Volume 12, No.12, December 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

UGC Approved Journal

RESEARCH PAPER

Available online at http://www.jgrma.info

RECENT ADVANCES IN ANOMALY AND DEFECT DETECTION USING MACHINE LEARNING IN SMART MANUFACTURING

Dr. Pradeep Laxkar[1]

[1] Associate Professor, Department of Computer Science and Engineering, ITM(SLS) University, Vadodara, Gujarat, pradeep.laxkar@gmail.com

Abstract: Smart manufacturing is a paradigm shift in conducting industrial processes, which is caused by the interdependence of improved digital technologies and smart automation. This evolution is of utmost importance for anomaly and defect detection, enabling a product with quality, efficiency, and predictive maintenance. This article reviews the key production techniques that enable the creation of smart factory ecosystems: Cyber-Physical Systems, Big Data analytics, cloud computing, autonomous robotics, and IIoT frameworks. It analyses the different levels of smart factory platforms, including mechanical design, process control, IoT configuration, and communication infrastructure. Moreover, it evaluates machine learning methods for anomaly and defect detection, including supervised, unsupervised, and semi-supervised approaches, and highlights their advantages and disadvantages. It also reviews recent trends such as Digital Twin integration, Edge AI, privacy-preserving learning, transfer learning, and explainable AI as indicators of new developments in industrial intelligence. Concomitantly, the paper identifies the main limitations, including security risks, difficulties in system integration, and safety concerns in human–robot collaboration. The present study provides unified views that can be utilised to enhance the reliability and efficiency of the smart manufacturing sector.

Keywords: Smart Manufacturing, Defect Detection, Machine Learning, Cyber-Physical Systems, Edge AI, Big Data.

1 INTRODUCTION

Traditional manufacturing systems include the designs of relatively rigid hierarchical architectures where the scopes are limited to the production arrangement and operation of resources [1]. New technologies are penetrating the manufacturing system and serving as crucial determinants for the automated manufacturing industry of the current industrial revolution to address the future challenges of providing progressively customized requirements [2], advanced quality, and shorter lead time by promoting manufacturing systems to a smart level. Smart manufacturing is not only about integrating technologies but also about managing societal, environmental, and workforce knowledge care.

The technological advances, increases in global competitiveness, diversification of customer requirements, dynamic market trends, digitalization, and constantly increasing process complexities of the 21st century have significantly influenced traditional manufacturing industries [3]. This divergence drives the traditional manufacturing industries towards smart manufacturing [4], which integrates the elements (robots, Big Data, cloud computing, Internet of Things (IoT), Industrial Internet of Things (IIoT), simulations, etc.) of the Industry 4.0 framework.

Anomaly Detection is an important component of the current manufacturing since it can determine an anomaly in the normal functioning of the system that might signify faults or inefficiency [5]. Within the framework of SM, anomalies can be described as an unexpected change of the state or a behavior of subsystems, processes or products, which are not in accordance with the existing norms. Quality problems can be avoided [6], waste can be minimized, and the overall efficiency of the process can be improved through early identification of such anomalies [7]. The increasing popularity of ML algorithms in AD demonstrates that the industry recognises their potential to enhance the results of the manufacturing process.

Defect detection in visual data can be considered a separate part of object detection used primarily as part of inspection systems in industrial applications. The applicability of inspection systems lies in Industry 4.0 and the creation of cognitive control systems. Inspection processes may vary from inter-operational to final quality control of manufactured products. The quality assessment or inspection objective can be diverse, from measurement and control procedures to defect monitoring. Many object detectors have been proposed in the past. They can be divided into single-step or two-step detectors [8]. YOLO and SSD are single-step detectors where the prediction of the final class and localization of the object are performed in a single step.

ML is a method of data analytics and a branch of artificial intelligence that enables machines to learn from data on their own and make and perform decisions or predictions. Over the past few years, ML has gained widespread popularity in manufacturing for material property prediction [9][10], distortion and failure prediction, smart manufacturing, natural language processing, and object

recognition. With advances in sensors and other electronic components, machines are now equipped with various sensors and communication devices [11], which have shown significant potential to improve processes, reduce operational times, enhance product quality, and increase automation.

1.1 Structure of the paper

This paper is organized to present recent advances in smart manufacturing and defect detection. Section 2 explains the most important manufacturing paradigms and the smart factory infrastructure. Section 3 discusses the application of machine learning methods to defect detection. Section 4 presents the top trends and the limitation of existing systems. Section 5 provides a summary of the most recent literature and research advances. Section 6 wraps up the study and outlines future research directions for autonomous and intelligent manufacturing systems.

2 UNDERSTANDING MANUFACTURING PARADIGMS IN SMART FACTORIES

Manufacturing industries are one of the key sectors with a major influence on the economy and the growth of a country [11]. Therefore, new technologies are continuously being developed to modify manufacturing processes and improve product yield and quality [12]. A new technology has emerged recently in the manufacturing industries, popularly known as “smart manufacturing”.

2.1 Technologies Associated with Smart Manufacturing

Smart manufacturing integrates various technologies related to manufacturing, computing, virtualization, connectivity, data handling, etc [13]. The scope of smart manufacturing technologies has become broader due to the interoperability of various technologies, resulting in cost-effectiveness, time-saving, easy configuration, better understanding, quick response to market demand, flexibility and remote monitoring [14]. This section provides a detailed explanation of the various technologies used in smart manufacturing.

2.1.1 Cyber-Physical Systems (CPS)

The combination of physical and virtual spaces is referred to as cyber-physical systems (CPSs), which aim to create a communicative interface between the digital and physical worlds by integrating computation, networking, and physical assets. CPSs have been an important topic in both research and the implementation of industrial technology since their introduction. The term Cyber-Physical Production System (CPPS) is used in the manufacturing industry to refer to the most recent advancements in computer science, information and communication technologies on the one hand, and manufacturing science and technology on the other.

2.1.2 Big Data Analytics & Cloud Computing

Within the framework of Industry 4.0, Big Data Analytics has the potential to provide global feedback and a high degree of coordination, both of which are necessary to achieve high production efficiency. The integration of Big Data Analytics and mining technology allows for the creation of intelligent analysis models and algorithms, which aid in the achievement of smart manufacturing [15]. The digital twin paradigm in Industry 4.0 is among the most prominent uses of Big Data. Another aspect in which Big Data has made significant contributions is big-data-driven manufacturing, which encompasses predictive and proactive manufacturing.

2.1.3 Autonomous Robotics

Robotics is one of the main pillars of Industry 4.0. Industrial manipulators, mobile robots, and collaborative robots are examples of robotics technologies involved in manufacturing processes and other Industry 4.0 applications [16]. While industrial robots are considered the key technology in automation, the latest technological innovations in robotics have boosted productivity, adaptability, versatility, reconfigurability, and safety in smart factories.

2.1.4 Smart Factory:

The smart factory is an essential component of Industry 4.0, which focuses on achieving smart production through networked manufacturing systems and vertical integration of production processes [17]. The smart factory is an idea that intelligently utilizes robotics, automation, embedded systems and information systems towards Industry 4.0. It is considered a transformation from classical (standard) to intelligent manufacturing, heading towards digital manufacturing and digital twin models, supported by many emerging technologies such as Cyber-Physical Systems (CPS), the Internet of Things (IoT), Big Data, cloud computing, and advanced AI.

2.2 System Architecture of the Smart Factory Platforms

As today's markets are being reshaped by ground-breaking technologies, there is more pressure on the industry to become more flexible and adaptable in order to meet the changing needs of markets. With more competition in efficiency, productivity, and quality in the global market, companies need to make big changes to their production plans, technologies, and management. The physical resources layer of the smart factory platform is shown in Figure 1:

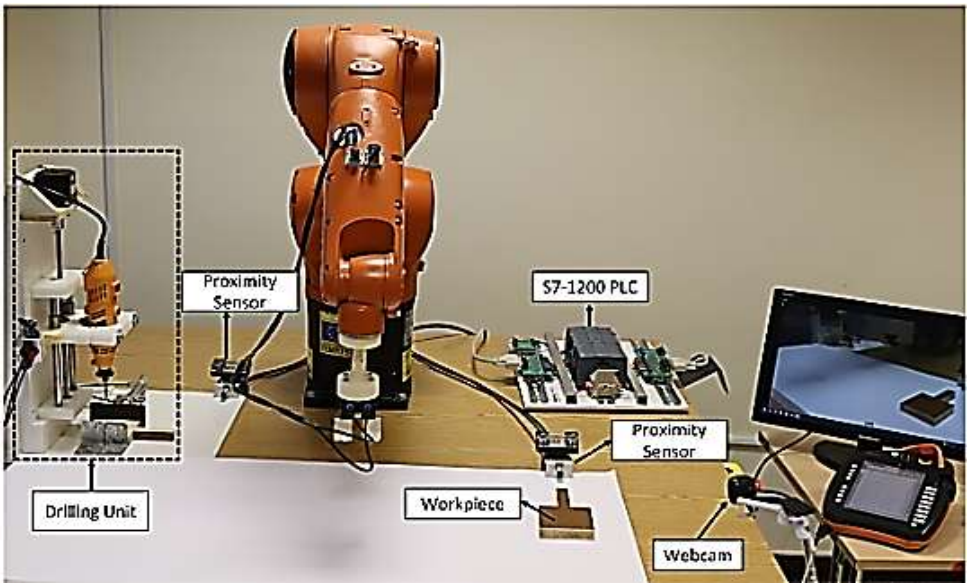

Figure 1: Experimental Platform of the Smart Factory

The following subsections describe the system architecture in more detail.

2.2.1 The Mechanical Design:

A vertical drill was designed to demonstrate a mini-factory process, and the KUKA was programmed to pick the specimen from a designated slot and transport it to the drilling platform to be drilled. A drilling machine is a device for producing holes in workpieces.

2.2.2 Process Control:

An Arduino microcontroller, which is based on the communication with the PLC (the main controller), was used to sequentially actuate the mechanism. Three sensors are connected to the PLC; two proximity sensors were used: the first detects the arrival of the workpiece to initiate the process, and the second detects its arrival at the drilling unit. The third sensor was a switch-activated sensor that is triggered by the linear vertical motion of the drill. The Arduino receives the signal of the second proximity sensor (checks the arrival of the workpiece to the drilling table) via the PLC.

2.2.3 IoT Platform Configuration:

IBM Watson IoT Platform is a platform where devices, gateways, and applications can be connected in the solution of IoT. This platform supports REST and MQTT protocols in its applications, devices, gateways, event processing, and administration [18]. This platform bridges the gap between field devices and data analytic services of IBM services or online user applications. The easy interfacing through the MQTT protocol as well as the user-friendly platform sufficed for this application.

2.2.4 Communication and Interfacing:

In the course of the implementation within the CPSs context and to ensure hardware compatibility with Industry 4.0, different system extension approaches were investigated analogous to the extension by a microcontroller board that integrates the PLC S7-1200 with the KRC4 through LabVIEW API [19], enabling communication to-and-from both manufacturing hardware, as well as cloud-devices interactions.

3 MACHINE LEARNING TECHNIQUES FOR ANOMALY AND DEFECT DETECTION

There are three major types of machine learning methods of anomaly detection: supervised learning, unsupervised learning and semi-supervised learning. They all have strengths and drawbacks [20], and the approach taken must be based on the application needs.

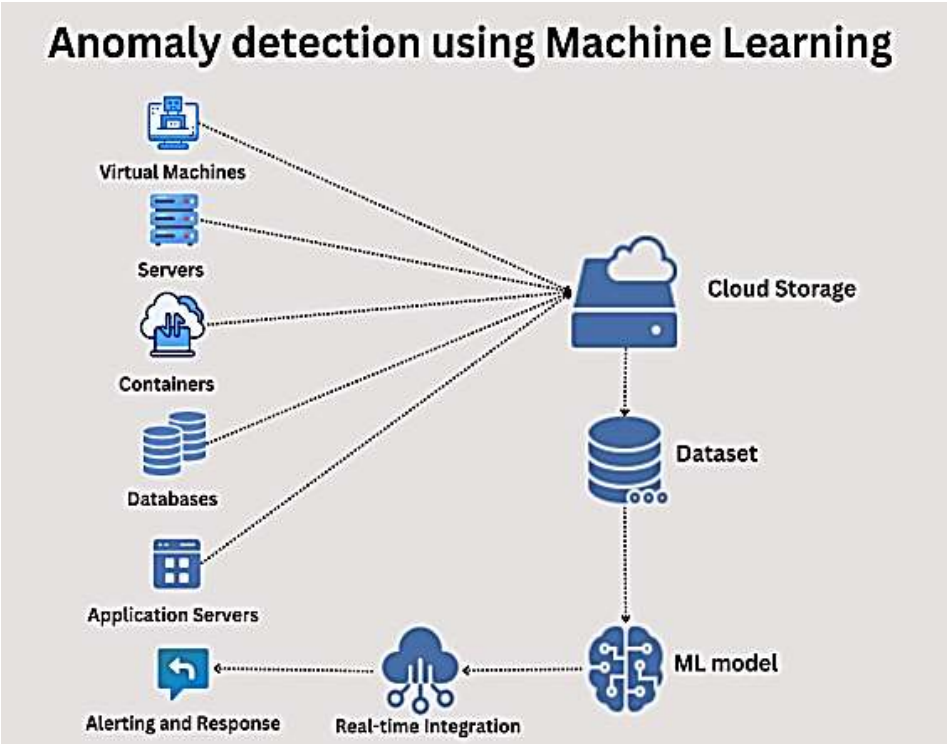

Figure 2: Anomaly detection using Machine Learning

Figure 2 represents an example of an anomaly detection system based on machine learning in which the data are gathered using many different sources including virtual machines, servers, containers, databases and application servers. This information is uploaded to a cloud storage and organized into a dataset which is subsequently trained and utilized to execute a machine learning model to detect anomalies. The output of the model is unified in real-time with the monitoring systems so that irregularities within the infrastructure are quickly detected and reacted in an automated alerting and response system.

3.1 Supervised Learning

Supervised learning is one machine learning method, which requires the use of an IT model that is trained on a dataset, which is labelled with the indicator of whether each data point is normal or an anomaly [21]. The trained model may then be applied to classify new data points into normal or anomalous.

3.1.1 Support Vector Machines (SVM)

SVM is a popular supervised learning algorithm that can be used for anomaly detection. SVMs work by finding a hyperplane that separates normal from anomalous data points in a high-dimensional space. SVM is most useful in point anomalies of high dimensional data.

3.1.2 Neural Networks

Neural networks are a class of supervised learning algorithms that can be used for anomaly detection [22]. Neural networks use hierarchical representations of data to learn and thus acquire complex patterns and relationships. Neural networks are also useful for identifying anomalies in time-series data.

3.2 Unsupervised Learning

Unsupervised learning is a machine learning methodology which entails training a model using an unlabeled dataset whereby the aim is to discover patterns or structures in the data. Directly related to anomaly detecting, unsupervised learning algorithms tend to detect points in the data that are quite anomalous when compared to most of the data.

3.2.1 Clustering Algorithms

Anomaly detection is often done using the clustering algorithms like k-means and DBSCAN [23]. These algorithms are based on the theory that similar data points are clustered together and data points that are not clustered into any of the clusters or are in a small cluster are regarded as an anomaly. Clustering algorithms are most useful where there are distinct clusters within the dataset where there is a point anomaly.

3.2.2 Density-Based Methods

Another category of unsupervised learning algorithms that are applied in detection of anomalies is density-based methods, including Local Outlier Factor (LOF) and Isolation Forest. The mechanisms operate on the estimation of data density and on points with data that are much less dense than their neighbours. Density-based approaches have found specific applications in identifying contextual anomalies in datasets with varying densities.

3.3 Semi-Supervised Learning

Semi-supervised learning is a machine learning approach that combines elements of supervised and unsupervised learning. Semi-supervised learning algorithms are also applied in the context of anomaly detection, where the training dataset is composed of a few labelled data and many unlabelled ones. The idea is to use labelled data to improve the model for unlabelled data.

3.3.1 Self-Training

Self-training is a semi-supervised learning algorithm, whereby a model is trained on the labelled data and it is used to give predictions on the labels of the unlabelled data. The resulting predicted labels are passed back through the model where they are re-trained and the cycle is repeated until convergence. Self-training works especially well in small quantities of labelled data to detect point anomalies in datasets.

3.3.2 Co-Training

Co-training is a semi-supervised learning algorithm, which uses multiple models which are trained on various views of the information. The models are then used to predict labels for the unlabelled data, and the predictions are used to retrain the models. Co-training is the most successful when using many sets of features to detect contextual anomalies in data.

4 RECENT TRENDS AND LIMITATIONS

Smart manufacturing is a developing area that is currently gaining momentum as a result of the integration of digital technologies, data-driven decision-making, and smart automation.

4.1 Emerging Trends for Defect Detection in Smart Manufacturing

The recent trends have been characterized by a tendency to replace isolated automation solutions with completely integrated, adaptive and intelligent ones [24].

4.1.1 Integration with Digital Twins

Digital Twins (DTs) The combination of Digital Twins (DTs) and machine learning in a smart manufacturing environment can improve anomaly and defect detection through the creation of a synchronized virtual model that reacts to real-time physical processes [25]. This combination enables automatic monitoring, presuming, and control. ML-based DTs are able to accomplish anomaly detection and predictive maintenance [26]. An example of such is a digital twin-driven tool condition monitoring system in machining where milling activities are analyzed using real-time vibration data and model frequency characteristics in the virtual model to identify wear and abnormalities in the mill.

4.1.2 Edge AI and Real-Time Inference

Edge AI is used in smart manufacturing to refer to the implementation of machine learning algorithms that run on edge devices, e.g. smart cameras, sensors, or gateways that are co-located with production machinery. This allows real time inference in the factory floor where quick detection of faults or equipment faults is essential to achieve high throughput, safety and minimization of waste. EDGE AI eliminates latency and privacy threats of transmitting massive amounts of data to centralized cloud servers because, in this type of processing, data are processed locally.

4.1.3 Privacy-Preserving ML (Federated Learning, Differential Privacy)

In intelligent production, it is important to protect confidential information including the parameters of proprietary machines, process analytics, and operational metrics. Privacy Preserving Machine Learning involves the use of such methods as Federated Learning (FL) and Differentiated privacy (DP) to create strong defect and anomaly detection models without violating the data confidentiality.

- **Federated Learning**: Allows the joint training of a global model by a number of manufacturing units or edge devices. Every device does not communicate raw data, but instead it calculates local model changes (e.g. gradients or weights) and transmits these to a central server. The server consolidates updates to perfect the global model, maintaining the privacy of

data whilst utilizing the varying data entries of sites [27]. In intelligent production, this means that various plants or machine categories could collaborate to enhance anomaly detection networks without disclosing their secret operations.

- **Differential Privacy**: Differential Privacy introduces a controlled random noise to the model updates or parameters and then sharing [28]. This averts inversion attacks that may lead to conclusions about sensitive data from individual production samples. The trick is to reconcile privacy assurance with the model's precision by setting the level of noise.

4.1.4 Transfer Learning and Domain Adaptation

Transfer Learning (TL) in smart manufacturing can be defined as an approach whereby the knowledge (i.e. feature representations, model parameters or learned tasks) in one domain (the source) is applied to improve performance in a related but distinct domain (the target) [29] Transfer Learning (TL) in smart manufacturing can be defined as an approach whereby the knowledge (i.e. feature representations, model parameters or learned tasks) in one domain (the source) is applied to improve performance in a related but distinct domain (the target) [30]. This is necessary in industrial environments, where it is often scarce and costly to obtain labelled data for each sensor type, machine, or operating condition. Domain Adaptation (DA) is a specialized variant of TL, dedicated to the case when the feature space is shared when between the source and the target, data distributions are different because of various aspects such as sensor properties, machine settings, or production conditions.

4.1.5 Explainable AI (XAI) in Industrial Applications

Artificial intelligence (AI) has grown rapidly across businesses due to its ability to improve efficiency, streamline operations, and offer new opportunities [31]. As businesses increasingly use AI systems for important decision-making, understanding how they make decisions has become a major issue. It has led to Explainable Artificial Intelligence (XAI), which aims to make AI systems' outputs understandable, explainable, and reliable. XAI is transforming the use of AI by organizations by elucidating machine learning models, handling accountability, fairness, and ethics as well as providing informed decision-making.

4.2 Limitations Recorded for Defect Detection in Smart Manufacturing

Smart manufacturing systems are considered to be faced security issues, a lack of system integration [14], a lack of return on investment in new technology and financial issues during the erection of new smart manufacturing systems and/or during the upgrade of existing industries with smart manufacturing technology.

4.2.1 Security Issues in Smart Manufacturing

The smart manufacturing system means the use of an integrated network system in a manufacturing system for sharing information between manufacturing or machining units to the end customers [32]. For this purpose, it requires network connectivity and is arranged especially through the internet. Sharing information through the internet requires the security of data and information throughout the system in various points with global unique identification and end to end data encryption.

4.2.2 System Integration

Another challenge of the implementation of a smart manufacturing system is the integration of new technology equipment with existing ones. The compatibility between existing and new devices creates various problems in implementing smart manufacturing technologies. The old machinery, which is controlled by certain communication protocols, might be outdated, and new devices may use different protocols.

4.2.3 Safety in Human-Robot Collaboration

The International Federation of Robotics defines Human-Robot collaboration as the ability of a robot to coordinate with workers in an industrial environment to perform specialised tasks. The main considerations should be done with occupational health and safety of personnel working on the site, any hazardous environment should be avoided, and necessary occupational health and safety measures should be maintained [33]. The main attention should be given while implementing the CPS system or industrial robotic systems to minimize any types of mechanical, electrical, thermal, noise, vibration, radiation, material/substance, work environment any hazards in the workplace in an industry.

5 LITERATURE REVIEW

This section provides a literature review on defect detection in smart manufacturing. It discusses the different approaches, tools, and technologies used to diagnose and solve problems remotely.

Archana *et al.* (2025) It has changed the face of smart manufacturing due to the integration of the IIoT and ML, and this enables real-time monitoring, predictive analytics, and autonomous decisions. Traditional manufacturing systems face significant difficulties because their predictive maintenance performed poorly: it could not detect defects effectively and resulted in high equipment

downtime. A dual applied IIoT-ML structure that combines LSTM technology for predictive maintenance with CNN solutions for defect identification and reinforcement learning approaches for production improvement [34].

Xu *et al*. (2025) provided a general framework of smart manufacturing in the context of Industry 5.0. Wherein, the embodied agents, like robots, sensors, and actuators, are the carriers for IndAI, facilitating the development of the self-learning intelligence in individual entities, the collaborative intelligence in production lines and factories (smart systems), and the swarm intelligence within industrial clusters (systems of smart systems). Through the framework of CPSSs, the key technologies and their possible applications for supporting the single-agent, multi-agent and swarm-agent embodied IndAI have been reviewed, such as the embodied perception, interaction, scheduling, multi-mode large language models, and collaborative training [35].

Salam *et al.* (2024) proposed a new method of integrating anomaly detection methods with Zero-Knowledge Proofs (ZKPs) to enhance the security architecture of the smart manufacturing system. Their approach combines the use of data preprocessing, such as statistical imputation and data smoothing with sophisticated anomaly detection based on classification algorithms and neural networks, especially the deep learning architectures. The identified anomalies are verified by a specialized ZKP scheme, zk-SNARKs, making the process of verification sufficiently robust without data confidentiality misconduct [36].

Manta-Costa *et al*. (2024) explores the consequences of I-ML in other production contexts, such as predictive maintenance, anomaly detection, and quality control and provides an overall overview of use cases as well as an identification of the emergent technologies and trends. They also discuss the urgent necessity of sustainable, reproducible, and reliable performance in industrial applications and discuss the strategies of overcoming the impediments to ML implementation in the industry [37].

Anand, Sheeba and Fancy (2024) the emergence of several technologies that are critical to the development of the Industrial IoT and smart manufacturing. These include next-generation material science, advanced robotics, cyber-physical systems, big data, advanced analytics, artificial intelligence (AI) and machine learning (ML), operational intelligence and generative design for additive manufacturing. Manufacturers are thinking about new business models based on real-world implementations, in which they offer services instead of products and use the digital twin to optimize the product's performance and availability [38].

Haricha *et al.* (2023) aimed to present a consistent and comprehensive vision of existing efforts in smart manufacturing and discussed the remaining open issues. Smart manufacturing (SM) is evolving as a new version of traditional manufacturing, revealing the magnitude and power of smart technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT). The wide applicability of these technologies is allowing important innovations across all industries. As the manufacturing industry has gained benefits, the current boost Smart Manufacturing is experiencing exceptional levels of interest [39].

Lee, Kim and Kim (2023) hybrid model proposed proved to be better than other anomaly detection algorithms. It helps to improve the efficiency of production by anticipating downtime in the production process. This research contributes to the literature on the monitoring and management of anomaly detection in smart factories. It also has practical implications for the manufacturing industry by recommending efficiency measures for smart factories to reduce downtime in manufacturing processes and improve product quality [40].

A systematic review of recent studies concerning Recent advances in smart manufacturing is provided in Table 1 to identify areas of interest, core findings, challenges, and contributions.

Table 1: Summary of literature review based on Recent advances in smart manufacturing

Reference	Focus Area	Key Findings	Challenges	Key Contribution
Archana et al. (2025)	IIoT and ML combination to predictive maintenance and defect detection.	Stacked LSTM predictive maintenance, CNN defect detection and reinforcement learning production; enhanced production decision-making in real-time.	The old systems were characterised by poor defect detection and high downtimes.	A suggested dual IIoT-ML architecture that uses deep learning and RL to optimize smart manufacturing.
Xu et al. (2025)	IndAI and CPSSs in Smart Manufacturing in Industry 5.0.	Proposed an overall system of embodied agents (robots, sensors, actuators) with Industrial AI (IndAI) on single, collaborative, and swarm scales.	Dealing with multi agent system complexity and incorporating technologies such as perception.	Introduced an IndAI implementation scheme based on CPSS, with a focus on such technologies as embodied perception, LLMs, and collaborative intelligence applied to Industry 5.0.
Salam et al., (2024)	Anomaly detection based on Zero-Knowledge Proofs (ZKPs).	Obtained the high anomaly detection accuracy with deep learning and checked the existence of anomalies with	Securing the confidentiality of data and ensuring that the data is not detected.	Proposed a privacy preserving and safe anomaly detection method based on ZKPs.

		zk-SNARKs to provide privacy.		
Manta-Costa et al. (2024)	I-ML in practice in manufacturing.	Applications (predictive maintenance, anomaly detection and quality control) discussed.	Barriers to reliability, reproducibility and to industrial adoption.	Proposed an in-depth discussion of new trends and technologies in the implementation of sustainable I-ML.
Anand, Sheeba and Fancy (2024)	Technologies that support IIoT and intelligent production.	Emphasized the significance of AI, digital twin, generative design, and service-based business models.	Multifaceted adoption of various technologies.	Recognized new technologies are revolutionizing the conventional manufacturing to smart and service-driven manufacturing.
Haricha et al. (2023)	Overall perspective of intelligent manufacturing revolution.	Highlighted the advantages of AI and IoT to transform conventional systems.	Integration and scalability problems.	Gave a detailed profile of SM trends and identified gaps that still exist.
Lee, Kim and Kim (2023)	Smart factories anomaly detection hybrid model.	Model maximally forecasts the downtime, which improves the production efficiency and products.	Requirement of correct and prompt anomaly detection in dynamic environments.	Created a hybrid model that was better than traditional in detecting anomalies and predicting downtime.

6 CONCLUSION AND FUTURE WORK

Smart manufacturing is changing the way old industrial practices are conducted with the integration of intelligence, connection, and automation to all levels of the manufacturing lifecycle. This particular review brings to light the huge influence that smart manufacturing has in present-day industry, a huge influence that is mainly attributed to the use of advanced digital technologies, interconnected systems, and intelligent decision-makers. It relies on the examination of major manufacturing paradigms like CPS, IIoT, robots, cloud computing, and Big data, besides the smart factory platform architecture, to point out the way these components together make it possible to have production environments that are efficient, flexible, and data-driven. Among other things, machine learning for anomaly and defect detection makes reliability even higher, while trends that include Digital Twins, Edge AI, privacy-preserving models, transfer learning, and explainable AI are redefining industrial intelligence users even more. Even though these technologies improve, security risks, integration of systems problems, and safety issues in human-robot collaboration are still some of the challenges that have to be dealt with. The resolution of these issues will be the road to the fully autonomous, resilient, and scalable smart manufacturing systems.

The autonomous smart factory of the future will be created using advanced digital twins, energy-efficient edge AI, and powerful privacy-preserving learning. A major part of this technology will be the improved human-robot collaboration safety, building explainable, trustworthy AI systems and making model adaptability across diverse machines. Such advancements will definitely extent having reliability, scalability and intelligent environment in the next generation manufacturing environment.

REFERENCES

[1] M. R. R. Deva, “Advancing Industry 4.0 with Cloud-Integrated Cyber-Physical Systems for Optimizing Remote Additive Manufacturing Landscape,” in *2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE)*, 2025, pp. 1–6. doi: 10.1109/NE-IECCE64154.2025.11182940.

[2] Vikas Thakran, “A Review of 3D printing methods for pharmaceutical manufacturing: Technologies and applications,” *Int. J. Sci. Res. Arch.*, vol. 4, no. 1, pp. 250–261, Dec. 2021, doi: 10.30574/ijsra.2021.4.1.0207.

[3] S. Garg, “AI-Driven Innovations in Storage Quality Assurance and Manufacturing Optimization,” *Int. J. Multidiscip. Res. Growth Eval.*, vol. 1, no. 1, pp. 143–147, 2020, doi: 10.54660/.IJMRGE.2020.1.1.143-147.

[4] V. Warke, S. Kumar, A. Bongale, and K. Kotecha, “Sustainable Development of Smart Manufacturing Driven by the Digital Twin Framework: A Statistical Analysis,” *Sustainability*, vol. 13, no. 18, p. 10139, Sep. 2021, doi: 10.3390/su131810139.

[5] G. Sarraf and V. Pal, “Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks,” *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[6] R. Q. Majumder, “A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, 2025, doi: 10.48175/IJARSCT-25619.

[7] I. Elía and M. Pagola, “Anomaly detection in Smart-manufacturing era: A review,” *Eng. Appl. Artif. Intell.*, vol. 139, p. 109578, 2025, doi: https://doi.org/10.1016/j.engappai.2024.109578.

[8] J. Klarák *et al.*, “From Anomaly Detection to Defect Classification,” *Sensors*, vol. 24, no. 2, p. 429, Jan. 2024, doi: 10.3390/s24020429.

[9] G. Maddali, “Efficient Machine Learning Approach Based Bug Prediction for Enhancing Reliability of Software and Estimation,” *Int. J. Res. Eng. Sci. Manag.*, vol. 8, no. 6, pp. 1–7, 2025.

[10] S. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 1–8, 2025.
[11] K. Murugandi, "Delivering Seamless SAP Integration for Logistics and Manufacturing : A Review of EDI Message Flow and Troubleshooting," vol. 13, no. 03, 2024.
[12] S. Sahoo and C.-Y. Lo, "Smart manufacturing powered by recent technological advancements: A review," *J. Manuf. Syst.*, vol. 64, pp. 236–250, Jul. 2022, doi: 10.1016/j.jmsy.2022.06.008.
[13] R. Patel and P. Patel, "Machine Learning-Driven Predictive Maintenance for Early Fault Prediction and Detection in Smart Manufacturing Systems," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 1, pp. 141–149, 2024, doi: 10.56472/25832646/JETA-V4I1P120.
[14] S. Phuyal, D. Bista, and R. Bista, "Challenges, Opportunities and Future Directions of Smart Manufacturing: A State of Art Review," *Sustain. Futur.*, vol. 2, p. 100023, 2020, doi: https://doi.org/10.1016/j.sftr.2020.100023.
[15] V. Verma, "Big Data and Cloud Databases Revolutionizing Business Intelligence," *TIJER – Int. Res. J.*, vol. 9, no. 1, pp. 48–58, 2022.
[16] R. Patel and P. Patel, "A Survey on AI-Driven Autonomous Robots for Smart Manufacturing and Industrial Automation," *Tech. Int. J. Eng. Res.*, vol. 9, no. 2, 2022, doi: 10.56975/tijer.v9i2.158819.
[17] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing Smart Factory of Industrie 4 . 0 : An Outlook," *Int. J. Distrib. Sens. Networks*, pp. 1–10, 2016, doi: 10.1155/2016/3159805.
[18] S. Amrale, "Anomaly Identification in Real-Time for Predictive Analytics in IoT Sensor Networks using Deep," vol. 14, no. 6, pp. 526–532, 2024.
[19] Vaidehi Shah, "Next-Gen Emergency Communication Using Low-Power Wide-Area and Software-Defined WANS," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 600–609, Sep. 2022, doi: 10.48175/IJARSCT-8349M.
[20] A. Parupalli, "Business-Oriented Employee Performance Assessment via Machine Learning in ERP Systems," vol. 11, no. 11, 2024.
[21] S. K. P. Yeshwanth Macha, "A Survey of DevOps Practices for Machine Learning and Artificial Intelligence Workflows in Modern Software Development," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, pp. 200–208, 2024, doi: 10.56472/25832646/JETA-V4I3P121.
[22] Vibhor Pal and Satyadhar Kumar Chintagunta, "Transformer-Based Graph Neural Networks for RealTime Fraud Detection in Blockchain Networks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1401–1411, Jul. 2023, doi: 10.48175/IJARSCT-11978Y.
[23] N. K. Pavan Nutalapati, Jayapal Reddy Vummadi, Suresh Dodda, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," *Int. Conf. Data Sci. Its Appl.*, pp. 880–885, 2025.
[24] V. Rajavel, "Novel Machine Learning Approach for Defect Detection in DFT Processes," *Am. Sci. Res. J. Eng. Technol. Sci.*, vol. 101, no. 1, pp. 325–334, 2025.
[25] Z. Liu, Z. Q. Lang, Y. Gui, Y. P. Zhu, and H. Laalej, "Digital twin-based anomaly detection for real-time tool condition monitoring in machining," *J. Manuf. Syst.*, vol. 75, no. September 2023, pp. 163–173, 2024, doi: 10.1016/j.jmsy.2024.06.004.
[26] V. Prajapati, "Exploring the Role of Digital Twin Technologies in Transforming Modern Supply Chain Management," vol. 14, no. 03, pp. 1387–1395, 2025.
[27] V. PAL, "Federated Contrastive Learning for Privacy- Preserving Medical Image Analysis," vol. 9, no. 1, pp. 601–606, 2022.
[28] P. Papadopoulos, W. Abramson, A. J. Hall, N. Pitropakis, and W. J. Buchanan, "Privacy and Trust Redefined in Federated Machine Learning," *Mach. Learn. Knowl. Extr.*, vol. 3, no. 2, pp. 333–356, Mar. 2021, doi: 10.3390/make3020017.
[29] R. P. Mahajan, "Transfer Learning for MRI image reconstruction: Enhancing model performance with pretrained networks," *Int. J. Sci. Res. Arch.*, vol. 15, no. 1, pp. 298–309, Apr. 2025, doi: 10.30574/ijsra.2025.15.1.0939.
[30] M. Abdallah *et al.*, "Anomaly Detection and Inter-Sensor Transfer Learning on Smart Manufacturing Datasets," *Sensors*, vol. 23, no. 1, p. 486, Jan. 2023, doi: 10.3390/s23010486.
[31] P. Dimple, "Explainable Artificial Intelligence (XAI) for industry applications : Enhancing transparency , trust , and informed decision-making in business operation Dimple Patil," no. November, 2024.
[32] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, pp. 1–8, 2025.
[33] R. Patel, "Offshore Oil Operations: Innovations in Maintenance, Safety, and Asset Integrity Management," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 8, no. 5, pp. 1–10, 2022.
[34] T. Archana, A. H. Malini, R. Kishore Kumar, D. B. Prakash, S. Kumaran, and S. S. Nath, "Smart Factory Integration with IIoT and Machine Learning for Optimized Manufacturing," in *2025 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM)*, Apr. 2025, pp. 1243–1248. doi: 10.1109/ICTMIM65579.2025.10988051.
[35] J. Xu, Q. Sun, Q.-L. Han, and Y. Tang, "When Embodied AI Meets Industry 5.0: Human-Centered Smart Manufacturing," *IEEE/CAA J. Autom. Sin.*, vol. 12, no. 3, pp. 485–501, Mar. 2025, doi: 10.1109/JAS.2025.125327.
[36] A. Salam *et al.*, "Securing Smart Manufacturing by Integrating Anomaly Detection with Zero-Knowledge Proofs," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3373697.
[37] A. Manta-Costa, S. O. Araújo, R. S. Peres, and J. Barata, "Machine Learning Applications in Manufacturing - Challenges, Trends, and Future Directions," *IEEE Open J. Ind. Electron. Soc.*, vol. 5, no. May, pp. 1085–1103, 2024, doi: 10.1109/OJIES.2024.3431240.

[38] M. Anand, T. M. Sheeba, and C. Fancy, "Role of AI and Digital Twin in Smart Manufacturing," in *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, Wiley, 2024, pp. 233–248. doi: 10.1002/9781394303601.ch11.
[39] K. Haricha, A. Khiat, Y. Issaoui, A. Bahnasse, and H. Ouajji, "Recent Technological Progress to Empower Smart Manufacturing: Review and Potential Guidelines," *IEEE Access*, vol. 11, pp. 77929–77951, 2023, doi: 10.1109/ACCESS.2023.3246029.
[40] K. S. Lee, S. B. Kim, and H.-W. Kim, "Enhanced Anomaly Detection in Manufacturing Processes Through Hybrid Deep Learning Techniques," *IEEE Access*, vol. 11, pp. 93368–93380, 2023, doi: 10.1109/ACCESS.2023.3308698.

