sensors

Article

Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability

Attila Frankó, Gergely Hollósi, Dániel Ficzere and Pal Varga *

Department of Telecommunications and Media Informatics, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary
* Correspondence: pvarga@tmit.bme.hu

Abstract: Industrial IoT (IIoT) has revolutionized production by making data available to stakeholders at many levels much faster, with much greater granularity than ever before. When it comes to smart production, the aim of analyzing the collected data is usually to achieve greater efficiency in general, which includes increasing production but decreasing waste and using less energy. Furthermore, the boost in communication provided by IIoT requires special attention to increased levels of safety and security. The growth in machine learning (ML) capabilities in the last few years has affected smart production in many ways. The current paper provides an overview of applying various machine learning techniques for IIoT, smart production, and maintenance, especially in terms of safety, security, asset localization, quality assurance and sustainability aspects. The approach of the paper is to provide a comprehensive overview on the ML methods from an application point of view, hence each domain—namely security and safety, asset localization, quality control, maintenance—has a dedicated chapter, with a concluding table on the typical ML techniques and the related references. The paper summarizes lessons learned, and identifies research gaps and directions for future work.

Keywords: machine learning; industry 4.0; industrial IoT; safety; security; asset localization; quality control; proactive maintenance; fault detection; prognostics

check for updates

Citation: Frankó, A.; Hollósi, G.; Ficzere, D.; Varga, P. Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability. *Sensors* **2022**, *22*, 9148. https://doi.org/10.3390/s22239148

Academic Editors: Raffaele Bruno, Leopoldo Angrisani, Nikos Fotiou and Ismail Butun

Received: 7 November 2022
Accepted: 21 November 2022
Published: 25 November 2022

1. Introduction

The motivations for industrial data processing have been the same for decades, namely to increase the revenue of investment by improving efficiency (i.e., by increasing productivity, and decreasing scrap, waste and energy usage), extending system lifetime, as well as enhancing safety and security. Sustainability has become yet another focal point of modern industry.

As people acknowledged the necessity of distributed data collection and massive data processing in various industrial areas, the research and innovation domain of IIoT (Industrial Internet of Things) began to thrive. Its business drive was promoted by the Industry 4.0 initiative, whereas its applications were extended from the very much overlapping Cyber-Physical Systems (CPS) domain. There is no generic, de-facto architecture for IIoT systems, although a layered approach is followed by domain experts. The purpose of splitting the layers could vary from communication types due to infrastructure need to the ecosystem stakeholder point of view; hence three, four or five layers can be identified. Figure 1 provides a layered architectural view which shows the strong separation of technologies between the layers. It also indicates the different security approaches at the different layers [1].

While machine learning is exploited in various IIoT application areas, it is used only on a small subset of target areas extensively (see Figure 2). Depending on the application area, there are various purposes for processing industrial data. These include decision support, optimization, prediction, anomaly detection, classification, and clustering, just to name a few. In order to achieve the desired results, we need data—which are generally available for industrial players if IIoT-based data collection is in place—and we need physical resources for data processing—which are now available mostly due to the boom in GPU production. Because data and resources have been made available, we are able to use ML (Machine Learning) methods to achieve better results than ever before in the above areas.

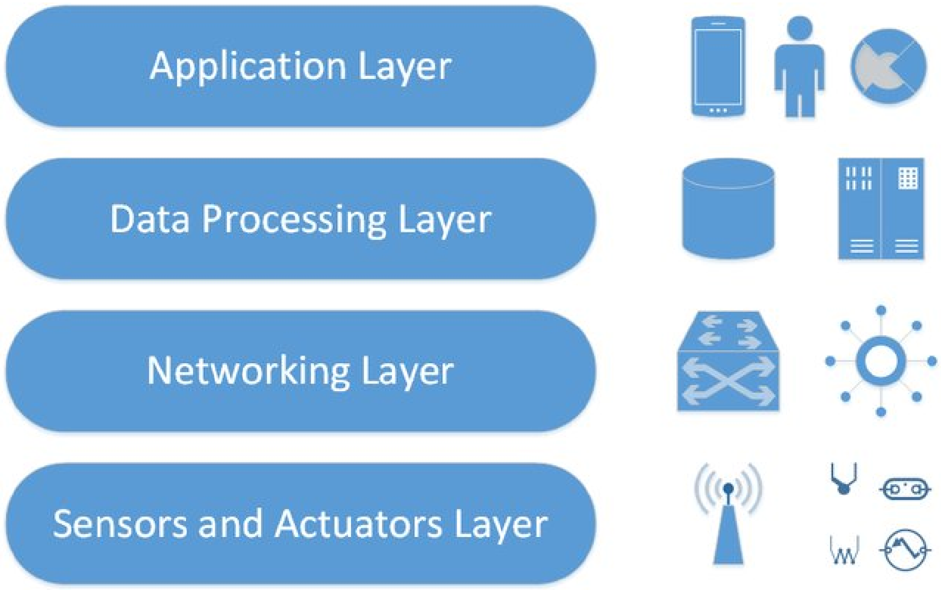

Figure 1. The architectural layers of IIoT systems [1].

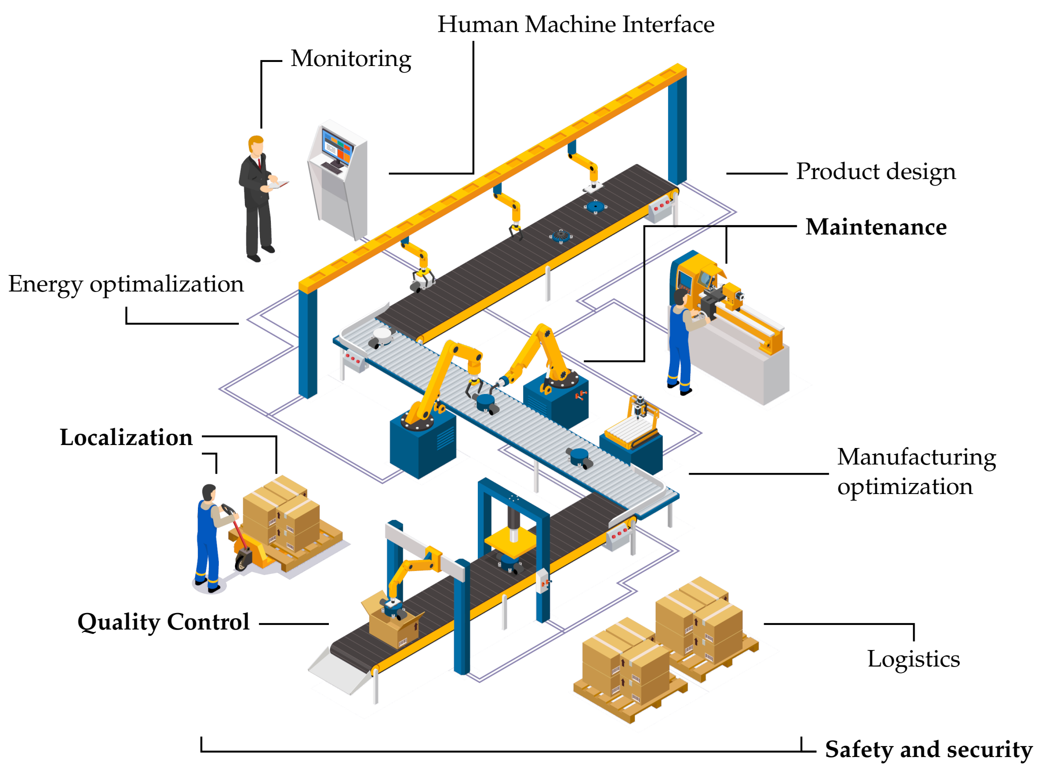

Figure 2. Production stages typically covered by the process of manufacturing. While machine learning can be applied in all areas of manufacturing, only a small subset of them use machine learning techniques extensively (shown in bold typeset).

In terms of finding details on these methods, the first resources to turn to are, naturally, textbooks. There are several great books on machine learning in general [2–4], and on modern tools regarding their application [5–8]. Further, we can find survey papers on utilizing machine learning in the industry. The authors of [9] provide a survey of the upcoming wave of machine learning in smart manufacturing. The specific topic of tackling faults by machine learning (ML) in the industry 4.0 era are surveyed in [10]. In a paper on machine learning multi-agent systems [11], the authors focus exclusively on their application in the oil and gas industry. Regarding different levels of industry 4.0, [12] focuses on ML methods applied in production planning and control. Similarly, a review of ML methods for the optimization of production processes is provided in [13].

To provide comparison with the topic of our current article, we can find more specific papers summarizing ML methods for smart production in general [14], or that review ML for production energy efficiency [15]. The authors of [16] provide a comprehensive overview of prognostic methods in the area of Industry 4.0. The authors of [17] focus on sustainability and predictive maintenance. Regarding reliability engineering and safety, the authors of [18] provide a targeted survey. Furthermore, ML support on safety assurance is surveyed in [19].

The main contribution of this paper is that it provides a structured state-of-the-art view of the domain, with well-structured comparison tables and details of the knowledge in this industry thus far. Although the area is very much an interest of industrial innovation, there is currently no structured, application-oriented overview available on machine learning methods in the Industrial Internet of Things (IIoT) domain. In particular, no complete overview of production quality, safety, maintenance and sustainability has been made available. Therefore, the aim of this current study is to fill this gap by providing a comprehensive overview of applied machine learning techniques within the aforementioned fields. Moreover, the paper also groups these applications by their main purposes to provide a deeper understanding of which techniques are used for certain typical tasks.

The structure of the paper is as follows. Each chapter addresses an application area, and provides a general overview of the issues and target solutions. Application examples are provided with the related ML methods. There are summary tables in each chapter, and a lessons learned section to highlight the main points. As such, Section 2 focuses on safety, security issues and solutions, Section 3 describes the main achievements in asset localization, Section 4 provides an overview of the methods and application use-cases for quality control, Section 5 targets maintenance and sustainability, and Section 6 concludes the paper.

2. Safety and Security

Industrial IoT is a convergence area of Operational Technology (OT) and Information Technology (IT), both of which contribute to the safety and security issues of Industrial IoT. Security and safety is undoubtedly one of the most important aspects of IIoT. To underline this, the Industry IoT Consortium has published a technical report [20] about the security issues in IIoT systems, summarizing all the experience and knowledge of the consortium.

The main goal in IIoT systems is reaching the trustworthy status, where trustworthiness "is the degree of confidence one has that the system performs as expected in respect to all the key system characteristics in the face of environmental disruptions, human errors, system faults and attacks". Figure 3 shows the key system characteristics of a trustworthy system when resisting external or internal threats. The key characteristics are [21]:

Security —Security ensures that the system is protected from unintended or unauthorized access, change, or destruction.

Privacy —Privacy provides organizations control over the collection, processing, and storage of their information, by deciding how this information can be shared both within their own organization and with others.

Reliability —Reliability guarantees that the system's operation is uninterrupted and error-free for the specified time. Availability is related to reliability, but also takes into account planned operation stops.

Safety – System Safety ensures that the people, property and environment are not at any unacceptable risk during the system's operation.

Resilience —System resilience provides a way to dynamically avoid, absorb and rapidly recover from changing adverse conditions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

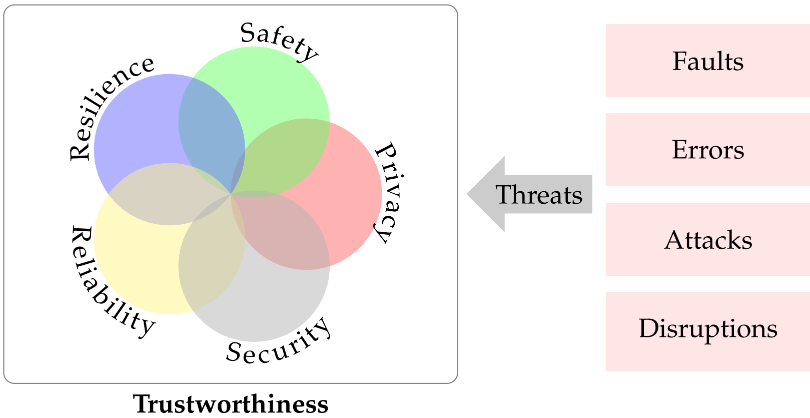

Figure 3. Trustworthiness of an IIoT System as specified by the Industrial IoT Consortium [20]. The key characteristics of the trustworthy IoT system are security, privacy, reliability, safety and resilience.

While a secure and safe industrial IoT system requires appropriate system design, implementation and deployment, machine learning-based solutions are widely used to provide additional layers of security and safety. There are a couple of survey works that review the security issues of IIoT systems, mainly focusing on general security issues; however, machine learning-based solutions are presented as well in [1,22]. In [23], a layer-wise analysis of security issues and solutions are shown, specifically, in 5G-based IIoT systems. Moreover, ref. [24] applies a layer-wise approach; besides information on common security issues, it provides an in-depth overview of the security aspects of edge and fog computing.

While all the key characteristics of trustworthy IIoT systems are important, most of the machine learning-based solutions concern protection against unintended and unauthorized access (i.e., security). One of its typical application areas is *intrusion detection* in which the learning method tries to detect unauthorized access to the system from arbitrary features, e.g., system logs, monitoring services, etc. To achieve this, most works use supervised learning techniques (i.e., classification) to detect intrusion from features, e.g., k-nearest neighbour (kNN) [25], support vector machines (SVM) [26–28], decision trees [29], Bayes networks [30–32], random forests [33] and also neural networks [34–36]. Besides common classification solutions, fuzzy methods and association-based methods can be found [37]. In the past, hidden Markov models (HMM) were also proposed [38,39]. The subject of intrusion detection is so extensive that a couple of comprehensive survey papers focus on this topic alone [40,41]. While classification is widely applied to intrusion detection, intrusion can be seen as an outlier against authorized users. The survey provided in [42] reviews the application areas of outlier detection in IoT systems, summarizing examples of intrusion detection in the field of IIoT. Alongside intrusion detection, a wider level of *anomaly detection* can be acquired using machine learning in IIoT systems, by applying unsupervised or supervised methods to identify outliers or abnormal behavior in the system [43–45].

Strongly related to intrusion detection, *authentication* can be supported by machine learning techniques. Machine learning algorithms alone are rarely used for authentication purposes; however, it can provide an additional security layer over classical authentication schemes. Authentication based on network traffic analysis is performed in [46], using ensemble learning techniques. WiFi-capable IoT devices can be authenticated through the actuation of daily activities, as shown in [47]. Bregman divergence combined with the k-nearest neighbour technique makes it possible to detect Man-in-the-Middle attacks during authentication [48]. Furthermore, using stacked autoencoders (SAE) and k-means clustering, a high accuracy was reached in detecting WiFi impersonation attacks [49]. Blockchains play an important role in IIoT systems security; they are applied for various purposes, e.g., for distributed secure databases. The authentication of users to access blockchain is often integrated with a deep learning method that is taught by transfer learning [50,51]. Interestingly, authentication can be performed in the physical layer alone. Ref [25] proposes a solution to authenticate IoT devices with RF fingerprinting, using a software-defined radio (SDR) solution. The paper investigates different machine learning methods, kNN, SVM and decision trees, and all are proved to be accurate enough to perform authentication based solely on RF information.

Privacy is mostly ensured by encryption (using cryptography); however, there are certain issues regarding IIoT systems. While a couple of machine learning methods have been applied (e.g., in intrusion detection, authentication, etc.), the training of deep neural networks requires extensive datasets. Besides public datasets, it is commonly required to train the networks on distributed real datasets; however, this can result in the so called "privacy leaking". There are solution and works that propose methods to avoid privacy leaking, e.g., privacy-preserving asynchronous deep learning schemes (DeepPAR [52]) or differential privacy and federated learning [53]. There are other methods for ensuring IIoT privacy using differential privacy; a thorough review can be found in [54].

Data integrity is a crucial part of a trustworthy IIoT system. Data integrity means that data are not modified over their lifetime; the data remain consistent and accurate. One of the most prevalent attacks against data integrity is false data injection (FDI); however, data integrity refers to all the possible combinations of data injection, data modification or even data relation disintegrity. The methods for data integrity checks commonly learn the distribution of valid data and identify outlier samples with a low likelihood. Data and the command injection were reviewed in [55], where a gas pipeline system remote terminal unit (RTU) was observed. Using six machine learning techniques (e.g., random forests, SVM, etc.), the injection attacks were accurately identified. Using k-means clustering, ref. [56] proposes a method for recognizing data modification in programmable logic controllers (PLC). In [57], deep belief networks and restricted Boltzmann-machines were applied to identify data injection attacks in smart grids. Using smart sensor data from a complex hydraulic IIoT system, autoencoders were trained to help avoid false data attacks in [58].

A reliable trustworthy IIoT systems requires high *availability*, meaning, that the system is ready to provide services to users. However, a common attack against IIoT devices is the so called denial-of-service (DoS) attack, which—by applying huge work load—prevents the device from providing services, and leads to it becoming temporarily unavailable. A common variation of this attack is the distributed DoS (DDoS) originating from a number of sources. Using a couple of network and log features, ref. [59] proposes a hybrid deep learning framework (deep belief networks, autoencoders, etc.) to classify the type of attack reaching the device, e.g., DoS attacks, among others. Using the game-theory approach, a reinforcement learning technique was proposed in [60] to identify DDoS attacks. Bayesian networks can also be successfully used to predict traffic delays and DDoS attacks; for example, in [61] the solution was inspired by the portfolio theory used in economics.

Industrial IoT systems have a special security issue, called *offload security*. Using machine learning algorithms in IIoT systems sometimes requires different calculations to be offloaded to edge devices, called edge or fog computing. This offloading gives rise to new kinds of security problems, since offloading tasks to the cloud or to the edge is vulnerable to security issues due to malicious devices. A typical solution uses blockchains and the reinforcement learning method to avoid the security problems of computation offloading, while implementing a double-dueling Q-network [62]. Other solutions typically use reinforcement learning methods, such as the solution in [63,64].

2.1. Datasets

There are a couple of public datasets available to train and validate machine learning algorithms in the topic of IIoT security. Reviewing these datasets can provide a deeper understanding of the machine learning algorithms, revealing the possible features and outcomes of each algorithm. The works presented before usually trained on these datasets.

One of the most famous intrusion detection datasets is the "The Third International Knowledge Discovery and Data Mining Tools Competition" KDD-99 dataset [65]. The dataset was prepared using the DARPA project, and contains 4 GB of network traffic from a period of seven weeks, containing attacks of four categories (DOS, R2L, U2R, probing).

The Canadian Institute for Cybersecurity provides a number of datasets regarding cyber security. The CSE-CIC-IDS2018 dataset [66] contains seven different attack scenarios in an infrastructure of 420 machines and 30 servers. Additionally, the institute provides a state-of-the-art dataset for detecting DDoS attacks [67].

Further datasets for intrusion detection and privacy attacks can be found in [68,69]. The University of Arizona provides datasets [70] for various security purposes, e.g., malware detection, intrusion detection, etc., as well.

2.2. Critics of Machine Learning Based Security

Zolanvari's work [71] provided some criticisms regarding IIoT security and the datasets used for training purposes. Most machine learning-based algorithms and solutions for IIoT security (e.g., intrusion detection, DDoS prevention) need some data for the training and validation phases. For example, network traffic datasets require carefully selected features for the machine learning algorithms to function properly. If the features do not vary with the attack, the algorithm cannot be successful. Additionally, sensor data in IIoT applications are usually obtained with different sampling frequencies over an extended time, which results in high dimensional datasets. Using raw data such as this will lead to a large delay in training and detecting processes. Furthermore, it is hard to acquire real IIoT data from companies due to confidentiality and privacy restrictions; therefore, all the solutions presented typically are trained on the same publicly available datasets. Interestingly, the main problem with the available datasets is that the number of real attacks are significantly low compared to normal behavior; the highly unbalanced datasets make it hard to train learning algorithms effectively.

2.3. Summary of Security and Safety

Machine learning in IIoT security is widely used as an additional layer of security to provide a truly trustworthy system. However, the usually applied techniques are limited to a couple well-defined of use cases. The most important are the intrusion detection methods, or more generally, anomaly detection methods. Most works train and utilize SVM or Bayesian networks to recognize unusual behavior or—explicitly—intrusion. Numerous methods are also applied in the authentication process, even in the case of authentication without credentials, e.g., only in the physical layer. The other key area of machine learning algorithms in IIoT security is that of the detection and avoidance of DDoS attacks, using unsupervised techniques, e.g., autoencoders. A special area of IIoT security is the security issues resulting from offloading calculations in edge computing, i.e., the so called offload security. Machine learning methods require training to perform successfully, for which a couple of publicly available datasets are available; however, some researchers are against using these datasets to train and validate secure machine learning-based solutions. The references for different applications presented in this section are shown in Table 1.

Table 1. Summary of applications of machine learning techniques in IIoT security and safety.

Application	Typical Machine Learning Techniques	References
Intrusion detection	Classification on network data (SVM, Bayes networks, decision tree, Random forest, neural network)	[25–42]
Authentication	Classification on network data, Clustering	[25,46–51]
Privacy leaking	Differential privacy and federated learning	[52–54]
Data integrity	Latent space methods (Boltzmann-machine, DBN), Classification (Random Forest, SVM)	[55–58]
Availability	Reinforcement learning and Neural networks (DBN, autoencoders)	[59–61]
Offload security	Reinforcement learning	[62–64]

3. Asset Localization

Asset localization is one of the most important and specialized features of IIoT systems, because either the manufacturing process or site security requires the location of—potentially semi-finished—products or assets to be tracked. There are a couple of typical use-cases for asset tracking and localization, which are depicted on Figure 4. While localization is mostly achieved with GPS (Global Positioning System) outdoor, it cannot be applied in indoor factories since the GPS signal is shadowed by the structure of the building. To overcome this issue, a couple of radio-based technologies are utilized and employed to provide a more or less accurate asset position in indoor situations. More specifically, all the radio technologies used in IoT or IIoT systems can provide measurements to acquire asset position; however, some solutions are more suitable for asset localization than others.

At first sight, localization is a geometric problem, because the properties of radio signal propagation can be calculated, i.e., the equations for the attenuation and the propagation delay are well-known. However, in indoor situations, especially on industrial sites, the dense multipath environment makes the propagation so random and stochastic that the received signal and its properties contain little information about the propagation. That is why a number of works apply complex machine learning methods to solve the localization problem instead of solving the geometrical problem. However, machine learning methods are also frequently used to improve the accuracy of the geometric solution.

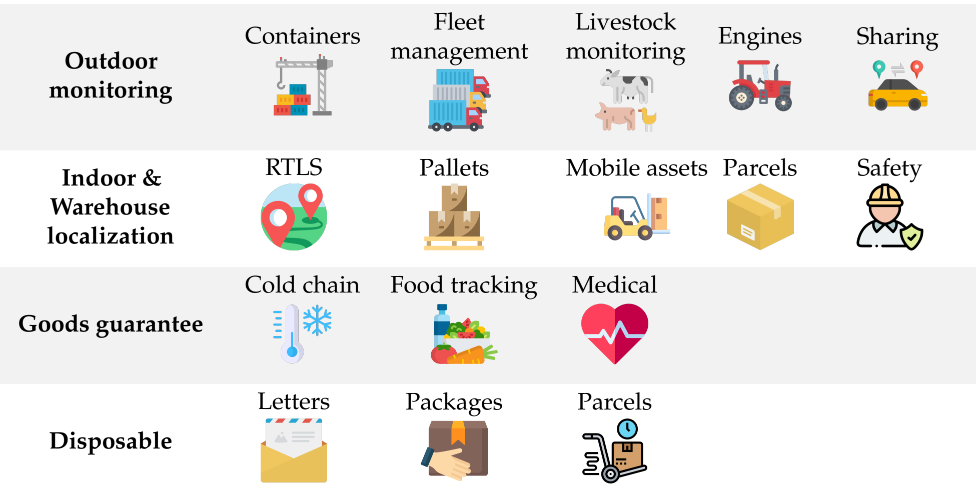

Figure 4. Typical use-cases for industrial indoor and outdoor asset tracking and localization. Beyond classical indoor and outdoor use-cases, there are a couple of less know topics, e.g., tracing the food chain or tracking disposable items (icons from Flaticon.com).

3.1. UWB

Ultra-Wideband (UWB) technologies are widely used in IIoT solutions to provide accurate localization, since UWB—by design—is especially suited to localization purposes.

The huge bandwidth (a couple of hundreds megahertz) of UWB makes it possible to apply very short pulses (e.g., 1–2 ns long) which helps to distinguish between the rays in multipath propagation to provide accurate timestamps for the received packets, resulting in a centimeter-capable localization. The method of location estimation in UWB systems is usually based on the calculation of the distances between anchors and tags (i.e., ranging); based on these calculated data, the geometric problem is solved by optimization. However, multipath propagation can distort the received signal, so errors in the timestamping process result in positioning errors.

To overcome this issue, ref. [72] investigates decision tree, random forest and kNN (k-nearest neighbour) algorithms to improve the accuracy of localization based purely on the calculated location information. A more sophisticated solution is to use the indicator provided by the receiver which helps to determine whether the timestamp belongs to the real first path (line-of-sight, LOS) or not (non line-of-sight, NLOS). Based on this information, ref. [73] uses a naive Bayes method to infer the improved position for the device.

In fact, machine learning methods are widely used in UWB systems to classify the reception as LOS or NLOS propagation. These methods are supported by the fact that most UWB chips provide the received channel impulse response (CIR) of the packet. Using CIR, the study in [74] trains a convolutional neural network to classify the reception of a packet as an LOS and NLOS reception, which helps the localization engine to weigh the measurement while calculating the position. Ref [75] also targets the classification of reception; however, it compares three machine learning techniques, namely support vector machines, random forests and dense neural networks. To make use of the temporal behaviour of the channel impulse response, ref. [76] investigates different combinations of convolutional neural networks and recurrent neural networks for CIR classification, showing that a CNN followed by stacked LSTM networks provides the best accuracy. The CIR can be used not only for classification, but for estimating the timestamping error of each of the received packets. Ref [77] uses convolutional networks to predict the error in timestamping based on the CIR of received packets, resulting in a one-order improvement in location accuracy on average compared to the geometric solution. The survey in [78] presents a couple of other UWB-based solutions, although not exclusively in the IIoT environment. A general approach for estimation of the position from CIR using deep learning techniques can be found in [79].

3.2. 5G

5G is a cutting-edge mobile technology, which supports on site installations besides large-scale infrastructure. In the 5G standard, great effort was made to improve the positioning capabilities of the previous LTE standard; since Release 17, IIoT localization has become an important topic of the standard [80]. 5G provides time- and angle-based positioning, and the variable parameters of the NR (New Radio) interface help to improve the accuracy of 5G positioning (e.g., higher bandwidth, variable subcarrier spacing, different antenna patterns, etc.).

While 5G supports different kinds of localization methods, these are mainly geometrical or closed-form solutions. However, a couple of works, which aim to improve the accuracy of the localization using machine learning methods, can be found—mainly concerning an IIoT environment, i.e., in indoor situations. One typical positioning method is "fingerprinting", which is based on readily observable radio channel properties, such as the receive signal strength (RSSI). To improve the accuracy of such solutions, ref. [81] tries to estimate and correct the error of the location using different machine learning models. To estimate the position, the kNN technique and vanilla neural networks were compared. Targeting the same problem, ref. [82] compares kNN- and SVR- (Support Vector Regression) based techniques to the defined DELTA method, which implements a dense neural network to infer the position from RSSI measurements.

A more sophisticated method in 5G localization is angle-based positioning. Using beamforming, the technique in [83] samples the received PDPs (Power Delay Profile), creates beamformed fingerprints and uses trained temporal convolutional neural networks (TCN) and LSTM networks to infer the location from the beamformed fingerprint. The TCN network is capable of tracking the location with an accuracy of a couple of meters on average. The solution has low energy consumption, even compared to GPS systems. Also using deep neural networks, ref. [84] optimizes the handover process by improving 5G localization based on beamforming. The solution's accuracy proved to be 1.25 m on average.

A comprehensive study on 5G and positioning can be found in [85], where a couple of methods—including machine learning-aided localization methods—are compared and introduced.

3.3. WiFi and Bluetooth Low Energy

The WiFi standard (IEEE 802.11) provides broadband communication technology, which is widely used in commercial and industrial areas. Without special hardware, WiFi localization solutions usually use fingerprinting techniques. To improve localization accuracy, a variety of trained machine learning models are used. The study in [86] compares the baseline kNN solution to the SVM and Random Forest techniques, while [87] integrated decision trees and naive Bayes methods to the comparison. The papers [88,89] use dense neural networks to learn fingerprint and localization mapping, while [90] utilizes denoising autoencoders to augment the received fingerprints and estimate the accurate location of the asset.

Bluetooth Low Energy (BLE) provides low-range, low-speed communication using low energy, and is widely used in a variety of areas. The basic localization technique in case of BLE is fingerprinting, and the same methods can be applied to improve the accuracy as in the WiFi case. However, there are works specifically related to BLE. Ref. [91] applies a special data augmentation process to train and evaluate random forest, XGBoost, decision tree and kNN-based algorithms for inferring the position from the RSSI measurements. The augmentation process helps learners to handle RSSI measurements with high fluctuation, thereby providing more accurate predictions. Ref. [92] is interesting as it introduces the applicability of the well-known LDA (Linear Discriminant Analysis) algorithm in fingerprinting. The work compares the LDA to naive Bayes, kNN and SVM techniques, showing an improvement in localization accuracy with a satisfactory execution time. A couple of other fingerprinting-based works can be found [93,94], and the study provided in [95] overviews the methods of fingerprinting in cases of BLE. Since the creation of Bluetooth 5.1, the BLE standard has made direction-of-arrival (DoA) methods available by using antenna arrays. Using the BLE DoA feature, [96] applies a tiny neural network applicable to a constrained device to replace the famous MUSIC (Multiple Signal Classification) algorithm when finding the signal direction.

3.4. Other

Apart from these widely used technologies, a couple of other solutions can be found in asset localization in IIoT systems. LOS/NLOS classification is shown in [97] for the less-common IEEE 802.15.4 systems, using SVM, random forests and neural networks. In [98], acoustic localization technology was employed in an IIoT underwater wireless sensor network, and linear regression was applied to predict the accuracy of node localization.

An increasing number of studies that analyze the applicability of the so-called device free localization (DFL), which provides user or asset location without any hardware attached, have been published. There are a couple of machine learning techniques utilized in those algorithms, e.g., block-sparse coding with the proximal operator [99] or Bayesian methods [100]. A useful summary of this topic and recent state-of-the-art can be found in [101,102].

3.5. Summary of Asset Localization

Asset localization in IIoT systems can be implemented using a variety of technologies, including UWB, 5G, WiFi, BLE, etc.; however, UWB is the only technology that specifically concentrates on localization. Machine learning methods are generally used for the following two purposes in case of each technology:

1. To learn the mapping between measurements and location
2. To improve the accuracy of the location deduced by closed-form, geometrical problems

The first is mainly used in case of fingerprinting—here, machine learning models try to learn the mapping between the measurements (mostly RSSI) and the location. The baseline solution is often the kNN learner; however, a couple of other regression methods are used, sometimes using classification on grids. The second one combines geometric models with machine learning models, where the following two basic methods can be distinguished: predicting LOS or NLOS propagation and predicting the localization error. The methods usually use additional information, e.g., the channel impulse response. The references for different applications presented in the section are shown in Table 2.

For further details, an in-depth study on indoor localization using machine learning techniques can be found in [103].

Table 2. Summary of applications of machine learning techniques in IIoT asset localization.

Application	Typical Machine Learning Techniques	References
Learning mapping between measurements and location	kNN, SVM, Random Forest, XGBoost, Regression tree, neural networks, etc.	[79,82,83,86–96]
Predicting non-LOS propagation	Neural network (CNN, TCN, etc.), SVM, Random Forests on channel impulse response	[72–76]
Predicting location error	Neural network on channel impulse	[77,81,98]

4. Quality Control

Quality control is a process by which entities review the quality of many factors involved in production. The primary responsibilities include monitoring, inspection, reducing product variation and eliminating failure cases. Functional and visual tests—often referred to as automated visual/surface inspection—are the two main steps of quality inspection in industrial manufacturing processes. Nowadays, both of these inspection categories are implemented by machines and not by humans in most cases; however, they rely on human expertise. Defective product detection demands well-defined quality requirements. To automate such quality inspection processes, these parameters have to be interpreted and tuned for specific automated identification processes, which is very challenging. Machine learning methods can help to overcome such difficulties.

4.1. Visual Quality Inspection

The existence of surface defects affects the product's appearance and quality in many industry domains. Therefore, one of the most widely applied quality inspection methods in manufacturing is the visual inspection of some aspects of the product. There are many solutions for surface and external defect inspection in many domains of the industry, including the metal, semi-conductor and fiber industries. This section introduces the main directions of visual quality inspection methods supported by machine learning. Figure 5 presents the general model for vision-based product quality inspection according to [104].

In general, defective product identification requires two well-defined steps, i.e., feature extraction and defect identification. Product features could be in the spatial domain or in the transform domain. Moreover, there are several feature extraction methods used in the state-of-the-art, including classification (KNN, Naive Bayes classifier, SVM, Decision trees), clustering (K-means, PCA) and regression (Linear regression, logistic regression) methods. With the advent of deep-learning algorithms, a set of features no longer needs to be designed, such as statistical or spectral features, as opposed to traditional methods. There are several examples in the state-of-the-art surface inspection for supervised (CNN, LSTM) and unsupervised (Autoencoder) learning solutions.

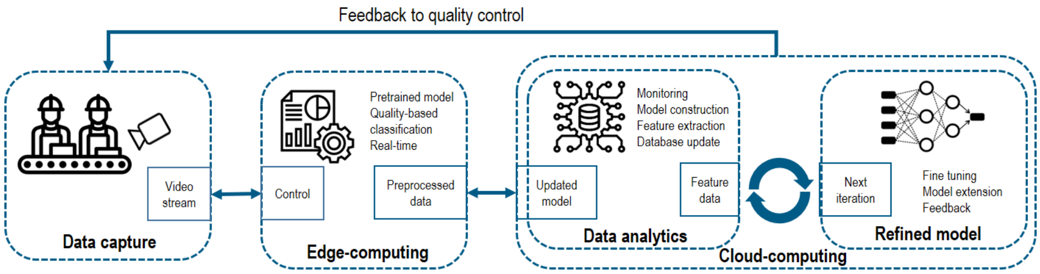

Figure 5. General architecture model for vision-based product quality inspection [104].

Ref. [105] presents a computer-vision system using machine learning approach to inspect both the internal and external parts of aerospace components. SVM is used to classify defects of the external parts of the product, while for defect classification of the internal parts, a combination of CNN and LSTM is applied. In contrast, ref. [106] presents a quality-level estimation system for the inspection of steel microstructures using the VGG network model. Ref. [107] uses Convolutional Neural Networks (CNN) and Convolutional Autoencoders (CAE) for casting surface inspection. Ref. [108] provides a solution based on supervised learning to inspect press-casting products using CNN, Random Forest, PCA, and XGBoost. Similarly, ref. [109] examines the application of supervised machine learning (random forest, gradient boosting) in defect detection, quality assurance and throughput improvement for optical transceiver manufacturing. Ref. [110] proposes a method for error detection by applying a CNN model to the optical inspection of assembling machines. The CNN-based solution is used in [111] for classifying Pin-in-Paste solder connections with a YOLOv4 architecture. The framework contains highly automatized image data labeling functionality using a Convolutional Autoencoder and near real-time solder joint localization based on a YOLO single-stage detector. Ref. [112] introduces surface defect detection for metal workpieces. The paper introduces both the results of ResNet50 and DenseNet40 architectures. Ref. [104] uses CNN and SVM for defect classification and provides a machine vision model to identify defective products. Ref. [113] introduces semi-supervised deep learning-based surface inspection techniques of labeled data for automated surface defect inspection. Ref. [114] presents an unsupervised clustering method of spatial patterns with wafer map measurement data. Measured test values are first pre-processed using computer vision techniques, followed by feature extraction based on variational autoencoders to decompose high-dimensional wafer maps into a low-dimensional latent representation.

4.2. Anomaly Detection

The other significant quality inspection category is anomaly detection. The goal of anomaly detection—also referred to as outlier detection—is to determine all instances dissimilar to the others or the required instances. Ref. [115] defines an outlier as an observation that deviates so significantly from other observations as to arouse suspicion that a different mechanism generated it. Ref. [116] introduces an architecture where the machine learning algorithm can detect defective bearings and continually tunes the quality testing process parameters. Specifically, the identification of defective bearings is performed using a voting classifier fed by statistical metrics measured from the collected experiments. The paper evaluates several machine learning methods, including k-neighbors, SVC, Decision Tree, Random Forest, Multi-Layer Perceptron, AdaBoost, Naive Bayes, Gradient Boost, and Voting Classifier methods. Ref. [117] proposes a method in which (1) the manufacturing processes classification is performed using the Support Vector Machine (SVM) algorithm, (2) the regularization parameter value and the gamma coefficient value of the SVM algorithm are optimized using the Horse Optimization Algorithm (HOA), (3) the HOA -based SVM results are compared to Particle Swarm Optimization (PSO)-based SVM results and Chicken Swarm Optimization (CSO)-based SVM results. Additionally, ref. [118] uses PSO and DNN for a similar problem. Both methods are validated on SEMCOM dataset [119].

Without application dependability or a case study, ref. [120] introduces an anomaly detection method based on the Gaussian Restricted Boltzmann Machine for industry product quality inspection. Ref. [121] addresses the critical issues of machine learning-based condition monitoring solutions. Ref. [122] studies several unsupervised learning techniques (Gaussian model, SVM, isolation forest, autoencoder) based on six industrial test datasets. Ref. [123] focuses on a particular application of telemetry—anomaly detection on time-series data. It presents an improved version of ReRe, a state-of-the-art Long Short Term Memory-based machine learning algorithm.

A fuzzy neural network-based fault diagnosis approach for condition monitoring is presented by [124] for rotating machines via vibration signals. Ref. [125] proposes a long short-term memory (LSTM)-Gauss-NBayes method for outlier detection in the IIoT. LSTM-NN builds a model on a normal time series and it detects outliers by utilizing the predictive error for the Gaussian Naive Bayes model. Ref. [126] proposes an on-device federated learning-based deep anomaly detection framework for sensing time-series data in IIoT. The framework used an attention mechanism-based convolutional neural network-long short-term memory (AMCNN-LSTM) model to detect anomalies accurately. Similarly, ref. [127] proposes a reliable anomaly detection strategy for IIoT using federated learning. Specifically, it applies the federated learning technique to build a universal anomaly detection model with each local model trained by the deep reinforcement learning algorithm.

In contrast, ref. [128] introduces a practical investigation on graph neural networks (GNNs) for anomaly detection in IIoT-enabled smart transportation, smart energy, and smart factory. Ref. [127] designs an anomaly detection algorithm that exploits deep learning techniques to assess the working conditions of the plant. AE and deepAE are responsible for initial dimensionality reduction, PCA is responsible for a further reduction, and K-means clustering performs the actual anomaly detection. Ref. [129] develops a methodology for detecting abnormal behavior in the context of aging IIoT using a PCA-based method.

4.3. Datasets for Anomaly Detection

There are a couple of public datasets that can be used to train and validate machine learning algorithms on IIoT quality inspection and outlier detection. Reviewing these datasets can provide a deeper understanding of the machine learning algorithms, revealing the possible features and outcomes of each algorithm. Ref. [119] provides a collection of databases, domain theories, and data generators that are used by the machine learning community for the empirical analysis of machine learning algorithms. There are several datasets from the manufacturing domain that are used for algorithm validation, including the semi-conductor domain. Ref. [130] provides access to a large collection of outlier detection datasets with ground truth (if available). The focus of the repository is to provide datasets from different domains and present them under a single platform for the research community, including several manufacturing domains (wafer map).

4.4. Summary of Machine Learning Based Quality Control

Visual quality inspection and surface detection are the most common quality inspection methods and are utilized in almost every domain of the industry and in manufacturing (see Table 3). Pretrained CNN networks (ResNet, DenseNet, VGG) can be leveraged for object recognition, while Autoencoders are used for feature extraction.

Since device failures seriously affect the production of industrial products in Industrial IoT (IIoT), accurate and even real-time anomaly detection is becoming increasingly important. Due to the nature of IIoT, federated learning solutions are used in many industrial domains. LSTM networks gained much attention as they are well-suited to classifying, processing and making predictions based on time series data, which are one of the most common data sources in anomaly detection problems.

Table 3. Summary of applications of machine learning techniques in IIoT quality control.

Application	Typical Machine Learning Techniques	References
Visual quality inspection	CNN (Yolo, VGG, ResNet, DenseNet), Autoencoders	[104,106,107,110–112,114]
Anomaly detection	LSTM and PSO, kNN, SVM, PCA, XGBoost, Regressions, etc.	[117,122,125–127,127,129]

5. Maintenance

Maintenance has always been an important aspect of industrial manufacturing as it includes crucial tasks that directly affect productivity. Traditionally, maintenance involves the following two key factors: the cost of repairing or replacing equipment and the cost of shutting down production lines when the required equipment or tools are unavailable. Therefore, maintenance evolves alongside industrial technologies and new approaches.

Two different approaches are reactiveand proactive maintenance. Reactive maintenance refers to the intuitive way of maintenance, which means that the maintenance task will be performed after an items wears-out or is broken. Proactive maintenance involves different methodologies to actively monitor the equipment, create strategies, and estimate the conditions in order to prevent failure to save cost by ensuring shorter-term and scheduled maintenance and longer operational capabilities.

The most widely adopted methodologies are predictive and preventive maintenance. While the first places emphasis on estimating the time of failure to enable scheduled maintenance—and therefore production line down-times—the other aims to establish a regular, periodic maintenance process for preventing failures and keeping machinery operational for as long as possible by expanding its life-time [131–133], as shown in Figure 6.

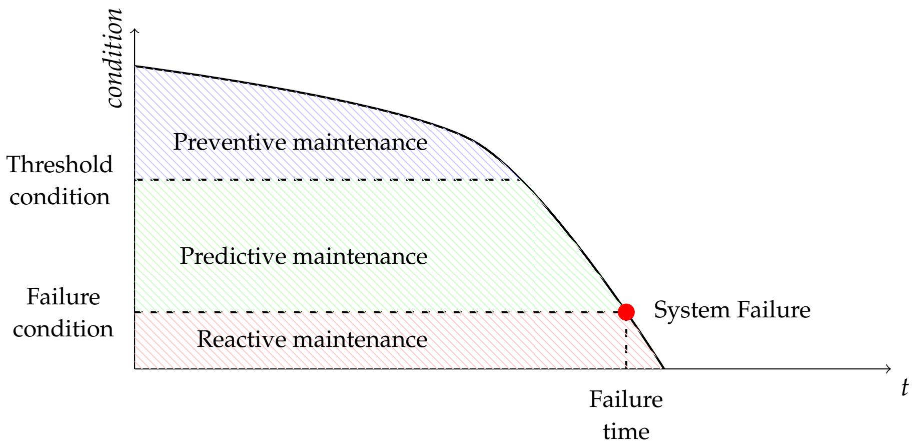

Figure 6. Difference between maintenance approaches in terms of condition and time

Usually, proactive maintenance refers to the application of predictive with preventive approaches in the same maintenance ecosystem to overcome the disadvantages of wasting working hours and costs by performing unnecessary, periodic maintenance.

5.1. Tasks of Proactive Maintenance

Industry 4.0 applications that usually involve IoT systems as well are not only the enablers of proactive maintenance; they also benefit from adopting it. This leads us to the concept of Cyber–physical systems that include numerous interconnected subsystems on a physical and a digital plane. Such a CPS collects data about the status and conditions of the subsystems or pieces of equipment which can be used for optimizing certain parameters of the system, thereby creating a feedback loop. This scheme can be also applied for maintenance tasks in order to create an CPS/IoT-enabled proactive maintenance system. Such a system consists of several main areas that can be classified as follows [134–136]:

Fault detection — Detecting malfunctions is a complex task which involves several data sources such as equipment monitoring sensors, environment monitoring sensors, telemetry data, etc., in order to be able to recognize failures. The most common data that are gathered by sensors are: vibration monitoring, sound or acoustic monitoring and oil-analysis or lubricant monitoring [137,138].

Diagnostics — Diagnostic processes are at the core of prognostics and strategy planning as they provide an analysis of failures and hazards, thus enabling the creation of models. One of the main task of diagnostics is Root cause analysis, which is a framework for investigating hazards and systematically discovering the possible root causes [139–141].

Prognostics — The aim of prognostics is to estimate the future condition of equipment by modelling it based on the results of diagnostics. In most cases, the final goal of prognostics is to calculate the Remaining Useful Life (RUL) and Mean Time to Failure (MTTF). These factors play a key role in predicting and preventing possible future malfunctions and failures and help to schedule required maintenance tasks in time [142].

As discussed, these areas of maintenance include tasks such as data analysis, pattern recognition, designing complex models of processes or object, and forecasting events (hazards and failures), which are areas where machine learning techniques traditionally outperform other methods and solutions. As the fields of maintenance, repair, and overhaul (MRO) do not have any strict regulations, state-of-the-art solutions can be constructed based on requirements and expectations, and they can also follow the already implemented solutions available in the literature or as an open-source project.

5.2. Fault Detection

Each area of maintenance requires a huge amount of data; Fault detection (FD) and anomaly detection are not exceptions. This task shares many solutions with the aforementioned anomaly detection method in quality control, due to their common nature. Since the main goal is to observe and identify failures, classification, clustering, regression and anomaly detection algorithms are best suited for this use-case [143].

In [144], a clustering-based solution is discussed for the fault detection of a Power Distribution Network, where the decision tree algorithm outperformed KNN and SVM in terms of accuracy. In [145], the authors proposed a clustering approach for detecting multi-component degradation in aircraft fuel systems. Decision tree-based solutions, such as the one detailed in [146,147], are also capable of providing an accurate detection rate, while maintaining a low computational complexity.

Nonetheless, using neural networks for this purpose is also a common solution, such as in [148], where a completed maintenance framework is built upon it. Artificial Neural Network-based solutions can be effectively used for feature extraction and for analysis time-series data, as is shown in [149,150]. Moreover, fault detection is the one of the main tasks of predictive maintenance that strongly relies on real-time computation. Ref. [151] presents a Convolutional Neural Network (CNN)-based solution for motor fault detection that can provide accurate estimations in real time.

5.3. Diagnostics

Since diagnostic tasks, most prominently Root cause analysis, investigate hazards by systematically creating problem subsets, classification or clustering based solutions are often required.

In [152], the authors proposed a Decision Tree and Principal Component Analysis (PCA)-based RCA solution for rotating machinery, where PCA can eliminate the redundant features, while Decision Tree can classify data with high precision. Ref. [153] also showed that Decision Tree and Ensemble algorithms perform the best for large amounts of data with uncertain problems. For the specific rotating machinery use-case, [154] applied Random Forest and KNN as classifiers within their proposed methodological framework for time-series data, while [155] also used Random Forest for time-domain classification.

RCA is not the only important diagnostic task, as diagnostics also includes modelling that serves as the basis for prognostics. Such tasks usually requires feature extraction to build models. In [156], the authors proposed a solution for rotating machinery fault diagnosis based on auto-encoder to perform feature extraction and a fish swarm algorithm to optimize its key parameters. Ref. [157] also proposes a similar method for rolling bearings, but with an enhanced Deep Wavelet Auto-encoder and Extreme Learning Machine. For bearings, different CNN-based solutions were introduced in [158,159] to process time and frequency series data from sensors. Another solution is presented in [157] using RNN and GRU for high accuracy and robust performance.

5.4. Prognostics

Besides estimating RUL and MTTF, prognostics usually involves design or create models that can describe the behaviour of the investigated equipment or component. There are numerous approaches that can be applied in this field, namely Physical model-based, knowledge-based, data-driven, etc., models, among which data-driven methods are now predominant due to the huge amount of available data and emerging machine learning applications. Nonetheless, certain learning techniques such as fuzzy logic can also be applied for knowledge-based predictions [160].

Regarding the data-driven approach in [161], a Support Vector Machine (SVM) and Restricted Boltzmann Machine (RBM)-based solution is proposed for estimating RUL. In this work, a dataset measured using a vibration sensor was classified with SVM, while RBM was used to enable learning without abnormal data. Such a functional combination is typical within this field, where one technique is applied for classification while the other is used for to overcome unbalanced data. According to [162], SVM is one of the most popular algorithms for classification; however, but statistical algorithms such as Bayesian Networks are still relevant, mostly in uncertain environments or in the case of a small amount of data [163,164].

A typical problem in modelling complex systems is the massive state space that makes it difficult to create a model that takes each feature into account. Therefore, reducing complexity is a common task in this field, where auto-encoder-based [165] solutions can be intensively applied. In [166], the authors proposed an Auto-Encoder Gated Recurrent Unit (GRU) for dimension reduction before calculating RUL; in [167], it was applied the same way, but within a framework.

Since such predictions are mostly based on time-series data, it is usually beneficial to implement systems that can deal with this type of data. Ref. [168] applied Long Short-Term Memory (LSTM) and Recurrent Neural Network (RNN) for High-speed railway power equipment, due to its powerful prediction ability for time-series. In [169], a combined LTSM-RNN solution was applied in the same manner; however, the study pointed out that it is suitable for only critical systems due its complexity, while for a huge amount of data vanilla-RNN is more suitable.

5.5. Manufacturing Optimization

This section introduces the key aspects and machine learning methods used for manufacturing optimization. It covers only the processes that are directly part of the production line and the manufacturing processes. The target variables of the manufacturing optimization process include the quality of the product, cost, time, power consumption or other product-specific parameters. Naturally, there are correlations between these optimization factors, yet, these are the most notable categories. The use of machine learning techniques is highly beneficial to pattern recognition, which is the core of the manufacturing optimization processes. With the help of ML techniques, correlations between different types of data or manufacturing domains can be identified and utilized to optimize the manufacturing process.

For electricity optimization, ref. [170] uses Q-learning in an automation system to reduce electricity consumption. In ref. [171], a mixed online bipartite matching-based Deep Q-network algorithm is proposed for profit-maximizing smart manufacturing. The paper formulates a joint optimization of the block size, task scheduling, and supply–demand configuration to maximize customers' net profit with the probabilistic delay requirements, which addresses the critical issue of efficiency and latency in the blockchain-based live manufacturing process. Conversely, the study in [172] uses a support vector regression algorithm with an RBF kernel for troubleshooting production data to identify parameters responsible for high energy conversion efficiency variances. Ref. [173] propose LithoGAN, an end-to-end lithography modeling framework based on a generative adversarial network (GAN), to map the input mask patterns directly to the output resist patterns. The results show that LithoGAN can predict resist patterns with high accuracy while achieving a speed that is orders of magnitude greater than conventional lithography simulation and previous machine learning-based approaches. Besides GAN and Q-learning, there are CNN and RNN applications in the field of ultrasound imaging. Ref. [174] proposes an automatic fetal ultrasound standard plane recognition model in an IIoT environment which learns the spatial and temporal features of the ultrasound video stream by using multi-task learning. The CNN component identifies fetal key anatomical structures, while the RNN component obtains the temporal information between adjacent frames, and it realizes the precise localization and tracking of fetal organs across frames.

Particle Swarm Optimization has been utilized in several optimization problems; ref. [175] proposes a PSO-based technique to optimize the hyperparameter settings of the LSTM in an FL environment, while in [176] combined multi-Objective particle swarm optimization (CMOPSO) is proposed for a green manufacturing energy system. Regression problems are also quite typical in the field of manufacturing optimization. Ref. [177] proposes optimizing semiconductor manufacturing processes through machine learning (ML) based on a regression algorithm. Ref. [178] compares the performance of different supervised machine learning methods for the field calibration of low-cost IoT sensors, including Linear Regression and Artificial Neural Network solutions. Furthermore, ref. [179] presents a method of using logistic regression to solve the inverse problem in electrical impedance tomography. However, there are generally fully connected NN solutions in the manufacturing industry. Ref. [180] proposes Finite Element Analysis and a NN model to optimize and create chip package design. Ref. [181] introduces an optimization method for Bipolar-CMOS-DMOS process development based on an Automatic Multi-objective Optimization solution and NN.

There are a couple of survey works in the field of manufacturing optimization. The study in [13] covers the majority of relevant literature from 2008 to 2018 concerned with machine learning and optimization approaches for product quality or process improvement in the the manufacturing industry. The review shows that there is hardly any correlation between the used data, the amount of data, the machine learning algorithms, the used optimizers, and the respective problem from the production. Additionally, there are works summarizing some of the recent advancements in ML with a focus on its applications in the process industries [182,183], such as in additive manufacturing [184]. Furthermore, ref. [185] summarize the designs of state and action, provides RL-based algorithms for scheduling, and reviews the applications of RL for different types of scheduling problems.

5.6. Datasets for Smart Maintenance

There are a couple of public datasets that can help to train and validate machine learning algorithms in smart maintenance tasks. Reviewing these datasets can provide a deeper understanding of the machine learning algorithms, revealing the possible features and outcomes of each algorithm. Given the lack of real, industrial data, most of these datasets are synthetic. As fault detection is involved both in quality control and maintenance, ref. [119] is also a useful source for smart maintenance applications. Ref. [186] uses MetroPT, a benchmark dataset for predictive maintenance collected in 2022 about an urban metro public transportation service in Porto. The data contain samples from analog sensor signals (pressure, temperature, current consumption), digital signals (control signals, discrete signals), and GPS information (latitude, longitude, and speed) for anomaly detection and failure-prediction purposes. Ref. [187] provides a dataset that consists of a sequence of alarms logged by packaging equipment in an industrial environment for classification, forecasting and anomaly detection purposes. The collection includes data logged by 20 machines, and deployed in different plants around the world, from 21 February 2019 to 17 June 2020. There are 154 distinct alarm codes, for which the distribution is highly unbalanced.

5.7. The MANTIS Proactive Maintenance Platform

The MANTIS project of Electronic Components and Systems for European Leadership started in 2015 with 47 different partners across Europe from 12 different countries. In [188], the authors detail that the main objective was to develop a CPS-based Proactive Maintenance Service Platform Architecture enabling Collaborative Maintenance Ecosystems. The requirements were set to match the expectations for optimising maintenance mechanisms for CPS [189]. They proposed the following four main proactive maintenance target areas: the Remaining Useful Life (RUL) of components, Fault Prediction (FP), Root Cause Analysis (RCA), and Maintenance Strategy Optimization (MSO). The architecture model follows the Industrial Internet of Things Reference Architecture of Industrial Internet Consortium and contains the following three main tiers: the edge tier, platform tier, and enterprise tier, as can be seen in Figure 7, and it also supports multi-stakeholder interactions, while the architecture has been validated by different evaluations. MANTIS uses the Lambda architecture pattern for data processing and it uses the Open Standards for the Physical Asset Management of Machinery Information Management Open System Alliance (MIMOSA) for common understanding, databus, and data ontology between partners and applications.

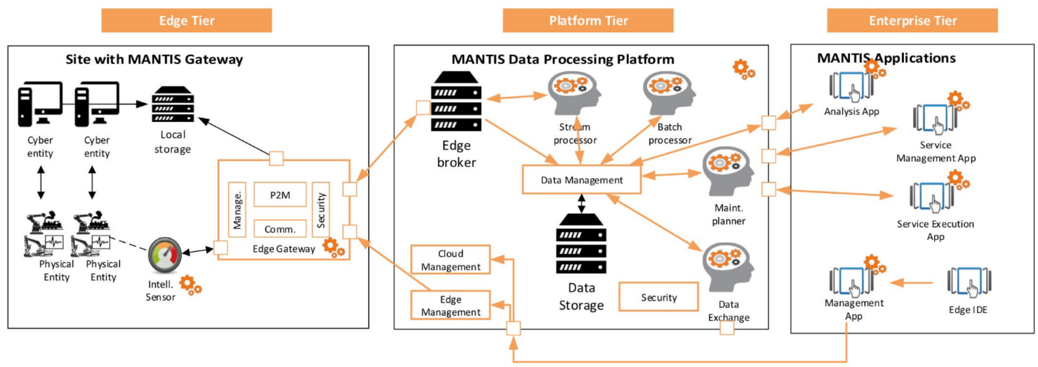

Figure 7. Overview of the MANTIS reference architecture [188].

In [190], the authors present an extension of MANTIS including a Big Data implementation and technologies, such as the Hadoop Distributed File System, Apache Spark. They used two techniques, namely Root Cause Analysis powered by Attribute Oriented Induction (AOI) Clustering and Remaining Useful Life based on time series forecasting. In the platform technological implementation, the following four main blocks are explained: Data Access and Ingestion through the Edge Broker, Data Storage systems, Batch Processor, and Human Machine Interfaces.

In [191], the authors detailed CPS-populated systems used for proactive maintenance using MANTIS. They introduced the main characteristics of a CPS and summarized three main research challenges, namely science and engineering foundations; system performance, quality and acceptance; and applied development and deployment. They also presented the interoperability perspective of MANTIS, including the specification, conceptual integration, application integration, and technical integration aspects.

In [192,193], the authors present complex case studies on continuous monitoring and proactive maintenance of the railroad tracks and railway switches. For the whole process, they used the concepts and the platform of MANTIS. They detailed the data-processing steps, implementation approaches and visualization solutions highlighting the advantages of the usage of MANTIS in each step.

5.8. Summary of Machine Learning Based Maintenance and Manufacturing Optimization

The main areas of proactive maintenance—fault detection, diagnostics and prognostics —share some common requirements and targets and, consequently, the tasks that need to be performed. These key tasks are usually classification, clustering, regression, complexity reduction, system modelling, and data series analysis. However, there are specific targets for these areas as the former ones are more closely related to fault detection and diagnostics while the latter ones are related to prognostics; the applied machine-learning techniques also overlap to a certain degree. A summary of the methods used in maintenance can be found in Table 4.

For clustering, KNN and SVM are typically used, while for classification and regression purposes decision trees, random forest and principal component analysis are used. The most popular techniques for modelling, complexity reduction, and data series analysis are neural network-based applications including CNN, auto-encoder, RNN, GRU and LSTM.

Naturally, there are very broad, application-specific optimization problems in the manufacturing industry and differences in their regularities in the context of the used machine learning techniques. Supervised machine learning techniques (regression, SVM) are used for prediction and as an analytical tool during the optimization process in most cases for classification purposes. Reinforcement learning, especially Q-learning, is utilized in several instances during manufacturing processes for decision-making problems such as single and multi-objective scheduling problems.

However, it can be concluded that there is only a fine margin between manufacturing optimization and quality inspection. In many cases, the two processes cannot be separated; there are several dependencies between such machine learning-supported manufacturing processes.

Table 4. Summary of applications of machine learning techniques in IIoT proactive maintenance.

Application	Typical Machine Learning Techniques	References
Fault Detection	KNN, SVM, Decision Tree, CNN	[143–151]
Diagnostics	Decision Tree, Random Forest, KNN, SVM, CNN, RNN	[152–157,157–159]
Prognostics	SVM, Bayesian Networks, RNN, CNN, Auto-Encoder, LSTM, Gated Recurrent Unit (GRM)	[160–169]
Manufacturing optimization	Unsupervised learning (Regressions, SVM, GAN), Reinforcement learning (Q-learning, LSTM)	[170,171,173–175,177,178,181]

6. Conclusions

This paper provided a comprehensive overview on machine learning techniques applied for various purposes in IIoT and Smart Production. The domains covered include safety and security, asset localization, quality control, and proactive maintenance.

IIoT security and safety is a very important aspect for the Industry 4.0 technology transition; hence, one can find many different application domains for ML techniques.

These include the identification of intrusion detection, supporting authentication, realizing privacy leaking, checking data integrity, supporting availability, and offloading security services. Asset localization is a very specific area of smart production, where machine learning has been applied extensively. The application areas for asset localization include learning mapping between measurements and location, predicting non-LOS propagation, and predicting location error. Regarding quality control, visual quality inspection and anomaly detection applications were found to specifically require machine learning approaches. In relation to maintenance, the main application areas include fault detection, diagnostics, prognostics, and some manufacturing optimization applications which were surveyed too.

Besides providing a general overview of the applied techniques for the listed application areas, this paper also summarized the related references found for application domains, making it easier for practitioners and researchers alike to find ML-application patterns for their given field. The paper also contains the most important references of public datasets for developing domain specific algorithms and applications (see Table 5). Each main chapter includes a dedicated lessons-learned section to reinforce the main findings about the state-of-the-art and the research gaps of the discussed application area.

Table 5. Summary of major and typical datasets for IIoT machine learning applications

Topic	Name of Dataset	Description
Smart maintenance	MetroPT [186]	Consists of samples of analog sensor signals (pressure, temperature, current consumption), digital signals (control signals, discrete signals), and GPS information (latitude, longitude, and speed).
	Alarm Logs in Packaging Industry (ALPI) [187]	Contains a sequence of alarms logged by packaging equipment in an industrial environment. The collection includes data logged by 20 machines, deployed in different plants around the world, from 21 February 2019 to 17 June 2020.
Quality inspection	UCI Machine Learning Repository [119]	A UCI collection of databases, domain theories, and data generators. There are several datasets from the manufacturing domain that are used for algorithm validation, including the semi-conductor domain.
	Outlier Detection DataSets [130]	ODDS provide access to a large collection of outlier detection datasets with ground truth (if available). The focus of the repository is to provide datasets from different domains including several manufacturing domains (wafer map).
Safety and security	KDD-99 dataset [65]	The dataset used for The Third International Knowledge Discovery and Data Mining Tools Competition, the competition task was to build a network intrusion detector algorithm.
	CSE-CIC-IDS2018 dataset [66]	The dataset includes seven different attack scenarios, namely Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attacks, and infiltration of the network from inside. The attacking infrastructure includes 50 machines and the victim organization has 5 departments including 420 PCs and 30 servers.
	CIC DDoS attack dataset [67]	The dataset contains different modern reflective DDoS attacks such as PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS and SNMP.
	Intrusion detection and privacy attack dataset [68,69]	Dataset for developing and evaluating different IEEE 802.11 Wi-Fi algorithms.
	The University of Arizona datasets [70]	Different malware and network traffic datasets for developing and evaluating network security algorithms.
Localization	UTIL: An Ultra-wideband Time-difference-of-arrival Indoor Localization Dataset [194]	An Ultra-wideband Time-difference-of-arrival Indoor Localization Dataset. Raw sensor data including UWB TDOA, inertial measurement unit (IMU), optical flow, time-of-flight (ToF) laser, and millimeter-accurate ground truth data were collected during the flights of drones.
	CSI Dataset towards 5G NR High-Precision Positioning [195]	This dataset can be used for indoor positioning, indoor-outdoor-integrated positioning, NLoS, 5G channel estimation and other types of research, providing researchers with CSI-level position-related feature data.

Author Contributions: Abstract, Introduction and Conclusions, P.V.; Safety and Security, Asset Localization, G.H.; Quality Control, D.F.; Maintenance, A.F. and D.F.; conceptualization, D.F., G.H., A.F. and P.V.; methodology, P.V.; investigation, D.F., G.H., A.F. and P.V.; resources, P.V.; writing—original draft preparation, D.F., G.H., A.F. and P.V.; supervision, P.V.; funding acquisition, D.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6. [CrossRef]
2. Mitchell, T.M. *Machine Learning*; McGraw-Hill Education: New York, NY, USA, 1997.
3. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*; MIT Press: Cambridge, MA, USA, 2016. Available online: http://www.deeplearningbook.org (accessed on 1 November 2022).
4. Shalev-Shwartz, S.; Ben-David, S. *Understanding Machine Learning: From Theory to Algorithms*; Cambridge University Press: Cambridge, UK, 2014.
5. Géron, A. *Hands-on Machine Learning with Scikit-Learn, Keras, and TensorFlow*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2022.
6. Müller, A.C.; Guido, S. *Introduction to Machine Learning with Python: A Guide for Data Scientists*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2016.
7. Lantz, B. *Machine Learning with R: Expert Techniques for Predictive Modeling*; Packt Publishing Ltd.: Birmingham, UK, 2019.
8. Lakshmanan, V.; Robinson, S.; Munn, M. *Machine Learning Design Patterns*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2020.
9. Sharp, M.; Ak, R.; Hedberg, T., Jr. A survey of the advancing use and development of machine learning in smart manufacturing. *J. Manuf. Syst.* **2018**, *48*, 170–179. [CrossRef] [PubMed]
10. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. Tackling faults in the industry 4.0 era—A survey of machine-learning solutions and key aspects. *Sensors* **2019**, *20*, 109. [CrossRef] [PubMed]
11. Hanga, K.M.; Kovalchuk, Y. Machine learning and multi-agent systems in oil and gas industry applications: A survey. *Comput. Sci. Rev.* **2019**, *34*, 100191. [CrossRef]
12. Usuga Cadavid, J.P.; Lamouri, S.; Grabot, B.; Pellerin, R.; Fortin, A. Machine learning applied in production planning and control: A state-of-the-art in the era of industry 4.0. *J. Intell. Manuf.* **2020**, *31*, 1531–1558. [CrossRef]
13. Weichert, D.; Link, P.; Stoll, A.; Rüping, S.; Ihlenfeldt, S.; Wrobel, S. A review of machine learning for the optimization of production processes. *Int. J. Adv. Manuf. Technol.* **2019**, *104*, 1889–1902. [CrossRef]
14. Cioffi, R.; Travaglioni, M.; Piscitelli, G.; Petrillo, A.; De Felice, F. Artificial intelligence and machine learning applications in smart production: Progress, trends, and directions. *Sustainability* **2020**, *12*, 492. [CrossRef]
15. Narciso, D.A.; Martins, F. Application of machine learning tools for energy efficiency in industry: A review. *Energy Rep.* **2020**, *6*, 1181–1199. [CrossRef]
16. Diez-Olivan, A.; Del Ser, J.; Galar, D.; Sierra, B. Data fusion and machine learning for industrial prognosis: Trends and perspectives towards Industry 4.0. *Inf. Fusion* **2019**, *50*, 92–111. [CrossRef]
17. Çınar, Z.M.; Abdussalam Nuhu, A.; Zeeshan, Q.; Korhan, O.; Asmael, M.; Safaei, B. Machine learning in predictive maintenance towards sustainable smart manufacturing in industry 4.0. *Sustainability* **2020**, *12*, 8211. [CrossRef]
18. Xu, Z.; Saleh, J.H. Machine learning for reliability engineering and safety applications: Review of current status and future opportunities. *Reliab. Eng. Syst. Saf.* **2021**, *211*, 107530. [CrossRef]
19. Schwalbe, G.; Schels, M. A survey on methods for the safety assurance of machine learning based systems. In Proceedings of the 10th European Congress on Embedded Real Time Software and Systems (ERTS 2020), Toulouse, France, 29–31 January 2020.
20. Martin, R.; Schrecker, S.; Soroush, H.; Molina, J.; LeBlanc, J.; Hirsch, F.; Buchheit, M.; Ginter, A.; Banavara, H.; Eswarahally, S.; et al. *Industrial Internet Security Framework Technical Report*; Technical Report; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2016. [CrossRef]
21. Fraile, F.; Tagawa, T.; Poler, R.; Ortiz, A. Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems. *IEEE Internet Things J.* **2018**, *5*, 4506–4514. [CrossRef]
22. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88.
23. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Netw.* **2021**, *123*, 102685. [CrossRef]
24. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
25. Baldini, G.; Giuliani, R.; Steri, G.; Neisse, R. Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [CrossRef]

26. Hosseini Bamakan, S.M.; Wang, H.; Yingjie, T.; Shi, Y. An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization. *Neurocomputing* **2016**, *199*, 90–102. . [CrossRef]
27. Kabir, E.; Hu, J.; Wang, H.; Zhuo, G. A novel statistical technique for intrusion detection systems. *Future Gener. Comput. Syst.* **2018**, *79*, 303–318. [CrossRef]
28. Bagaa, M.; Taleb, T.; Bernabe, J.B.; Skarmeta, A. A Machine Learning Security Framework for Iot Systems. *IEEE Access* **2020**, *8*, 114066–114077. [CrossRef]
29. Zissis, D. Intelligent security on the edge of the cloud. In Proceedings of the 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), Madeira Island, Portugal, 27–29 June 2017; pp. 1066–1070. [CrossRef]
30. Goeschel, K. Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp. 1–6. [CrossRef]
31. Mehmood, T.; Md Rais, H.B. Machine learning algorithms in context of intrusion detection. In Proceedings of the 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 15–17 August 2016; pp. 369–373. [CrossRef]
32. Jincy, V.J.; Sundararajan, S. Classification Mechanism for IoT Devices towards Creating a Security Framework. In *Intelligent Distributed Computing*; Buyya, R., Thampi, S.M., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 265–277.
33. Hassan, M.M.; Gumaei, A.; Huda, S.; Almogren, A. Increasing the Trustworthiness in the Industrial IoT Networks through a Reliable Cyberattack Detection Model. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6154–6162. [CrossRef]
34. Shenfield, A.; Day, D.; Ayesh, A. Intelligent intrusion detection systems using artificial neural networks. *ICT Express* **2018**, *4*, 95–99.
35. Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access* **2017**, *5*, 21954–21961. [CrossRef]
36. Vinayakumar, R.; Soman, K.P.; Poornachandran, P. Applying convolutional neural network for network intrusion detection. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Manipal, India, 13–16 September 2017; pp. 1222–1228. [CrossRef]
37. Tajbakhsh, A.; Rahmati, M.; Mirzaei, A. Intrusion detection using fuzzy association rules. *Appl. Soft Comput.* **2009**, *9*, 462–469. [CrossRef]
38. Hoang, X.D.; Hu, J.; Bertok, P. A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference. *J. Netw. Comput. Appl.* **2009**, *32*, 1219–1228. [CrossRef]
39. Warrender, C.; Forrest, S.; Pearlmutter, B. Detecting intrusions using system calls: Alternative data models. In Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No. 99CB36344), Oakland, CA, USA, 9–12 May 1999; pp. 133–145. [CrossRef]
40. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
41. Branch, J.W.; Giannella, C.; Szymanski, B.; Wolff, R.; Kargupta, H. In-network outlier detection in wireless sensor networks. *Knowl. Inf. Syst.* **2013**, *34*, 23–54.
42. Al Samara, M.; Bennis, I.; Abouaissa, A.; Lorenz, P. A Survey of Outlier Detection Techniques in IoT: Review and Classification. *J. Sens. Actuator Netw.* **2022**, *11*, 4 .
43. Lee, S.Y.; Wi, S.R.; Seo, E.; Jung, J.K.; Chung, T.M. ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017; pp. 1–6. [CrossRef]
44. Miettinen, M.; Marchal, S.; Hafeez, I.; Asokan, N.; Sadeghi, A.R.; Tarkoma, S. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 2177–2184. [CrossRef]
45. Siddavatam, I.A.; Satish, S.; Mahesh, W.; Kazi, F. An ensemble learning for anomaly identification in SCADA system. In Proceedings of the 2017 7th International Conference on Power Systems (ICPS), Pune, India, 21–23 December 2017; pp. 457–462. [CrossRef]
46. Meidan, Y.; Bohadana, M.; Shabtai, A.; Guarnizo, J.D.; Ochoa, M.; Tippenhauer, N.O.; Elovici, Y. ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 506–509. [CrossRef]
47. Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-Enabled IoT. In Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chennai, India, 10–14 July 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
48. Eigner, O.; Kreimel, P.; Tavolato, P. Detection of Man-in-the-Middle Attacks on Industrial Control Networks. In Proceedings of the 2016 International Conference on Software Security and Assurance (ICSSA), St. Pölten, Austria, 24–25 August 2016; pp. 64–69. [CrossRef]
49. Aminanto, M.E.; Kim, K. Improving Detection of Wi-Fi Impersonation by Fully Unsupervised Deep Learning. In *Information Security Applications*; Kang, B.B., Kim, T., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 212–223.

50. Wang, X.; Garg, S.; Lin, H.; Piran, M.J.; Hu, J.; Hossain, M.S. Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7725–7733. [CrossRef]
51. Anjomshoaa, A.; Curry, E. Blockchain as an Enabler for Transfer Learning in Smart Environments. *arXiv* **2022**, arXiv:2204.03959.
52. Zhang, X.; Chen, X.; Liu, J.K.; Xiang, Y. DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2081–2090. [CrossRef]
53. Arachchige, P.C.M.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S.; Atiquzzaman, M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6092–6102. [CrossRef]
54. Jiang, B.; Li, J.; Yue, G.; Song, H. Differential Privacy for Industrial Internet of Things: Opportunities, Applications, and Challenges. *IEEE Internet Things J.* **2021**, *8*, 10430–10451. [CrossRef]
55. Beaver, J.M.; Borges-Hink, R.C.; Buckner, M.A. An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications. In Proceedings of the 2013 12th International Conference on Machine Learning and Applications, Miami, FL, USA, 4–7 December 2013; Volume 2, pp. 54–59. [CrossRef]
56. Alves, T.; Das, R.; Morris, T. Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers. *IEEE Embed. Syst. Lett.* **2018**, *10*, 99–102. [CrossRef]
57. He, Y.; Mendis, G.J.; Wei, J. Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Trans. Smart Grid* **2017**, *8*, 2505–2516. [CrossRef]
58. Aboelwafa, M.M.N.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. *IEEE Internet Things J.* **2020**, *7*, 8462–8471. . [CrossRef]
59. Potluri, S.; Henry, N.F.; Diedrich, C. Evaluation of hybrid deep learning techniques for ensuring security in networked control systems. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–8. [CrossRef]
60. Li, Y.; Quevedo, D.E.; Dey, S.; Shi, L. SINR-Based DoS Attack on Remote State Estimation: A Game-Theoretic Approach. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 632–642. [CrossRef]
61. Hogan, M.; Esposito, F. Stochastic delay forecasts for edge traffic engineering via Bayesian Networks. In Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–4. [CrossRef]
62. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Secure Computation Offloading in Blockchain based IoT Networks with Deep Reinforcement Learning. *arXiv* **2019**, arXiv:1908.07466. https://doi.org/10.48550/ARXIV.1908.07466.
63. Xiao, L.; Xie, C.; Chen, T.; Dai, H.; Poor, H.V. A Mobile Offloading Game Against Smart Attacks. *IEEE Access* **2016**, *4*, 2281–2291. [CrossRef]
64. Liu, X.; Yu, W.; Liang, F.; Griffith, D.; Golmie, N. On deep reinforcement learning security for Industrial Internet of Things. *Comput. Commun.* **2021**, *168*, 20–32. [CrossRef]
65. Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P. *Cost-Based Modeling and Evaluation for Data Mining with Application to Fraud and Intrusion Detection: Results from the JAM Project*; IEEE: Piscataway, NJ, USA, 1999.
66. Canadian Institute for Cybersecurity. CSE-CIC-IDS2018 Dataset. Available online: https://registry.opendata.aws/cse-cic-ids2018 (accessed on 1 November 2022).
67. Canadian Institute for Cybersecurity. CIC-DDoS2019 Dataset. Available online: https://www.unb.ca/cic/datasets/ddos-2019.html (accessed on 1 November 2022).
68. Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 184–208. [CrossRef]
69. Chatzoglou, E.; Kambourakis, G.; Kolias, C. Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset. *IEEE Access* **2021**, *9*, 34188–34205. [CrossRef]
70. University of Arizona, AZSecure-data.org. Intelligence and Security Informatics Data Sets. Available online: https://www.azsecure-data.org/other-data.html (accessed on 1 November 2022).
71. Zolanvari, M.; Teixeira, M.A.; Jain, R. Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 9–11 November 2018; pp. 112–117. [CrossRef]
72. Yin, A.; Lin, Z. Machine Learning aided Precise Indoor Positioning. *arXiv* **2022**, arXiv:2204.03990.
73. Che, F.; Ahmed, A.; Ahmed, Q.Z.; Zaidi, S.A.R.; Shakir, M.Z. Machine Learning Based Approach for Indoor Localization Using Ultra-Wide Bandwidth (UWB) System for Industrial Internet of Things (IIoT). In Proceedings of the 2020 International Conference on UK-China Emerging Technologies (UCET), Glasgow, UK, 20–21 August 2020; pp. 1–4. [CrossRef]
74. Stahlke, M.; Kram, S.; Mutschler, C.; Mahr, T. NLOS Detection using UWB Channel Impulse Responses and Convolutional Neural Networks. In Proceedings of the 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2–4 June 2020; pp. 1–6. [CrossRef]
75. Lian Sang, C.; Steinhagen, B.; Homburg, J.; Adams, M.; Hesse, M. Identification of NLOS and Multi-Path Conditions in UWB Localization Using Machine Learning Methods. *Appl. Sci.* **2020**, *10*, 3980. [CrossRef]
76. Jiang, C.; Shen, J.; Chen, S.; Chen, Y.; Liu, D.; Bo, Y. UWB NLOS/LOS Classification Using Deep Learning Method. *IEEE Commun. Lett.* **2020**, *24*, 2226–2230. [CrossRef]

77. Ridolfi, M.; Fontaine, J.; Van Herbruggen, B.; Joseph, W.; Hoebeke, J.; De Poorter, E. UWB anchor nodes self-calibration in NLOS conditions: A machine learning and adaptive PHY error correction approach. *Wirel. Netw.* **2021**, *27*, 3007–3023. [CrossRef]
78. Xianjia, Y.; Qingqing, L.; Queralta, J.P.; Heikkonen, J.; Westerlund, T. Applications of UWB Networks and Positioning to Autonomous Robots and Industrial Systems. In Proceedings of the 2021 10th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 7–10 June 2021; pp. 1–6. [CrossRef]
79. Niitsoo, A.; Edelhäußer, T.; Eberlein, E.; Hadaschik, N.; Mutschler, C. A Deep Learning Approach to Position Estimation from Channel Impulse Responses. *Sensors* **2019**, *19*, 1064. [CrossRef]
80. 3GPP. Study on NR Positioning Enhancements. Technical Specification (TS) 38.857, 3rd Generation Partnership Project (3GPP). 2021. Version 17.0.0. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3732 (accessed on 1 November 2022).
81. Al-Habashna, A.; Wainer, G.; Aloqaily, M. Machine learning-based indoor localization and occupancy estimation using 5G ultra-dense networks. *Simul. Model. Pract. Theory* **2022**, *118*, 102543. [CrossRef]
82. El Boudani, B.; Kanaris, L.; Kokkinis, A.; Kyriacou, M.; Chrysoulas, C.; Stavrou, S.; Dagiuklas, T. Implementing Deep Learning Techniques in 5G IoT Networks for 3D Indoor Positioning: DELTA (DeEp Learning-Based Co-operaTive Architecture). *Sensors* **2020**, *20*, 5495. [CrossRef]
83. Gante, J.; Sousa, L.; Falcao, G. Dethroning GPS: Low-Power Accurate 5G Positioning Systems Using Machine Learning. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2020**, *10*, 240–252. [CrossRef]
84. Klus, R.; Klus, L.; Solomitckii, D.; Valkama, M.; Talvitie, J. Deep Learning Based Localization and HO Optimization in 5G NR Networks. In Proceedings of the 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2–4 June 2020; pp. 1–6. [CrossRef]
85. Mogyorósi, F.; Revisnyei, P.; Pašić, A.; Papp, Z.; Törös, I.; Varga, P.; Pašić, A. Positioning in 5G and 6G Networks: A Survey. *Sensors* **2022**, *22*, 4757. [CrossRef]
86. Salamah, A.H.; Tamazin, M.; Sharkas, M.A.; Khedr, M. An enhanced WiFi indoor localization system based on machine learning. In Proceedings of the 2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Madrid, Spain, 4–7 October 2016; pp. 1–8. [CrossRef]
87. Sabanci, K.; Yigit, E.; Ustun, D.; Toktas, A.; Aslan, M.F. WiFi Based Indoor Localization: Application and Comparison of Machine Learning Algorithms. In Proceedings of the 2018 XXIIIrd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED), Tbilisi, Georgia, 24–27 September 2018; pp. 246–251. [CrossRef]
88. Xue, J.; Liu, J.; Sheng, M.; Shi, Y.; Li, J. A WiFi fingerprint based high-adaptability indoor localization via machine learning. *China Commun.* **2020**, *17*, 247–259. [CrossRef]
89. Njima, W.; Ahriz, I.; Zayani, R.; Terre, M.; Bouallegue, R. Deep CNN for Indoor Localization in IoT-Sensor Systems. *Sensors* **2019**, *19*, 3127. [CrossRef]
90. Abbas, M.; Elhamshary, M.; Rizk, H.; Torki, M.; Youssef, M. WiDeep: WiFi-based Accurate and Robust Indoor Localization System using Deep Learning. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom), Kyoto, Japan, 11–15 March 2019; pp. 1–10. [CrossRef]
91. Jain, C.; Sashank, G.V.S.; N, V.; Markkandan, S. Low-cost BLE based Indoor Localization using RSSI Fingerprinting and Machine Learning. In Proceedings of the 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 25–27 March 2021; pp. 363–367. [CrossRef]
92. Subhan, F.; Saleem, S.; Bari, H.; Khan, W.Z.; Hakak, S.; Ahmad, S.; El-Sherbeeny, A.M. Linear Discriminant Analysis-Based Dynamic Indoor Localization Using Bluetooth Low Energy (BLE). *Sustainability* **2020**, *12*, 10627. . [CrossRef]
93. Cannizzaro, D.; Zafiri, M.; Jahier Pagliari, D.; Patti, E.; Macii, E.; Poncino, M.; Acquaviva, A. A Comparison Analysis of BLE-Based Algorithms for Localization in Industrial Environments. *Electronics* **2020**, *9*, 44. [CrossRef]
94. Hu, Q.; Wu, F.; Wong, R.; Millham, R.; Fiaidhi, J. A novel indoor localization system using machine learning based on bluetooth low energy with cloud computing. *Computing* **2021** . [CrossRef]
95. Ji, T.; Li, W.; Zhu, X.; Liu, M. Survey on indoor fingerprint localization for BLE. In Proceedings of the 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 4–6 March 2022; Volume 6, pp. 129–134. [CrossRef]
96. Perrone, M.; Pau, D.P.; Piazzese, N.I. Constrained Neural Estimation of Bluetooth Direction of Arrival with Non-Uniform Arrays. In Proceedings of the 2022 IEEE International Conference on Consumer Electronics (ICCE), Virtual, 7–9 January 2022; pp. 1–6. [CrossRef]
97. Bombino, A.; Grimaldi, S.; Mahmood, A.; Gidlund, M. Machine Learning-Aided Classification Of LoS/NLoS Radio Links In Industrial IoT. In Proceedings of the 2020 16th IEEE International Conference on Factory Communication Systems (WFCS), Porto, Portugal, 27–29 April 2020; pp. 1–8. [CrossRef]
98. Gang, Q.; Muhammad, A.; Khan, Z.U.; Khan, M.S.; Ahmed, F.; Ahmad, J. Machine Learning-Based Prediction of Node Localization Accuracy in IIoT-Based MI-UWSNs and Design of a TD Coil for Omnidirectional Communication. *Sustainability* **2022**, *14*, 9683. [CrossRef]
99. Zhao, L.; Huang, H.; Su, C.; Ding, S.; Huang, H.; Tan, Z.; Li, Z. Block-Sparse Coding-Based Machine Learning Approach for Dependable Device-Free Localization in IoT Environment. *IEEE Internet Things J.* **2021**, *8*, 3211–3223. [CrossRef]

100. Savazzi, S.; Nicoli, M.; Carminati, F.; Riva, M. A Bayesian Approach to Device-Free Localization: Modeling and Experimental Assessment. *IEEE J. Sel. Top. Signal Process.* **2014**, *8*, 16–29. [CrossRef]
101. Shit, R.C.; Sharma, S.; Puthal, D.; James, P.; Pradhan, B.; Moorsel, A.v.; Zomaya, A.Y.; Ranjan, R. Ubiquitous Localization (UbiLoc): A Survey and Taxonomy on Device Free Localization for Smart World. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3532–3564. [CrossRef]
102. Patwari, N.; Wilson, J. RF Sensor Networks for Device-Free Localization: Measurements, Models, and Algorithms. *Proc. IEEE* **2010**, *98*, 1961–1973. [CrossRef]
103. Nessa, A.; Adhikari, B.; Hussain, F.; Fernando, X. A Survey of Machine Learning for Indoor Positioning. *IEEE Access* **2020**, *8*, 214945–214965. [CrossRef]
104. Benbarrad, T.; Kenitar, S.B.; Arioua, M. Intelligent machine vision model for defective product inspection based on machine learning. In Proceedings of the 2020 International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Kenitra, Morocco, 25–27 November 2020; pp. 1–6. [CrossRef]
105. Beltrán-González, C.; Bustreo, M.; Del Bue, A. External and internal quality inspection of aerospace components. In Proceedings of the 2020 IEEE 7th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Pisa, Italy, 22–24 June 2020; pp. 351–355. [CrossRef]
106. Nishiura, H.; Miyamoto, A.; Ito, A.; Suzuki, S.; Fujii, K.; Morifuji, H.; Takatsuka, H. Machine-learning-based Quality-level-estimation System for Inspecting Steel Microstructures. In Proceedings of the 2021 17th International Conference on Machine Vision and Applications (MVA), Virtual, 25–27 July 2021; pp. 1–4. [CrossRef]
107. Oh, S.; Cha, J.; Kim, D.; Jeong, J. Quality Inspection of Casting Product Using CAE and CNN. In Proceedings of the 2020 4th International Conference on Imaging, Signal Processing and Communications (ICISPC), Kumamoto, Japan, 23–25 October 2020; pp. 34–38. [CrossRef]
108. Lin, C.H.; Hu, G.H.; Ho, C.W.; Hu, C.Y.; Kuo, P.C. Press Casting Quality Detection and Analysis Based on Machine Learning. In Proceedings of the 2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Hualien, Taiwan, 16–19 November 2021; pp. 1–2. [CrossRef]
109. Choong, L.M.; Cheng, W.K. Machine Learning in Failure Analysis of Optical Transceiver Manufacturing Process. In Proceedings of the 2021 International Conference on Computer & Information Sciences (ICCOINS), Online, 13–15 July 2021; pp. 160–162. [CrossRef]
110. Kim, J. Development of Visual Inspection System for Assembly Machine. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; pp. 859–861. [CrossRef]
111. Schmidt, K.; Rauchensteiner, D.; Voigt, C.; Thielen, N.; Bönig, J.; Beitinger, G.; Franke, J. An Automated Optical Inspection System for PIP Solder Joint Classification Using Convolutional Neural Networks. In Proceedings of the 2021 IEEE 71st Electronic Components and Technology Conference (ECTC), Virtual, 1 June–4 July 2021; pp. 2205–2210. [CrossRef]
112. He, H.; Yuan, M.; Liu, X. Research on Surface Defect Detection Method of Metal Workpiece Based on Machine Learning. In Proceedings of the 2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 9–11 April 2021; pp. 881–884. [CrossRef]
113. Zheng, X.; Wang, H.; Chen, J.; Kong, Y.; Zheng, S. A Generic Semi-Supervised Deep Learning-Based Approach for Automated Surface Inspection. *IEEE Access* **2020**, *8*, 114088–114099. [CrossRef]
114. Tulala, P.; Mahyar, H.; Ghalebi, E.; Grosu, R. Unsupervised Wafermap Patterns Clustering via Variational Autoencoders. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8. [CrossRef]
115. Hawkins, D.M. *Identification of Outliers*; Springer: Berlin/Heidelberg, Germany, 1980; Volume 11.
116. Bonomi, N.; Cardoso, F.; Confalonieri, M.; Daniele, F.; Ferrario, A.; Foletti, M.; Giordano, S.; Luceri, L.; Pedrazzoli, P. Smart quality control powered by machine learning algorithms. In Proceedings of the 2021 IEEE 17th International Conference on Automation Science and Engineering (CASE), Lyon, France, 23–27 August 2021; pp. 764–770. [CrossRef]
117. Moldovan, D.; Anghel, I.; Cioara, T.; Salomie, I. Machine Learning in Manufacturing: Processes Classification Using Support Vector Machine and Horse Optimization Algorithm. In Proceedings of the 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 10–11 December 2020; pp. 1–6. [CrossRef]
118. Moldovan, D.; Anghel, I.; Cioara, T.; Salomie, I. Particle Swarm Optimization Based Deep Learning Ensemble for Manufacturing Processes. In Proceedings of the 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 3–5 September 2020; pp. 563–570. [CrossRef]
119. Dua, D.; Graff, C. *UCI Machine Learning Repository*; UCI: Aigle, Switzerland, 2017.
120. Zhang, Y.; Peng, P.; Liu, C.; Zhang, H. Anomaly Detection for Industry Product Quality Inspection based on Gaussian Restricted Boltzmann Machine. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 1–6. [CrossRef]
121. Yuan, F.Q. Critical issues of applying machine learning to condition monitoring for failure diagnosis. In Proceedings of the 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bali, Indonesia, 4–7 December 2016; pp. 1903–1907. [CrossRef]
122. Hu, H.; Nguyen, N.; He, C.; Li, P. Advanced Outlier Detection Using Unsupervised Learning for Screening Potential Customer Returns. In Proceedings of the 2020 IEEE International Test Conference (ITC), Washington, DC, USA, 1–6 November 2020; pp. 1–10. [CrossRef]

123. Vajda, D.; Pekar, A.; Farkas, K. Towards Machine Learning-based Anomaly Detection on Time-Series Data. *Infocommunications J.* **2021**, *XIII*, 36–44. [CrossRef]
124. Wang, C.C.; Lee, C.W.; Ouyang, C.S. A machine-learning-based fault diagnosis approach for intelligent condition monitoring. In Proceedings of the 2010 International Conference on Machine Learning and Cybernetics, Qingdao, China, 11–14 July 2010; Volume 6, pp. 2921–2926. [CrossRef]
125. Wu, D.; Jiang, Z.; Xie, X.; Wei, X.; Yu, W.; Li, R. LSTM Learning With Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 5244–5253. [CrossRef]
126. Liu, Y.; Garg, S.; Nie, J.; Zhang, Y.; Xiong, Z.; Kang, J.; Hossain, M.S. Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. *IEEE Internet Things J.* **2021**, *8*, 6348–6358. [CrossRef]
127. Wang, X.; Garg, S.; Lin, H.; Hu, J.; Kaddoum, G.; Jalil Piran, M.; Hossain, M.S. Toward Accurate Anomaly Detection in Industrial Internet of Things Using Hierarchical Federated Learning. *IEEE Internet Things J.* **2022**, *9*, 7110–7119. [CrossRef]
128. Wu, Y.; Dai, H.N.; Tang, H. Graph Neural Networks for Anomaly Detection in Industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 9214–9231. [CrossRef]
129. Genge, B.; Haller, P.; Enăchescu, C. Anomaly Detection in Aging Industrial Internet of Things. *IEEE Access* **2019**, *7*, 74217–74230. [CrossRef]
130. Rayana, S. *ODDS Library*; ODDS: Hong Kong, China, 2016.
131. *EN 13306:2017*; Maintenance. Maintenance Terminology. iTeh, Inc.: Newark, DE, USA, 2017; ISBN 978-0-580-90370-0.
132. Krupitzer, C.; Wagenhals, T.; Züfle, M.; Lesch, V.; Schäfer, D.; Mozaffarin, A.; Edinger, J.; Becker, C.; Kounev, S. A Survey on Predictive Maintenance for Industry 4.0. *arXiv* **2020**, arXiv:2002.08224.
133. Frankó, A.E.; Varga, P. A Survey on Machine Learning based Smart Maintenance and Quality Control Solutions. *Infocommunications J.* **2021**, *XIII*, 28–35. [CrossRef]
134. Merkt, O. On the Use of Predictive Models for Improving the Quality of Industrial Maintenance: An Analytical Literature Review of Maintenance Strategies. In Proceedings of the 2019 Federated Conference on Computer Science and Information Systems (FedCSIS), Leipzig, Germany, 1–4 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 693–704.
135. Ruschel, E.; Santos, E.A.P.; Loures, E.d.F.R. Industrial maintenance decision-making: A systematic literature review. *J. Manuf. Syst.* **2017**, *45*, 180–194. [CrossRef]
136. Lee, J.; Wang, H. New technologies for maintenance. In *Complex System Maintenance Handbook*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 49–78.
137. Ahmad, R.; Kamaruddin, S. An overview of time-based and condition-based maintenance in industrial application. *Comput. Ind. Eng.* **2012**, *63*, 135–149. [CrossRef]
138. Albano, M.; Ferreira, L.L.; Di Orio, G.; Maló, P.; Webers, G.; Jantunen, E.; Gabilondo, I.; Viguera, M.; Papa, G.; Novak, F. Sensors: The Enablers for Proactive Maintenance in the Real World. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; pp. 569–574. [CrossRef]
139. Mann, L.; Saxena, A.; Knapp, G.M. Statistical-based or condition-based preventive maintenance? *J. Qual. Maint. Eng.* **1995**, *1*, 46–59. [CrossRef]
140. Chemweno, P.; Morag, I.; Sheikhalishahi, M.; Pintelon, L.; Muchiri, P.; Wakiru, J. Development of a novel methodology for root cause analysis and selection of maintenance strategy for a thermal power plant: A data exploration approach. *Eng. Fail. Anal.* **2016**, *66*, 19–34. . [CrossRef]
141. Maurer, M.; Festl, A.; Bricelj, B.; Schneider, G.; Schmeja, M. Automl for log file analysis (alfa) in a production line system of systems pointed towards predictive maintenance. *Infocommunications J.* **2021**, *3*, 13. [CrossRef]
142. de Jonge, B.; Teunter, R.; Tinga, T. The influence of practical factors on the benefits of condition-based maintenance over time-based maintenance. *Reliab. Eng. Syst. Saf.* **2017**, *158*, 21–30. [CrossRef]
143. Theissler, A.; Pérez-Velázquez, J.; Kettelgerdes, M.; Elger, G. Predictive maintenance enabled by machine learning: Use cases and challenges in the automotive industry. *Reliab. Eng. Syst. Saf.* **2021**, *215*, 107864. [CrossRef]
144. Sowah, R.A.; Dzabeng, N.A.; Ofoli, A.R.; Acakpovi, A.; Koumadi, K.M.; Ocrah, J.; Martin, D. Design of Power Distribution Network Fault Data Collector for Fault Detection, Location and Classification using Machine Learning. In Proceedings of the 2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST), Accra, Ghana, 22–24 August 2018; pp. 1–8. [CrossRef]
145. Zaporowska, A.; Liu, H.; Skaf, Z.; Zhao, Y. A clustering approach to detect faults with multi-component degradations in aircraft fuel systems. *IFAC-PapersOnLine* **2020**, *53*, 113–118.
146. Amihai, I.; Gitzel, R.; Kotriwala, A.M.; Pareschi, D.; Subbiah, S.; Sosale, G. An Industrial Case Study Using Vibration Data and Machine Learning to Predict Asset Health. In Proceedings of the 2018 IEEE 20th Conference on Business Informatics (CBI), Vienna, Austria, 11–13 July 2018; Volume 1, pp. 178–185. [CrossRef]
147. Kolokas, N.; Vafeiadis, T.; Ioannidis, D.; Tzovaras, D. A generic fault prognostics algorithm for manufacturing industries using unsupervised machine learning classifiers. *Simul. Model. Pract. Theory* **2020**, *103*, 102109. . [CrossRef]
148. Kim, D.; Lee, S.; Kim, D. An Applicable Predictive Maintenance Framework for the Absence of Run-to-Failure Data. *Appl. Sci.* **2021**, *11*, 5180. [CrossRef]

149. Zabihi-Hesari, A.; Ansari-Rad, S.; Shirazi, F.A.; Ayati, M. Fault detection and diagnosis of a 12-cylinder trainset diesel engine based on vibration signature analysis and neural network. *Proc. Inst. Mech. Eng. Part C J. Mech. Eng. Sci.* **2019**, *233*, 1910–1923. [CrossRef]
150. Lei, Y.; Yang, B.; Jiang, X.; Jia, F.; Li, N.; Nandi, A.K. Applications of machine learning to machine fault diagnosis: A review and roadmap. *Mech. Syst. Signal Process.* **2020**, *138*, 106587. [CrossRef]
151. Ince, T.; Kiranyaz, S.; Eren, L.; Askar, M.; Gabbouj, M. Real-Time Motor Fault Detection by 1-D Convolutional Neural Networks. *IEEE Trans. Ind. Electron.* **2016**, *63*, 7067–7075. [CrossRef]
152. Sun, W.; Chen, J.; Li, J. Decision tree and PCA-based fault diagnosis of rotating machinery. *Mech. Syst. Signal Process.* **2007**, *21*, 1300–1317. [CrossRef]
153. Kimotho, J.K.; Sondermann-Woelke, C.; Meyer, T.; Sextro, W. Application of event based decision tree and ensemble of data driven methods for maintenance action recommendation. *Int. J. Progn. Health Manag.* **2013**, *4*, 1–6. [CrossRef]
154. Sánchez, R.V.; Lucero, P.; Vásquez, R.E.; Cerrada, M.; Macancela, J.C.; Cabrera, D. Feature ranking for multi-fault diagnosis of rotating machinery by using random forest and KNN. *J. Intell. Fuzzy Syst.* **2018**, *34*, 3463–3473. [CrossRef]
155. Vamsi, I.V.; Abhinav, N.; Verma, A.K.; Radhika, S. Random forest based real time fault monitoring system for industries. In Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
156. Shao, H.; Jiang, H.; Zhao, H.; Wang, F. A novel deep autoencoder feature learning method for rotating machinery fault diagnosis. *Mech. Syst. Signal Process.* **2017**, *95*, 187–204. [CrossRef]
157. Haidong, S.; Hongkai, J.; Xingqiu, L.; Shuaipeng, W. Intelligent fault diagnosis of rolling bearing using deep wavelet auto-encoder with extreme learning machine. *Knowl. Based Syst.* **2018**, *140*, 1–14. [CrossRef]
158. Li, G.; Deng, C.; Wu, J.; Xu, X.; Shao, X.; Wang, Y. Sensor Data-Driven Bearing Fault Diagnosis Based on Deep Convolutional Neural Networks and S-Transform. *Sensors* **2019**, *19*, 2750. [CrossRef] [PubMed]
159. Wang, J.; Mo, Z.; Zhang, H.; Miao, Q. A Deep Learning Method for Bearing Fault Diagnosis Based on Time-Frequency Image. *IEEE Access* **2019**, *7*, 42373–42383. [CrossRef]
160. Zonta, T.; da Costa, C.A.; da Rosa Righi, R.; de Lima, M.J.; da Trindade, E.S.; Li, G.P. Predictive maintenance in the Industry 4.0: A systematic literature review. *Comput. Ind. Eng.* **2020**, *150*, 106889. [CrossRef]
161. Hwang, S.; Jeong, J.; Kang, Y. SVM-RBM based Predictive Maintenance Scheme for IoT-enabled Smart Factory. In Proceedings of the 2018 Thirteenth International Conference on Digital Information Management (ICDIM), Berlin, Germany, 24–26 September 2018; pp. 162–167.
162. Huang, H.Z.; Wang, H.K.; Li, Y.F.; Zhang, L.; Liu, Z. Support vector machine based estimation of remaining useful life: Current research status and future trends. *J. Mech. Sci. Technol.* **2015**, *29*, 151–163. [CrossRef]
163. Abu-Samah, A.; Shahzad, M.; Zamai, E.; Said, A.B. Failure prediction methodology for improved proactive maintenance using Bayesian approach. *IFAC-PapersOnLine* **2015**, *48*, 844–851. [CrossRef]
164. Cai, Z.; Sun, S.; Si, S.; Yannou, B. Maintenance Management System Based on Bayesian Networks. In Proceedings of the 2008 International Seminar on Business and Information Management, Wuhan, China, 19 December 2008; Volume 2, pp. 42–45. [CrossRef]
165. Gopalakrishnan, P.K.; Kar, B.; Bose, S.K.; Roy, M.; Basu, A. Live Demonstration: Autoencoder-Based Predictive Maintenance for IoT. In Proceedings of the 2019 IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019; p. 1.
166. Lu, Y.W.; Hsu, C.Y.; Huang, K.C. An Autoencoder Gated Recurrent Unit for Remaining Useful Life Prediction. *Processes* **2020**, *8*, 1155. [CrossRef]
167. Zhao, R.; Wang, D.; Yan, R.; Mao, K.; Shen, F.; Wang, J. Machine Health Monitoring Using Local Feature-Based Gated Recurrent Unit Networks. *IEEE Trans. Ind. Electron.* **2018**, *65*, 1539–1548. [CrossRef]
168. Wang, Q.; Bu, S.; He, Z. Achieving Predictive and Proactive Maintenance for High-Speed Railway Power Equipment with LSTM-RNN. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6509–6517. [CrossRef]
169. Rahhal, J.S.; Abualnadi, D. IOT Based Predictive Maintenance Using LSTM RNN Estimator. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; pp. 1–5. [CrossRef]
170. Li, H. An approach to improve flexible manufacturing systems with machine learning algorithms. In Proceedings of the IECON 2016—42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 23–26 October 2016; pp. 54–59. [CrossRef]
171. Teng, Y.; Li, L.; Song, L.; Yu, F.R.; Leung, V.C.M. Profit Maximizing Smart Manufacturing Over AI-Enabled Configurable Blockchains. *IEEE Internet Things J.* **2022**, *9*, 346–358. [CrossRef]
172. Klöter, B. Application of machine learning for production optimization. In Proceedings of the 2018 IEEE 7th World Conference on Photovoltaic Energy Conversion (WCPEC) (A Joint Conference of 45th IEEE PVSC, 28th PVSEC & 34th EU PVSEC), Waikoloa Village, HI, USA, 10–15 June 2018; pp. 3489–3491. [CrossRef]
173. Ye, W.; Alawieh, M.B.; Lin, Y.; Pan, D.Z. LithoGAN: End-to-End Lithography Modeling with Generative Adversarial Networks. In Proceedings of the 2019 56th ACM/IEEE Design Automation Conference (DAC), Vegas, NV, USA, 2–6 June 2019; pp. 1–6.

174. Pu, B.; Li, K.; Li, S.; Zhu, N. Automatic Fetal Ultrasound Standard Plane Recognition Based on Deep Learning and IIoT. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7771–7780. [CrossRef]
175. Qolomany, B.; Ahmad, K.; Al-Fuqaha, A.; Qadir, J. Particle Swarm Optimized Federated Learning For Industrial IoT and Smart City Services. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
176. Tian, X.; Ma, B.; Meng, C. Research on CMOPSO Particle Swarm Optimization Algorithm for Green Manufacturing Energy System in Ecological Park. In Proceedings of the 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 March 2021; Volume 5, pp. 2155–2159. [CrossRef]
177. Moriya, T. Machine Learning Approaches Optimizing Semiconductor Manufacturing Processes. In Proceedings of the 2021 5th IEEE Electron Devices Technology & Manufacturing Conference (EDTM), Chengdu, China, 8–11 April 2021; pp. 1–3. [CrossRef]
178. Okafor, N.U.; Delaney, D.T. Application of Machine Learning Techniques for the Calibration of Low-cost IoT Sensors in Environmental Monitoring Networks. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–3. [CrossRef]
179. Rymarczyk, T.; Klosowski, G.; Kozlowski, E. Innovative Methods of Tomographic Image Reconstruction Based on Machine Learning to Improve Monitoring and optimization in Industrial Processes. In Proceedings of the 2019 19th International Symposium on Electromagnetic Fields in Mechatronics, Electrical and Electronic Engineering (ISEF), Nancy, France, 29–31 August 2019; pp. 1–2. [CrossRef]
180. Jiahe, L. Machine Learning Aided Design Optimization for Micro-chip Reliability Improvement. In Proceedings of the 2020 3rd World Conference on Mechanical Engineering and Intelligent Manufacturing (WCMEIM), Shanghai, China, 4–6 December 2020; pp. 131–135. [CrossRef]
181. Kim, J.; Yoo, J.H.; Jung, J.; Kim, K.; Bae, J.; Kim, Y.s.; Kwon, O.; Kwon, U.; Kim, D. Novel Optimization Method using Machine-learning for Device and Process Competitiveness of BCD Process. In Proceedings of the 2020 International Conference on Simulation of Semiconductor Processes and Devices (SISPAD), Virtual, 23 September–6 October 2020; pp. 343–346. [CrossRef]
182. Dogan, A.; Birant, D. Machine learning and data mining in manufacturing. *Expert Syst. Appl.* **2021**, *166*, 114060. [CrossRef]
183. Gopaluni, R.B.; Tulsyan, A.; Chachuat, B.; Huang, B.; Lee, J.M.; Amjad, F.; Damarla, S.K.; Kim, J.W.; Lawrence, N.P. Modern Machine Learning Tools for Monitoring and Control of Industrial Processes: A Survey. *IFAC-PapersOnLine* **2020**, *53*, 218–229.
184. Wang, C.; Tan, X.; Tor, S.; Lim, C. Machine learning in additive manufacturing: State-of-the-art and perspectives. *Addit. Manuf.* **2020**, *36*, 101538. [CrossRef]
185. Wang, L.; Pan, Z.; Wang, J. A Review of Reinforcement Learning Based Intelligent Optimization for Manufacturing Scheduling. *Complex Syst. Model. Simul.* **2021**, *1*, 257–270. [CrossRef]
186. Veloso, B.; Gama, J.; Ribeiro, R.P.; Pereira, P.M. A Benchmark dataset for predictive maintenance. *arXiv* **2022**, arXiv:2207.05466.
187. Tosato, D.; Dalle Pezze, D.; Masiero, C.; Susto, G.A.; Beghi, A. *Alarm Logs in Packaging Industry (ALPI)*; Università Studi Padova Tech. Rep. ; Università Studi Padova: Padova, Italy, 2020. [CrossRef]
188. Hegedűs, C.; Varga, P.; Moldován, I. The MANTIS Architecture for Proactive Maintenance. In Proceedings of the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; pp. 719–724.
189. Jantunen, E.; Zurutuza, U.; Ferreira, L.L.; Varga, P. Optimising maintenance: What are the expectations for Cyber Physical Systems. In Proceedings of the 2016 3rd International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC), Vienna, Austria, 11 April 2016; pp. 53–58. [CrossRef]
190. Larrinaga Barrenechea, F.; Zugasti Uriguen, E.; Garitano Garitano, I.; Zurutuza Ortega, U. A Big Data implementation of the MANTIS Reference Architecture for Predictive Maintenance. *Proc. Inst. Mech. Eng. Part I J. Syst. Control Eng.* **2019**, *233*, 1361–1375. [CrossRef]
191. Di Orio, G.; Maló, P.; Barata, J.; Albano, M.; Ferreira, L.L. Towards a Framework for Interoperable and Interconnected CPS-populated Systems for Proactive Maintenance. In Proceedings of the 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), Porto, Portugal, 18–20 July 2018; pp. 146–151. [CrossRef]
192. Hegedűs, C.; Ciancarini, P.; Frankó, A.; Kancilija, A.; Moldován, I.; Papa, G.; Poklukar, Š.; Riccardi, M.; Sillitti, A.; Varga, P. Proactive maintenance of railway switches. In Proceedings of the 2018 5th international conference on control, decision and information technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 725–730.
193. Papa, G.; Poklukar, Š.; Frankó, A.; Sillitti, A.; Kancilija, A.; Šterk, M.; Hegedűs, C.; Moldován, I.; Varga, P.; Riccardi, M.; et al. Improving the Maintenance of Railway Switches through Proactive Approach. *Electronics* **2020**, *9*, 1260. [CrossRef]
194. Zhao, W.; Goudar, A.; Qiao, X.; Schoellig, A.P. UTIL: An Ultra-wideband Time-difference-of-arrival Indoor Localization Dataset. *arXiv* **2022**, arXiv:2203.14471. https://doi.org/10.48550/ARXIV.2203.14471.
195. Gao, K.; Wang, H.; Lv, H. *CSI Dataset towards 5G NR High-Precision Positioning*; IEEE DataPort: Piscataway, NJ, USA, 2021. [CrossRef]