



Review

Machine Learning and IoT-Based Solutions in Industrial Applications for Smart Manufacturing: A Critical Review

Paolo Visconti ^{1,*}, Giuseppe Rausa ¹, Carolina Del-Valle-Soto ², Ramiro Velázquez ³, Donato Cafagna ¹ and Roberto De Fazio ^{1,3}

¹ Department of Innovation Engineering, University of Salento, 73100 Lecce, Italy; giuseppe.rausa@unisalento.it (G.R.); donato.cafagna@unisalento.it (D.C.); roberto.defazio@unisalento.it (R.D.F.)

² Facultad de Ingeniería, Universidad Panamericana, Zapopan 45010, Mexico; cvalle@up.edu.mx

³ Facultad de Ingeniería, Universidad Panamericana, Aguascalientes 20296, Mexico; rvelazquez@up.edu.mx

* Correspondence: paolo.visconti@unisalento.it; Tel.: +39-0832-297334

Abstract: The Internet of Things (IoT) has radically changed the industrial world, enabling the integration of numerous systems and devices into the industrial ecosystem. There are many areas of the manufacturing industry in which IoT has contributed, including plants' remote monitoring and control, energy efficiency, more efficient resources management, and cost reduction, paving the way for smart manufacturing in the framework of Industry 4.0. This review article provides an up-to-date overview of IoT systems and machine learning (ML) algorithms applied to smart manufacturing (SM), analyzing four main application fields: security, predictive maintenance, process control, and additive manufacturing. In addition, the paper presents a descriptive and comparative overview of ML algorithms mainly used in smart manufacturing. Furthermore, for each discussed topic, a deep comparative analysis of the recent IoT solutions reported in the scientific literature is introduced, dwelling on the architectural aspects, sensing solutions, implemented data analysis strategies, communication tools, performance, and other characteristic parameters. This comparison highlights the strengths and weaknesses of each discussed solution. Finally, the presented work outlines the features and functionalities of future IoT-based systems for smart industry applications.

Keywords: machine learning; IoT; smart manufacturing; Industry 4.0; additive manufacturing; predictive maintenance; industrial process control; worker's health; data safety



Citation: Visconti, P.; Rausa, G.; Del-Valle-Soto, C.; Velázquez, R.; Cafagna, D.; De Fazio, R. Machine Learning and IoT-Based Solutions in Industrial Applications for Smart Manufacturing: A Critical Review. *Future Internet* **2024**, *16*, 394. <https://doi.org/10.3390/fi16110394>

Academic Editors: Marcelo García and Paulina Ayala

Received: 15 September 2024

Revised: 19 October 2024

Accepted: 23 October 2024

Published: 26 October 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The industrial manufacturing sector has expanded significantly due to continuous technological advances to simplify production procedures and increase product yield and quality [1]. Introducing a paradigm capable of connecting all the components involved in the production process in real-time can improve the product's quality, the production plant's safety, and the control of operating status through predictive maintenance (PdM). At the same time, it can ensure the safeguard of the operator's health through constant monitoring of his physiological and environmental parameters of the workplace. This paradigm is the Internet of Things (IoT); the data received from the sensors are recorded in databases and appropriately processed to receive information regarding production progress, safety, environmental conditions, etc.

The fields of application of the IoT are multiple. In the biomedical field, wearable devices have been created capable of acquiring clinical data, such as electro-cardiogram (ECG), electro-encephalogram (EEG), body temperature, and photoplethysmography (PPG) signals for clinical diagnosis [2]. For example, Bonfanti S. B. et al. [3] designed an IoT node to collect clinical data and detect atrial fibrillation through an ECG analysis. In the agricultural sector, IoT introduces Smart Agriculture 4.0, a smart farming method that enhances the precision of fertilizer, pesticide, and herbicide applications [4]. Drones facilitate

weed detection, while robots help farmers milk animals. Numerous parameters are also monitored to enhance yield, improve environmental conditions, irrigation process, pests and fertilizers, manage unwanted plants, ground conditions, and greenhouse production environment, and minimize the cost of process inputs [5]. Generally speaking, the IoT is widely recognized for improving product warehousing operations' efficiency, productivity, safety, convenience, and response time. It also helps address labor shortages in various logistics and warehouse operations, reduces costs, and has a positive environmental impact. The picking process represents 50–55% of total warehouse costs and significantly impacts plant performance. The IoT can improve warehouse visibility and traceability, increasing picking efficiency [6]. Another area in which the IoT has made a significant contribution is PdM. This preventive maintenance approach allows planning maintenance interventions more effectively based on the information acquired from the machine itself. In an era in which production plants are increasingly critical for the industry's stability, adopting PdM techniques allows for maintaining high plant efficiency while reducing maintenance costs. For this reason, by identifying the deterioration of the equipment, PdM enables the reduction of the frequency of unplanned maintenance interventions and the probability of failures to a minimum [7].

The new idea of Industry 4.0 results from the digitalization of the production process, combined with IoT-based methods (such as smart objects–OS). This new idea, representing the fourth industrial revolution, views the factory as an adaptable and productive production line where the product controls its manufacturing processes [8]. Numerous IoT applications provide quick benefits by empowering manufacturers to implement digital transformations from efficiency, automation, competitiveness, and customer-centricity perspectives. Data from the production chain are used to create new income streams [8]. The Industry 4.0 objective is to move away from the third industrial revolution's automation of mass production and toward more flexible and efficient manufacturing. It may be characterized as a technological revolution emphasizing increasing industrial automation and digitalization [1]. Smart manufacturing (SM), which uses advanced technologies like artificial intelligence (AI), IoT, cloud computing, and cyber-physical systems (CPS), is a result of this industrial digitization (Figure 1) [9,10].

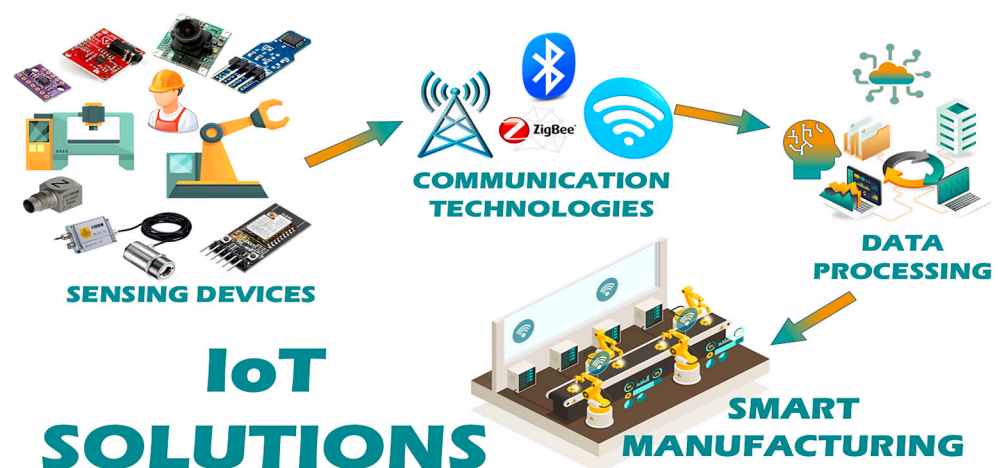


Figure 1. Information flow on the IoT paradigm. The information acquired by the sensing devices embedded in the plant or supporting the operator monitoring is transferred to a data-processing platform through various data-transfer technologies (wired and wireless). The acquired data are processed to obtain information, including quality of the production process, operator conditions, machine status, production progress, consumption, air pollution, etc.

Cyber-physical systems (CPS) integrate the physical and digital worlds through information technology and communication networks. They combine software, hardware, and physical components to monitor and control real-world processes, creating an inter-

action between cyberspace and physical elements [11]. The goal of Industry 4.0 is the sustainable modernization and simplification of industrial processes and production. It uses cutting-edge technologies such as additive manufacturing, robotics, and IoT [12].

Security has always been a critical element in an industrial context as it prevents production interruptions, prevents accidents, and improves staff training. Using sensing devices and data processing through ML methods has resulted in smart personal protective equipment (PPE) [13] that has helped monitor workers' health in the workplace and check that such smart devices are being worn correctly. The challenges in the field of operator safety are creating more compact, more ergonomic, easily wearable, and self-recharging devices [14]. With the digitalization of industry, new specific security risks have emerged, such as data theft and manipulation, attacks on automation systems, and cybersecurity. The solutions analyzed in this paper aim to overcome implementation difficulties such as technological complexity, the management of large amounts of data, the evolution of cyber threats, and threat classification [15].

Additive manufacturing (AM), an essential pillar of digital technology, is a production method that changes the traditional manufacturing process. AM is a general name for manufacturing technologies that add material layer by layer to create desired physical parts. Many of the steps required by traditional production processes have been eliminated with additive manufacturing [16]. For example, AM removes the need to design the machining cycle, eliminates the need for bulky machining centers, eliminates the need to manage chips after machining, and makes maintenance easier and faster [16]. This technology, which initially emerged as rapid prototyping (RP) systems, has evolved into direct production by developing various AM processes. Although there are many varieties, the most prominent AM technologies are stereolithography (SLA), selective laser sintering (SLS), three-dimensional printing (3DP), laminated object fabrication, and fused deposition modeling (FDM) [17]. One of the main applications of the IoT paradigm in the field of AM within smart manufacturing is monitoring the printing process to eliminate or minimize production defects [18]. For example, using an augmented interface or a digital twin for conventional AM processes allows for early identification of manufacturing defects, thus increasing the predictability of the process [19,20]. One real-world example of the IoT applied to additive manufacturing (AM) is given by the Fast Radius company, now part of SyBridge Technologies company (Spring Lake Drive Itasca, IL, USA) [21]. In 2018, the World Economic Forum recognized its Chicago facility as one of the top nine smart factories worldwide, specialized in AM alongside CNC machining and injection molding. A key element of Fast Radius' success is its proprietary IoT platform, which collects data from every part designed and produced in its virtual warehouse. This data helps teams identify suitable applications for 3D printing and assess the engineering and economic feasibility of manufacturing components [21]. The Geico Taikisha Group gives another example of a real-world IoT application. The Geico Group, a global leader in designing and building automated auto body paint shops, leveraged IoT digital twin technology to stay connected with customers by providing access to detailed production data [22]. This connection allowed Geico to monitor machine performance, identify common issues, and enhance the performance of paint shop cells for their clients. Customers also benefited from these digital twin capabilities, enabling them to run live simulations to explore potential efficiencies, address vulnerabilities, and achieve cost savings. This transparency helped predict maintenance needs and downtime, reducing costs. Additionally, with smart energy management features, customers could optimize resource usage for sustainability and further savings [22].

While Industry 4.0 focuses on integrating smart technologies into manufacturing and supply chains, a new paradigm called Industry 5.0 will enhance this digital transformation by fostering deeper collaboration between humans and machines within their digital ecosystems [23–28]. This partnership combines the precision and speed of industrial automation with human creativity, innovation, and critical thinking, leading to more meaningful and efficient outcomes [24]. In other words, the goal of Industry 5.0 is to create

a balance between automation and human–machine interaction with the idea of supporting and enhancing human intelligence instead of replacing it [25]. Industry 5.0 is less about introducing a new industrial revolution and more about enhancing the technologies of Industry 4.0 by fostering closer collaboration between humans and robots [25]. It builds on the pillars of Industry 4.0 (AM, augmented reality, autonomous robots, big data and analytics, cloud connectivity, cybersecurity, horizontal and vertical system integration, IoT, and digital twins) by emphasizing human creativity and well-being as key components of industrial processes [24]. The aim is to combine machines' speed and efficiency with humans' imagination and skills.

The following three concepts form the core principles of Industry 5.0 [29]. The first one, a human-centric industry, focuses on prioritizing human needs and interests in the production process. Rather than asking how workers can adapt to new technology, Industry 5.0 explores how technology can better serve workers. While robots excel in precision and endurance, they lack the critical and creative thinking abilities humans bring. The second concept, a resilient industry, is characterized by robust industrial production, capable of withstanding disruptions and supporting critical infrastructure during crises. The pandemic exposed vulnerabilities in manufacturing and supply chains, emphasizing the need for greater agility and resilience in these systems. Finally, the third one, a sustainable industry, focuses on minimizing environmental impact by adopting circular economy practices. Key initiatives include reducing energy use, greenhouse gas emissions, and waste while preserving natural resources and preventing their depletion and degradation. The long-term benefits of Industry 5.0 align with its core principles, such as attracting and retaining talent, achieving energy savings, and enhancing overall resilience. These advantages help businesses stay competitive and relevant by adapting effectively to a changing world and emerging markets [24]. In conclusion, technology should be tailored to meet workers' needs, enhancing their abilities and contributions to industrial processes. New software tools offer valuable insights to improve manufacturing efficiency and promote sustainable production. AI-powered soft sensors can help reduce the over-consumption of raw materials and energy by providing real-time information on product quality, enabling smarter decision making in production [19,26,30].

Based on previous considerations, this manuscript offers an overview of all the applications of IoT systems in the industrial field, discussing the different approaches proposed in the literature and the obtained results. Specifically, the analysis of four macro-topics is proposed (Figure 2):

- Safety: The safety background is analyzed by extending the concept to the two fundamental areas of Industry 4.0, considering safety in the workplace by safeguarding the health of the operator and cybersecurity to prevent cyber-attacks.
- Predictive maintenance: The various IoT approaches adopted to minimize maintenance costs are discussed, eliminating unwanted downtime and ensuring longer machine life.
- Process control: the study of IoT techniques to control an industrial process and prevent divergences or failures.
- Additive manufacturing: IoT applications combined with the production of artifacts through the 3D-printing process are addressed.

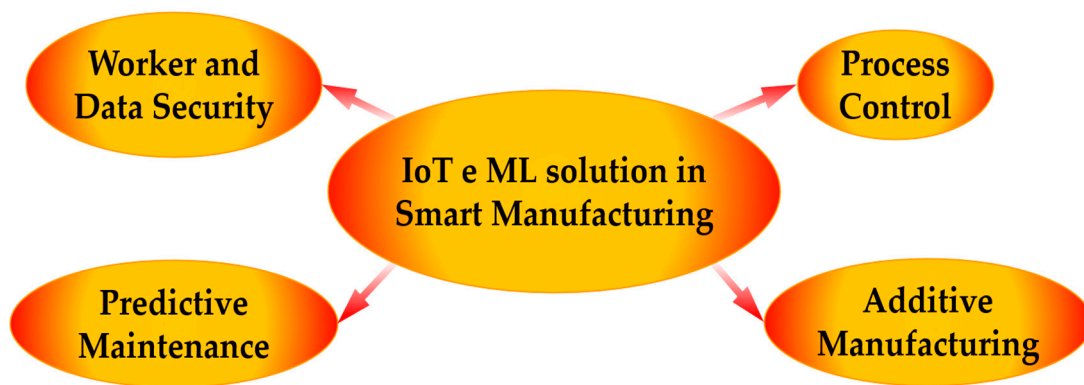


Figure 2. Overview of the manuscript's treated topics.

Also, to support the scientific value of this research work, each section includes the following information:

- A comparative analysis of the analyzed works is reported, and each research work's main features and strengths are compared to the others;
- An overview table is provided, and the main characteristics of each work addressed in this review paper are defined.

This review paper is divided into several sections as follows. In Section 1, after introducing the discussed topics, the selection method of the scientific articles analyzed in the review is reported. In particular, the systematic selection of articles related to machine learning and IoT-based solutions in smart manufacturing is performed by adopting the PRISMA methodology. Section 2 presents an overview and a comparison of ML algorithms adopted mainly in smart manufacturing fields. Section 3 analyzes security in the field of smart manufacturing, considering both operator safety and cybersecurity for data protection. Section 4 discusses predictive maintenance by analyzing the IoT technologies used to predict and plan targeted maintenance interventions, eliminating unwanted machine downtime. In Section 5, the various IoT approaches for process control, adopted to predict the drifts of the production process, are analyzed. In Section 6, the most recent IoT technologies in the field of AM are discussed. Finally, in Section 7, comments and conclusions are reported. At the end of each section, the study is summarized through a summary table indicating the main elements that make up the IoT application adopted by the authors, together with a comparative analysis highlighting the strengths and weaknesses.

Selection Method of Analyzed Articles Based on PRISMA Methodologies

Before starting the discussion, defining the criteria used to select and exclude the most appropriate scientific articles is necessary. The adopted criteria are explicitly defined, considering many elements of the documents analyzed, such as applicability to the topics covered, relevance, publication year, and redundancy with other articles. This paper aims to offer the reader the broadest vision of IoT's current state of the art in smart manufacturing. The systematic selection of articles related to ML and IoT-based solutions in the smart manufacturing field is performed by adopting the PRISMA methodology, enabling readers to evaluate the reliability and applicability of the selected method [31,32]. The selection process begins with an evaluation of the title to see if it contains references to the topics to be covered in this manuscript; it continues with an analysis of the abstract to see if the content is close to the issues to be covered; finally, we proceed to read and comprehend the manuscript under investigation. If the manuscript is unclear, the content is explored using other sources. The flowchart in Figure 3 illustrates the document selection process with the following steps: the title's relevance, the abstract's affinity, and the interest documents' overall content. Furthermore, this document selection methodology is applied to all the topics of this review paper.

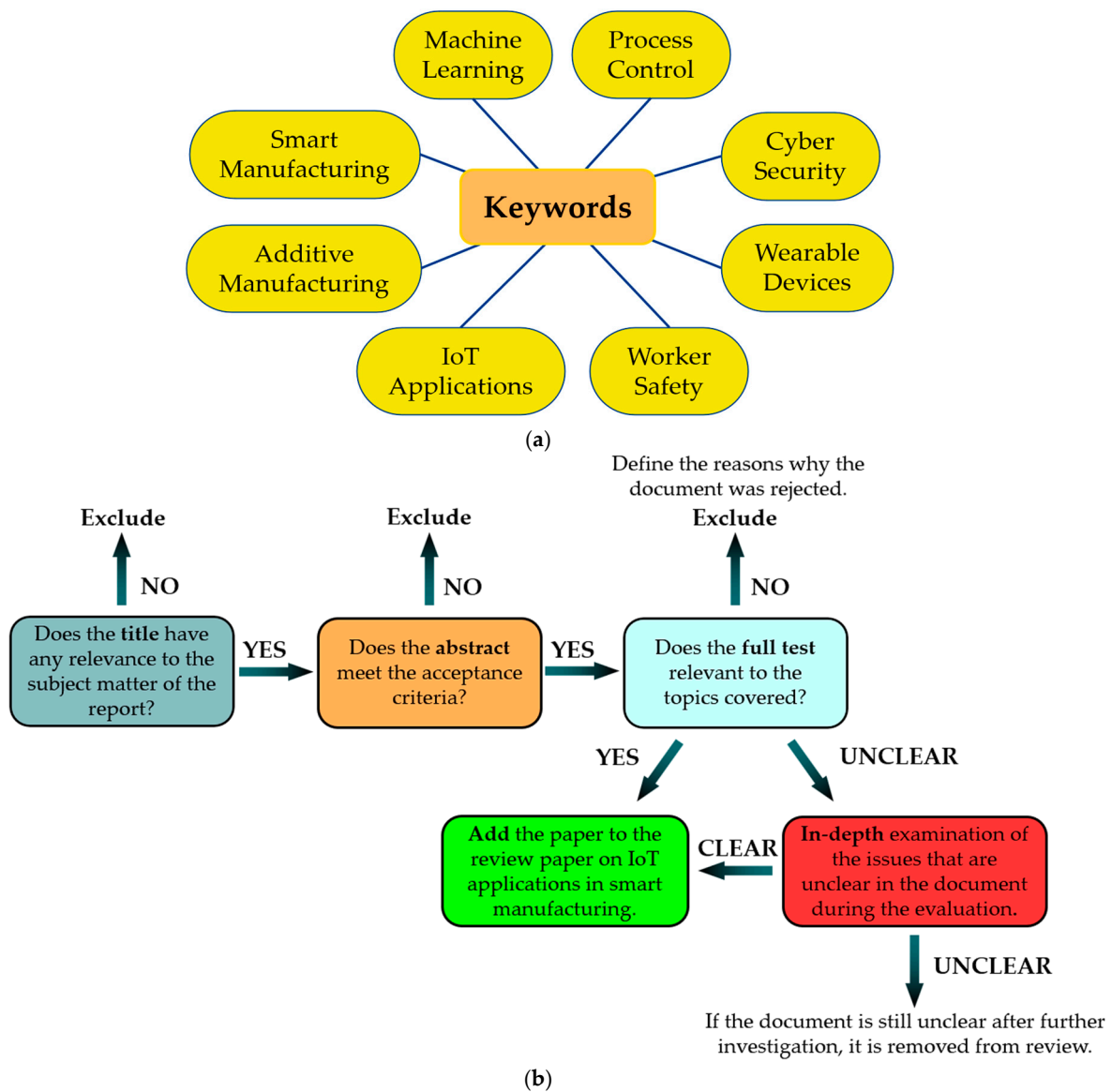


Figure 3. Document selection method; (a) main keywords to filter the documents present in the literature; (b) description of articles selecting method with topics related to the presented review paper.

For an accurate analysis of smart manufacturing based on IoT applications in the fields mentioned above, the authors have analyzed 135 documents, divided into review papers, conference articles, research articles, and web sites. The main sources from which the articles were acquired are Elsevier, MDPI, IEEE, and Springer, with a small number of articles from other sources. The diagrams shown in Figure 4 highlight the distribution of the acquisition sources (Figure 4a) and the distribution of the types of articles analyzed (Figure 4b).

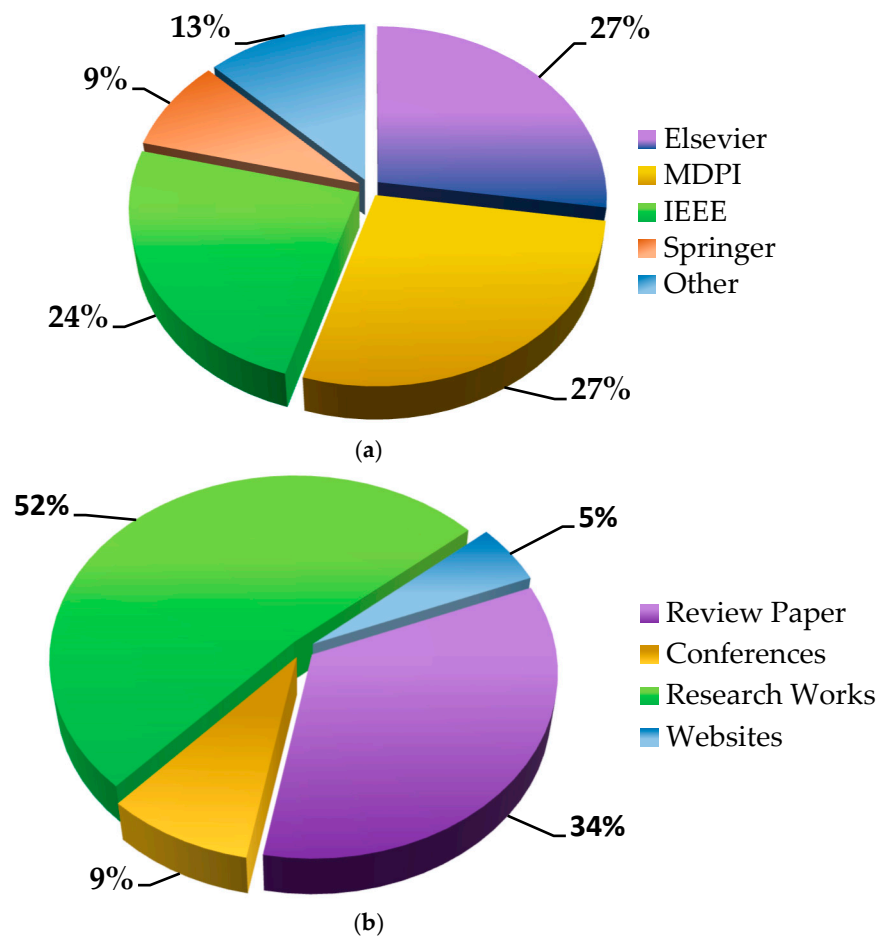


Figure 4. Diagrams related to the publishers of identified documents (a) and scientific articles' typology (b).

2. Description and Comparison of Machine Learning Algorithms for Data Processing in Smart Manufacturing

This section provides an overview of ML algorithms for data processing adopted in smart manufacturing, trying to report the main ML algorithms used by the authors. The selection of documents used to create this section was based on the search for articles and reviews that are mainly concerned with the topic of ML.

Smart manufacturing is augmenting physical science with modern data analytics to improve decision making and system performance. As sensors and the IoT become more widely used, the need for large amounts of industrial data, rapid processing, and the ability to handle a wide variety of data becomes increasingly necessary [33].

Incorporating ML in manufacturing helps to increase efficiency and improve production operations. ML is a smart manufacturing technology that uses production data to improve industrial facilities' machine performance. ML is a subfield of artificial intelligence (AI) that uses statistical techniques to let computer systems learn from data without explicit programming. Numerous tasks, including prediction, classification, clustering, and optimization, may be carried out using machine learning [34]. ML programs identify focus areas in the production process to collect data and provide actionable insights for improvements. The program then provides algorithms with the data required to enable learning. Once this process is initiated, machines can continuously learn and improve processes independently without direct programming from human workers. By utilizing the data collected by machine learning programs, manufacturers can make more informed production decisions to drive improvement and business growth [34].

In many smart manufacturing contexts, the use of ML algorithms has contributed notable advantages, such as the possibility of automating some processes that would normally require human intervention. For example, PdM combats maintenance schedules that are not always accurate by using ML algorithms to identify a potential problem before a failure occurs [35]. Inspection, monitoring, and process control are other areas where ML has had considerable success, acquiring information from cameras and sensors and promoting accurate and rapid inspection of parts.

The ML algorithms are classified into four different types: supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning (Figure 5) [36].

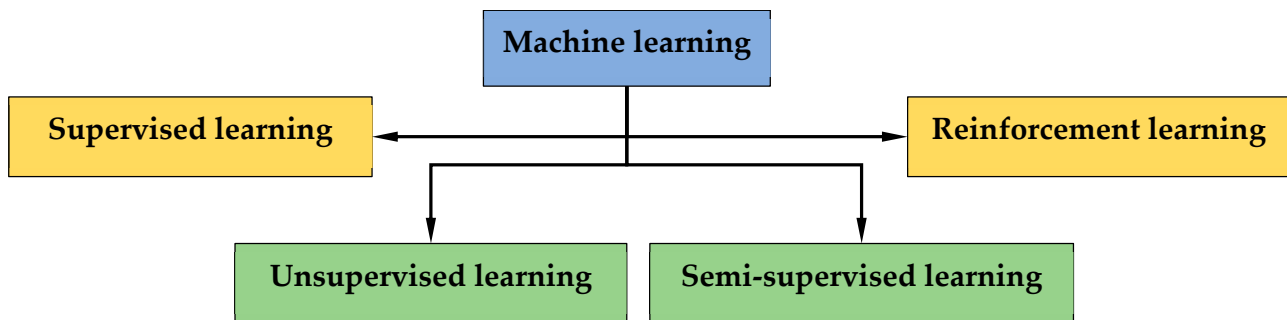


Figure 5. Classification of the machine learning algorithms.

- **Supervised learning:** This algorithm trains itself using a labeled dataset where each input datum corresponds to a well-defined output. By looking at these labeled examples, the algorithm can transfer the input attributes to the intended output [37–39]. The classification is to classify or enumerate the data into predetermined classes or categories. Generally, the output is a discrete value representing a class or a category. Supervised MLs include classification and regression algorithms. Classification algorithms predict a result as a discrete value indicating the object’s membership in a specific class. Regression algorithms, on the other hand, differ from classification in that the results are expressed through continuous values. This classification of machine learning algorithms includes regression algorithms, logistic regression, Naïve Bayes, K-nearest neighbors (KNN), decision trees, random forest, and XGBoost [40–44].
- **Unsupervised learning:** This is the process of extracting patterns or structures from data without knowing the outcome. The method is used for an unlabeled data collection to learn an input representation that captures the underlying data structure. Unsupervised learning is divided into clustering, dimensionality reduction, density estimation, and anomaly detection [38,45]. Clustering is grouping similar data points based on specific characteristics or similarities. Dimensionality-reduction techniques aim to reduce the number of features in a dataset while preserving important information. Density estimation involves estimating the probability density function of a dataset. Anomaly detection identifies data points that deviate significantly from expected or normal behavior [46]. Examples of unsupervised learning algorithms are the stacked auto-encoder algorithm (SAE) [47], k-means, k-medoids, and fuzzy c-means [38].
- **Semi-supervised learning:** Semi-supervised learning combines supervised and unsupervised learning methods, using labeled and unlabeled data to improve model performance [38]. The main categories of this approach are as follows:
 - **Self-training:** an algorithm that trains a model on labeled data, then uses the model to label unlabeled instances, integrating them into the labeled dataset and repeating the process.
 - **Graph-based methods:** Data points are represented as nodes in a graph, propagating labels through it to label unlabeled nodes.

- Co-training: Multiple models are trained on different subsets of the data, exchanging labels for unlabeled instances.
 - Multi-view learning: Data are analyzed from different perspectives, and models work together to optimize overall performance.
- Reinforcement learning: This type of ML consists of training an agent through the feedback obtained from its responses on the application environment [38]. This agent is assigned rewards and penalties for the activities performed to define a policy that allows the maximum reward to be assigned [43].

ML is a process by which a computer system is trained to make accurate predictions using new data. Training, learning, and evaluation are the three basic steps in building an ML model. The model's accuracy depends on the quality of the initial data and the algorithm's performance. The first step is to acquire input and output data, i.e., features (input) and labels (output). The second data step is to train the model using the data from the previous step. In the third step, the performance is evaluated once the algorithm training is completed. For this performance evaluation, loss functions are used to observe how much the predicted value diverges from the real value. Two loss functions are used mainly: the mean absolute error (MAE) and the mean square error (MSE) [48]. Figure 6 schematically shows the operating phases of an ML algorithm.

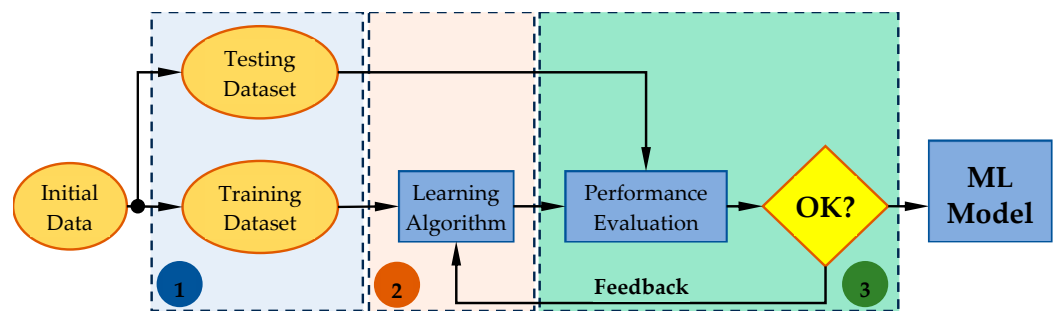


Figure 6. Operating scheme of a machine learning algorithm. The first phase involves acquiring testing and training data, followed by the algorithm training phase, and finally, evaluating the algorithm's performance.

The main ML algorithms used in smart manufacturing are described as follows:

- ✓ Regression algorithms: These predict a numerical value based on other input variables. They are used in many predictive analytics applications, such as stock price forecasting in finance, weather forecasting, and market demand assessment. Linear regression is the simplest type, as it aims to predict a numerical value based on a single input variable. The algorithm generates a line representing the relationship between the input variable and the predicted numerical value.
- ✓ Logistic regression: This is more complex than the linear variant and is used to predict the value of a binary variable based on other input variables [49]. The algorithm generates an "S" curve that describes the probability of the output value based on the input variable. Among the possible applications, for example, is that logistic regression can predict if a patient will develop a disease based on documented risk factors (input data).
- ✓ Naïve Bayes: This is an algorithm based on Bayes' theorem, which assumes that the presence or absence of a particular feature in a document is not related to the presence or absence of other features [49]. The operation of the Naïve Bayes algorithm is based on estimating the conditional probabilities of the independent variables given the dependent variables. Simple and fast to execute, this algorithm can, however, suffer from accuracy problems.
- ✓ K-nearest neighbors (KNN): This is a classification algorithm based on the characteristics of objects close to the one being classified [49]. In other words, the KNN

algorithm classifies an object based on its proximity to other known objects. The operation of the KNN algorithm is based on the estimation of the distance between the characteristics of the object to be classified and those of the objects already known to the system. The KNN algorithm, therefore, uses the k objects closest to the object to be classified to determine its class. The choice of the value of k is made through various heuristic techniques.

- ✓ Decision tree algorithm: This is a graphical representation of a set of decision rules and their consequences [49]. Each internal node of the tree represents a variable, while each arc starting from an internal node represents a possible value for that variable. Finally, each leaf of the tree represents the predicted value for the target variable, starting from the values of the other properties. Decision trees are also used in more complex algorithms involving their combination.
- ✓ Random forest: This is a supervised learning algorithm that uses an ensemble technique to improve the accuracy and stability of the model [44]. It is used for classification and regression problems to predict a numerical value or a class based on one or more input variables. The operation of the random forest algorithm involves creating a set of decision trees, each of which is trained on a random subset of the data. This model generates a native independence between the trees, which results in a series of uncorrelated predictions, except in the final combination. The random forest algorithm is appreciated for its accuracy and flexibility, to the point that it is widespread in many fields, such as image classification, medical diagnosis, and fraud detection.
- ✓ XGBoost: This is a boosting algorithm commonly used for classification and regression problems. In particular, XGBoost is an advanced form of gradient boosting that improves efficiency and predictive performance through optimizations, such as missing data handling and regularization [44].
- ✓ Support vector machine: This is a supervised learning method used primarily for classification problems, but it can also be adapted for regression. SVM can classify unlabeled data by using a hyperplane to identify data clustering. The output of SVM is not, however, nonlinearly separable. When using SVM in data analysis, choosing the right kernel and parameters is essential for resolving such issues [44,49].

Another subcategory of AI is deep learning (DL), which uses deep neural networks to handle complex types of data [49]. Unlike traditional ML techniques, DL uses complex neural network architectures, often with many layers, to extract features and representations from data [33]. The main differences between DP and ML methods are based on three different levels: feature learning, model building, and model training. In traditional ML, in-depth knowledge of the observed phenomenon is necessary because the features are extracted manually, while DL features are learned from the model. Traditional methods use the extracted features for model construction to build a data-based model. In contrast, in the case of DP, a highly hierarchical end-to-end model structure is generated with a non-linear combination of multiple layers. Finally, regarding model training, the traditional ML methods train the parameters step by step; instead, DL models train all the parameters involved simultaneously [33]. Among the DL algorithms, the most used are as follows:

- Convolutional neural networks (CNNs) are widely used as tools for image classification thanks to the shape extraction process [50];
- Recurrent neural networks (RNNs) are generally used for speech recognition because they use sequential or time-series data. In particular, they are mainly used when it is necessary to make predictions about future outcomes, and they have a significant capacity for learning nonlinear features and processing time-sequence data [51].

Table 1 reports the main algorithms used in the various areas of smart manufacturing, highlighting the main applications, characteristics, advantages, and limitations to facilitate the choice of the most appropriate one depending on the application. For each AI algorithm, the main use in the field of safety, PdM, and process control is also reported.

Table 1. ML and DP algorithm used in smart manufacturing for security, predictive maintenance, and process control.

AI Algorithm	Security		Predictive Maintenance	Process Control	Characteristics
	Worker Security	Cybersecurity			
Decision Trees	Used for workers’ diagnosis, disease classification, and treatment decisions	For classification and anomaly detection	Used to identify failure conditions based on decision criteria	Used to classify or predict outcomes; interpretable and easy to visualize	Easy to interpret and visualize; tend to overfit and are unstable
Random Forests	Used for workers’ disease classification and complex data processing	For the classification and management of complex and non-linear databases	Used to improve forecast accuracy and reduce the risk of overfitting	Used to enhance the robustness and accuracy of forecasts	More robust and precise than decision trees but require more time and computational resources for processing
SVM	Used for medical image classification and diagnosis	Perform malware classifications and detections	Used to classify machine operating states and predict failures based on historical data	Used for classification and regression; particularly effective in high-dimensional spaces	Very effective in high-dimensional spaces; require a good choice of parameters and are sensitive to noise in the data
KNN	Used for workers’ disease classification and identification of similar patients	Used to recognize suspicious activities	Used to identify anomalies in operating data	Non-parametric method that classifies data based on their nearest neighbors in the dataset	Simple to implement and intuitive in its operating logic, but computationally expensive for large datasets
CNN	Used for analyzing medical images, such as MRIs and X-rays	For image analysis and network analysis at a more advanced level.	Used to analyze thermal or visual images	-	Particularly effective for processing grid-structured data; they require large datasets to be trained effectively and are susceptible to overfitting
ANN	Used for predicting clinical outcomes and diagnoses based on complex data	-	Used to model non-linear relationships in data and are useful for failure prediction	-	They are versatile and can model complex nonlinear relationships; they require significant data pre-processing and may require a long training phase
Recurrent Neural Networks (RNN) and LSTM	Used for analyzing time sequences, such as patient data tracked over time	-	Used for time-series analysis; can capture long-term dependencies in operating data	Time-prediction algorithms, useful for predicting sequential data in processes	RNNs work well with sequential and temporal data but can have problems with long sequences and are more difficult to train than other algorithms; LSTMs solve the sparse gradient problem and require considerable computational resources

3. Overview of IoT System Security Applications in the Industrial Field

Safety has always been fundamental for industries and companies to protect operators and machines. With the advent of digitalization, which has opened new frontiers and opportunities, safety (now called cybersecurity) has taken on a new role: preventing cyber-attacks. Therefore, the introduction of the IoT has enabled the creation of different approaches to operator safety and cybersecurity [15].

With the introduction of the IoT, security in the industrial sector is divided into two macro areas: one for monitoring operator health and safety (industrial safety management, ISM) and the other for data privacy and protection. As part of IoT-based solutions, ISM is a crucial area with many development opportunities, especially regarding human safety. However, increasing industrial productivity and product quality is highly dependent on safety. The operators will be affected psychologically and physically if an accident occurs at work because of a safety procedure violation [52]. It also damages industry equipment and infrastructure, disrupting production. As consequence, workers lose confidence in their equipment and, at the same time, company owners suffer financial losses due to lost production time and industrial efficiency. As a result, companies stand to lose a lot from any violation's type of industrial safety regulations and standard operating procedures (SOPs) (Figure 7) [52].



Figure 7. IoT for security applications in the industrial field: worker safety.

Mobile technology advancements bring more intelligent and connected objects into our daily lives. The IoT is a movement that is becoming crucial to the networking and communications industry. However, weak security defaults, inconsistent communication and protocol standards, and update delivery issues have worsened cybersecurity threats to critical IoT equipment. Putting a heavy focus on securing the IoT devices in an intrusion detection system is a workable approach to lower risks and thwart these attacks [53].

X. Zhan et al. propose a clever system framework, highlighted in Figure 8, which uses digital twin (DT) and IoT technologies to achieve the real-time monitoring of workplace safety in the warehouse and ensure cyber–physical space synchronization for information traceability and visibility [54]. In this work, the authors have created an IoT-based workplace safety monitoring system (SOSMS) to find anomalous stationarity in cold rooms and acquire workers' spatiotemporal information in real time to help managers get a remote overall picture of the safety of personnel. The stacked auto-encoder (SAE) has an unsupervised deep neural structure intended to detect abnormal steady states in human movement, which may indicate an impending accident. The model's automated online updating mechanism is designed to work with calibration standards to keep up with the environment's changing state. Moreover, cyber–physical visibility and spatiotemporal traceability are improved by DT technology, which replicates actual things in cyberspace, enabling managers to implement emergency protocols and security monitoring efficiently.

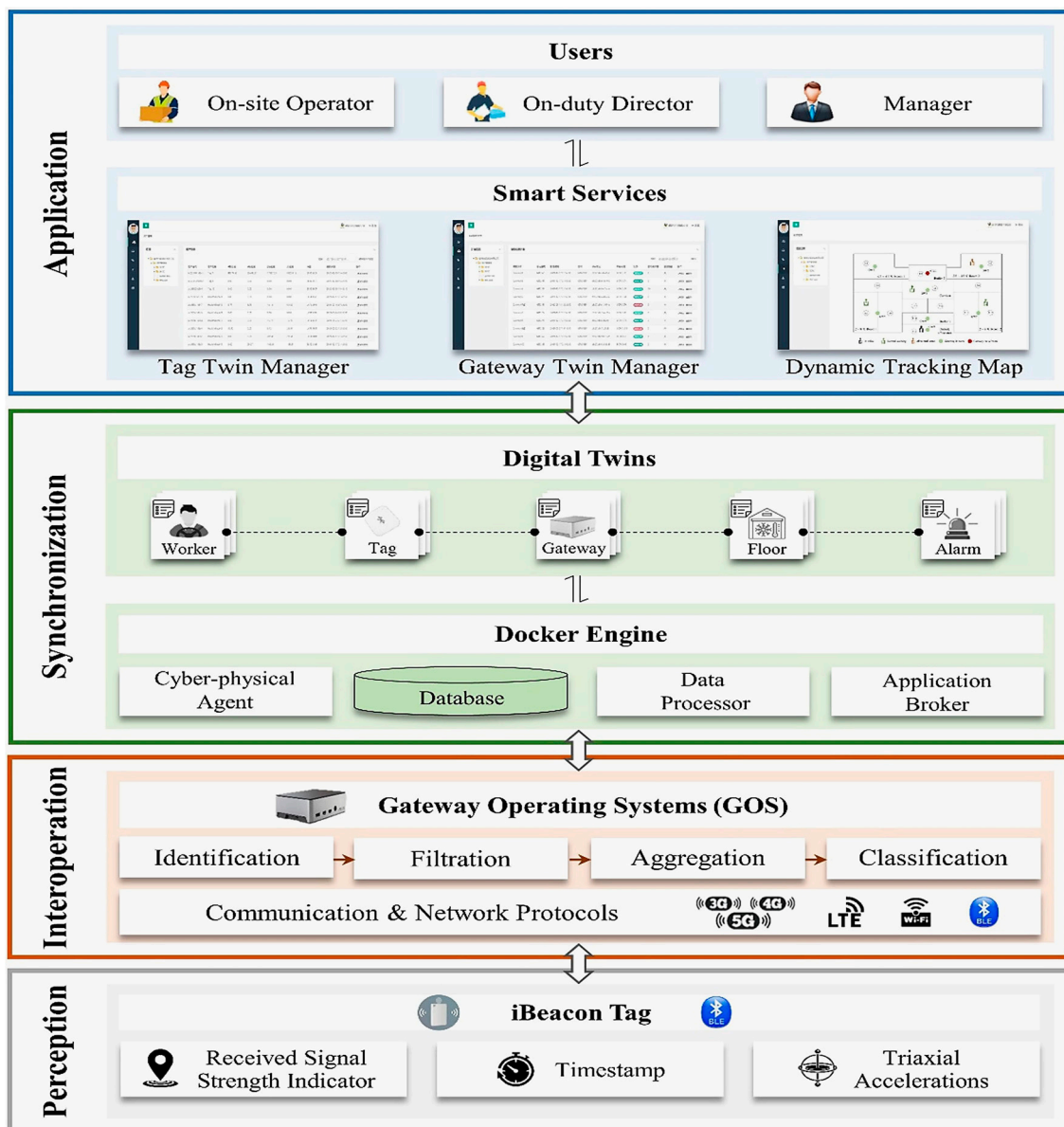


Figure 8. The overview of the smart occupational safety monitoring system [53].

For operator safety monitoring, Zhang et al. also addressed monitoring workers during mining operations [55]. They built an industrial IoT-enhanced intelligent crowd detection system for crowd monitoring for coal mine safety. Firstly, they proposed a particle swarm optimization–Elman neural network (PE) algorithm to predict the moving human pose. Secondly, they developed an ADI–LSTM algorithm, an absolute degree of incidence (ADI) and a long short-term memory (LSTM) neural network. Based on IoT-enhanced intelligent crowd detection that can predict the position of a moving human body and the pressure value exerted by machinery during mining through the pressure acting on the bearings, they evaluated the interaction between machines, people, and the environment to determine whether they were in a dangerous area. Similarly, in [56], the authors introduce geofencing technology to implement a digital boundary around selected geographic locations; this last can be based on several technologies, like the global positioning system (GPS) or radio frequency identification (RFID) [57], enabling the implementation of several strategies, such as zone-based safety alert, equipment safety, emergency response, site-access control, etc. Geofencing technology can improve worker security, area-based alerts, and activity monitoring within the framework of the construction

industry. Also, Lelitha K. et al. developed a helmet as a protective device to improve miners' health management and prevent injuries [58]. The STM32 module uses multiple sensors to continuously analyze, i.e., the environment's temperature, humidity, and toxic gases. It also constantly analyzes the operator's health, including heart rate and vibrations from blasting and excavation. Next, a Bluetooth Low Energy (BLE) module transmits the data to the control center. Their proposed device also has an anti-panic button that alerts the control unit in the event of an emergency for the operator. They also installed a helmet camera to monitor and recognize the operator's gestures; they used the Advanced RISC Machine (ARM) Cortex-M platform and the TensorFlow Lite microframework to execute Python programs. The safety of mine workers is not the only area where the IoT has contributed to numerous innovations; in the construction sector, the IoT has allowed other different solutions to improve the safety of the construction worker.

In the literature, there are other studies in which the concept of smart technology has been widely integrated into the design of wearable applications [59]. For workers operating in dangerous environments, smart vests were created to be worn for their greater safety. The vest monitors the environmental and biophysical parameters (heart rate, temperature, etc.); it is also able to self-power by storing energy from movements (piezoelectric transducers), from the sun, and thermoelectric generators [60]. In the event of an alarm, the information is sent to a cloud database and then consulted via a web app. For this reason, K. M. Mehata et al. have developed a helmet and smart band by implementing different sensors that monitor the safety and health of workers using heart rate sensors, temperature sensors, accelerometers, and IR sensors to track the vital parameters of the operator [61]. The authors have used mobile phones for communication and data exchange, which quickly send SMSs through the Global System Mobile (GSM) module to inform the assigned personnel about any incidents. The technology also uses an algorithm associated with an accelerometer that allows predicting the fall of the operator. Similarly, the authors in [62] developed a creative plan for an independent system that monitors, locates, and alerts construction site workers in dangerous areas with IoT-based construction vehicles [63]. Their technology combines three techniques, directional antennas, 40 kHz ultrasonic waves, and 868 MHz radio frequency, to locate and identify construction workers precisely. A collection of parts comprises the wearable device's design: a General Packet Radio Service (GPRS) module, an activation sensor, an alert actuator, and a radio transceiver (transmitter/receiver). The wearable gadget has a low-power consumption power-saving strategy that prolongs battery life by keeping it in deep sleep mode until a radio frequency (RF) field is detected. In Figure 9, the architecture chosen by the authors is shown.

To monitor the health of construction workers, J. H. Kim et al. also realized an IoT-based platform using a smart band ready-to-use wearable [64]. The created platform is intended for builders who work in high temperatures. It consists of two elements: the overall heat assessment (OHS) and the personal management system (PMS), the latter of which uses fuzzy theory to assess each worker's health risk level [65]. At the same time, the former organizes breaks for teams of workers based on a thermal comfort index (TCI). A microcontroller unit (MCU) incorporated in the device houses two modules (LoRa and GPS), three sensors (accelerometer, skin temperature, and PPG), and a power source. Furthermore, authorized staff may use a PC or smartphone to locate a construction worker's position and current state and make any required choices from a distance [66].

The work carried out by Márquez-Sánchez et al. in [67] combines the use of three items of PPE, a helmet, a bracelet, and a belt that can acquire biophysical and environmental parameters. The data are then processed through algorithms by a deep convolutional neural network (DCNN). Similarly, Bontempi et al. in [68] have developed a new concept of PPE, in particular, gloves that integrate commercial devices, such as an energy collection system, a UHF-RFID tag for information exchange, and a microcontroller for the recognition of the correct use of the PPE. The exchange of information is performed by the EPCglobal Class-1 Generation-2 communication protocol.

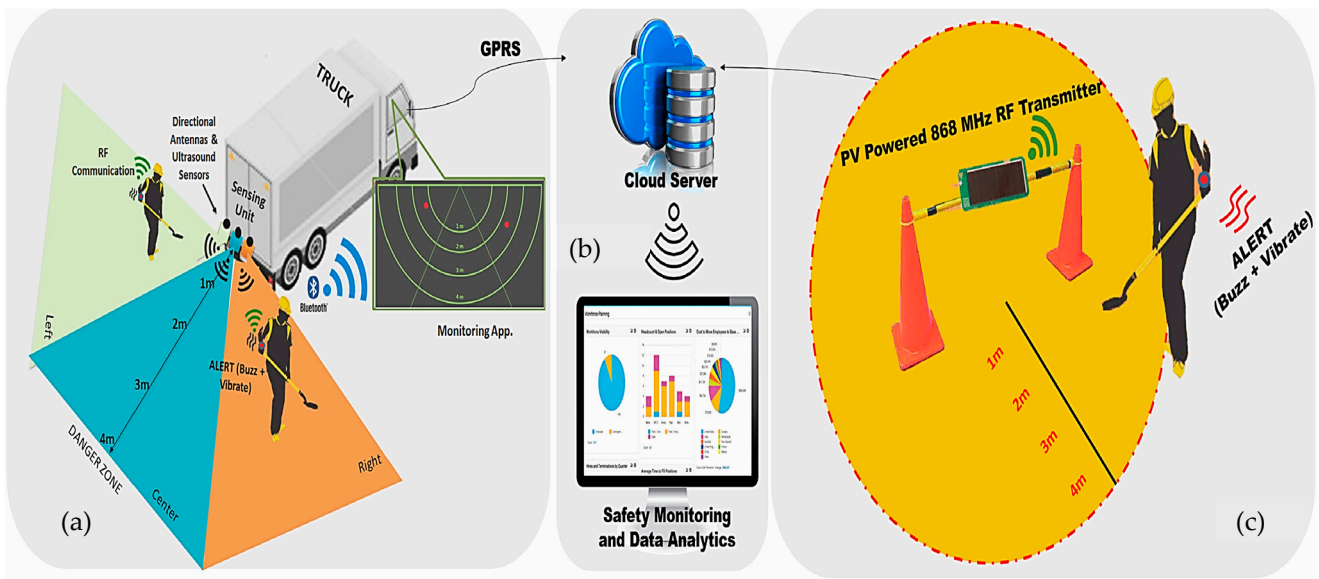


Figure 9. Overall representation of the IoT architecture, proposed by the authors in [62]; (a) reversing accident prevention; (b) intelligent warnings to avoid potential dangers; (c) IoT middleware platform.

With the advancement of technology and the inventiveness of researchers, the concept of smart has not only been applied to jackets but has also been extended to T-shirts, as shown in Figure 10. All sensing devices integrated into the shirt for monitoring biological parameters are powered by a 380 mAh battery, which is recharged through sunlight, temperature, and the body movements of the operator who wears it. Furthermore, gas detection sensors can detect the concentrations of carbon dioxide, oxygen, formaldehyde, and hydrogen sulfide in the environment in which the worker operates [69,70].

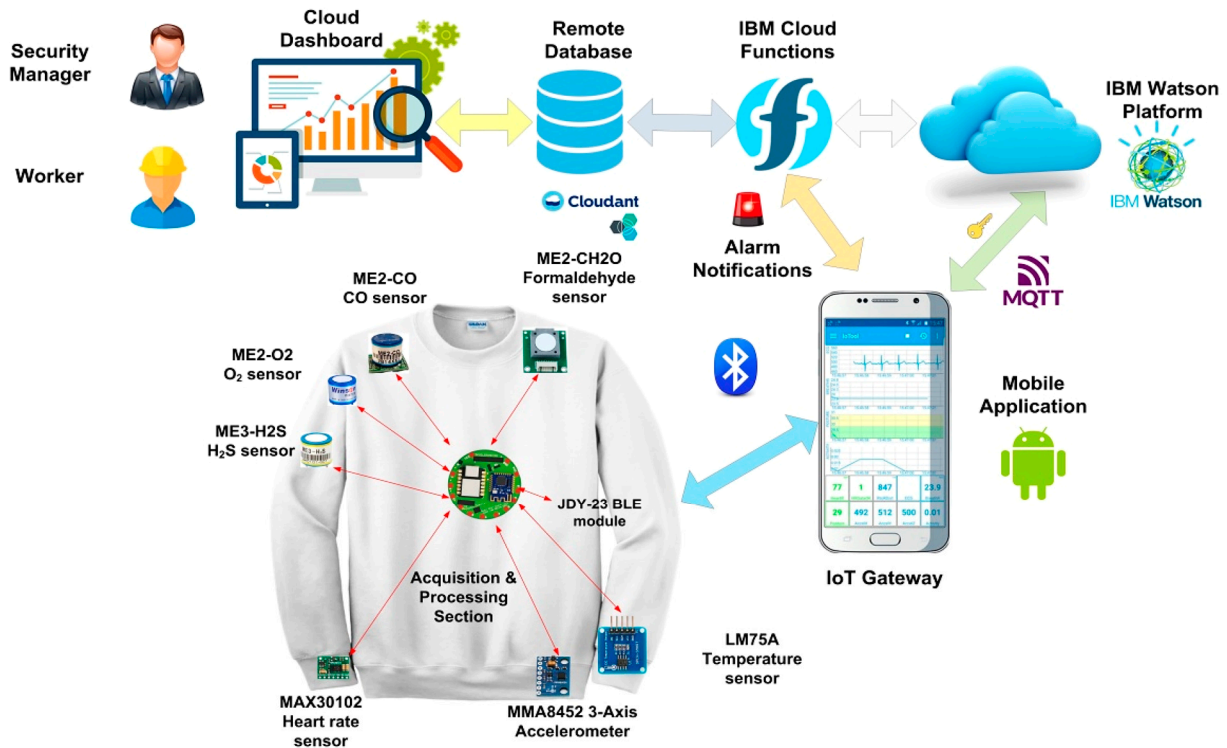


Figure 10. Schematic of the IoT paradigm applied to a smart shirt, highlighting all the sensing devices and the transfer and visualization scheme of the data collected during the worker’s operations [69,70].

Finally, IoT systems have been able to contribute to worker safety in the agriculture industry as well. For this purpose, Montanaro et al. in Ref. [71] propose a modular design to determine worker locations, machines, and obstacles to ensure the safety of the path of remote-controlled farm machines (RCFM) using specific notifications for timely interventions of workers on the ground. Figure 11 shows the main features and positioning functionalities based on passive ultra high frequency–radio frequency identification (UHF-RFID) technology supported by commercial BLE beacons to monitor and prevent accidents that may occur when workers are on the ground. UHF-RFID tags were applied on PPE, such as helmets and jackets, obtaining the best configuration with all four tags positioned vertically [14]. The worker position is obtained with triangulation through the received signal strength indicator (RSSI) obtained from the Beacon devices deployed in the field.

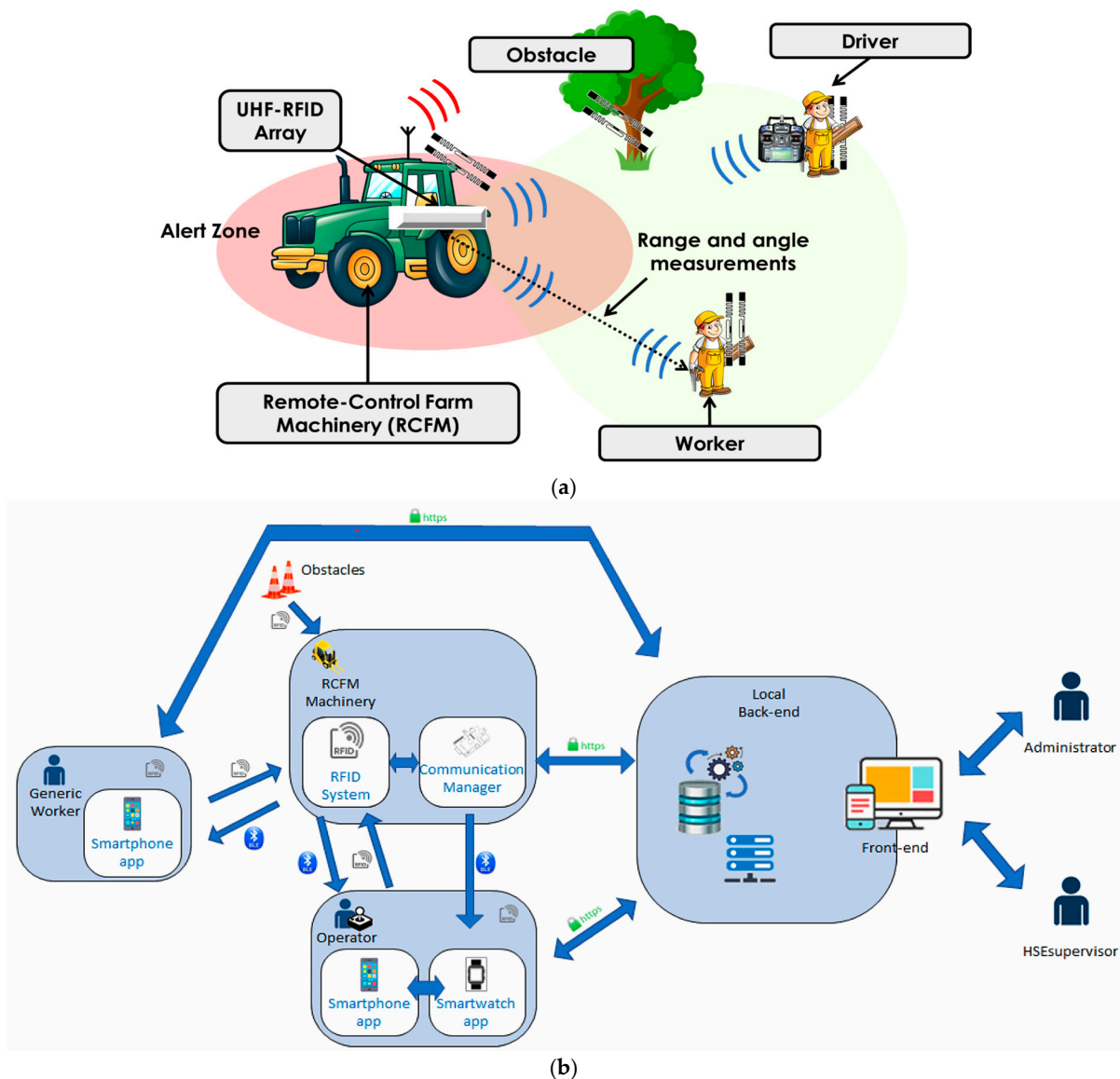


Figure 11. Architecture (a) and functional block diagram (b) of the monitoring system of worker security in the agricultural fields proposed in [71].

Another way to monitor worker safety is to verify that the operator is wearing PPE, presenting a new evolution of security strategies. For this reason, Gallo et al. used a deep learning approach to video streaming analysis with YOLOv4. In their case, when

an operator is not wearing PPE, an acoustic or light signal is emitted [72]. The important aspect is that the streaming video is directly analyzed by the device placed in the area.

As said before, the advent of digitalization and the increase in cyber threats have given a strong incentive to the need to protect information and data, that is, cybersecurity, which has become a fundamental asset for companies. Cybersecurity encompasses many practices and strategies to protect data confidentiality, integrity, and availability. It is not just about adopting advanced technologies but also involves a change of mindset in risk management and operator training. Today, it is imperative that the actors operating in the industries understand the importance of cybersecurity as an integral part of their daily operations, creating a more secure and resilient environment against ever-evolving cyber threats (Figure 12).

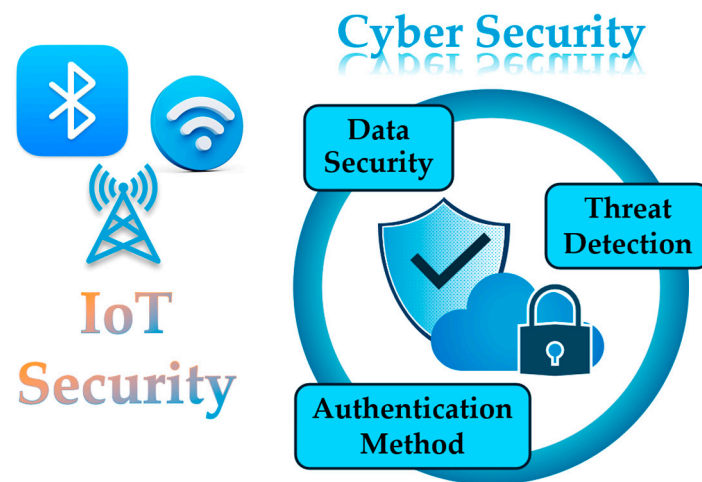


Figure 12. Characteristics aspects of cybersecurity.

To strengthen cybersecurity, Abuhasel et al. use upgraded Rivest–Shamir–Adelman (RSA) and hash signatures to increase the data security of IoT devices [73]. The prime number of the suggested RSA algorithm is 512 bits. A hash signature is used for device authentication. An effective clustering method based on node degree, distance to cluster, residual energy, and fitness (NDRF) is suggested for sensor devices with lengthy network lifetimes. The Salp Swarm Algorithm (SSA) is implemented to determine the fitness of sensor nodes. Resource scheduling utilizing the SoftMax Deep Neural Network (DNN) is proposed to lower latency and communication overhead for IoT devices. SoftMax-DNN classifies all cluster head requests to determine the optimal resource scheduling based on processing, storage, and bandwidth needs. The suggested structure performs better regarding latency, security strength, and energy usage [74].

On the other hand, in [75], Wadsworth et al. provided a method for putting safety measures on the IoT's CPS to safeguard the system's operations. They established a set of predetermined safety-critical parameter boundary criteria that allow a CPS to function safely for heating and cooling. Assume it is recommended that the CPS operate beyond these boundaries. If this happens, the system will immediately cut off all external communications networks and enter a safe operating mode that will remain in place until an administrator evaluates the system locally and removes it from the safe mode. An IoT testbed and sample CPS that monitors and regulates a target environment's temperature were set up to test and verify this technique. It is also important to be able to classify and identify hazards; Moradbeikie et al., with the introduction of IoT in industrial control systems (ICS), managed to differentiate risks by using information from many IoT environmental sensors [76]. With the help of the IoT, they suggest a risk management strategy that recognizes risks based on the physical characteristics of these systems. Four types of dangers have been identified: random assault, stealth attack, temporary failure, and permanent failure. To control the risks in the system, risk management consists of three

main components, risk detection, risk analysis, and system reconfiguration, based on the data that sensors have collected from the real world.

Peserico et al. discussed the difficulties of maintaining working safety networks and protocols in IoT ecosystems [77]. First, the adoption of security protocols on wireless networks and the design aspects of functional safety networks are analyzed. In particular, Fail Safety over Ether-CAT (FSOE) is discussed, and the results of an extensive test session with a prototype system built with commercial WiFi-based devices are also provided.

In e-healthcare, IoT-based solutions use medical sensors to record, preserve, analyze, and capture patients' day-to-day activities in real-time. These solutions allow for managing massive amounts of data at a low cost via scalable cloud-enabled storage through analytics platforms. Patients' private information is in danger when records are exchanged on centralized server-based platforms during the transition.

Blockchain is a new generation of safe data technology that is revolutionizing business and industry [78]. In this regard, Khan et al. in [79] presented an innovative and secure architecture for the security of e-healthcare data using a distributed ledger technology based on a blockchain known as BloMT. Additionally, they created a distributed tiered hierarchy for medical wireless sensor networks (WSNs) to manage and optimize data. This structure improves the network resources, and fosters trust in the peer-to-peer (P2P) environment enabled by blockchain technology. Lastly, the BHIIoT (blockchain for industrial Internet of Things) safeguards shared resources in blocks kept in an unchangeable blockchain archive by using the NuCypher threshold re-encryption process. Industry 4.0 introduces additional security risks beyond conventional industrial networks due to the integration of operating technology (OT) and IT infrastructures. Defense-in-depth (DiD) tactics provide many levels of protection, each focusing on a distinct set of menaces to address the complexity of this issue. Given that data pass through intermediate entities, or middleboxes, before achieving their purpose, Mosteiro-Sanchez et al. in [80] propose a combination of DiD, a lightweight end-to-end (E2E) encryption algorithm called attribute-based encryption (ABE), and object security (e.g., OSCORE) to achieve a comprehensive E2E security method. If middleboxes are compromised, vulnerable information could be exposed to prospective hackers if not encrypted along this path. Figure 13 shows how the three security zones are divided.

The absence of a threat database is one of the many obstacles that still need to be overcome to use a universal approach for threat modeling in smart manufacturing systems. Consequently, to close this gap and save time and effort, AbuEmera et al. created a rule-based threat database and component catalog to handle potential security concerns in smart manufacturing systems [81]. They perform STRIDE (a spoofing, tampering, repudiation, and information disclosure model that focuses on identifying potential risks in each system component) based threat modeling against a smart factory use case using Microsoft Threat Modeling Tool. First, their data flow model of the development process refers to the ENISA high-level model based on the Purdue model; Figure 14 illustrates the levels that make up the model. The model comprises production machines, sensing devices, control devices (HMI and PLC panels), data processing and visualization software, and cloud servers.

Hammad M. et al. improved what was previously called flexible manufacturing system (FMS) by defining a new paradigm, the IoT-enabled system, overcoming the previous limitations of the FMS, such as high initial costs, obsolete technology, integration complex in the system, and long setup times [82]. IoT-enabled systems allow the analysis of valuable data continuously gathered from several sources across the industrial ecosystem. This approach improves decision making, PdM, process optimization, and energy efficiency. In fact, by facilitating secure communication in an IoT-enabled system representing the smart manufacturing sector, these solutions provide a unique method of mutual authentication among the FMS unit, users, and server. Session keys are established to accomplish this security. Outperforming prior schemes, the authors in [82] devised a technique that displays strong resilience against numerous security assaults. Its considerable security benefits outweigh the minor increase in communication overhead compared to various baseline methods. First, they suggest a plan that permits key agreement and mutual au-

thentication to strengthen the security of the smart manufacturing sector. The proposal states that the server will provide mutual authentication among users and the FMS unit and between the user and the server. During this process, session keys are formed via the FMS unit, the server, and the user. A physical unclonable function (PUF) is used with bitwise XOR operations, elliptic curve cryptography (ECC), and cryptographic hash functions to mitigate resource restrictions and defend against physical tampering attacks in IoT contexts. Alrowais et al. developed a tool capable of classifying cyber threats through AI tools, introducing MFO-RELM [83]. It combines advanced optimization techniques and machine learning algorithms to tackle complex problems. Wu et al. proposed a system that consists of hybrid routers and an IoT gateway [84]. In addition to supporting BLE and long-range (LoRa) wireless protocols, the router has a solar energy harvester to increase its lifespan. LoRa wireless technology may expand the reach of short-range BLE networks and facilitate essential edge computing functions like initial data processing. However, Mrabet et al. propose a five-layer architecture that incorporates blockchain technology (BCT) to capture sensor access control information and machine learning (ML) to detect cyberattacks [85]. The performance of their architecture was based on the use of some metrics such as accuracy, precision, sensitivity, and correlation coefficient (CMM), employing different machine learning algorithms such as artificial neural network (ANN), decision tree (DT), random forest, Naive Bayes, AdaBoost, and support vector machine (SVM). Kim et al. in [86] propose a threat detection system based on edge computing by transferring a large amount of data to servers processed by deep learning algorithms such as CNN to make a smart factory less vulnerable to malware attacks.

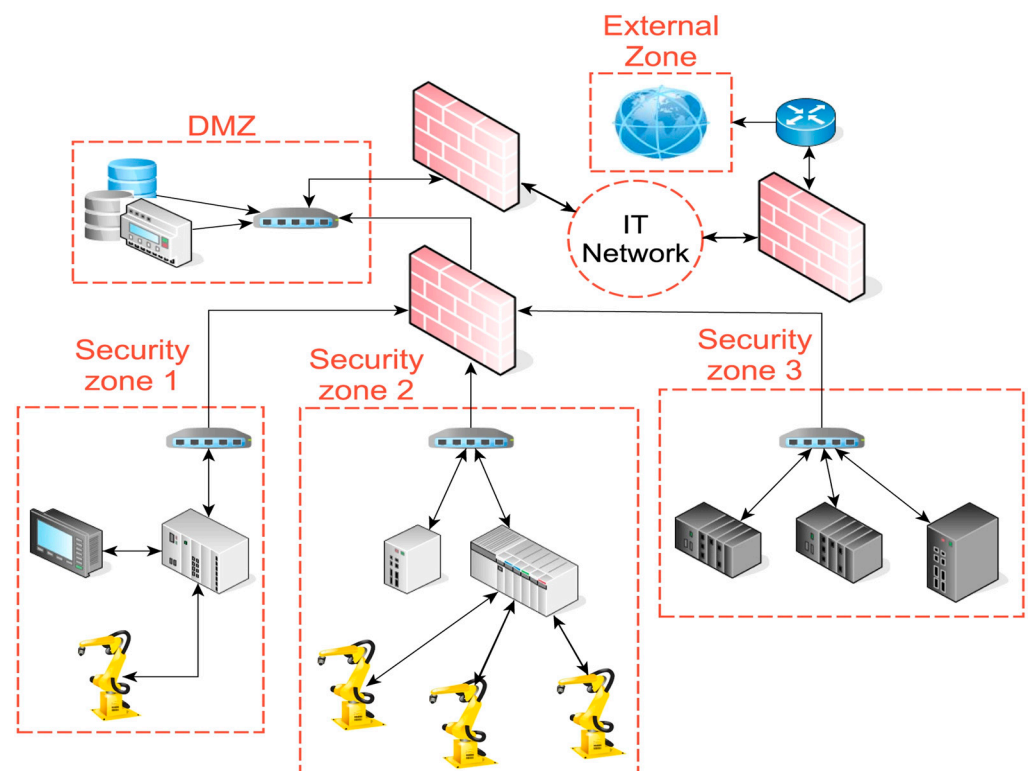


Figure 13. OT network segmentation with three security zones and a DMZ separated by firewalls proposed by Mosteiro-Sanchez et al. in [80].

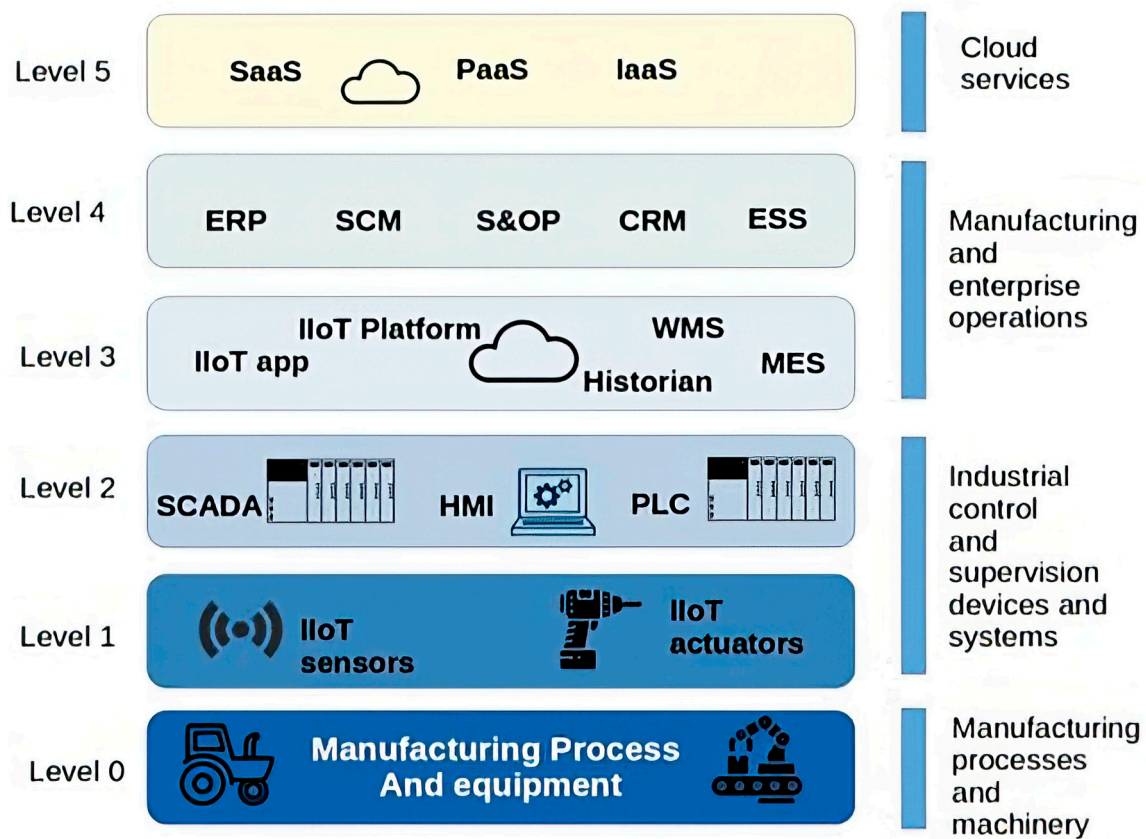


Figure 14. Representation of the ENISA IIoT high-level reference model adopted by AbuEmera et al. in [81].

3.1. Comparative Analysis in the Case of Worker Safety

The analysis carried out on the IoT paradigm of safety in smart manufacturing has highlighted the innovative aspects that have significantly improved, on the one hand, the worker’s safety during the performance of his activities and, on the other, the data protection from cyber-attacks. In the context of operator protection, many authors have set themselves the objective of verifying physiological parameters such as PPG, accelerometer, body temperature, and position. This last parameter is of fundamental importance as it makes it possible to check anomalous stops made by the operator in high-risk areas of the industrial plant and dialogue with the machines assisting the operator to prevent accidents. This communication is made possible thanks to short- and long-range wireless communication protocols such as BLE, LoRa, WiFi, and GSM platforms that are available via mobile phones. All the data detected by the sensors are then processed by specific algorithms specifically designed by the authors and already known in the literature. All this information is finally sent to a supervisor who monitors the worker’s health status and presence in dangerous areas. In particular, this technology prevents workers from staying at high temperatures for long periods in the construction sector.

An extremely important real-world application in the case of worker safety is related to the health of workers exposed to high temperatures [64,87–89]. As extreme weather worsens due to the climate crisis, increasing heat waves will severely affect workers exposed to high temperatures. To function properly, the human body must regulate its temperature within a narrow range since prolonged heat exposure can lead to heat-related illnesses, including heat cramps, exhaustion, and life-threatening heatstroke. Rising core body temperatures also diminish work capacity, causing discomfort, fatigue, and impaired judgment, which can result in workplace errors and collapses [90]. To address these dangers, companies are seeking innovative solutions to protect their workers. Environmental monitoring

has traditionally been used to prevent heat stress, but advancements in physiological monitoring, supported by IoT-based technology, now allow for real-time, personalized safety measures. This shift from a one-size-fits-all approach to a worker-centric model enhances both health and productivity in extreme conditions.

One concrete application is the SlateSafety BAND V2 [91]. It uses a photoplethysmography (PPG) sensor to monitor heart rate by detecting changes in blood volume through light reflectance on the skin. It, along with other sensors' data, represents the foundation for SlateSafety's metrics, including real-time heart rate, body temperature, and exertion levels [91]. The core temperature algorithm, proven accurate in a peer-reviewed study from the University of Alabama, helps protect workers from heat-related illnesses by reliably monitoring key physiological indicators [92]. Moreover, this band ensures data protection through industry-standard protocols and allows organizations to customize biometric alert thresholds. Its connectivity options, including built-in cellular connectivity and the SlateSafety GATEWAY V2 for areas with limited service, make it highly versatile. The SlateSafety GO mobile app allows local data access even in areas without cell connectivity or power. If connectivity is temporarily unavailable, the device stores data and safety algorithms, which can be uploaded later for historical analysis [91].

Another real-world application has been proposed by Kenzen company [93]. Kenzen offers smart PPE with wearable technology and proprietary algorithms to provide real-time insights to workers, supervisors, and Environmental Health and Safety (EHS) decision-makers [94]. A wearable device worn on the upper arm monitors a worker's physiological responses to heat in real-time. Kenzen also factors in personal details like height, weight, age, medical history, and environmental conditions to assess each worker's risk of heat-related issues, calculating their individual heat susceptibility for more tailored safety measures. Heat susceptibility refers to an individual's sensitivity to heat, which increases their risk for heat-related injuries or illnesses. Workers can be categorized as low, moderate, or high risk. Machine learning algorithms can detect, adapt to, and notify EHS managers of site-specific changes that may not be easily noticeable daily. Moreover, they can monitor vulnerable workers more closely during extreme heat and adjust workloads based on each person's risk level [94]. Recently, Garney Construction, a leading water and wastewater contractor, used these insights to help managers create customized safety procedures for their worksites across the U.S. [95].

To compare the different solutions proposed in the literature, Table 2 highlights the main characteristics of the IoT platforms used for monitoring workers' health in a synthetic way. The table presents five main elements, among which are the IoT entity or the object or the set of elements that contribute to creating the smart platform, the communication technology (therefore, the basis with which all the elements interconnect for the exchange of data), the recipient of the IoT device, the algorithm used by the authors for the processing of the data previously acquired, and finally, the cost–benefits and implementations.

Table 2. Comparative analysis of references previously discussed related to the IoT-based workers' safety applications.

Reference	IoT Entity	Communication Technologies	Detected/Inferred Quantity	Detection Algorithm	Cost–Benefits and Implementations
X. Zhan et al. [54]	Sensor node	BLE	Worker stationary time	SAE	Plug-and-play system, cost-effective fashion
J. Zhang et al. [55]	Sensor node with camera	N.A.	Machine trajectory and applied pressure	Swarm optimization–Elman neural network (PE.) ADI-LSTM	Challenging to fulfil global performance optimization standards
K. Lelitha et al. [58]	Helmets for mining workers	BLE	Hand gestures and environmental parameters	Python code and ARM Cortex-M	Low cost, rapid implementation of smart PPE

Table 2. Cont.

Reference	IoT Entity	Communication Technologies	Detected/Inferred Quantity	Detection Algorithm	Cost-Benefits and Implementations
K. M. Mehata et al. [61]	Smart band helmet	GSM	Body temperature, heart rate, and posture	Algorithm proposed by the authors	Low-cost smart PPE and easy implementation
R. Kanan et al. [62]	Wearable band	GPRS	Worker position with respect to the vehicle	Algorithm proposed by the authors	Reduces the risk of accidents on construction sites with low investment and operating costs
J. H. Kim et al. [64]	Smart band	GPS, LoRa	PPG, body temperature, and position	Fuzzy logic	Effective platform to monitor a worker's physiological data
Márquez-Sánchez et al. [67]	Smart PPE	WiFi, MQTT	Biophysical and environmental parameters	DCNN	Significant investment for companies with excellent security benefits
T. Montanaro et al. [71]	PPE with UHF-RFID	BLE	Worker or obstacle position	Position algorithm	Low implementation costs but with limitations in the application of RFID tags for better effectiveness
A. Bontempi et al. [68]	PPE with UHF-RFID	EPCglobal Class-1 Generation-2	Appropriate PPE usage	N.A.	Low-cost technology and easy to implement on other PPE
Gallo et al. [72]	Sensor node with camera	N.A.	Monitoring that operators wear PPE	Deep learning YOLOv4	High performance at moderate cost of application

N.A.: Not Available.

3.2. Comparative Analysis Referred to Cybersecurity

Cybersecurity is a complex challenge, given the high interconnectedness and increasing number of devices. The solutions presented highlight the importance of holistic approaches integrating cryptography, risk management, and robust security protocols to protect industrial systems from growing cyber threats. Each initiative contributes to building a more secure and trusted ecosystem, which is essential for the future evolution of IoT technologies. Security in IoT devices is crucial; millions of devices are connected and vulnerable to attacks. Security initiatives in IoT ecosystems, innovations in data security, and approaches to new paradigms are recent strategies studied in the previously analyzed articles, aiming to ensure data security and system reliability:

- Security Initiatives in IoT Ecosystems: 512-bit RSA and firm hash algorithms are used to protect IoT data. This approach is combined with effective clustering methods based on parameters such as node degree, distance, residual energy, and fitness, with the Salp Swarm Algorithm (SSA) used to determine suitability in the context of the sensor network. In some cases, for security in CPSs, they put the system into safe mode when boundary criteria are exceeded, resulting in a rapid response to critical solutions. Risk management is an essential aspect. It is possible to proactively address emerging threats by managing risk in three phases: detection, analysis, and reconfiguration. Finally, a further initiative to ensure cybersecurity concerns the importance of security protocols in wireless networks.
- Innovations in Data Security: One innovation in data security is blockchain, which ensures that data is stored securely by strengthening trust in the peer-to-peer system. Also innovative is the implementation of deep protection combined with an encryption algorithm to ensure end-to-end security, particularly important context given that data can pass through vulnerable entities.

- New Paradigm Approaches: Two new cybersecurity paradigms are IIoT-enabled flexible systems and hybrid edge Computing routers. First, using techniques such as mutual authentication and key agreement, the new approach overcomes the limitations of previous technologies that improve data analysis and operational efficiency. The second combines hybrid routing and IoT gateways using technologies such as BLE and LoRa to extend the reach of networks while facilitating data processing in edge devices.

Figure 15 briefly outlines these different strategies and technologies.

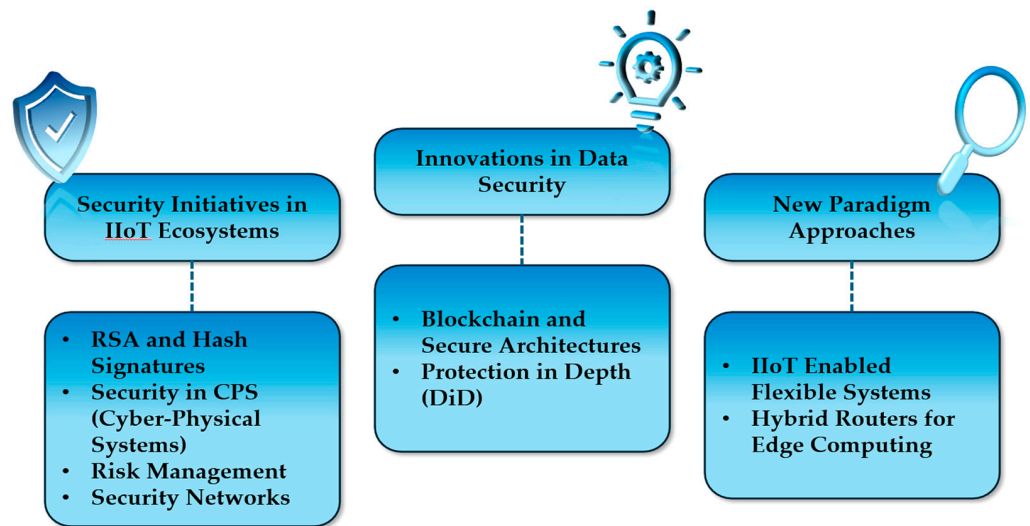


Figure 15. Summary of comparative analysis of IoT approaches in cybersecurity.

Table 3 summarizes the characteristics of the IoT paradigm proposed by the authors about cybersecurity to protect acquired data. In addition to the entity of the IoT platform and the communication technology, the application scope, i.e., whether it concerns data security, threat detection, or authentication methods. Any data decryption algorithms and ML algorithms used for data processing are also highlighted.

Table 3. Comparative analysis of references previously discussed related to IoT-based data security applications.

Reference	IoT Entity	Communication Technologies	Application	Crypting Algorithm	Detection Algorithm
K. A. Abuhasel et al. [73]	IoT Framework (IoT sensing devices, gateways, and fog services nodes)	LoRa, ZigBee, Sigfox, WiFi, Bluetooth	Data security	RSA	SoftMax-DNN
A. Wadsworth et al. [75]	IoT platform (Raspberry Pi 3b)	Ethernet	Threat detection	Security protocol block (SPB)	N.A.
A. Moradbeikie [76]	IoT field and control layers	N.A.	Threat detection	N.A.	Fuzzy clustering
G. Peserico et al. [77]	Secure master and slave (Raspberry Pi)	WiFi network	Data security	FSoE	N.A.

Table 3. Cont.

Reference	IoT Entity	Communication Technologies	Application	Crypting Algorithm	Detection Algorithm
A.A.Khan et al. [79]	Healthcare IIoT devices	N.A.	Data security	NuCypher threshold re-encryption (BHIoT)	N.A.
A.Mosteiro-Sanchez et al. [80]	OT devices	Profibus, Profinet, Ethernet/IP or EtherCAT	Data security	ABE	N.A.
E.A. AbuEmera et al. [81]	SCADA systems	WAN	Threat detection	N.A.	STRIDE-based threat model
M. Hammad et al. [82]	FMS unit	WiFi network	Authentication method	Custom encryption strategy (ECC + XOR bitwise + PUF)	DY thread model
F. Wu et al. [84]	IoT gateway (Raspberry Pi3 B+) Router (nRF52840)	BLE and LoRa	Data security	AES 128-b	N.A.
H. Mrabet et al. [85]	Cyber-physical system (CPS)	BLE, Ethernet, LoRA, WiFi, Zigbee	Threat detection	N.A.	ANN, decision tree, random forest, Naive Bayes, AdaBoost, SVM
H. Kim et al. [86]	Cyber-physical system (CPS)	BLE, Ethernet, LoRA, WiFi, Zigbee	Threat detection	N.A.	CNN

N.A.: Not Available.

Differently from Table 2, an additional column (column 5) relating to the decryption algorithms used to convert encrypted data into their original readable format has been added. The decryption algorithm is a fundamental process that ensures data security during transfer. During the analysis of the various research papers reported in this section, it was possible to observe that different AI algorithms were used; in fact, it is possible to come across supervised learning algorithms, unsupervised learning algorithms, and deep learning algorithms.

4. IoT Overview for Predictive Maintenance in Smart Manufacturing

Companies are changing drastically in the smart manufacturing age as a result of the integration of IoT and digital technology. Before the advent of Industry 4.0, safety was the main priority, with the goal of shielding machinery and personnel from dangers and mishaps. However, attention has steadily turned to PM techniques, which maximize operational effectiveness while guaranteeing safety. Predictive maintenance relies on real-time data analysis, allowing companies to predict failures and malfunctions rather than react to them. This approach improves the reliability and efficiency of production processes and reduces operating costs and downtime, significantly increasing productivity. These benefits are briefly highlighted in Figure 16. In particular, many companies have adopted PdM techniques [96]. This approach improves resource management and scheduling PdM interventions, preventing unplanned and expensive machine downtime. Intelligent manufacturing and maintenance are now the focus of Industry 4.0 due to the rapid growth of human civilization from the information age to the smart automation era. The pressing need to detect upcoming breakdowns and reduce unplanned downtime of industrial equipment might be met by data-driven intelligent predictive maintenance (IPdM); it is considered a vital component of the IoT in the future [97].

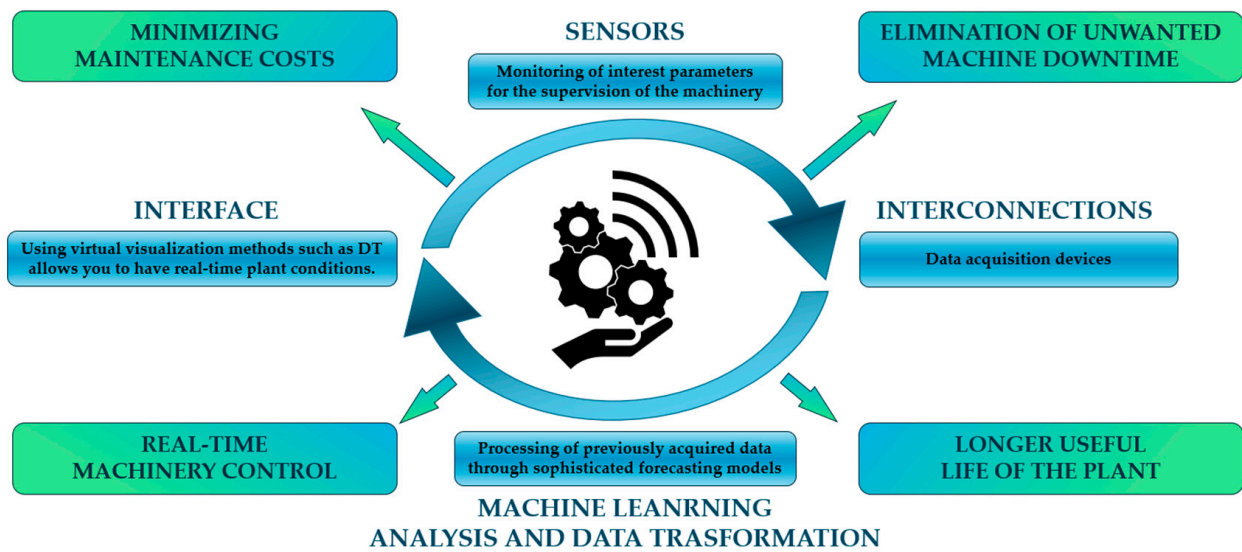


Figure 16. Schematic representation of the features and advantages introduced by the PdM.

Technologies used for predictive maintenance include sensors to monitor the operating status of components, data analysis algorithms to identify trends and anomalies in tracking data, and decision support systems to plan maintenance interventions efficiently.

Predictive maintenance is widely used in high-criticality industries such as manufacturing, aviation, and energy, where system safety and reliability are paramount. This approach reduces maintenance costs, improves system availability, and extends their useful life. Companies adopting smart manufacturing techniques have a competitive advantage as they can bring higher profit margins, reduced maintenance costs, power savings, and high-quality products [98]. In popular PdM procedures, a standard maintenance approach is often implemented for the same defect without considering the machine’s life cycle. When the same problem occurs at different life cycle stages, using the same maintenance method will inevitably lead to over- or under-maintenance. Furthermore, most PdM studies analyze maintenance choices or predict failures [7].

To provide predictive maintenance of a plant, Chen et al. in [99] adopted an IoT architecture by using smart sensors to monitor the operating status of centrifugal pumps in real time to predict possible failures and intervene before a component failure occurs, thus increasing the level of intelligence of the machine. Figure 17 shows the architecture proposed in Ref. [99]. They started by looking into the typical centrifugal pump failure and the features of the vibration signals that arise after a failure. The authors’ system comprises cloud servers, data collectors, and wireless and wired sensors. The wireless sensors are linked to a collector with sophisticated data communication features and are outfitted with 4G, WiFi, RJ45, RS485, and other data interfaces. The ARM (Advanced RISC Machine) CPU and LINUX operating systems are built within the collector processor. The test results showed that the sensors could recognize the signals produced by the centrifugal pump vibrations to automatically identify equipment faults.

Nangia et al. deduced a PdM approach with IoT sensors to help manufacturing industries predict machine failures before asset failure occurs [98]. Their work discusses a case study from the manufacturing industry where the solution is developed using ML’s binary classification support vector machine (SVM), classification and regression trees (C&RT), and boosted classification trees (BCT). In the first stage, they identified the organization’s critical assets; then, they obtained data from IoT sensors positioned on the machines, which are kept in cloud or database storage. The raw data are pre-processed in the third stage to generate higher prediction reliability and accuracy. The data are split into training and test data in the next stage. In the fifth stage, the output is analyzed and evaluated based on the prediction accuracy of the ML algorithms. In the final stage, the

model is deployed to the company. To create the PdM model, supervised machine learning algorithms were applied. During the operational phase of a plant, all the sensors involved in monitoring record data, and in this regard, Fordal et al. examined the combined use of value chain and maintenance data to enhance value chain performance via forecasting [100]. The chosen strategy comprises theoretical and practical experiments that provide a fresh idea for an ANN model with sensor data inputs and a PdM platform. Their work aims to monitor the correct functioning of the wood-splitting saw in a woodworking company. Their solution monitors the blade temperature, blade tensioning wheels temperature, and vibrations because, with the increase in productivity, the wood splitter is subjected to greater stresses than those designed for, and heating would compromise both the saw’s mechanical resistance and the product’s quality.

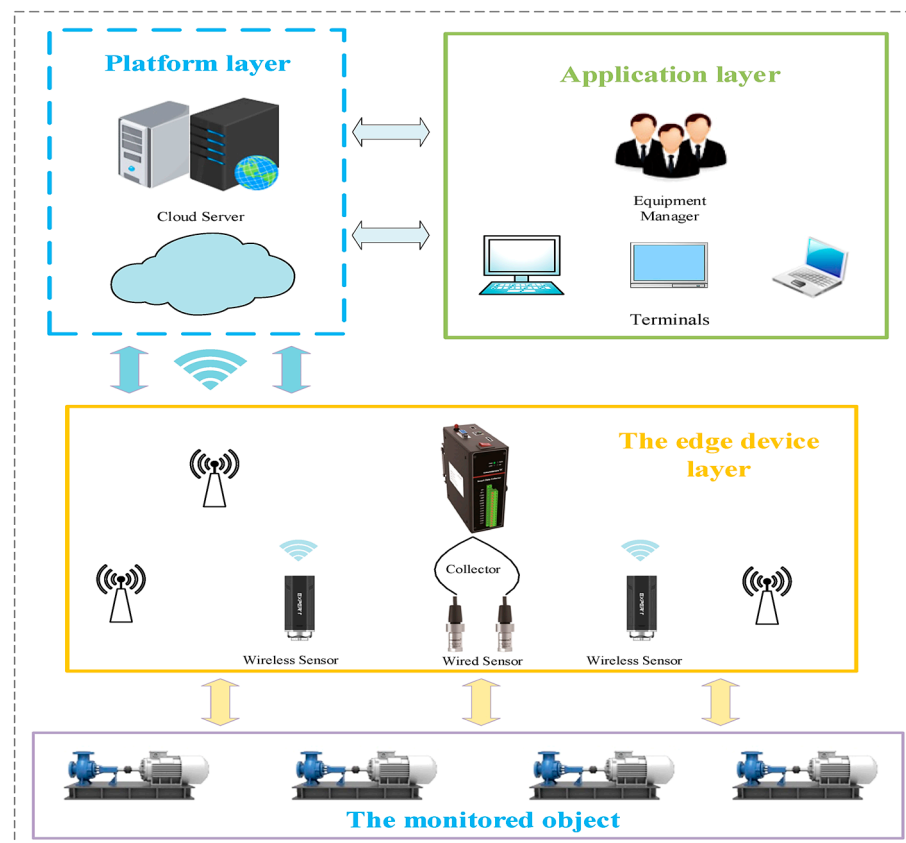


Figure 17. The architecture proposed by Chen et al. in [99] is divided into three layers. The machines under observation make up the first stratum. The edge device layer, which mainly comprises sensors and collectors, makes up the second layer. The Internet service platform, which consists of a cloud server and software operating on it, defines the third layer. The program occupies the final layer.

Ayvaz et al. developed a PdM system for production lines based on real-time data acquired from IoT sensors [101]. The system uses machine learning methods to identify signals of probable failures before they happen. The authors performed a comparative analysis between the XGBoost algorithm and random forest models, demonstrating that combining these two models produces better results than the individual algorithms. Figure 18 shows the architecture proposed by the authors of reference [101].

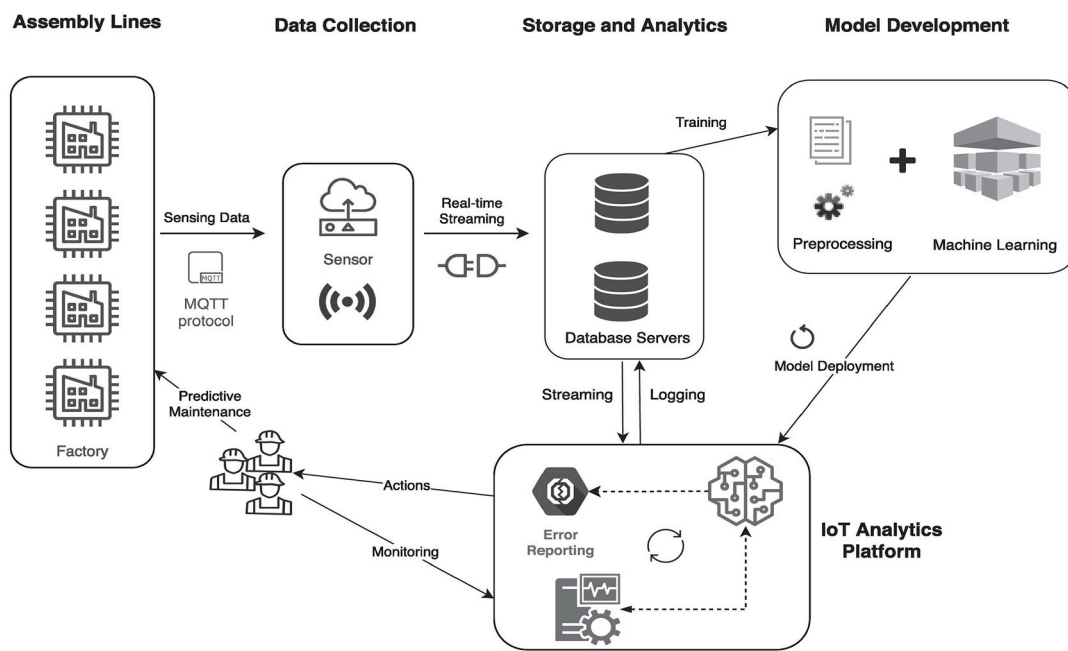


Figure 18. Architecture proposed in [101]. The data are acquired, sent to a cloud, and recorded in a database. The MQTT protocol converts all the collected data into a single type.

In order to identify priority areas and enable digital technologies for IoT deployment, predictive maintenance, remote examination, and data-management platforms, Gbadamosi et al. in [102] proposed a strategy for IoT implementation in railway asset maintenance by adopting a qualitative methodology through a series of focus group workshops. Note-taking, idea mapping, and audio re-recording were some data-collecting techniques used. Concept maps were incorporated for modeling and concept analysis, while audio recordings were transcribed and utilized for theme analysis.

Existing PdM studies typically concentrate on a predictive model without addressing maintenance decisions or optimization based on known system breakdown patterns. To address this issue, Sang et al. in [103] propose a predictive maintenance model for Industry 4.0 (PMMI 4.0), which uses a novel proposed solution PMS4MMC to support an optimized maintenance planning plan for multiple machine components driven by a data-driven long short-term memory (LSTM) model for RUL (remaining useful life) estimation [104], demonstrating the validity of their proposal through a real case study with related data. Most of the state-of-the-art ML approaches for PdM use various condition monitoring data such as vibration, current, temperature, etc., and failure data to predict the remaining useful life (RUL) of components; what is not monitored is the component wear and tear because it is not easy to identify. Rosati et al. [105] introduced and tested a decision support system (DSS) powered by IoT, big data, and machine learning (ML) to solve a PdM task involving advanced processing and measurement machines. Unlike others, their novel approach relies on a feature extraction strategy and an ML prediction model based on specific topics collected at the lower and upper levels of the manufacturing system. The IoT sensing technology is based on Message Queuing Telemetry Transport (MQTT [106]) [107]. After synchronizing, all the data is gathered and stored in an Azure Blob cloud storage account and a Structured Query Language (SQL) database. During each MCM production cycle, feature extraction is performed using trapezoidal numerical integration (TNI) to calculate a key performance indicator (KPI) for each processing parameter. Within the steel sector, Ruiz-Sarmiento et al. examine the implementation of a PdM paradigm on the equipment used in the hot rolling process, which produces steel sheets, while keeping an eye on the drum deterioration within the heating coils of Steckel rolling mills [108]. Based on a Bayesian filter, a machine learning technique, this machinery’s progressive deterioration

is estimated and predicted, enabling operators to make well-informed judgments about maintenance procedures.

Many storage companies adopt the cold chain to store particular products that require the control of environmental parameters such as temperature, humidity, barometric pressure, carbon dioxide (CO₂), and organic compounds. For this purpose, D. Mourtzi et al. have designed and created a framework for the remote monitoring of refrigeration and cold storage systems (RCSS) based on the implementation of a wireless sensor network (WSN) for data acquisition and intelligent algorithms for PdM of these plants [109]. The sensors are installed inside the cooling space of a refrigerator. More specifically, a WiFi XBee module has been used. The data are stored and processed by a set of algorithms developed as web services, constituting the WebSocket cloud platform [110]. F. Civerchi et al. developed the NGS-PlatOne system to achieve continuous and widespread industrial machinery monitoring via battery-powered IoT sensing devices inside a power plant [111]. Their proposed system performs temperature and vibration monitoring. The temperature and vibration control monitoring devices and all other monitoring devices arranged as a sensor node may abstract the variables under observation and events observed as resources offered via embedded web services. Consequently, a RESTful paradigm is made possible in the limited environment by allowing each resource to be handled via the CoAP protocol operating on 6LoWPAN. A simple vibration analysis is carried out in the accelerometer node by analyzing the root mean square (RMS) and peak-to-peak (P2P) characteristics throughout time periods on each axis. When these values are greater than the programmable thresholds, a failure event is signaled, and advanced algorithms that perform frequency domain analysis have not been implemented to process the accelerometer node data due to their complexity. The authors in [112] propose a novel approach for PdM. In particular, they propose a way to manage resources by integrating self-learning into genetic algorithm (GA)-based fog computing. In particular, the algorithm called Fogworkflowsim simulates GA's cost, energy, and time performance along with MaxMin, MinMin, RoundRobin, and FCFS [113]. Kudelina et al. propose a new ML approach based on the vibration signal spectrum for bearing failure prediction [35]. Their study compares the effectiveness of traditional NN algorithms with a new approach integrating fuzzy logic, achieving a prediction accuracy of 99.40%. Natanael et al. instead applied the concept of PM to a toothpaste filling plant by analyzing the information received from the onboard sensors, such as vibrations and temperature [114]. They used two different ML methods for data processing: random forest regression and linear regression. The authors also used the Arduino AT MEGA 2560 microcontroller for data acquisition.

Based on the considerations related to ML algorithms discussed in this section, it is possible to highlight the advantages and critical issues related to their use. For example, the C&RT algorithm, although easy to implement, is sensitive to imprecise data and subject to overfitting, an aspect surpassed by the random forest, even if slower and less interpretable. The boosted classification trees offer better performance and robustness but are more complex and difficult to implement. The SVM is effective in high-dimensional space but is not as interpretable as the ANN, which is suitable for modeling complex relationships. Instead, the DBF algorithm overcomes the problem of interpretability but is sensitive to unbalanced data. Although simple to implement, linear regression is sensitive to outliers and complex data. Finally, the fuzzy logic algorithm models uncertainty in a natural way because it better reflects the complexity and variability of the real world, which is useful for precise decisions but less used in traditional ML.

Comparative Analysis of Predictive Maintenance Applications

The following discussion shows the different methodologies employed in predictive maintenance in various industries, highlighting the integration of IoT and machine learning approaches to improve maintenance practices, reduce downtime, and optimize operational efficiency. Each study uniquely contributes to the evolving PdM landscape, offering frameworks, algorithms, and case studies highlighting this technological advancement.

The key points and contributions of the different field studies are summarized below, followed by the limitations that a PdM approach may entail.

Most studies exploit IoT technologies, smart sensors, and machine learning techniques, significantly improving the ability to monitor and predict machine failures in real-time by focusing on predictive maintenance. This proactive approach improves operational efficiency by reducing downtime and costs related to unscheduled maintenance. Integrating advanced data analysis techniques, such as SVM (support vector machine), random forest, XGBoost, and LSTM, improves the accuracy of failure predictions. Some studies, such as Fordal et al., show how integrating data from different sources (maintenance and value chain) can lead to significant performance improvements. The adoption of IoT and cloud architectures facilitates the expansion of such systems to various industries and applications, making them adaptable to different operational needs. Finally, creating models for predicting residual useful life and resource management promotes greater efficiency and the responsible use of materials.

On the other hand, integrating IoT systems and advanced algorithms can be complex and require specialized skills and a significant initial investment. In particular, many approaches and models have been developed for specific situations and may not be easily transferable to other applications or industries. Although many solutions are scalable in theory, in practice, there may be technical difficulties in managing and analyzing large volumes of data without considering that the quality of data collected by sensors can affect predictions. Issues such as noisy signals or faulty sensors can compromise the results. Furthermore, the costs associated with IoT monitoring systems and supporting technologies (e.g., cloud, big data analytics) can be burdensome for companies, especially small and medium-sized enterprises. Data collection and analysis at large scales can threaten privacy and security, making additional protection measures necessary, and predictive models, such as those based on LSTMs, may require an adequate amount of historical data to be effective, which can be a limitation in contexts with scarce or unreliable data.

In Table 4, a comparative analysis of the IoT paradigm related to predictive maintenance previously analyzed through some proposals found in the literature is illustrated synthetically. The comparative analysis is based on the nature of the monitored system, the communication technology for data exchange, the prediction algorithm used by the authors, and the performances obtained by them.

Table 4. Comparative evaluation of references previously discussed related to IoT-based predictive maintenance.

Reference	Monitored System	Monitored Parameters	Communication Technology	Prediction Algorithm	Performance	Cost–Benefits and Implementations
Nangia et al. [98]	Monitoring machine Failures	Temperature, humidity, pressure, current, vibration and other	Ethernet on IIoT cloud	C&RT BCT SVM	89.1% (C&RT) ^(A) 89.9% (BCT) ^(A) 89.3% (SVM) ^(A)	High performance, complex monitoring process, improved using cloud computing
Chen et al. [99]	Real-time operating status of centrifugal pumps	Vibrations signals	Wired and wireless technology (4G, WIFI)	N.A.	85% ^(A)	low-cost and easy-to-implement solution
Fordal et al. [100]	Splitting saw monitoring	Temperature, vibrations, and power usage	Ethernet on IIoT cloud	ANN	N.A.	Entry-level solution to enable I4.0
Ayvaz et al. [101]	Monitoring of production lines	Motion, speed, weight, temperature, current, vacuum, and air pressure	MQTT	ML algorithms Random forest	98.2% ^(A)	Complex monitoring process with significant cost savings

Table 4. Cont.

Reference	Monitored System	Monitored Parameters	Communication Technology	Prediction Algorithm	Performance	Cost–Benefits and Implementations
Sang et al. [103]	Machine components for RUL	Global maintenance data	NGSI REST API and PERP Proxy	FIRMWARE	N.A.	High monitoring performance and medium investment costs
Rosati et al. [105]	Machining centers and measuring machine	Acceleration, speed, and position	MQTT	RF	0.089 ^(B)	High performance with low-cost investment
Ruiz-Sarmiento et al. [108]	Machinery of production steel sheets	18 Variables (coiler temperature, steel densities, pressure, and forces in the roll stand)	Local network	DBF (discrete Bayes filter)	2.98 ^(C)	Complex monitoring process with significant cost savings
D. Mourtzi et al. [109]	Monitoring of refrigeration and cold storage systems (RCSS)	Temperature, humidity, barometric pressure, eCO ₂ , and organic compound	WiFi XBee	N.A.	N.A.	Low-cost, high fidelity, plug-and-play solution
F. Civerchi et al. [111]	Power plant machine monitoring	Temperature and vibrations	CoAP protocol on 6LoWPAN	P2P and RMS	N.A.	Low-cost and easy-to-implement solution
Y.K. Teoh et al. [112]	Condition of manufacturing equipment	Physical parameters	Wired, wireless, and Intranet connections	GA [115]	95.1% ^(A) 94.5% ^(A)	Application with lower maintenance costs and lower energy consumption
K. Kudelina et al. [35]	Bearing faults monitoring	Vibrations	Wired connections	Neural network with fuzzy logic	99.40%	Plug-and-play application with rapid increase in machine efficiency
D. Natanael et al. [114]	Monitoring of filling machine	Temperature and vibrations	Wired connections	Random forest regression Linear regression	88% 59%	Low-cost application but still under development

^(A) accuracy; ^(B) MAE: mean absolute error; ^(C) RMSE: root mean square error; N.A. Not Available.

5. State of the Art on IoT Systems for Industrial Process Control

Process control is another important aspect of smart manufacturing that keeps the production process within tolerance limits while safeguarding process quality. While PdM relies on ML algorithms and data analysis to predict machine failures and to allow for targeted and timely maintenance interventions, on the other hand, process control monitors and adjusts operating parameters to ensure that a system operates efficiently and in compliance with the desired standards. Both systems use real-time data. In particular, predictive maintenance uses sensors to monitor equipment status, while the process control analyzes data to keep the production process within specific limits. Integrating these two approaches allows to implement maintenance strategies that reduce downtime and improve the stability and efficiency of production processes.

The programmable logic controller (PLC), which is mostly used to operate low-level regulatory feedback control loops, has been a key device of industrial control systems throughout the automation revolution, despite the enormous recent breakthroughs in automation technology carried out by the paradigm of Industry 4.0 and its hyperconnected environment. There is currently no updated version of the PLC that aims to fulfill the needs of an Industry 4.0-focused control system. Industry 4.0 refers to integrating different digital technologies in sophisticated information systems and intelligent manufacturing to increase operational efficiency and output. The idea of industrial cyber–physical systems (ICPSs), considered the next generation of industrial control systems (ICSs) from a systems and control viewpoint, is the result of this integration. [116]. Several design concepts mandated by Industry 4.0 must be considered when automating or digitizing industrial processes (Figure 19). These principles include the following:

- Integration of production processes into the value chain, enabling smart factories to achieve end-to-end management of the entire production process from supply chain to services and life cycle management.
- Interoperability is the ability of all system components to connect, communicate, and interact transparently using standardized data and communication models.
- Decentralization, allowing different sub-systems to make decisions locally and autonomously to achieve a final organizational goal.
- Real-time performance, which requires that production processes collect, communicate, and consolidate data at the proper rates so strategic decisions can be taken timely.
- Modularity allows individual parts to be upgraded, expanded, or replaced with the most minor disturbance to production operations. This feature enables smart factories to quickly adjust to changing production needs and physical environments.

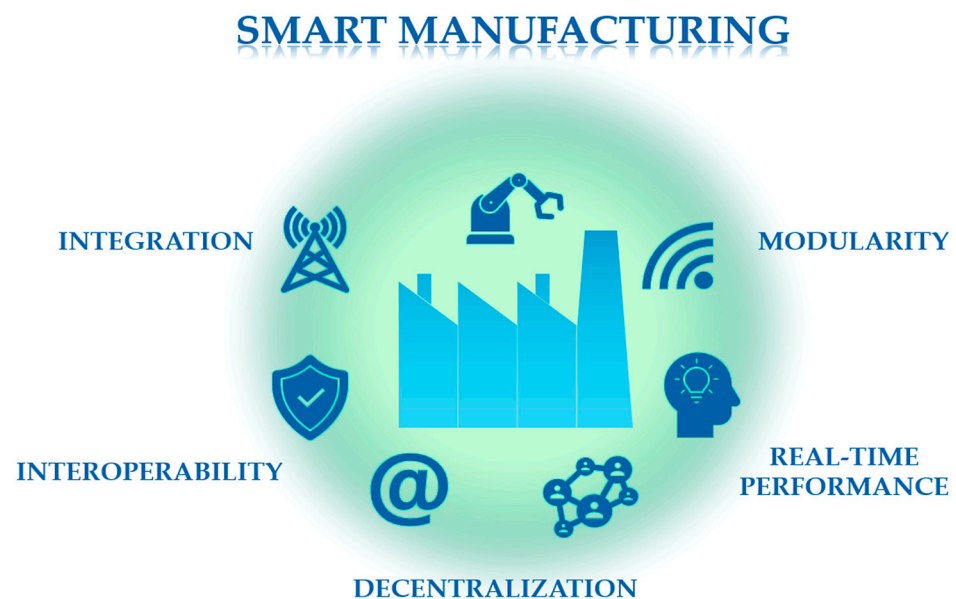


Figure 19. Aims of the SM technologies based on IoT solutions in industrial fields.

In the last several years, there has been much focus on the Internet of Things (IoT) and cloud computing because they may provide a fresh method for intelligent sensing, communication among humans and machines, and the efficient sharing and use of resources when required. The method used from Khan et al. [117] is based on a private cloud system that collects data in real time from smart technologies connected to shop floor products. With the method dictated by gathering shop-floor objects, the research intends to build a generic framework for information and data capture, processing, and collecting at the periphery of huge production controllers. The various parts of the developed cyber-physical mechanism will be implemented in a cloud setting to move towards the Internet of Things. Ioannis et al. [118] present the architecture, design, practical implementation, and evaluation of an end-to-end platform that addresses these challenges. The platform offers adjustable and interoperable methods for gathering, organizing, and directing data streams from heterogeneous cyber-physical production systems; additionally, it facilitates sophisticated data analytics using a unique machine learning architecture that uses quantitative rule mining. Garmaroodi et al. [119] developed a fault-detection system for the CHRIST Osmotron water purifier using certain sensors and data-mining techniques. Six sensors were used to gather data every two weeks before and after the system refurbishment, including good and bad operations. Their research developed two anomaly-detection approaches in IIoT, specifically for water cleaning systems based on ML and data mining. Bhaskaran et al. [120] dealt with monitoring and controlling pipeline transportation systems before the failure that leads to fatal accidents. The NarrowBand Internet of Things (NB-IOT) module,

which has a high-level engineering interface, embeds the IoT into the Supervisory Control and Data Acquisition (SCADA) platform to enhance supervisory performance. SCADA provides local intelligence using an LQR-PID controller in their suggested technique. When the local intelligence cannot respond to threats in advance, the web server uses an NB-IoT module to quickly disable its performance.

To connect virtual and real systems, a DT was suggested by Xia et al. to model production cells, mimic system behaviors, forecast process faults, and regulate manipulated variables adaptively [121]. They created a network of connections across the environments, starting with the production cell that was adjusted to settings like computer-aided applications, product lifecycle management software, and process control platforms to achieve almost synchronous controls. With this work, the authors demonstrated that implementing virtual commissioning as a first step toward system-level digital twinning will accelerate intelligent control systems' training, testing, and validation [122]. S. Muruganandam et al. presented an Operation-Constrained Process Control (OCPC) to eliminate the time delay errors in the operation cycles of intelligent machines [123]. With the proposed method, the authors consider the completion time, operation cycles, and efficiency metrics to identify production errors and time delays. Based on the productivity data, further modifications or allocations of ordinary operation cycles are defined. Productivity analysis is performed based on historical data using federated learning [124]. AI indicators are used in IIoT smart factories to facilitate unattended interventions and streamline production. K. Y. Shin et al. provide a novel engineering approach in smart manufacturing systems engineering (SMSE) by achieving smart product quality monitoring systems (SmartPQMS) [125]. This approach has been implemented in the production cycle of steel and iron.

Comparative Analysis of Process Control Applications

The in-depth analysis of IoT and cloud computing highlights the crucial role of these tools in optimizing industrial operations and resources. The research mentioned provides a diverse panorama of applications and methodologies adopted to improve the interaction between machines and systems, with a strong focus on data collection and analysis. In particular, using a private cloud provides a solid foundation for making data immediately accessible and usable for making more informed decisions. At the same time, adopting an end-to-end approach for data management in cyber-physical systems demonstrates that continuity and interconnectivity between data are essential to ensure efficiency and operational speed. The importance of data analytics is further supported by machine learning and mining techniques that enable the detection of anomalies in systems. This aspect is particularly critical in industries where even a small imperfection can have significant consequences. In monitoring and control, using IoT technologies for plant supervision represents a growing need in the current industrial landscape. Integrating SCADA systems with NB-IoT networks leads to better failure prevention and smarter and more responsive asset management. The innovation of digital twinning marks a significant step towards integrating the physical and virtual worlds. This fusion certainly revolutionizes the monitoring of operations and the training and validation of intelligent control systems. Finally, the importance of adopting quality control and monitoring metrics, now facilitated by advanced technologies such as AI, allows for the optimization of interactions in smart factories. The conclusion highlights a central theme: Despite the different methodologies and research objectives, there is a convergence in the approach to IoT and cloud computing as tools for innovation and continuous improvement. The digitalization of industrial processes and advanced data analysis techniques are crucial to improving efficiency and the ability to respond to emerging issues in production. In this context, smart factories are the industry's future, ready to respond to market challenges with agility and precision. Table 5 summarizes the characteristics of each analyzed reference, with the application performance shown in the last column.

Table 5. Comparative analysis of the references proposed in this paper relating to IoT-based process control solutions.

Reference	Monitored Process	Application	Monitored Parameters	Inferring Algorithm	Performance
S. I. Khan et al. [117]	Shop floor manufacturing process	Production and quality control	Processing speed, idle time, parts per minute, and processed or unprocessed parts	N.A.	N.A.
I. T. Christou et al. [118]	Automotive and female fashion manufacturing	Predictive maintenance and quality assessment	N.A.	R4RE	3.76% 7.702% ^(A)
M.S.S. Garmaroodi et al. [119]	Water purification system (CHRIST Osmotron)	Anomaly detection	Pressure and electrical conductivity	SVM (Approach 1) ANN (Approach 2)	100% (Approach 1)
P. E. Bhaskaran et al. [120]	Monitoring of the transmission system of the condotte	Lab-scale DCS (distributed control system)-based fluid transportation system	Flow and pressure	SCADA with NB-IoT	26.2% ^(C)
K. Xia et al. [121]	Implementation of a DT to improve the level of training, process control, and testing	Automation of intelligent production systems	Simulation of real-life robotic cell behaviors	Machine learning (ML)-based dynamic scheduling agent digital engine	N.A.
S. Muruganandam et al. [123]	Optimization of operating cycles (OCPC)	Identification of time lags and errors in production	Operational cycle, completion time, and output efficiency metrics	Federated learning	90.181 ^(B) %
K. Y. Shin et al. [125]	Monitoring of the steel and iron production cycle	Product quality monitoring systems	N.A.	SmartPQMS (data mining, ML, deep learning, and reinforcement learning technology)	N.A.

^(A) MAPE: mean absolute percentage error; ^(B) efficiency; ^(C) enhanced performance; N.A.: not available.

6. IoT Systems Applied to Additive Manufacturing

Additive manufacturing (AM) represents another important pillar of the Industry 4.0 paradigm. AM, also known as 3D Printing, is a contemporary technology that enables the creation of 3D items without traditional production (Figure 20). The process is called “additive” as it builds material layers one at a time to create final 3D objects [126]. Compared to traditional manufacturing techniques, AM offers the benefits of printing complicated forms, shorter production times, less waste, novel features, and cost-effectiveness. As a result, prototypes, meals, tissues, jewels, buildings, tools, and other items are being made using this rapidly developing technology. Since AM is a data-intensive manufacturing area, several ML techniques may be used to tackle problems with selecting, optimizing, monitoring, controlling, and designing AM process parameters. As a result, researchers’ interest in the breadth of ML applications to tackle AM challenges is expanding quickly [127]. IoT encourages more customization, less material waste, and quick manufacturing in AM processes. The integration of 3D Printing with cyber–physical systems holds promise for manufacturing, design, and maintenance procedures. It also gives the user design freedom and the ability to perform multi-dimensional extrusion [128].

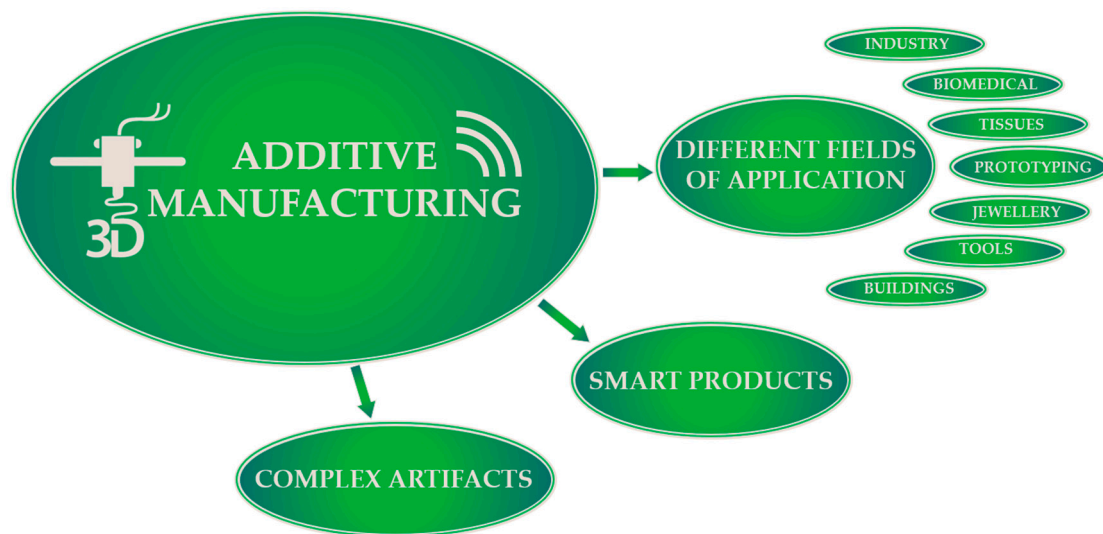


Figure 20. Main advantages and fields of application of additive manufacturing.

Another tenet of the Industrial Internet of Things (IIoT) concept is additive manufacturing, where sophisticated measuring tools could be needed to track important parameters. At the same time, artifacts are being produced to assess the deployment site's environmental indicators. Fedullo et al., in their work, consider the application of IIoT low-power wide-area network (LPWAN) technologies in an experimental setup of additive manufacturing [129]. Their research led to the realization of different objects by designing a powder bed 3D printer. These objects were sensorized at the start of the realization to monitor production process and next phase in the destination locations where such artifacts are inserted. This application required a battery for a considerable duration and the integrated sensors' ability to transmit data securely, even at long ranges. The authors also analyzed two LoRa (long range) end node types: the Microchip RN2483 LoRa Mote and the Tinovi PM-IO-5-SM LoRaWAN IO Module.

The work conducted by Majeed et al. [130] aims to build a framework that combines big data analytics, additive manufacturing, and sustainable smart manufacturing technologies that benefit additive manufacturing enterprises. They proposed a big data-driven sustainable smart additive manufacturing (BD-SSAM) framework that benefited AM industry leaders in making better decisions for the early lifecycle stage of the product, presenting an application scenario from the additive manufacturing plant to demonstrate the suggested framework. Their case study focused on fabricating AlSi10Mg alloy elements using AM's selective laser melting (SLM) technique [131]. The results show that energy consumption and product quality are properly controlled, which benefits sustainable smart manufacturing, pollution minimization, and neater realization. A metal additive manufacturing-based integrated process chain idea for tool manufacture is presented by Moshiri et al. in [132]. The suggested method describes the key stages for the synergistic integration of production assets and attempts to take advantage of a completely digitalized production line. The production line is equipped with a digital infrastructure that collects and processes data from numerous monitoring sensors to implement corrective measures and continuously optimize the process. The goal of the proposed work is to fully monitor the collection of production data to identify responses, manage performance, and ensure that all goods and equipment are fully traceable. Specifically, working environment conditions were immediately captured through real-time monitoring to provide additional data processing, feedback (correction), and ongoing production process improvement. In the field of additive manufacturing, important help is given by the use of digital twins that allow to obtain a more reliable design method by eliminating any form of waste of both time and material because they allow to simulate a system or an object, especially when it is complex. DT is obtained by fusing software, IoT, AI, and virtual models for simulation to

create increasingly realistic models. Digital models are also able to simulate any failures through simulations. The goal of the DT method is to optimize the printing process by obtaining a better consumption of resources and reducing a company's costs [18].

In this regard, D.R. Gunasegaram et al. explain how using a DT combined with the 3D printing of metal materials allows for cheaper and repeatable printing while ensuring high quality [133]. In their work, a study was performed on a laser powder bed printing (L-PBF) process. In fact, they noted that by programming the laser power based on the data collected by the pyrometer, they were able to avoid hot spots during the manufacturing phase of the artifact. Still, they dedicated considerable time to modeling and analysis to collect correlation data. For this reason, they noted that using ML tools raised to a higher level with physical data could control numerous parameters, allowing them to eliminate hot spots and other defects. Similarly, DT has been used by J. Haw et al. for the optimization of the idealization, design, and verification phase of biomedical scaffolds [134]. It is important to note that AM is well suited to biomedical production prostheses since these prostheses can have extremely complex shapes that would be significantly expensive to produce with traditional production methods. In the work proposed by L. Guo et al. in [135], an architecture is created in which a DT model is obtained from the collaboration between a cloud-edge platform dedicated to 3D additive manufacturing. This architecture, with an effective data transfer, allows the remote viewing of the progress of the print, and through the DT, the progress of the print is displayed in a virtual way.

Comparative Analysis of Additive Manufacturing Applications

The advancements in the IoT and additive manufacturing depict a transformative landscape in production processes, emphasizing the synergy between data analytics, real-time monitoring, and smart manufacturing techniques. Incorporating sophisticated measurement tools is paramount in continuously tracking crucial parameters during production of artifacts and assessing environmental factors at deployment sites. In parallel, the big data-driven sustainable smart additive manufacturing (BD-SSAM) framework focuses on improving product lifecycle management, highlighting how the use of data can contribute to reducing energy consumption, improving product quality, decreasing pollution levels, and increasing overall efficiency. This approach emphasizes the potential of data-driven decision making to achieve significant sustainability benefits in the manufacturing sector.

The integration of IoT and LPWAN technologies in additive manufacturing has demonstrated how using sensor objects, realized by 3D printing, can generate smart products. These sensors play a crucial role in continuously monitoring production parameters and evaluating real-world performance once installed. It turns out that effective long-range data transmission and extended battery life are key to maintaining operational efficiency and reliability in additive manufacturing environments. In addition, an integrated process chain for additive metal production was proposed, highlighting the need for the full digitization and interconnection of production assets. Real-time monitoring is essential to facilitate continuous process optimization, guarantee product quality, and ensure equipment traceability. This digitization is essential for data acquisition and analysis, leading to informed corrective decisions during production.

An innovative aspect is the application of digital twins in additive manufacturing optimization. Through IoT, AI, and virtual modeling, DT enables the simulation and prediction of production outcomes and facilitates proactive maintenance and efficient resource optimization. The integration of DT with 3D printing is proving to be effective in counteracting production defects through real-time adjustments and machine learning tools to improve parameter control. Finally, significant progress has been observed in DT application in designing and verifying biomedical scaffolds, highlighting how additive manufacturing can tackle complex projects and offer economic advantages over traditional methods. The collaborative potential of cloud and edge computing emerges as a key factor in enabling remote monitoring and efficient data transfer in 3D printing processes. The convergence of IoT, big data, and digital twin technologies within additive manufacturing heralds a new

era of production methods characterized by increased agility, improved sustainability, and heightened cost-effectiveness. As these technologies continue to evolve, they promise to redefine manufacturing paradigms, paving the way for enhanced operational capabilities and innovation across various industries. The ongoing advancements in these fields exemplify the potential for smarter manufacturing solutions and underline the importance of harnessing data and technology for long-term industrial growth and sustainability. Table 6 summarizes the main topics of the analyzed articles indicating the technological readiness of the developed application.

Table 6. Summary of the topics covered by the references analyzed.

Reference	Topic	Technological Readiness
T. Fedullo et al. [129]	Implementation of IIoT LPWAN technologies within additive manufacturing products for information collection during production and at the point of installation	AM approach has high application potential in the field of smart manufacturing and is not only for the creation of intelligent objects
A. Majeed et al. [130]	Realization of a big data-based framework (BD-SSAM) as a decision-making tool for companies in the AM field	New framework SSAM for the product manufacturing cycle that aims to control energy consumption and quality
M. Moshiri et al. [132]	Complete monitoring of data collection to optimize the production process through AM, minimize costs, and improve product quality	A new concept of an integrated and modular intelligent production system, with full system monitoring, consumption data analysis, safer working environment, and scalable and flexible modular configuration
D. R. Gunasegaram et al. [133]	Improving the quality of realization using DT models enhanced with ML tools	The application of DT in AM is mature but still in the development phase; it is not yet standardized and requires significant investments in terms of resources and technical skills, but it allows significant improvements in production quality control with considerable adaptability
J. Haw et al. [134]	Use of DT as a tool to optimize and improve the manufacturing phases of biomedical scaffolds	DT in the biomedical field to produce scaffolds is a technology of considerable importance as it allows the creation of increasingly ergonomic prostheses, allowing for a more optimized design
L. Guo et al. [135]	Decentralized monitoring of the AM process using DT	DT is a great tool for decentralizing additive manufacturing because it allows for production simulations, optimization of the manufacturing process, and real-time monitoring

Nowadays, the constant and precise monitoring of the main AM parameters is essential. Monitoring the printing parameters, combined with the data processing provided by ML algorithms and DT models, allows for an optimized manufacturing process management. This manufacturing paradigm involves the production of higher-quality products, an essential aspect of market competition. With the quality of the product, another factor of interest is the minimization of costs linked to the reduction of waste and a greater production speed.

7. Conclusions and Future Developments

In the last few years, the IoT paradigm has undoubtedly influenced many fields, such as industry, agriculture, biomedicine, warehousing, construction, etc. These are just some sectors in which the IoT has significantly contributed, improving manufacturing efficiency, scheduling maintenance interventions, and safeguarding workers' health and cybersecurity. In the framework of Industry 4.0, the IoT has also enabled a more detailed and widespread control process by providing new control architectures that will allow real-time process

monitoring so that no drifts could induce a reduction in product quality. It is worth noting that a fundamental aspect of IoT smart manufacturing applications is the massive presence of sensing devices directly installed in the plant to gather data, and the development of ML algorithms to process the data and detect anomalies and risk conditions. Moreover, the application of IoT strategies requires a significant flow of data, which very often contains sensitive information. For this reason, cybersecurity architectures are essential to prevent possible cyber-attacks and data theft.

This paper has provided a targeted vision of the IoT paradigm in the main fields of smart manufacturing. After an accurate selection of the scientific literature based on PRISMA method, this paper has presented an overview of IoT applications in manufacturing process control, predictive maintenance, data protection, worker safety, and additive manufacturing. A comparative analysis has been provided for each covered topic, focusing on architectural aspects, data analysis, and communication technologies, as well as characteristic aspects of each topic and bringing out strengths and limitations of analyzed solutions. In this way, the features, functionalities, and real-world applications of IoT in the framework of smart manufacturing have been outlined.

In the future, to optimize smart manufacturing processes, the goal is to improve the interactions between IoT systems and ML by enhancing different aspects: data integration by developing models for data acquisition from various sources (IoT sensors, ERP, production management systems); improvement of the quality of information for ML; development of new standards and protocols that facilitate interoperability between IoT systems and devices; and improvement of predictive models through the use of advanced ML techniques. Considering security aspects, a starting point of the research will be to develop encryption protocols and secure access strategies to better ensure privacy and data security. Taking into account that the implementation of IoT and ML methodologies needs an in-depth knowledge of several aspects, companies will need to train their staff by investing time and capital to have skilled operators. With continuous technological progress, the enhancement of processing software, and the adoption of high-performance ML algorithms, it will be possible to process an ever-increasing amount of data at a higher speed, obtaining a more precise and rapid response to input data. In conclusion, in the near future, the IoT paradigm will be the central cornerstone on which all companies will revolve.

Author Contributions: Conceptualization, P.V., G.R., and R.D.F.; methodology, P.V., R.V., and R.D.F.; validation, R.V., D.C., and R.D.F.; formal analysis, G.R., C.D.-V.-S., D.C., and R.D.F.; investigation, P.V., C.D.-V.-S., D.C., and R.D.F.; resources, P.V., G.R., R.V., and R.D.F.; data curation, G.R. and R.D.F.; writing—original draft preparation, P.V., G.R., and R.D.F.; writing—review and editing, P.V., C.D.-V.-S., D.C., and R.V.; visualization, G.R., C.D.-V.-S., and R.D.F.; supervision, P.V., D.C., and R.V.; funding acquisition, P.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data are available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Sahoo, S.; Lo, C.-Y. Smart Manufacturing Powered by Recent Technological Advancements: A Review. *J. Manuf. Syst.* **2022**, *64*, 236–250. [[CrossRef](#)]
2. Khanna, A.; Selvaraj, P.; Gupta, D.; Sheikh, T.H.; Pareek, P.K.; Shankar, V. Internet of Things and Deep Learning Enabled Healthcare Disease Diagnosis Using Biomedical Electrocardiogram Signals. *Expert Syst.* **2023**, *40*, 12864. [[CrossRef](#)]
3. Bonfanti, S.B.; Crocioni, G.; Cunsolo, F.; Gruosso, G. Implementation of an IoT Node for Biomedical Applications. In Proceedings of the 4th International Forum on Research and Technology for Society and Industry (RTSI), Palermo, Italy, 10–13 September 2018; IEEE: New York, NY, USA, 2018; pp. 1–6. [[CrossRef](#)]
4. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Enhancing Smart Farming through the Applications of Agriculture 4.0 Technologies. *Int. J. Intell. Netw.* **2022**, *3*, 150–164. [[CrossRef](#)]

5. Prakash, C.; Singh, L.P.; Gupta, A.; Lohan, S.K. Advancements in Smart Farming: A Comprehensive Review of IoT, Wireless Communication, Sensors, and Hardware for Agricultural Automation. *Sens. Actuators A Phys.* **2023**, *362*, 114605. [CrossRef]
6. Kumar, D.; Kr Singh, R.; Mishra, R.; Fosso Wamba, S. Applications of the Internet of Things for Optimizing Warehousing and Logistics Operations: A Systematic Literature Review and Future Research Directions. *Comput. Ind. Eng.* **2022**, *171*, 108455. [CrossRef]
7. Liu, C.; Zhu, H.; Tang, D.; Nie, Q.; Zhou, T.; Wang, L.; Song, Y. Probing an Intelligent Predictive Maintenance Approach with Deep Learning and Augmented Reality for Machine Tools in IoT-Enabled Manufacturing. *Robot. Comput.-Integr. Manuf.* **2022**, *77*, 102357. [CrossRef]
8. Saravanan, G.; Parkhe, S.S.; Thakar, C.M.; Kulkarni, V.V.; Mishra, H.G.; Gulothungan, G. Implementation of IoT in Production and Manufacturing: An Industry 4.0 Approach. *Mater. Today Proc.* **2022**, *51*, 2427–2430. [CrossRef]
9. Del Real Torres, A.; Andreiana, D.S.; Ojeda Roldán, Á.; Hernández Bustos, A.; Acevedo Galicia, L.E. A Review of Deep Reinforcement Learning Approaches for Smart Manufacturing in Industry 4.0 and 5.0 Framework. *Appl. Sci.* **2022**, *12*, 12377. [CrossRef]
10. Keerthi, C.K.; Jabbar, M.A.; Seetharamulu, B. Cyber Physical Systems (CPS): Security Issues, Challenges and Solutions. In Proceedings of the International Conference on Computational Intelligence and Computing Research (ICIC), Coimbatore, India, 14–16 December 2017; IEEE: New York, NY, USA, 2017; pp. 1–4. [CrossRef]
11. Ryalat, M.; ElMoaqet, H.; AlFaouri, M. Design of a Smart Factory Based on Cyber-Physical Systems and Internet of Things towards Industry 4.0. *Appl. Sci.* **2023**, *13*, 2156. [CrossRef]
12. Ghimire, T.; Joshi, A.; Sen, S.; Kapruan, C.; Chadha, U.; Selvaraj, S.K. Blockchain in Additive Manufacturing Processes: Recent Trends & Its Future Possibilities. *Mater. Today Proc.* **2022**, *50*, 2170–2180. [CrossRef]
13. Gallo, G.; Rienzo, F.D.; Garzelli, F.; Ducange, P.; Vallati, C. A Smart System for Personal Protective Equipment Detection in Industrial Environments Based on Deep Learning at the Edge. *IEEE Access* **2024**, *10*, 110862–110878. [CrossRef]
14. Rasouli, S.; Alipouri, Y.; Chamanzad, S. Smart Personal Protective Equipment (PPE) for Construction Safety: A Literature Review. *Saf. Sci.* **2024**, *170*, 106368. [CrossRef]
15. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics* **2023**, *12*, 1333. [CrossRef]
16. Mecheter, A.; Tarlochan, F.; Kucukvar, M. A Review of Conventional versus Additive Manufacturing for Metals: Life-Cycle Environmental and Economic Analysis. *Sustainability* **2023**, *15*, 12299. [CrossRef]
17. Duman, B.; Süzen, A.A. Modeling of IoT-based additive manufacturing machine's digital twin for error detection. *J. Eng. Sci. Des.* **2023**, *11*, 486–497. [CrossRef]
18. Chigilipalli, B.K.; Karri, T.; Chetti, S.N.; Bhiogade, G.; Kottala, R.K.; Cheepu, M. A Review on Recent Trends and Applications of IoT in Additive Manufacturing. *Appl. Syst. Innov.* **2023**, *6*, 50. [CrossRef]
19. Urhal, P.; Weightman, A.; Diver, C.; Bartolo, P. Robot Assisted Additive Manufacturing: A Review. *Robot. Comput.-Integr. Manuf.* **2019**, *59*, 335–345. [CrossRef]
20. Shen, T.; Li, B. Digital Twins in Additive Manufacturing: A State-of-the-Art Review. *Int. J. Adv. Manuf. Technol.* **2024**, *131*, 63–92. [CrossRef]
21. Fast Radius. Available online: <https://fastradius.com/expertise/manufacturing-quality-standards/#additive> (accessed on 15 October 2024).
22. Geico S.p.a. Available online: <https://geico-spa.com/en/innovation/smart-paintshop/> (accessed on 15 October 2024).
23. Industry 5.0—European Commission. Available online: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en (accessed on 14 October 2024).
24. Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. A Literature Review of the Challenges and Opportunities of the Transition from Industry 4.0 to Society 5.0. *Energies* **2022**, *15*, 6276. [CrossRef]
25. Pizoń, J.; Gola, A. Human–Machine Relationship—Perspective and Future Roadmap for Industry 5.0 Solutions. *Machines* **2023**, *11*, 203. [CrossRef]
26. Ghobakhloo, M.; Mahdiraji, H.A.; Iranmanesh, M.; Jafari-Sadeghi, V. From Industry 4.0 Digital Manufacturing to Industry 5.0 Digital Society: A Roadmap Toward Human-Centric, Sustainable, and Resilient Production. *Inf. Syst. Front.* **2024**. [CrossRef]
27. Martini, B.; Bellisario, D.; Coletti, P. Human-Centered and Sustainable Artificial Intelligence in Industry 5.0: Challenges and Perspectives. *Sustainability* **2024**, *16*, 5448. [CrossRef]
28. Sharma, M.; Tomar, A.; Hazra, A. Edge Computing for Industry 5.0: Fundamental, Applications, and Research Challenges. *IEEE Internet Things J.* **2024**, *11*, 19070–19093. [CrossRef]
29. Chi, H.R.; Wu, C.K.; Huang, N.-F.; Tsang, K.-F.; Radwan, A. A Survey of Network Automation for Industrial Internet-of-Things Toward Industry 5.0. *IEEE Trans. Ind. Inform.* **2023**, *19*, 2065–2077. [CrossRef]
30. Vacchi, M.; Siligardi, C.; Settembre-Blundo, D. Driving Manufacturing Companies toward Industry 5.0: A Strategic Framework for Process Technological Sustainability Assessment (P-TSA). *Sustainability* **2024**, *16*, 695. [CrossRef]
31. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n71. [CrossRef]

32. Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. PRISMA 2020 Explanation and Elaboration: Updated Guidance and Exemplars for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n160. [[CrossRef](#)]
33. Wang, J.; Ma, Y.; Zhang, L.; Gao, R.X.; Wu, D. Deep Learning for Smart Manufacturing: Methods and Applications. *J. Manuf. Syst.* **2018**, *48*, 144–156. [[CrossRef](#)]
34. Yaghoubi, E.; Yaghoubi, E.; Khamees, A.; Razmi, D.; Lu, T. A Systematic Review and Meta-Analysis of Machine Learning, Deep Learning, and Ensemble Learning Approaches in Predicting EV Charging Behavior. *Eng. Appl. Artif. Intell.* **2024**, *135*, 108789. [[CrossRef](#)]
35. Kudelina, K.; Raja, H.A. Neuro-Fuzzy Framework for Fault Prediction in Electrical Machines via Vibration Analysis. *Energies* **2024**, *17*, 2818. [[CrossRef](#)]
36. Sarker, I.H. Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Comput. Sci.* **2021**, *2*, 160. [[CrossRef](#)] [[PubMed](#)]
37. Nasteski, V. An Overview of the Supervised Machine Learning Methods. *Horiz. B* **2017**, *4*, 51–62. [[CrossRef](#)]
38. An, Q.; Rahman, S.; Zhou, J.; Kang, J.J. A Comprehensive Review on Machine Learning in Healthcare Industry: Classification, Restrictions, Opportunities and Challenges. *Sensors* **2023**, *23*, 4178. [[CrossRef](#)]
39. Osisanwo, F.Y.; Akinsola, J.E.T.; Awodele, O.; Hinmikaiye, J.O.; Olakanmi, O.; Akinjobi, J. Supervised Machine Learning Algorithms: Classification and Comparison. *Int. J. Comput. Trends Technol. (IJCTT)* **2017**, *48*, 128–138. [[CrossRef](#)]
40. Hassan, S.U.; Ahamed, J.; Ahmad, K. Analytics of Machine Learning-Based Algorithms for Text Classification. *Sustain. Oper. Comput.* **2022**, *3*, 238–248. [[CrossRef](#)]
41. Beskopylny, A.N.; Stel'makh, S.A.; Shcherban', E.M.; Mailyan, L.R.; Meskhi, B.; Razveeva, I.; Kozhakin, A.; Pembek, A.; Elshaeva, D.; Chernil'nik, A.; et al. Prediction of the Compressive Strength of Vibrocentrifuged Concrete Using Machine Learning Methods. *Buildings* **2024**, *14*, 377. [[CrossRef](#)]
42. Gupta, V.; Mishra, V.K.; Singhal, P.; Kumar, A. An Overview of Supervised Machine Learning Algorithm. In Proceedings of the 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 16–17 December 2022; pp. 87–92. [[CrossRef](#)]
43. Faria, J.M. Machine Learning Safety: An Overview. In Proceeding of the 26th Safety-Critical Systems Symposium, York, UK, 6–8 February 2018; p. 1.
44. Wang, P.; Wu, H.; Liu, X.; Xu, C. Machine Learning-Assisted Prediction of Stress Corrosion Crack Growth Rate in Stainless Steel. *Crystals* **2024**, *14*, 846. [[CrossRef](#)]
45. Wang, J.; Biljecki, F. Unsupervised Machine Learning in Urban Studies: A Systematic Review of Applications. *Cities* **2022**, *129*, 103925. [[CrossRef](#)]
46. Rolf, B.; Beier, A.; Jackson, I.; Müller, M.; Reggelin, T.; Stuckenschmidt, H.; Lang, S. A Review on Unsupervised Learning Algorithms and Applications in Supply Chain Management. *Int. J. Prod. Res.* **2024**, 1–51. [[CrossRef](#)]
47. Yu, W.; Chen, Y. Data-Driven Polyline Simplification Using a Stacked Autoencoder-Based Deep Neural Network. *Trans. GIS* **2022**, *26*, 2302–2325. [[CrossRef](#)]
48. Thai, H.-T. Machine Learning for Structural Engineering: A State-of-the-Art Review. *Structures* **2022**, *38*, 448–491. [[CrossRef](#)]
49. Ahsan, M.M.; Luna, S.A.; Siddique, Z. Machine-Learning-Based Disease Diagnosis: A Comprehensive Review. *Healthcare* **2022**, *10*, 541. [[CrossRef](#)] [[PubMed](#)]
50. Bechelli, S.; Delhommelle, J. Machine Learning and Deep Learning Algorithms for Skin Cancer Classification from Dermoscopic Images. *Bioengineering* **2022**, *9*, 97. [[CrossRef](#)]
51. Hu, J.; Jiang, Q.; Shen, Y.; Qian, C.; Xu, F.; Zhu, Q. Application of Recurrent Neural Network to Mechanical Fault Diagnosis: A Review. *J. Mech. Sci. Technol.* **2022**, *36*, 527–542. [[CrossRef](#)]
52. Misra, S.; Roy, C.; Sauter, T.; Mukherjee, A.; Maiti, J. Industrial Internet of Things for Safety Management Applications: A Survey. *IEEE Access* **2022**, *10*, 83415–83439. [[CrossRef](#)]
53. Kaur, B.; Dadkhah, S.; Shoeleh, F.; Neto, E.C.P.; Xiong, P.; Iqbal, S.; Lamontagne, P.; Ray, S.; Ghorbani, A.A. Internet of Things (IoT) Security Dataset Evolution: Challenges and Future Directions. *Internet Things* **2023**, *22*, 100780. [[CrossRef](#)]
54. Zhan, X.; Wu, W.; Shen, L.; Liao, W.; Zhao, Z.; Xia, J. Industrial Internet of Things and Unsupervised Deep Learning Enabled Real-Time Occupational Safety Monitoring in Cold Storage Warehouse. *Saf. Sci.* **2022**, *152*, 105766. [[CrossRef](#)]
55. Zhang, J.; Yan, Q.; Zhu, X.; Yu, K. Smart Industrial IoT Empowered Crowd Sensing for Safety Monitoring in Coal Mine. *Digit. Commun. Netw.* **2023**, *9*, 296–305. [[CrossRef](#)]
56. Nachiappan, B.; Rajkumar, N.; Viji, C.; Mohanraj, A. Ensuring Worker Safety at Construction Sites Using Geofence. *SSRG Int. J. Civ. Eng.* **2024**, *11*, 107–113. [[CrossRef](#)]
57. Khan, S.I.; Ray, B.R.; Karmakar, N.C. RFID Localization in Construction with IoT and Security Integration. *Autom. Constr.* **2024**, *159*, 105249. [[CrossRef](#)]
58. Lalitha, K.; Ramya, G.; Shunmugathammal, M. AI-Based Safety Helmet for Mining Workers Using IoT Technology and ARM Cortex-M. *IEEE Sens. J.* **2023**, *23*, 21355–21362. [[CrossRef](#)]
59. De Fazio, R.; Cafagna, D.; Marcuccio, G.; Minerba, A.; Visconti, P. A Multi-Source Harvesting System Applied to Sensor-Based Smart Garments for Monitoring Workers' Bio-Physical Parameters in Harsh Environments. *Energies* **2020**, *13*, 2161. [[CrossRef](#)]

60. De Fazio, R.; Dinoi, L.M.; De Vittorio, M.; Visconti, P. A Sensor-Based Drone for Pollutants Detection in Eco-Friendly Cities: Hardware Design and Data Analysis Application. *Electronics* **2021**, *11*, 52. [[CrossRef](#)]
61. Mehata, K.M.; Shankar, S.K.; Karthikeyan, N.; Nandhinee, K.; Hedwig, P.R. IoT Based Safety and Health Monitoring for Construction Workers. In Proceedings of the 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 25–26 April 2019; IEEE: New York, NY, USA, 2019; pp. 1–7. [[CrossRef](#)]
62. Kanan, R.; Elhassan, O.; Bensalem, R. An IoT-Based Autonomous System for Workers' Safety in Construction Sites with Real-Time Alarming, Monitoring, and Positioning Strategies. *Autom. Constr.* **2018**, *88*, 73–86. [[CrossRef](#)]
63. Nourildean, S.W.; Hassib, M.D.; Mohammed, Y.A. Internet of Things Based Wireless Sensor Network: A Review. *Indones. J. Electr. Eng. Comput. Sci. (IJECS)* **2022**, *27*, 246. [[CrossRef](#)]
64. Kim, J.H.; Jo, B.W.; Jo, J.H.; Kim, D.K. Development of an IoT-Based Construction Worker Physiological Data Monitoring Platform at High Temperatures. *Sensors* **2020**, *20*, 5682. [[CrossRef](#)]
65. De Fazio, R.; De Vittorio, M.; Visconti, P. Innovative IoT Solutions and Wearable Sensing Systems for Monitoring Human Biophysical Parameters: A Review. *Electronics* **2021**, *10*, 1660. [[CrossRef](#)]
66. De Fazio, R.; Katamba, D.M.; Lay Ekuakille, A.; Ferreira, M.J.; Kidiambo, S.; Giannoccaro, N.I.; Velazquez, R.; Visconti, P. Sensors-Based Mobile Robot for Harsh Environments: Functionalities, Energy Consumption Analysis and Characterization. *Acta Imeko* **2021**, *10*, 209. [[CrossRef](#)]
67. Márquez-Sánchez, S.; Campero-Jurado, I.; Herrera-Santos, J.; Rodríguez, S.; Corchado, J.M. Intelligent Platform Based on Smart PPE for Safety in Workplaces. *Sensors* **2021**, *21*, 4652. [[CrossRef](#)]
68. Bontempi, A.; Demarchi, D.; Ros, P.M. Design of Wireless Power Smart Personal Protective Equipment for Industrial Internet of Things. *IEEE Access* **2024**, *12*, 79613–79625. [[CrossRef](#)]
69. De Fazio, R.; Al-Hinnawi, A.-R.; De Vittorio, M.; Visconti, P. An Energy-Autonomous Smart Shirt Employing Wearable Sensors for Users' Safety and Protection in Hazardous Workplaces. *Appl. Sci.* **2022**, *12*, 2926. [[CrossRef](#)]
70. Visconti, P.; De Fazio, R.; Velazquez, R.; Al-Naami, B.; Ghavifekr, A.A. Wearable Sensing Smart Solutions for Workers' Remote Control in Health-Risk Activities. In Proceedings of the 8th Int Conference on Control, Instrumentation and Automation (ICCIA), Tehran, Iran, 2–3 March 2022; IEEE: New York, NY, USA, 2022; pp. 1–5. [[CrossRef](#)]
71. Montanaro, T.; Sergi, I.; Motroni, A.; Buffi, A.; Nepa, P.; Pirozzi, M.; Catarinucci, L.; Colella, R.; Chietera, F.P.; Patrono, L. An IoT-Aware Smart System Exploiting the Electromagnetic Behavior of UHF-RFID Tags to Improve Worker Safety in Outdoor Environments. *Electronics* **2022**, *11*, 717. [[CrossRef](#)]
72. Gallo, G.; Di Rienzo, F.; Ducange, P.; Ferrari, V.; Tognetti, A.; Vallati, C. A Smart System for Personal Protective Equipment Detection in Industrial Environments Based on Deep Learning. In Proceedings of the 2021 IEEE International Conference on Smart Computing (SMARTCOMP), Irvine, CA, USA, 23–27 August 2021; pp. 222–227. [[CrossRef](#)]
73. Abuhasel, K.A.; Khan, M.A. A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing. *IEEE Access* **2020**, *8*, 117354–117364. [[CrossRef](#)]
74. Li, G.; Ren, L.; Fu, Y.; Yang, Z.; Adetola, V.; Wen, J.; Zhu, Q.; Wu, T.; Candan, K.S.; O'Neill, Z. A Critical Review of Cyber-Physical Security for Building Automation Systems. *Annu. Rev. Control* **2023**, *55*, 237–254. [[CrossRef](#)]
75. Wadsworth, A.; Thanoon, M.I.; McCurry, C.; Sabatto, S.Z. Development of IIoT Monitoring and Control Security Scheme for Cyber Physical Systems. In Proceedings of the 2019 SoutheastCon, Huntsville, AL, USA, 11–14 April 2019; IEEE: New York, NY, USA, 2019; pp. 1–5. [[CrossRef](#)]
76. Moradbeikie, A.; Jamshidi, K.; Bohlooli, A.; Garcia, J.; Masip-Bruin, X. An IIoT Based ICS to Improve Safety Through Fast and Accurate Hazard Detection and Differentiation. *IEEE Access* **2020**, *8*, 206942–206957. [[CrossRef](#)]
77. Peserico, G.; Morato, A.; Tramarin, F.; Vitturi, S. Functional Safety Networks and Protocols in the Industrial Internet of Things Era. *Sensors* **2021**, *21*, 6073. [[CrossRef](#)]
78. Leng, J.; Ye, S.; Zhou, M.; Zhao, J.L.; Liu, Q.; Guo, W.; Cao, W.; Fu, L. Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 237–252. [[CrossRef](#)]
79. Khan, A.A.; Bourouis, S.; Kamruzzaman, M.M.; Hadjouni, M.; Shaikh, Z.A.; Laghari, A.A.; Elmannai, H.; Dhahbi, S. Data Security in Healthcare Industrial Internet of Things with Blockchain. *IEEE Sens. J.* **2023**, *23*, 25144–25151. [[CrossRef](#)]
80. Mosteiro-Sanchez, A.; Barcelo, M.; Astorga, J.; Urbieto, A. Securing IIoT Using Defence-in-Depth: Towards an End-to-End Secure Industry 4.0. *J. Manuf. Syst.* **2020**, *57*, 367–378. [[CrossRef](#)]
81. AbuEmera, E.A.; ElZouka, H.A.; Saad, A.A. Security Framework for Identifying Threats in Smart Manufacturing Systems Using STRIDE Approach. In Proceedings of the 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 14–16 January 2022; IEEE: New York, NY, USA, 2022; pp. 605–612. [[CrossRef](#)]
82. Hammad, M.; Badshah, A.; Abbas, G.; Alasmay, H.; Waqas, M.; Khan, W.A. A Provable Secure and Efficient Authentication Framework for Smart Manufacturing Industry. *IEEE Access* **2023**, *11*, 67626–67639. [[CrossRef](#)]
83. Alrowais, F.; Althahabi, S.; Alotaibi, S.S.; Mohamed, A.; Ahmed Hamza, M.; Marzouk, R. Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment. *Comput. Syst. Sci. Eng.* **2023**, *45*, 687–700. [[CrossRef](#)]
84. Wu, F.; Qiu, C.; Wu, T.; Yuce, M.R. Edge-Based Hybrid System Implementation for Long-Range Safety and Healthcare IoT Applications. *IEEE Internet Things J.* **2021**, *8*, 9970–9980. [[CrossRef](#)]

85. Mrabet, H.; Alhomoud, A.; Jemai, A.; Trentesaux, D. A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. *Appl. Sci.* **2022**, *12*, 4641. [[CrossRef](#)]
86. Kim, H.; Lee, K. IIoT Malware Detection Using Edge Computing and Deep Learning for Cybersecurity in Smart Factories. *Appl. Sci.* **2022**, *12*, 7679. [[CrossRef](#)]
87. Alzarrad, A.; Miller, M.; Chowdhury, S.; McIntosh, J.; Perry, T.; Shen, R. Harnessing Virtual Reality to Mitigate Heat-Related Injuries in Construction Projects. *CivilEng* **2023**, *4*, 1157–1168. [[CrossRef](#)]
88. Li, C.; Wang, J.; Wang, S.; Zhang, Y. A Review of IoT Applications in Healthcare. *Neurocomputing* **2024**, *565*, 127017. [[CrossRef](#)]
89. Javed, S.; Ghazala, S.; Faseeha, U. Perspectives of Heat Stroke Shield: An IoT Based Solution for the Detection and Preliminary Treatment of Heat Stroke. *Eng. Technol. Appl. Sci. Res.* **2020**, *10*, 5576–5580. [[CrossRef](#)]
90. Kakamu, T.; Endo, S.; Hidaka, T.; Masuishi, Y.; Kasuga, H.; Fukushima, T. Heat-Related Illness Risk and Associated Personal and Environmental Factors of Construction Workers during Work in Summer. *Sci. Rep.* **2021**, *11*, 1119. [[CrossRef](#)]
91. SlateSafety. Available online: <https://slatesafety.com/> (accessed on 10 October 2024).
92. Callihan, M.; Cole, H.; Stokley, H.; Gunter, J.; Clamp, K.; Martin, A.; Doherty, H. Comparison of Slate Safety Wearable Device to Ingestible Pill and Wearable Heart Rate Monitor. *Sensors* **2023**, *23*, 877. [[CrossRef](#)]
93. Kenzen. Available online: <https://kenzen.com/> (accessed on 14 October 2024).
94. Kenzen. Available online: <https://kenzen.com/end-to-end-health-and-safety-monitoring/> (accessed on 14 October 2024).
95. Garney. Available online: <https://www.garney.com/about/safety/> (accessed on 14 October 2024).
96. Pech, M.; Vrchota, J.; Bednář, J. Predictive Maintenance and Intelligent Sensors in Smart Factory: Review. *Sensors* **2021**, *21*, 1470. [[CrossRef](#)]
97. Wang, H.; Zhang, W.; Yang, D.; Xiang, Y. Deep-Learning-Enabled Predictive Maintenance in Industrial Internet of Things: Methods, Applications, and Challenges. *IEEE Syst. J.* **2023**, *17*, 2602–2615. [[CrossRef](#)]
98. Nangia, S.; Makkar, S.; Hassan, R. IoT Based Predictive Maintenance in Manufacturing Sector. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC), New Delhi, India, 20–22 February 2020. [[CrossRef](#)]
99. Chen, L.; Wei, L.; Wang, Y.; Wang, J.; Li, W. Monitoring and Predictive Maintenance of Centrifugal Pumps Based on Smart Sensors. *Sensors* **2022**, *22*, 2106. [[CrossRef](#)] [[PubMed](#)]
100. Fordal, J.M.; Schjølberg, P.; Helgetun, H.; Skjermo, T.Ø.; Wang, Y.; Wang, C. Application of Sensor Data Based Predictive Maintenance and Artificial Neural Networks to Enable Industry 4.0. *Adv. Manuf.* **2023**, *11*, 248–263. [[CrossRef](#)]
101. Ayvaz, S.; Alpay, K. Predictive Maintenance System for Production Lines in Manufacturing: A Machine Learning Approach Using IoT Data in Real-Time. *Expert Syst. Appl.* **2021**, *173*, 114598. [[CrossRef](#)]
102. Gbadamosi, A.-Q.; Oyedele, L.O.; Delgado, J.M.D.; Kusimo, H.; Akanbi, L.; Olawale, O.; Muhammed-Yakubu, N. IoT for Predictive Assets Monitoring and Maintenance: An Implementation Strategy for the UK Rail Industry. *Autom. Constr.* **2021**, *122*, 103486. [[CrossRef](#)]
103. Sang, G.M.; Xu, L.; De Vrieze, P. A Predictive Maintenance Model for Flexible Manufacturing in the Context of Industry 4.0. *Front. Big Data* **2021**, *4*, 663466. [[CrossRef](#)]
104. Smagulova, K.; James, A.P. A Survey on LSTM Memristive Neural Network Architectures and Applications. *Eur. Phys. J. Spec. Top.* **2019**, *228*, 2313–2324. [[CrossRef](#)]
105. Rosati, R.; Romeo, L.; Cecchini, G.; Tonetto, F.; Viti, P.; Mancini, A.; Frontoni, E. From Knowledge-Based to Big Data Analytic Model: A Novel IoT and Machine Learning Based Decision Support System for Predictive Maintenance in Industry 4.0. *J. Intell. Manuf.* **2023**, *34*, 107–121. [[CrossRef](#)]
106. Lakshminarayana, S.; Praseed, A.; Thilagam, P.S. Securing the IoT Application Layer from an MQTT Protocol Perspective: Challenges and Research Prospects. *IEEE Commun. Surv. Tutor.* **2024**. [[CrossRef](#)]
107. HariPriya, A.P.; Kulothungan, K. Secure-MQTT: An Efficient Fuzzy Logic-Based Approach to Detect DoS Attack in MQTT Protocol for Internet of Things. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 90. [[CrossRef](#)]
108. Ruiz-Sarmiento, J.-R.; Monroy, J.; Moreno, F.-A.; Galindo, C.; Bonelo, J.-M.; Gonzalez-Jimenez, J. A Predictive Model for the Maintenance of Industrial Machinery in the Context of Industry 4.0. *Eng. Appl. Artif. Intell.* **2020**, *87*, 103289. [[CrossRef](#)]
109. Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. Design and Development of an IoT Enabled Platform for Remote Monitoring and Predictive Maintenance of Industrial Equipment. *Procedia Manuf.* **2021**, *54*, 166–171. [[CrossRef](#)]
110. Kannagi, A.; Gori Mohammed, J.; Sabari Giri Murugan, S.; Varsha, M. Intelligent Mechanical Systems and Its Applications on Online Fraud Detection Analysis Using Pattern Recognition K-Nearest Neighbor Algorithm for Cloud Security Applications. *Mater. Today Proc.* **2023**, *81*, 745–749. [[CrossRef](#)]
111. Civerchia, F.; Bocchino, S.; Salvadori, C.; Rossi, E.; Maggiani, L.; Petracca, M. Industrial Internet of Things Monitoring Solution for Advanced Predictive Maintenance Applications. *J. Ind. Inf. Integr.* **2017**, *7*, 4–12. [[CrossRef](#)]
112. Teoh, Y.K.; Gill, S.S.; Parlikad, A.K. IoT and Fog-Computing-Based Predictive Maintenance Model for Effective Asset Management in Industry 4.0 Using Machine Learning. *IEEE Internet Things J.* **2023**, *10*, 2087–2094. [[CrossRef](#)]
113. Liu, X.; Fan, L.; Xu, J.; Li, X.; Gong, L.; Grundy, J.; Yang, Y. FogWorkflowSim: An Automated Simulation Toolkit for Workflow Performance Evaluation in Fog Computing. In Proceedings of the 34th International Conference on Automated Software Engineering (ASE), San Diego, CA, USA, 11–15 November 2019; IEEE/ACM: New York, NY, USA, 2019; pp. 1114–1117. [[CrossRef](#)]

114. Natanael, D.; Sutanto, H. Machine Learning Application Using Cost-Effective Components for Predictive Maintenance in Industry: A Tube Filling Machine Case Study. *J. Manuf. Mater. Process.* **2022**, *6*, 108. [\[CrossRef\]](#)
115. Alhijawi, B.; Awajan, A. Genetic Algorithms: Theory, Genetic Operators, Solutions, and Applications. *Evol. Intell.* **2024**, *17*, 1245–1256. [\[CrossRef\]](#)
116. Mellado, J.; Núñez, F. Design of an IoT-PLC: A Containerized Programmable Logical Controller for the Industry 4.0. *J. Ind. Inf. Integr.* **2022**, *25*, 100250. [\[CrossRef\]](#)
117. Khan, S.I.; Kaur, C.; Al Ansari, M.S.; Muda, I.; Borda, R.F.C.; Bala, B.K. Implementation of Cloud Based IoT Technology in Manufacturing Industry for Smart Control of Manufacturing Process. *Int. J. Interact. Des. Manuf. (IJIDeM)* **2023**. [\[CrossRef\]](#)
118. Christou, I.T.; Kefalakis, N.; Soldatos, J.K.; Despotopoulou, A.-M. End-to-End Industrial IoT Platform for Quality 4.0 Applications. *Comput. Ind.* **2022**, *137*, 103591. [\[CrossRef\]](#)
119. Garmaroodi, M.S.S.; Farivar, F.; Haghighi, M.S.; Shoorehdeli, M.A.; Jolfaei, A. Detection of Anomalies in Industrial IoT Systems by Data Mining: Study of CHRIST Osmotron Water Purification System. *IEEE Internet Things J.* **2021**, *8*, 10280–10287. [\[CrossRef\]](#)
120. Bhaskaran, P.E.; Maheswari, C.; Thangavel, S.; Ponnibala, M.; Kalavathidevi, T.; Sivakumar, N.S. IoT Based Monitoring and Control of Fluid Transportation Using Machine Learning. *Comput. Electr. Eng.* **2021**, *89*, 106899. [\[CrossRef\]](#)
121. Xia, K.; Sacco, C.; Kirkpatrick, M.; Saidy, C.; Nguyen, L.; Kircaliali, A.; Harik, R. A Digital Twin to Train Deep Reinforcement Learning Agent for Smart Manufacturing Plants: Environment, Interfaces and Intelligence. *J. Manuf. Syst.* **2021**, *58*, 210–230. [\[CrossRef\]](#)
122. Barbieri, G.; Bertuzzi, A.; Capriotti, A.; Ragazzini, L.; Gutierrez, D.; Negri, E.; Fumagalli, L. A Virtual Commissioning Based Methodology to Integrate Digital Twins into Manufacturing Systems. *Prod. Eng. Res. Dev.* **2021**, *15*, 397–412. [\[CrossRef\]](#)
123. Muruganandam, S.; Salameh, A.A.; Pozin, M.A.A.; Manikathan, S.V.; Padmapriya, T. Sensors and Machine Learning and AI Operation-Constrained Process Control Method for Sensor-Aided Industrial Internet of Things and Smart Factories. *Meas. Sens.* **2023**, *25*, 100668. [\[CrossRef\]](#)
124. Li, L.; Fan, Y.; Tse, M.; Lin, K.-Y. A Review of Applications in Federated Learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. [\[CrossRef\]](#)
125. Shin, K.-Y.; Park, H.-C. Smart Manufacturing Systems Engineering for Designing Smart Product-Quality Monitoring System in the Industry 4.0. In Proceedings of the 19th International Conference on Control, Automation and Systems (ICCAS), Jeju, Republic of Korea, 15–18 October 2019; IEEE: New York, NY, USA, 2019; pp. 1693–1698. [\[CrossRef\]](#)
126. Altıparmak, S.C.; Yardley, V.A.; Shi, Z.; Lin, J. Extrusion-Based Additive Manufacturing Technologies: State of the Art and Future Perspectives. *J. Manuf. Process.* **2022**, *83*, 607–636. [\[CrossRef\]](#)
127. Xames, M.D.; Torsha, F.K.; Sarwar, F. A Systematic Literature Review on Recent Trends of Machine Learning Applications in Additive Manufacturing. *J. Intell. Manuf.* **2023**, *34*, 2529–2555. [\[CrossRef\]](#)
128. Ashima, R.; Haleem, A.; Bahl, S.; Javaid, M.; Kumar Mahla, S.; Singh, S. Automation and Manufacturing of Smart Materials in Additive Manufacturing Technologies Using Internet of Things towards the Adoption of Industry 4.0. *Mater. Today Proc.* **2021**, *45*, 5081–5088. [\[CrossRef\]](#)
129. Fedullo, T.; Morato, A.; Peserico, G.; Trevisan, L.; Tramarin, F.; Vitturi, S.; Rovati, L. An IoT Measurement System Based on LoRaWAN for Additive Manufacturing. *Sensors* **2022**, *22*, 5466. [\[CrossRef\]](#)
130. Majeed, A.; Zhang, Y.; Ren, S.; Lv, J.; Peng, T.; Waqar, S.; Yin, E. A Big Data-Driven Framework for Sustainable and Smart Additive Manufacturing. *Robot. Comput.-Integr. Manuf.* **2021**, *67*, 102026. [\[CrossRef\]](#)
131. Armstrong, M.; Mehrabi, H.; Naveed, N. An Overview of Modern Metal Additive Manufacturing Technology. *J. Manuf. Process.* **2022**, *84*, 1001–1029. [\[CrossRef\]](#)
132. Moshiri, M.; Charles, A.; Elkaseer, A.; Scholz, S.; Mohanty, S.; Tosello, G. An Industry 4.0 Framework for Tooling Production Using Metal Additive Manufacturing-Based First-Time-Right Smart Manufacturing System. *Procedia CIRP* **2020**, *93*, 32–37. [\[CrossRef\]](#)
133. Gunasegaram, D.R.; Murphy, A.B.; Matthews, M.J.; DebRoy, T. The Case for Digital Twins in Metal Additive Manufacturing. *J. Phys. Mater.* **2021**, *4*, 040401. [\[CrossRef\]](#)
134. Haw, J.; Sing, S.L.; Liu, Z.H. Digital Twins in Design for Additive Manufacturing. *Mater. Today Proc.* **2022**, *70*, 352–357. [\[CrossRef\]](#)
135. Guo, L.; Cheng, Y.; Zhang, Y.; Liu, Y.; Wan, C.; Liang, J. Development of Cloud-Edge Collaborative Digital Twin System for FDM Additive Manufacturing. In Proceedings of the 19th International Conference on Industrial Informatics (INDIN), Palma de Mallorca, Spain, 21–23 July 2021; IEEE: New York, NY, USA, 2021; pp. 1–6. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.