT, along with technologies like IoT, Big Data, and cloud computing. With advancements in AI and robotics, this revolution brings new levels of automation and optimization, offering vast potential for innovation and further industrial advancement.

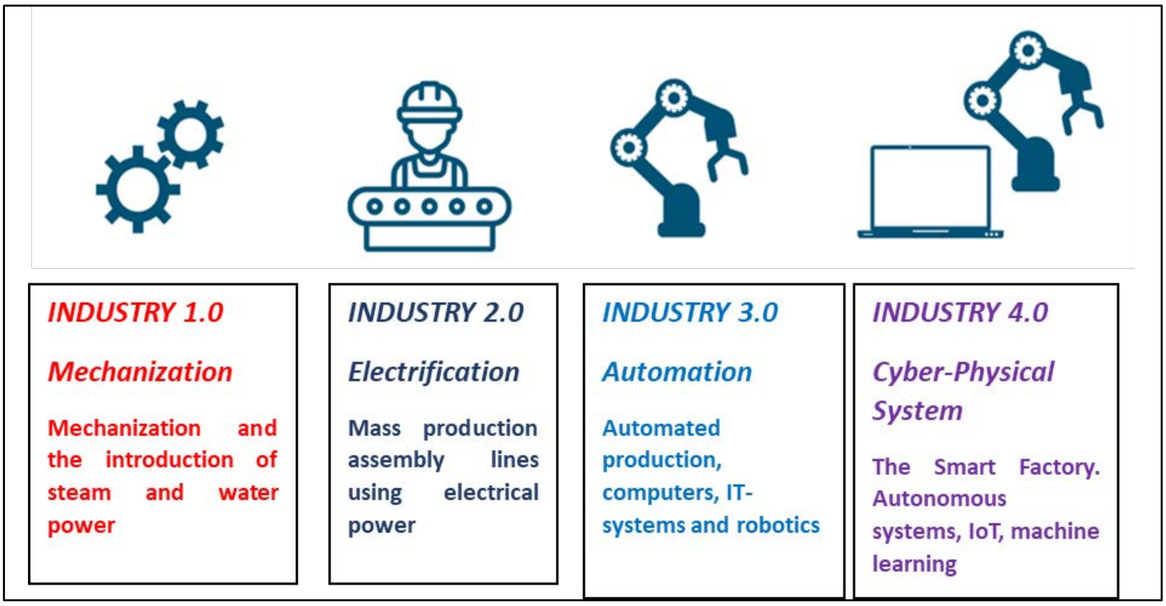

Figure 1 Industrial revolution journey

1.2. Design principles of industry 4.0

The main transformation to Industry 4.0 done by A principles. The following are the concern principles:

Interoperability: People, machines, and objects must be able to connect with one another via the Internet of Things. One of the key ideas is this one.

Virtualization: Cyber-physical systems (CPSs) that will replicate and replicate the real world in a virtual environment. It is also used to keep an eye on adjacent objects. That's the simplest technique to put a virtual copy of everything.

Decentralization: CPSs will operate autonomously in the future. It will provide some for problem-solving and personalized products. This makes the manufacturing environment more adaptable. When there are competing objectives or failures, the subject is referred to a higher level.

Real-Time Capability: A smart factory can connect, store, or analyze data in real-time and make new decisions based on the most recent results. Internal processes fall under 1T, such as production line machine failure. Smart objects can perform many identifying tasks. The manufacturing system's adaptability and efficiency may be enhanced by the real-time capability.

E Service-Orientation: The production process needs to be customer-focused. It is necessary for the internet of services to have effective connections with both people and smart devices in order to generate products that are tailored to the needs of the client.

Modularity: This need to be among the key features of a smart manufacturing. In general, a week is needed for market research and production adjustments. The key characteristics of smart factories are their rapid adoption and sessional and market changes.

2. Industry 4.0 Technologies

As Industry 4.0 is combination of many Technologies so fig 2 represent classification of Industry 4.0

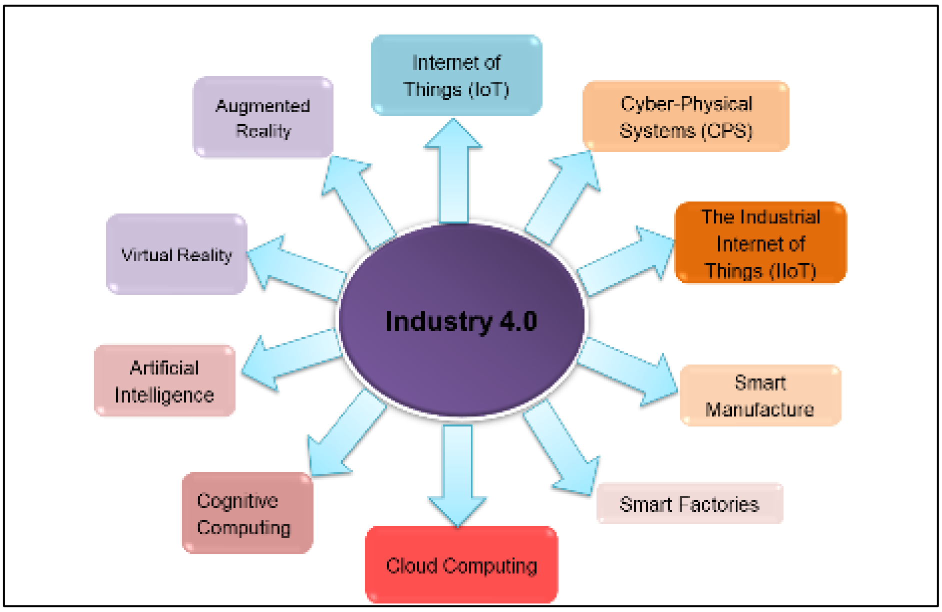

Figure 1 Industry 4.0 Classification

2.1. Internet of Things (LOT)

A network of physical items equipped with sensors, software, and other technologies is known as the internet of things (IoT). These items can communicate in real time over networks with other Internet-connected gadgets and systems. Together with automated systems, these linked gadgets collect Internet of Things data that may be analyzed to help with tasks or discover ways to streamline a procedure.

Carretero et.al The Internet of Things (IoT) is a network of Internet-enabled objects that are seamlessly integrated into the information network, enabling a highly distributed network of devices to communicate with both humans and other devices, with the potential to improve services and bring benefits to users[1]. Coetzee et al. The Internet of Things is a new paradigm driven by the expansion of the internet to include physical objects, enabling smarter services across various application domains, but facing challenges around trust, security, standardization, and governance.[2]Miorandi et al. present Internet of Things vision, applications, and research challenges[3]. Rose et al. provides an overview of the Internet of Things, including its definitions, enabling technologies, connectivity models, and transformational potential[4]. Zheng et al. discuss how "smart Internet" that enables intelligent interconnections between diverse physical objects and people, leading to a wide range of smart applications and services[5]. an overview of the Internet of Things (IoT) with a focus on the desirable device characteristics for various IoT applications, and identifies the key enabling technologies such as RFID, sensors, and wireless communication protocols[6]. Gubbi et al. presents a cloud-centric vision for the worldwide implementation of the Internet of Things (IoT), discussing the key enabling technologies and application domains that are likely to drive IoT research, and concluding with the need for convergence of wireless sensor networks, the internet, and distributed computing[7]. Junaidi et al. discussed Internet of Things (IoT) technology, including its history, the various technologies involved, and its applications in different fields such as the medical field, cloud computing, and other scientific domains[8]. Fuqaha et al. discuss how Internet of Things (IoT) is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT[9]. Kumar et al discuss how IOT is application in different filed like IoT for Smart city, Health care, smart traffic management, etc[10].

2.2. Cyber-Physical Systems (CPS)

A computerized system in which a mechanism is managed or observed by computer-based algorithms is known as a cyber-physical system (CPS) or intelligent system. The physical and software components of cyber-physical systems are intricately linked, capable of functioning on many temporal and spatial scales, displaying a variety of unique behavioral modalities, and interacting with one another in context-dependent ways. Transdisciplinary methods are used in CPS, combining design, process science, mechatronics, and electronic systems theory.

In order to monitor, coordinate, and control physical and engineering systems, cyber-physical systems combine communication and computation [11][12]. These systems change the way we interact with the physical environment by using networks and embedded computers to monitor and manage physical processes through feedback loops [13]. The book by Thunberg et al. offers a thorough introduction to the concepts of cyber-physical system design, specification, modeling, and analysis, including formal modeling approaches[14]. Using a pruning approach, Zheng et al. provide a set of techniques for better resilient state estimates as well as for identifying and localizing cyber-physical system attacks [15] .In order to assess actual industrial cyber-physical systems cyber events, Kayan et al. describe and use a multi-dimensional adaptive attack taxonomy [16]. The development of ML and DL algorithms for cybersecurity countermeasures in smart grid-cyber-physical systems (SG-CPS) is covered by Husan et al. It examines the limitations that must be removed in order to enhance performance and accomplish real-time implementation. To create a thorough grasp of the cybersecurity context in SG-CPS, the many kinds of cyberattacks, cybersecurity needs, and security standards and procedures are also covered [17]. Gaba et al. describe how to use deep learning to analyze various attack detection methods offered for CPS. With regard to deep learning modules, we will be utilizing the exceptional potential for cyberattack detection for CPS. High-quality datasets are readily available for the public's use, which helps to achieve the impressive performance [18]. Chen and colleagues talk about Modern transportation relies heavily on cyber-physical systems (CPSs), especially transportation cyber-physical systems (TCPSs) for emergency supply logistics. TCPS enhances the effectiveness, security, and dependability of emergency supply transportation systems by employing real-time data gathering, processing, and communication technology [19]. Tyagi et al. talk on the challenges of CPSs systems, which are utilized in a variety of fields, including energy, transportation, the environment, and healthcare [20].

2.3. The Industrial Internet of Things (IIoT)

Industrial uses of the IIoT include software-defined production processes, medical devices, and robotics. The Internet of Things encompasses more than just the typical consumer electronics and internet-connected physical objects. Additional features of the next generation of Industrial IoT (IIoT) devices include low cost, automation, intelligence provision, reduced overhead, efficiency, and remote data exchange.

The Industrial Internet of Things (IIoT) is an emerging paradigm that applies Internet of Things (IoT) technologies to industrial domains, enhancing productivity and efficiency (Willner, 2018). It represents a digital transformation across various sectors, including energy, healthcare, and manufacturing, by integrating Operational Technology (OT) with Information and Communication Technology (ICT)[21]. IIoT is considered a process innovation that can increase machine efficiency, reduce costs, and improve production processes [22]. It utilizes various devices such as sensors, actuators, and RFIDs to build powerful industrial systems and applications. The development of high-speed internet has facilitated remote access and accelerated the growth of IoT devices[23]. IIoT is seen as a fundamental tool for creating and sustaining competitive advantage not only for industries but also for nations in the 21st century [21]. In our contemporary interconnected global world, the idea of an intelligent environment made up of autonomous devices with sensory, control, and decision-making capabilities connected via a network has evolved from an idealized ideal to a concrete reality. In order to facilitate the seamless integration of IIoT into their operational frameworks, Angurala et al. propose a technical acceptance model tailored for businesses [24]. To guarantee a safe and effective transmission method between devices in the network, Rathee et al. suggested a hybrid trusted model by combining the objective model and fuzzy evaluation matrix approach. In comparison to state-of-the-art solutions, the suggested method is tested and simulated across a range of criteria, including detection ratio, network-related performance, and functional tests [25].

Jyothi et al. proposed intelligent recognition system enhances IIoT cybersecurity by detecting cyberattacks using singular value decomposition (SVD) for feature reduction and SMOTE to address data imbalance. It employs various machine learning and deep learning models for both binary and multi-class classification. Tested on the ToN_IoT dataset, the system achieved 99.98% accuracy and significantly reduced error rates [26]. Ramesh Krishnan et al. examines the advancements in IIoT, highlighting its role in boosting industrial efficiency and innovation. It addresses critical security challenges such as cyberattacks, infrastructure vulnerabilities, and data privacy concerns. The study emphasizes the need for robust cybersecurity measures and explores future research directions for a secure and resilient IIoT ecosystem[27].

3. Smart Manufacture

Computer-integrated manufacturing, high levels of adaptability and quick design modifications, digital information technology, in addition flexible technical workforce training are all components of smart manufacturing, a broad category of manufacturing. Other objectives can occasionally include supply chain optimization, efficient production, recyclability, and rapid adjustments to production levels in response to demand.

Smart manufacturing represents the next industrial revolution, integrating advanced technologies to enhance production efficiency and performance [28]. It utilizes big data, artificial intelligence, robotics, and interconnected systems to optimize manufacturing processes and resource allocation [28][29]. Key components include cyber-physical systems, Internet of Things, cloud computing, and data science [28]. Smart manufacturing aims to improve yield, reduce human error, and meet customized demands through autonomous machines and robots. It encompasses various technologies such as virtual and augmented reality, additive manufacturing, and Industrial Internet of Things Artificial intelligence plays a crucial role in quality checks, maintenance, design, environmental impact reduction, factory integration, and post-production support [30]. While smart manufacturing offers numerous opportunities, challenges in implementation and standardization remain. Overall, smart manufacturing is poised to revolutionize the industrial sector through technological convergence and innovation. In their conceptual framework for Industry 4.0 smart manufacturing systems, Zheng et al. provide examples of smart design, smart machining, smart control, smart monitoring, and smart scheduling [31]. A new industrial paradigm is being driven by smart manufacturing, which is the fusion of traditional manufacturing and modern ICT, according to Kang et al. The study highlights important technologies, existing system structures, and emerging trends by examining international policies, technology roadmaps, and literature. This offers a thorough grasp of the development and strategic orientation of smart manufacturing [32]. Tao et al. emphasize how big data, powered by IoT, cloud computing, and artificial intelligence, is revolutionizing smart manufacturing. It offers a conceptual framework to enable data-driven strategies and provides a historical picture of the industrial data lifecycle. Examples of applications show how big data boosts manufacturing competitiveness [33].

3.1. Smart Factories

A smart factory is an automated manufacturing facility that continuously gathers and exchanges data via linked equipment, production systems, and gadgets. Decisions to enhance procedures and resolve any potential problems are then made using this data.

Smart factories represent a significant advancement in manufacturing, Integrating Internet of Things (IoT), artificial intelligence, and automation technologies to improve productivity, quality, and flexibility, smart factories mark a major development in production [34][35]. These manufacturers maximize operations and react dynamically to market needs by using linked industrial equipment and real-time communication [36]. Bagherian et al. address system complexity, technological constraints, and connectivity problems as main obstacles to smart factory implementation. Applying the Best Worst Method, it emphasizes the need of flexible software, strong IT infrastructure, and handles issues including ethical questions and e-waste. The results provide strategic understanding for efficient implementation of smart manufacturing [37]. Muzammal et al. and Khang et al. underline how strongly Industry 4.0 technologies and sustainability interact to propel the development of smart factories. It underlines how developments in IoT, artificial intelligence, and automation maximize manufacturing, improve energy economy, and assist waste reduction [38][39]. The most major difficulties in the way smart production factories are implemented, according to Samani et al., are recruit and retention of experienced managers, unclear return on investment, and attract and retention of multi-skilled people. Moreover, among the main enablers to meet the difficulties listed above are big data, IT-based management, and the Internet of Things [40].

3.2. Cloud Computing

Cloud computing is the provision of computing resources as a service, which means that the cloud provider, not the end user, owns and manages the resources. These resources can range from browser-based apps (like Netflix or Tik Tok), third-party photo and digital media storage services (like iCloud or Dropbox), or third-party servers that support the computing infrastructure of a personal, professional, or research project.

Cloud computing is an Internet-based technology that delivers computing resources as services over a network, allowing users to pay only for what they consume [41]. It evolved from virtualization, grid computing, and utility computing concepts, offering computational resources on demand as a metered service [42].Cloud computing encompasses both software-as-a-service (SaaS) applications and the underlying hardware and software systems in data centres, with public clouds providing utility computing to the general public and private clouds serving internal organizational needs. This technology offers numerous benefits, including cost savings, scalability, and elasticity of resources without premiums for large-scale operations [43]. Cloud computing is emerging as a platform for sharing various resources, such as infrastructure, software, and applications, while meeting requirements for reliability, data availability, scalability, and customer satisfaction [44]. Karamchand et al discuss how cloud computing plays a crucial role in driving business transformation by enhancing scalability, agility, and cost efficiency. It enables real-time collaboration, seamless data access, and integration with emerging technologies like AI and IoT. The study highlights cloud computing as a key enabler of digital innovation, operational efficiency, and competitive advantage [45]. Golec wt al. discuss quantum cloud computing holds the potential to revolutionize data processing by integrating the power of quantum computing with the accessibility of cloud infrastructure. This approach addresses challenges like limited accessibility and environmental sensitivity of quantum systems. The study outlines key benefits such as enhanced scalability, speed, and security, while also identifying critical research gaps including qubit stability and efficient resource allocation [46]. Sachdeva et al. discuss the difficulties and moral dilemmas related to cloud-based medical solutions, including cybersecurity and data privacy. Our goal is to help readers comprehend the importance of cloud computing in contemporary medical applications and its potential to transform patient care and biomedical research by offering a thorough overview [47]. Wang et al. offer a system for adaptive security protection that builds a multi-layered defense architecture by utilizing deep learning. When tested in a real-world corporate setting, the suggested solution achieves a 99.999% availability rate, an average reaction time of 18 ms, and a detection accuracy of 97.3%. The suggested strategy offers a fresh and practical approach to cloud computing security, as evidenced by experimental results that show a significant improvement in detection accuracy, response efficiency, and resource utilization [48].

3.3. Cognitive Computing

The term "cognitive computing" (CC) describes technological platforms that are, in general, grounded in the scientific fields of signal processing and artificial intelligence. One may argue that cognitive computing is a game-changer in technology. It can easily communicate with people and other machines, understands language, and recognizes faces, objects, text, and situations. It can even distinguish voices.

Cognitive computing aims to emulate human intelligence in AI systems, focusing on complex cognitive functions like perception, reasoning, and problem-solving. It represents a paradigm shift from traditional AI approaches, leveraging advanced algorithms, neural networks, and machine learning techniques [49].Cognitive computers (κC) are envisioned as intelligent processors capable of autonomous knowledge learning and intelligence generation, powered by intelligent mathematics and brain-inspired architectures [50]. The field draws from multiple disciplines, with underlying computing paradigms including Von-Neuman, Neuromorphic Engineering, and Quantum Computing [51]. Cognitive computing addresses limitations of current AI systems, such as lack of self-awareness, social capacities, and adaptability. Its applications are expanding, particularly in healthcare, where it automates knowledge-rich tasks and offers potential solutions to complex challenges [52]. Cognitive computing can address limitations of AI systems and has applications in healthcare, cybersecurity, big data, and IoT [53]. Multi-Granularity Cognitive Computing (MGCC) integrates traditional intelligent information processing with the multi-granularity cognitive law of the human brain [54]. Cognitive computing has a transformative impact on healthcare by enhancing diagnosis, treatment, and delivery [55].

3.4. Artificial Intelligence

Artificial intelligence (AI) is the term used to describe the simulation of human intelligence in robots that have been trained to think and behave like people. The phrase can also be used to describe any computer that demonstrates traits like learning and problem-solving that are typical of the human intellect. The ability to reason and take actions that have the best likelihood of accomplishing a particular goal is the ideal feature of artificial intelligence.

Artificial Intelligence (AI) is the simulation of human intelligence in machines, enabling them to perform tasks that typically require human cognitive abilities [56]. The field of AI has significantly enhanced performance in various sectors, including manufacturing, service systems, and expert systems [57]. Janmanchi et al. explores the intersection of Artificial Intelligence and human reasoning, emphasizing AI's potential to simulate cognitive functions and address complex mental health challenges. It highlights the capabilities of AI reasoning in solving problems traditionally managed by human cognition [58]. Process mining and phenotyping, data mining and machine learning, temporal data mining, uncertainty and Bayesian networks, text mining, clinical practice prediction, and knowledge representation and guidance are all covered in Holems et al.'s book [59]. Kalota et al. introduces the foundational concepts of Artificial Intelligence and Generative AI, including machine learning, deep learning, neural networks, and large language models. It aims to bridge the knowledge gap for educators and professionals unfamiliar with these technologies. The study also explores the practical applications and implications of Gen-AI in business and education. Additionally, it highlights current challenges in adopting and understanding generative AI [60]. Bunian et al. highlights the transformative role of AI, ML, IoT, and cloud computing in driving the shift toward smart manufacturing under the Industry 4.0 framework. It emphasizes how AI enables sustainability, supply chain optimization, and waste reduction. The integration of intelligent systems enhances agility, productivity, and data-driven decision-making [61]. Patel et al. presents a conceptual framework for integrating blockchain into AI-assisted manufacturing systems to enhance security, transparency, and trust. It highlights how the synergy between AI and blockchain can accelerate product design, improve collaboration, and secure supply chains. The study emphasizes the unique security needs of manufacturing beyond generic blockchain applications. It also identifies key challenges and organizational risks, underscoring the importance of robust data protection in modern manufacturing[62].

3.5. Augmented Reality

Using augmented reality (AR), production processes can be effectively represented by superimposing virtual information over real-world perspectives. AR's most likely production function in ASEAN nations is to teach aspiring technicians and employees how production systems operate in real time.

Augmented Reality (AR) is an emerging technology that overlays virtual content onto the real world, enhancing user experiences across various domains. AR applications have become increasingly portable and accessible on mobile devices, with potential for widespread adoption in education and everyday life [63]. The technology combines physical and virtual objects in a hybrid space, allowing users to interact with digital content in real-world contexts [64]. AR has diverse applications, including prototyping, sales and marketing, gaming, healthcare, and education (Integration with other technologies like computer vision, artificial intelligence, and IoT further expands AR's capabilities [64]. While AR offers numerous benefits, challenges remain in its implementation and adoption. As AR continues to evolve, it is expected to play an increasingly significant role in various aspects of daily life [65]. Husar et al. concentrated on technological advancement, the primary outcomes produced by the AR application, and the deployment of AR mobile in industry [66]. Jose et al. highlights Augmented Reality (AR) as a transformative interface enhancing human-machine interaction in manufacturing. AR supports applications in training, design, maintenance, and production, accelerating the shift toward Industry 4.0 and mass customization. Its growing adoption is driven by accessible hardware and ease of implementation[67].

4. Challenges of implementing Industry 4.0

4.1. Cybersecurity

The interconnection and digitization of systems is a fundamental characteristic of Industry 4.0, leading to an increase in the number of devices connected to the Internet of Things (IoT). This expansion presents a significant cybersecurity challenge, particularly in safeguarding sensitive data and protecting intellectual property. As manufacturing systems become more interconnected, the risk of cyberattacks and unintended data breaches grows exponentially. To address these threats, it is imperative to implement comprehensive and robust security measures. These measures should include advanced encryption techniques, secure communication protocols, and continuous monitoring systems to mitigate the risk of unauthorized access and ensure the integrity of both operational data and intellectual property. Effective cybersecurity strategies are essential to maintaining trust, confidentiality, and the operational resilience of smart manufacturing systems.

4.2. Data Security

One of the primary challenges in adopting Industry 4.0 is ensuring data security. As businesses increasingly transition to digital environments, they face persistent threats from cybercrime, particularly concerning the protection of sensitive customer data. Migrating to cloud-based platforms introduces additional vulnerabilities, as companies move their data and operations away from traditional, on-premises systems. This shift can expose businesses to greater risks, including unauthorized access, data breaches, and cyberattacks. Therefore, robust cybersecurity frameworks must be implemented, ensuring that cloud environments are equipped with advanced protection mechanisms such as encryption, access controls, and real-time threat detection to safeguard data integrity and privacy. Such measures are crucial to mitigating the security risks associated with digital transformation in Industry 4.0.

4.3. Team Support

Effective team support is critical when transitioning to new technologies within the context of Industry 4.0. The shift to advanced systems and digital processes may be met with resistance, as employees might find it challenging to adapt to the new model. To facilitate successful adoption, it is essential to establish clear expectations, communicate the strategic purpose behind the technological investment, and highlight the tangible benefits that the transition will bring to both the organization and individual roles. Throughout the implementation process, transparency is key to fostering trust and collaboration. By involving the team early on, providing adequate training, and addressing concerns, organizations can ensure smoother integration of Industry 4.0 technologies and maximize their potential.

4.4. Leveraging Data

A significant challenge in the adoption of Industry 4.0 is the effective utilization of data to make informed, data-driven decisions. The vast amount of information generated through interconnected devices and systems can be overwhelming, and to leverage this data effectively, organizations require not only advanced tools and technologies but also a well-trained workforce. Training programs, knowledge acquisition, and comprehensive documentation are essential to help employees understand data patterns, interpret insights, and apply these findings to enhance operational efficiency, drive business transformation, and foster growth. Additionally, organizations must establish clear frameworks for data governance and analysis to ensure that decision-making processes are based on accurate, actionable information.

4.5. Trained Human Resources

In order for frontline executives to embrace new technologies, they require training. Investing in new technology, such as Industry 4.0, does not mean that you should leave system maintenance to IT management. Rather, the service provider's regular personnel training and ongoing support can be advantageous to you.

4.6. Legal Issues

Industry 4.0 is a cyber-physical network where sensors, machines, web apps, cloud, facilities, and humans are interlinked and a huge amount is transferred among each other. Before adopting digitalization, proper legal compliances and issues should be considered to avoid problems later. Proper privacy and security measures should be considered before adopting data-driven business models. Proper legal research has to be conducted by project managers.

4.7. Huge capital and investment required

The transition of conventional operations, procedures, and systems to a digital model, known as Industry 4.0, necessitates significant investments in machinery, cloud infrastructure, skilled workers, sensors, legal fees, software and hardware expenses, RFID tags, operations, staff training programs, backups, etc. When developing a financial model of the complete system, all costs must be taken into account, along with their advantages and disadvantages.

4.8. Advantages of industry 4.0

- Competitive advantage: Businesses who can successfully implement these new tactics and technologies stand to gain a variety of competitive benefits from Industry 4.0 smart solutions and services.
- Enhanced Efficiency in Operations: With Industry 4.0, it is hoped that businesses will become even more profitable as they are able to extract more from the same number of resources.
- Better Products and Services: Industry 4.0 will increase operations' visibility and throughput, enabling them to keep providing value to consumers and winning their business, regardless of product quality, safety, or customer experiences.
- Market expansion and new market development: new services, goods, and software will be required to enable the change of organizations with any technology revolution. New product categories, employment, and other things will be created as a result.
- Quicker Reaction to Customer Needs: Many sectors are unable to keep up with the rapid changes in customer needs. Every few months, they demand new features, new designs, and new technologies. Agility is a key component of Industry 4.0, enabling you to react to market changes more quickly than your rivals.

- Assurance of Quality: Product quality can be perfected thanks to Industry 4.0. With product tracking during distribution, you can also guarantee quality outside of the facility. You can also minimize your expenses by getting rid of that elusive 1% or so of faulty products.
- Quickness: The production process is sped up when the product is aware of its specifications. Industry 4.0 promotes agility and increases the system's intelligence.

4.9. Disadvantages of industry 4.0

- High Cost: Technology is not the only significant expense to take into account. but the knowledge that makes it possible to use the technology possessing expertise in more recent domains like as IoT, augmented reality, and Al might result in significant financial limitations, in addition to a lack of comprehension among all stakeholders.
- High Failure Rate: The challenge with implementing Industry 4.0 projects is that, when it comes to setting goals, there is frequently a lack of focus. These are frequently multi-stakeholder, cross-functional initiatives, which can lead to competing objectives and project failure.
- Cybersecurity: More and more people, goods, and machinery are being and will be connected to the internet. While this allows us to access data more easily through the cloud, it also makes it easier for hackers to get access to networks.
- Requirement for Highly Skilled Labor: Humans are still necessary for manufacturing and industry overall in order to facilitate production. The shift to digitally connected systems, however, has increased demand for highly skilled labor, which may inadvertently decrease demand for low-skilled labor.
- Disruption of the Industry and Market: As new technologies become available, current solutions will eventually be phased out. Much like the world's blockbusters. Because of what Industry 4.0 delivers to the market, some industries will not be able to exist.

5. Research Gaps and Future Directions

The evolution of Industry 4.0 and smart factory technologies has revealed several critical research gaps that warrant further investigation. A primary gap exists in understanding the complex relationships between higher education institutions and industry requirements, particularly regarding skill development for emerging technologies. Research has shown that there is a significant disconnect between academic curricula and the rapidly evolving needs of smart manufacturing environments. The integration of cyber-physical systems and Internet of Things (IoT) technologies in manufacturing has created new challenges that require innovative research approaches. Future research directions should focus on strengthening the collaboration between educational institutions, industry stakeholders, and government bodies to develop comprehensive frameworks for skills assessment and development. Additionally, there is a pressing need for comparative studies across different countries to understand how varying levels of technological implementation impact manufacturing outcomes.

The scope of technology adoption and its effects on workforce development remains inadequately documented, particularly in developing economies. Case studies examining the establishment of life-long learning cultures in smart factory environments could provide valuable insights for future implementation strategies. Research should also address the equitable distribution of technological knowledge and resources across different industrial sectors. Furthermore, investigations into the standardization of smart factory protocols and the development of universal implementation frameworks could significantly benefit the field.

The integration of artificial intelligence and machine learning in manufacturing processes presents another crucial area for future research, particularly in optimizing decision-making processes and predictive maintenance systems. Researchers should also explore the sustainability aspects of smart factory implementations, including energy efficiency and environmental impact considerations. The development of comprehensive metrics for measuring smart factory performance and return on investment represents another significant research opportunity. Finally, cybersecurity challenges in interconnected manufacturing systems require dedicated research attention to ensure the resilient operation of smart factories in an increasingly digital industrial landscape.

6. Conclusion

A significant change in the production landscape, Industry 4.0 is the result of the convergence of cutting-edge technology. Adopting smart manufacturing systems has several advantages, such as enhanced production flexibility, better quality control, and increased efficiency. To fully achieve the potential of Industry 4.0, however, issues including high costs, cybersecurity threats, and the demand for trained labor must be resolved. Future developments in manufacturing will be influenced by technologies like 5G, AI, AR/VR, and blockchain, which will spur additional innovation and efficiency in the industry.

As manufacturers continue to adopt and integrate Industry 4.0 technologies, the transition to smart manufacturing will be crucial in ensuring competitiveness, sustainability, and the ability to meet ever-evolving consumer demands. The journey toward smart manufacturing is just beginning, and its successful implementation will unlock new possibilities for the global manufacturing industry.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] J. Carretero and J. D. García, "The Internet of Things: Connecting the world," Pers. Ubiquitous Comput., vol. 18, no. 2, pp. 445–447, 2014, doi: 10.1007/s00779-013-0665-z.

[2] L. Coetzee and J. Eksteen, "The internet of things - Promise for the future? An introduction," 2011 IST-Africa Conf. Proceedings, IST 2011, pp. 1–9, 2011.

[3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[4] L. C. Karen Rose, Scott Eldridge, "THE INTERNET OF THINGS: AN OVERVIEW," Mod. Plast., vol. 64, no. 9, pp. 54–55, 2015.

[5] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. T. Mouftah, "The internet of things [Guest Editorial]," IEEE Commun. Mag., vol. 49, no. 11, pp. 30–31, 2011, doi: 10.1109/MCOM.2011.6069706.

[6] I. Journal, "Internet of Things : A Survey of IoT Applications based on their desirable device characteristics," Int. J. Recent Eng. Res. Dev., vol. 02, no. 10, pp. 10–20, 2017.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[8] A. Junaidi, "INTERNET OF THINGS, SEJARAH, TEKNOLOGI DAN PENERAPANNYA : REVIEW," J. Ilm. Teknol. Infomasi Terap., vol. 1, no. 3, 2015, doi: 10.33197/jitter.vol1.iss3.2015.66.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[10] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement : a review," J. Big Data, 2019, doi: 10.1186/s40537-019-0268-2.

[11] R. (Raj) Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in Proceedings of the 47th Design Automation Conference, in DAC '10. New York, NY, USA: Association for Computing Machinery, 2010, pp. 731–736. doi: 10.1145/1837274.1837461.

[12] K. Kim and P. R. Kumar, “Cyber – Physical Systems : A Perspective at the Centennial,” Proc. IEEE, vol. 100, pp. 1287–1308, 2012, doi: 10.1109/JPROC.2012.2189792.

[13] E. A. Lee, “Cyber Physical Systems : Design Challenges,” 2008.

[14] J. Thunberg, Cyber-Physical Systems : A Model-Based Approach.

[15] Y. Zheng, S. Member, A. Sayghe, S. Member, and O. M. Anubi, “Automated Attack Generative Model Algorithm Design for Resilient Cyber-Physical Systems using an Automated Attack Generative Model,” 2021.

[16] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, “Cybersecurity of Industrial Cyber-Physical Systems: A Review,” ACM Comput. Surv., vol. 54, no. 11s, Sep. 2022, doi: 10.1145/3510410.

[17] M. Kamrul, R. Aliyu, S. Islam, T. Reddy, and N. Safie, “Review article A review on machine learning techniques for secured cyber-physical systems in smart grid networks,” Energy Reports, vol. 11, no. November 2023, pp. 1268–1290, 2024, doi: 10.1016/j.egyr.2023.12.040.

[18] Gaba et al., “A Systematic Analysis of Enhancing Cyber Security Using Deep Learning for Cyber Physical Systems,” IEEE Access, vol. 12, pp. 6017–6035, 2024, doi: 10.1109/ACCESS.2023.3349022.

[19] Z. Chen, S. Zhang, and H. Dui, “Importance-based risk evaluation methodology in transportation cyber-physical systems,” pp. 1–14, 2025.

[20] A. Kumar and N. Sreenath, “Internet of Things and Cyber-Physical Systems Cyber Physical Systems : Analyses , challenges and possible solutions,” Internet Things Cyber-Physical Syst., vol. 1, no. December, pp. 22–33, 2021, doi: 10.1016/j.iotcps.2021.12.002.

[21] A. Willner, “The Industrial Internet of Things,” in Internet of Things A to Z, John Wiley and Sons, Ltd, 2018, pp. 293–318. doi: https://doi.org/10.1002/9781119456735.ch11.

[22] G. Jose and F. De Araujo, “THE INTERNET OF THE INDUSTRY OF THINGS : OPPORTUNITIES AND,” vol. 2020, pp. 1–17, 2017.

[23] P. M. T. Dangat, R. Chandgude, P. Kushwaha, M. Champeli, and P. Pardeshi, “Industrial Internet of Things (IIOT),” no. March, 2024.

[24] M. Angurala, Y. Sharma, and S. Mishra, “Empowering Industries: Unveiling the Potential of Industrial Internet of Things,” in 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), 2024, pp. 166–170. doi: 10.23919/INDIACom61295.2024.10498451.

[25] G. Rathee, R. Iqbal, C. A. Kerrache, and H. Song, “TrustNextGen: Security Aspects of Trustworthy Next-Generation Industrial Internet of Things,” IEEE Internet Things J., vol. 11, no. 15, pp. 25568–25576, 2024, doi: 10.1109/JIOT.2024.3361801.

[26] E. V. N. Jyothi, M. Kranthi, S. Sailaja, U. Sesadri, S. N. Koka, and P. C. S. Reddy, “An Adaptive Intrusion Detection System in Industrial Internet of Things(IIoT) using Deep Learning,” in 2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS), 2024, pp. 1–6. doi: 10.1109/ISTEMS60181.2024.10560245.

[27] R. K. S, S. I. Kalilulah, V. T. Indu, M. Gokuldhev, S. Deepa, and G. Sushma, “Advancements and Security Challenges in the Industrial Internet of Things (IIoT),” in 2024 International Conference on Integration of Emerging Technologies for the Digital World (ICIETDW), 2024, pp. 1–6. doi: 10.1109/ICIETDW61607.2024.10939109.

[28] A. Kusiak, “Smart manufacturing,” Int. J. Prod. Res., vol. 56, no. 1–2, pp. 508–517, 2018, doi: 10.1080/00207543.2017.1351644.

[29] A. T. Hassan, L. A. H. Al-Kindi, and A. B. Abdulghafour, “‘Industrie 4.0’ and Smart Manufacturing: A State of the Art Review,” in 2023 15th International Conference on Developments in eSystems Engineering (DeSE), 2023, pp. 1–6. doi: 10.1109/DeSE58274.2023.10100115.

[30] S. Sahoo and C.-Y. Lo, “Smart manufacturing powered by recent technological advancements: A review,” J. Manuf. Syst., vol. 64, pp. 236–250, 2022, doi: https://doi.org/10.1016/j.jmsy.2022.06.008.

[31] P. Zheng et al., “Smart manufacturing systems for Industry 4 . 0 : Conceptual framework , scenarios , and future perspectives,” vol. 13, no. 2, pp. 137–150, 2018.

[32] H. S. Kang et al., “Smart Manufacturing : Past Research , Present Findings , and Future Directions,” vol. 3, no. 1, pp. 111–128, 2016, doi: 10.1007/s40684-016-0015-5.

[33] F. Tao, Q. Qi, A. Liu, and A. Kusiak, "Data-driven smart manufacturing," J. Manuf. Syst., vol. 48, pp. 157–169, 2018, doi: https://doi.org/10.1016/j.jmsy.2018.01.006.

[34] J. Lee, "Smart Factory Systems," pp. 230–235, 2013, doi: 10.1007/s00287-015-0891-z.

[35] K. Musaeva, I. Vyachina, and M. Aliyeva, "Smart factories and their impact on modern manufacturing enterprises : prospects and challenges in the era of the digital economy," vol. 10, pp. 3–7, 2024.

[36] D. R. Sjödin et al., "Smart Factory Implementation and Process Innovation Smart Factory Implementation and Process Innovation A Preliminary Maturity Model for Leveraging Digitalization in Manufacturing," Res. Manag., vol. 0, no. 0, pp. 0–1, 2018, doi: 10.1080/08956308.2018.1471277.

[37] A. Bagherian, A. L. Srivastav, and S. Mukherjee, "Barriers and strategies of smart factory evolution in industry 4.0: an empirical study," Int. J. Comput. Integr. Manuf., vol. 0, no. 0, pp. 1–33, 2025, doi: 10.1080/0951192X.2025.2461055.

[38] S. M. Muzammal, M. Tayyab, F. Zahra, N. Z. Jhanjhi, and H. Ashraf, "Smart factories greener future: A synergy of Industry 4.0 and sustainability," in Digital Transformation for Improved Industry and Supply Chain Performance, IGI Global, 2024, pp. 70–92.

[39] A. Khang, V. Abdullayev Hajimahmud, A. Misra, and E. Litvinova, Machine vision and industrial robotics in manufacturing: Approaches, technologies, and applications. Boca Raton: CRC Press, 2024.

[40] A. Samani and F. Saghafi, "A hybrid model of implementing a smart production factory within the Industry 4.0 framework," J. Model. Manag., vol. 19, no. 1, pp. 215–239, Jan. 2024, doi: 10.1108/JM2-07-2022-0185.

[41] E. H. Kaur and E. Pooja, "Cloud Computing : A Review," 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:8071857

[42] A. Kalapatapu and M. Sarkar, "Cloud computing: an overview," Cloud Comput. Methodol. Syst. Appl., pp. 3–29, 2012.

[43] M. Armbrust, A. D. Joseph, R. H. Katz, and D. A. Patterson, "Above the Clouds : A Berkeley View of Cloud Computing," 2009.

[44] H. Singh, "Cloud Computing : An Internet Based Computing," vol. 2, no. 3, pp. 116–121, 2012.

[45] G. K. Karamchand, "Scaling New Heights : The Role of Cloud Computing in Business Transformation II . Driving Business Scalability Through Cloud Computing," vol. 5, no. 1, pp. 1–6, 2024.

[46] M. Golec, E. S. Hatay, M. Golec, M. Uyar, M. Golec, and S. S. Gill, "Journal of Economy and Technology," vol. 2, no. June, pp. 190–199, 2024, doi: 10.1016/j.ject.2024.05.001.

[47] S. Sachdeva et al., "Heliyon Unraveling the role of cloud computing in health care system and biomedical sciences," Heliyon, vol. 10, no. 7, p. e29044, 2024, doi: 10.1016/j.heliyon.2024.e29044.

[48] Wang and X. Yang, "Research on Enhancing Cloud Computing Network Security using Artificial Intelligence Algorithms," 2024.

[49] A. Singla, S. Engineering, and A. Singla, "Journal of Artificial Intelligence General Science JAIGS," vol. 1, no. 1, pp. 4–7, 2024.

[50] Y. Wang et al., "The odyssey to next-generation computers : cognitive computers (κ C) inspired by the brain and powered by intelligent mathematics," no. May 2017, 2023.

[51] S. Elnagar and M. A. Thomas, "What is Cognitive Computing ? An Architecture and State of The Art," pp. 1–26.

[52] H. Kaur and A. Malik, "Review on Cognitive Computing Techniques in Healthcare," in 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), 2023, pp. 536–541. doi: 10.1109/ICSCCC58608.2023.10176762.

[53] A. G. Sreedevi, T. Nitya Harshitha, V. Sugumaran, and P. Shankar, "Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review," Inf. Process. Manag., vol. 59, no. 2, p. 102888, 2022, doi: https://doi.org/10.1016/j.ipm.2022.102888.

[54] G. Wang, "MGCC: Multi-Granularity Cognitive Computing," in Rough Sets, J. Yao, H. Fujita, X. Yue, D. Miao, J. Grzymala-Busse, and F. Li, Eds., Cham: Springer Nature Switzerland, 2022, pp. 30–38.

[55] A. Jain, N. Jain, A. Verma, and A. Jain, "Cognitive Computing's Role in Shaping the Future Landscape of Healthcare," in 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2024, pp. 1–5. doi: 10.1109/SCEECS61402.2024.10482075.

[56] C. Nagendraswamy and A. Salis, "A review article on artifi cial intelligence," 2021, doi: 10.29328/journal.abse.1001012.

[57] A. Pannu, "Artificial Intelligence and its Application in Different Areas," vol. 4, no. 10, pp. 79–84, 2015.

[58] J. Harika, P. Baleeshwar, K. Navya, and H. Shanmugasundaram, "A Review on Artificial Intelligence with Deep Human Reasoning," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 81–84. doi: 10.1109/ICAAIC53929.2022.9793310.

[59] Conference on Artificial Intelligence in Medicine (2005-) (15th : 2015 : Pavia, Italy), Artificial intelligence in medicine: 15Th conference on artificial intelligence in medicine, {AIME} 2015, Pavia, Italy, June 17-20, 2015. Proceedings, 2015th ed. Cham, Switzerland: Springer International Publishing, 2015.

[60] F. Kalota, "education sciences," 2024.

[61] S. Bunian, M. A. Al-ebrahim, and A. A. Nour, "Role and Applications of Artificial Intelligence and Machine Learning in Manufacturing Engineering : A Review," 2024.

[62] D. Patel, C. K. Sahu, and R. Rai, "Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing," Int. J. Prod. Res., vol. 62, no. 3, pp. 1041–1071, 2024, doi: 10.1080/00207543.2023.2262050.

[63] S. C. Yuen and E. Johnson, "Augmented Reality : An Overview and Five Directions for AR in Education," vol. 4, pp. 119–140, 2011.

[64] S. Sarkar, A. S, A. V, and D. K, "Exploration and Aspects on Augmented Reality," in 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), 2022, pp. 1–6. doi: 10.1109/ICPECTS56089.2022.10047434.

[65] F. Manuri and A. Sanna, "A Survey on Applications of Augmented Reality," vol. 5, no. 1, pp. 18–27, 2016.

[66] J. Husár and L. Knapčíková, "Implementation of Augmented Reality in Smart Engineering Manufacturing : Literature Review," pp. 119–132, 2024.

[67] S. J. Jose, B. and Adarsh, "Application of Augmented Reality in Manufacturing," Emerg. Technol. Digit. Manuf. Smart Factories (pp. 167-192). IGI Glob. Sci. Publ., 2024.