



Article

The Management of IoT-Based Organizational and Industrial Digitalization Using Machine Learning Methods

Aoqi Xu ¹, Mehdi Darbandi ², Danial Javaheri ³ , Nima Jafari Navimipour ^{4,5,*} , Senay Yalcin ⁶ and Anas A. Salameh ⁷

¹ School of Economics, Fujian Normal University, Fuzhou 350007, China

² Department of Electrical and Electronic Engineering, Eastern Mediterranean University, Gazimagusa 99628, Turkey; mehdi.darbandi@edu.devinci.fr

³ Department of Computer Engineering, Chosun University, Gwangju 61452, Republic of Korea; javaheri@chosun.ac.kr

⁴ Department of Computer Engineering, Kadir Has University, Istanbul 34083, Turkey

⁵ Future Technology Research Center, National Yunlin University of Science and Technology, Douliou, Yunlin 64002, Taiwan

⁶ Department of Computer Engineering, Nisantasi University, Istanbul 34485, Turkey; senay.yalcin@nisantasi.edu.tr

⁷ Department of Management Information Systems, College of Business Administration, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; a.salameh@psau.edu.sa

* Correspondence: jnnima@yuntech.edu.tw or nima.navimipour@khas.edu.tr

Abstract: Recently, the widespread adoption of the Internet of Things (IoT) model has led to the development of intelligent and sustainable industries that support the economic security of modern societies. These industries can offer their participants a higher standard of living and working services via digitalization. The IoT also includes ubiquitous technology for extracting context information to deliver valuable services to customers. With the growth of connected things, the related designs often suffer from high latency and network overheads, resulting in unresponsiveness. The continuous transmission of enormous amounts of sensor data from IoT nodes is problematic because IoT-based sensor nodes are highly energy-constrained. Recently, the research community in the field of IoT and digitalization has labored to build efficient platforms using machine learning (ML) algorithms. ML models that run directly on edge devices are intensely interesting in the context of IoT applications. The use of intelligence ML algorithms in the IoT can automate training, learning, and problem-solving while enabling decision-making based on past data. Therefore, the primary aim of this research is to provide a systematic procedure to review the state-of-the-art on this scope and offer a roadmap for future studies; thus, a structure is introduced for industry sustainability, based on ML methods. The publications were reviewed using a systematic approach that divided the papers into four categories: reinforcement learning, semi-supervised learning, unsupervised learning, and supervised learning. The results showed that ML models could manage IoT-enabled industries efficiently and provide better results compared to other models, with significant differences in learning time and performance. The study findings are considered from a variety of angles concerning the industrial sector's capacity management of the new elements of Industry 4.0 by combining the industry IoT and ML. Additionally, unique and relevant instructions are provided for the designers of expert intelligent production systems in industrial domains.

Keywords: internet of things; industrial IoT; machine learning; industrial digitalization; sustainability; energy; digital economy



Citation: Xu, A.; Darbandi, M.; Javaheri, D.; Navimipour, N.J.; Yalcin, S.; Salameh, A.A. The Management of IoT-Based Organizational and Industrial Digitalization Using Machine Learning Methods. *Sustainability* **2023**, *15*, 5932. <https://doi.org/10.3390/su15075932>

Academic Editors: Marc A. Rosen and Gwanggil Jeon

Received: 19 December 2022

Revised: 15 March 2023

Accepted: 20 March 2023

Published: 29 March 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Significant quantitative and qualitative changes in sustainable industries have occurred due to rapid progress in the fields of information technology (IT) and the Internet,

which is integrated into the elements of companies. According to experts, the fourth industrial revolution (Industry 4.0) will commence in the coming decades. Digitalization, information and communication technology (ICT), machine learning (ML), robots, and artificial intelligence (AI) will drive the industrial revolution and result in the transfer of decision-making to machines. The following societal trends will significantly impact management practices and research [1]. However, many risks are associated with digitizing conventional processes and equipment, including volatility, ambiguity, complexity, and uncertainty. Therefore, digitalization presents both enormous challenges and enormous potential for enterprises. The digital economy is volatile, uncertain, sustainable, and complex due to the impacts of emerging technology on all economic and social sectors [2].

In order to create and implement technology to maintain a competitive advantage, firms must go digital; this will trigger the digital revolution, which will alter every industry. The introduction of digital technologies has allowed digitalization to permeate every part of our lives. An organization can modify its business model and organizational structure with the help of digitalization to stay competitive, increase productivity, lower production costs, and forge new connections with customers. The use of digital technologies in a wide range of applications and the changes that these technologies bring in the context of companies, people, and smart objects, are referred to as digitalization [2]. Upcoming organizations must change to remain competitive and provide for their consumers and staff [3]. The phrase “Industrial Internet of Things” (IIoT), on the other hand, describes the application of IoT technology to the industrial sector. Integration and the advancement of IoT and industrial automation technologies are its primary goals [4]. The IIoT enabled the never-before-seen integration of monitoring, production, and management subsystems.

While some firms and sustainable industries are now resisting technological advancement, others welcome the idea of artificial intelligence (AI). As a result of their willingness to pay for AI hardware, software, and interfaces, many financiers are investing more money in AI enterprises to accelerate the use of AI in marketing. Internet goliaths such as Facebook, Google, and others try to create tools to jumpstart customized advertising and enhanced search engines. However, it is crucial to comprehend how traditional industries invest their money in AI projects. In terms of ML, AI is supposed to open up the next digitalization frontier. In light of the impending digital developments, businesses should be ready for this kind of development as this would give the corporate sector a competitive edge in the real world [5].

One effective way to manage organizational and industrial digitalization is by integrating ML methods into Industry 4.0. ML serves as a leader in recognizing, planning for, and responding to occurrences in each area [6]. ML will spark the next wave of digital disruption. It is predicted that businesses will prepare themselves. Businesses that used ML early on are benefiting from its use, compared to others. Future technologies based on ML include computer vision, agents, robotics, sustainable industries, natural language processing, and autonomous vehicles. Digitalization is the foundation of the new generation of ML applications. The majority of the time, industries that embraced digitization are also setting the pace for ML. They are also expected to stimulate growth. ML is anticipated to hasten market share, revenue, and profit margin changes. Conversely, there are numerous industries, goods, and services that have been disrupted by technology [7].

The novel element of the current article is in the type of applied method (a systematic literature review (SLR)) in the aforementioned fields. The systematic approach represents a very important and widely studied method for reviewing articles in a specific domain, one that has been emphasized in many papers, such as in Refs. [8–11]. In this study, the applied method delivers a clear and comprehensive overview of available ML- and IoT-based organizational and industrial digitalization methods. Moreover, SLR can help us to identify research gaps in this field. However, as far as we know, there is as yet no systematic review analyzing IoT-based organizational and industrial digitalization using machine learning methods. In addition, unlike similar review papers, the grouping is complete in this paper and covers all the papers in this domain. The provided categorization in this

paper includes: (1) supervised, (2) unsupervised, (3) semi-supervised, and (4) reinforcement learning methods. This categorization has not been used before in any published article on this issue. The most important goal of a systematic review is also to obtain answers to the questions that are most necessary for researchers in terms of a review of the related articles. One of the most important results of an SLR is to help researchers who want to research the topic under study to identify the journals that contribute the most to the publication of the topic in question. Furthermore, it identifies the most important challenges and open issues, which can provide a roadmap for future researchers to direct further investigation. In addition to this, the applied method in this study can introduce researchers to the most important articles related to the subject under study. In addition, the most important innovation in this article is that we have reviewed new and updated articles in this study that have not as yet been considered in any other study. The present article aims to solve the issues of current papers; paper construction is subordinated to this target. This study has been performed to deliver an inclusive summary of the management of IoT-based organizational and industrial digitalization using ML methods. The authors have chosen several targets that must be achieved via this study:

- Proposing an SLR and investigating the strategies for the management of IoT-based organizational and industrial digitalization, using ML methods;
- Offering useful reports around the topic of IoT-based organizational and industrial digitalization;
- Detecting obstacles, prosperity criteria, and total notions that the management of the IoT-based organizational and industrial digitalization may encounter, utilizing ML methods;
- Summarizing the chosen articles comparatively;
- Categorizing the studied approaches and highlighting their important features;
- Identifying gaps in previous studies and providing solutions for future studies.

The present investigation addresses the issues below: Section 2 offers background and related works; Section 3 discusses the methodology; Section 4 reviews the background and the chosen articles; Section 5 offers a discussion of the presented results. Section 6 concludes the article and acknowledges the limitations of this work.

2. Background and Related Works

Intelligent manufacturing systems and digitalization are the foundations on which the modern manufacturing, production, and industry sectors are being built. These revolutionary adjustments, also known as Industry 4.0, are being made to achieve digital transformation for organizational advantage. The development and facilitation of the smart manufacturing system follow data, information, and operational technologies through edge computing, blockchain, and ML [12]. The development of IoT and other intelligent automation applications is being significantly fueled by expanding digitalization, which is becoming more widely accessible. Digitalization's arrival is more than just a generational shift; it creates new opportunities for all IT industries [13]. Many articles have been written on this subject, which will be reviewed in the following section.

Bauer et al. [14] examined the digitalization of industrial value chains and evaluated case studies regarding Industry 4.0 in Germany. Seven industrial partners made up part of the project's 14 partners, who also created methodologies and tools for implementing the application of intelligent digitalization and industrial automation. Over 385 case studies were examined using comparison criteria in the report. Additionally, application cases were categorized according to the degree of development of industry 4.0 promises and ambitions. In terms of Industry 4.0, the three tiers of "information," "interaction," and "intelligence" were utilized to separate applications, based on their level of maturity.

Matt et al. [15] addressed the current increase in publications on the subject of digitization by conducting a thorough study of the literature on this significant organizational and technological change in the manufacturing industry. They established 4 thematic areas (technologies, impacts, enabling factors, and impediments) and produced a relevant

segmentation of the existing publications after describing the various conceptualizations of digitalization and the stages of its progress. They then conceptualized and empirically defined a future research agenda on industrial digitization.

Tian [16] systematically examined the research results of China's industrial digitalization and economic practices to promote the deepening and systematization of research in this field and provide a reference for enabling digital transformation. Firstly, the connotation, characteristics, and denotation of industrial digitalization were defined, based on relevant domestic studies. Secondly, combined with a discussion of the changes in industrial structure, their paper summarized the three driving modes of China's industrial digitalization: the backward-forcing mode, dominated by social motivation, the integration mode, dominated by technological motivation, and the value-added service mode, dominated by innovation motivation. Thirdly, the formation mechanism of the industry chain being reshaped by digitalization was summarized and interpreted.

Osipova and Idrisov [17] studied the organizational and legal issues in the agro-industrial complex, public-private partnerships, and the digitalization of production. They addressed the major legal, social, and economic issues of the Russian Federation's agro-industrial complex. The Russian agro-industrial complex's most pressing challenges were shown graphically. The legal framework governing the agro-industrial complex and government operations was also examined in the essay. Investigations were conducted into the concept of public-private partnerships, the potential applications of digital technology in agriculture, and the agroecologists' effect on the agro-industrial complex. In legal science, the issue of the legal status of agrarian law was considered. Other nations that dealt with the organizational and legal issues of the agro-industrial complex were also examined. A solution to the issue was suggested, considering the various outcomes in the field of agricultural development.

Bigliardi et al. [18] discussed the digital transformation of the supply chain. The trend of the article was related to the progress of digital technologies, such as blockchain, IoT, ML, etc., toward a more intelligent model. Employing a keyword-based organizing framework, they attempted to discover, categorize, and explore relevant intellectual contributions in this subject in relation to the major conversation topics surrounding supply chain digitization. The acquired results revealed the primary concerns surrounding supply chain digitalization.

A summary of the five important review articles discussed in this section, including the useful points made in the articles and the relevant details compared to the current paper, is presented in Table 1.

Table 1. Summarization of the key points of the studied review articles.

Ref	Year	Citations until 10 December 2022	Type of Paper	Journal	Examining the Challenges	Classification	Review of ML Methods	Examining the Role of the IoT
[14]	2018	41	Review	LogForum	No	Done	No	No
[15]	2022	11	Systematic	European Management Journal	Done	Done	No	No
[16]	2022	No	Systematic	Academic Journal of Business & Management	Done	Done	No	No
[17]	2022	2	Review	Agriculture Digitalization and Organic Production	Done	No	No	No
[18]	2022	6	Review	Procedia Computer Science	Done	No	No	No
Our paper	-	-	Systematic	-	Done	Done	Done	Done

As shown in Table 1, numerous studies have been published on the topic of digitalization, but none have been based on IoT-based digitalization utilizing ML. Therefore, the literature on IoT-based organizational and industrial digitalization utilizing ML approaches lacks adequate depth and systematization. This paper addresses the recent increase in publications on IoT-based digitalization by conducting a systematic review of this significant technological and organizational transformation using ML methods; this topic is of relevant interest to the scientific community. Our goal is to improve knowledge of this phenomenon and offer a critical assessment of the state of the art of IoT-based industrial digitalization research.

3. Materials and Methods

This study addresses the recent increase in publications on IoT-based digitalization by conducting an SLR of the literature on this significant technological and organizational transformation using ML methods; this topic is of relevant interest to the scientific community. The goal is to achieve a better comprehension of this phenomenon and present a critical assessment of the current status of the science regarding IoT-based industrial digitalization [19]. This paper addresses four aspects of literature reviews:

1. The goals of the study

The purpose of a literature review may be to integrate (e.g., reconcile opposing viewpoints or close the gap between theories and practices), critique (e.g., analyze the literature critically to show how unwarranted the prior ideas were), or focus on a particular issue (such as what topics have been studied in the past, what can be studied in the future, what issues have hindered the development of some topics, etc.) [20,21]. This study intends to consolidate prior material and identify the fundamental issue of the literature review regarding IoT-based digitalization utilizing ML techniques.

2. Organization

The literature review could be ordered in chronological, conceptual, or methodological order. In this research, the chronological order comes first, followed by the conceptual order.

3. Targeted readership

The audience of a review refers to the individuals or groups of individuals to whom it is directed; in the case of a literature review, the audience consists of industrial decision-makers and specialist scholars.

4. Coverage

Coverage focuses on the reviewer's process for evaluating the studied documents' suitability and caliber after a literature search, whether the author picked adequately representational coverage out of several options, including exhaustive, exhaustive with chosen reference, central, representative, or pivotal analyses. Various levels of rigor can be applied to stand-alone literature reviews, from straightforward annotated bibliographies to extensively studied summaries of the source material [22]. This article focuses on an SLR, which is a more thorough method of completing a stand-alone literature review. We adapted the definition in Refs. [23,24] of a research literature review as our operative definition of an SLR for this article: a process that is systematic, explicit, and repeatable for locating, assessing, and combining the already completed and recorded works of researchers, academics, and practitioners [25,26]. Next, the steps in the SLR method are documented below.

3.1. Research Questions

The selection of research topics is the most crucial stage of an SLR [27,28]. These inquiries constitute the basis of the auto-search query; they specify the data gathered from each source article and limit the aggregate process. The research questions are as follows:

- RQ1: What are the results of an SLR on IoT-based digitalization using ML methods?

- RQ2: What well-liked algorithms are employed to manage organizational and IIoT-based digitalization using ML methods?
- RQ3: What are the next developments, unresolved problems, and difficulties in using ML methods for organizational and IIoT-based digitalization?

3.2. Search Strategy

A methodical search was performed to identify pertinent publications that were registered in the Medline and Web of Science databases between 1 January 2018 and 10 December 2022. Backward and forward snowball search types were employed to discover additional articles on Google Scholar using the reference lists of the included studies and reviews [29]. The keywords that were searched for were “IoT”, “Internet of Things”, “Digitalization”, “Industrialization”, “ML”, “Machine learning”, “Unsupervised learning”, “Supervised learning”, “Semi-supervised learning”, and “Reinforcement learning”.

3.3. Inclusion and Exclusion Criteria

The papers that met the following criteria were included: (1) studies with any perspective in IoT-based digitalization using the ML methods; (2) published studies from 1 January 2018 until 10 December 2022; (3) studies published in English in a peer-reviewed journal. Additionally, studies were omitted if they were: (1) reviews, notes, commentaries, or editorials related to IoT-based digitalization, (2) duplicate articles, or (3) articles that described the study protocol or study design. Figure 1 clearly outlines the procedures for choosing the articles based on the inclusion/exclusion criteria.

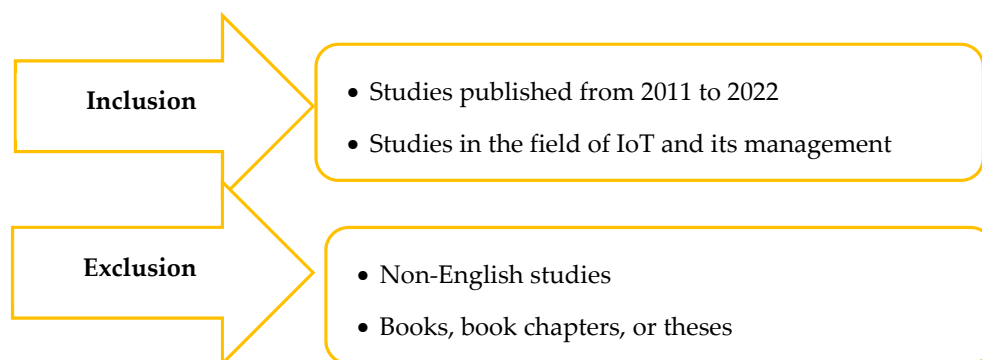


Figure 1. Inclusion and non-inclusion criteria.

3.4. Selection and Data Extraction

After deleting any duplicate articles, all titles and abstracts were evaluated to determine which studies met the inclusion and exclusion criteria. After an initial screening, the co-authors reviewed a random sample by assessing the comparability of the included and omitted studies. The whole texts of the remaining studies were compared to the inclusion criteria, after the papers that passed the initial screening’s exclusion criteria had been eliminated, and any inconsistencies were discussed. Figure 2 depicts a flowchart of the study selection approach. Figure 2 shows that 87 were articles identified during the keyword search. Fourteen duplicate articles, 26 non-English articles, 9 articles with irrelevant titles, and 18 items with irrelevant or unavailable full texts were eliminated. Finally, twenty articles were chosen.

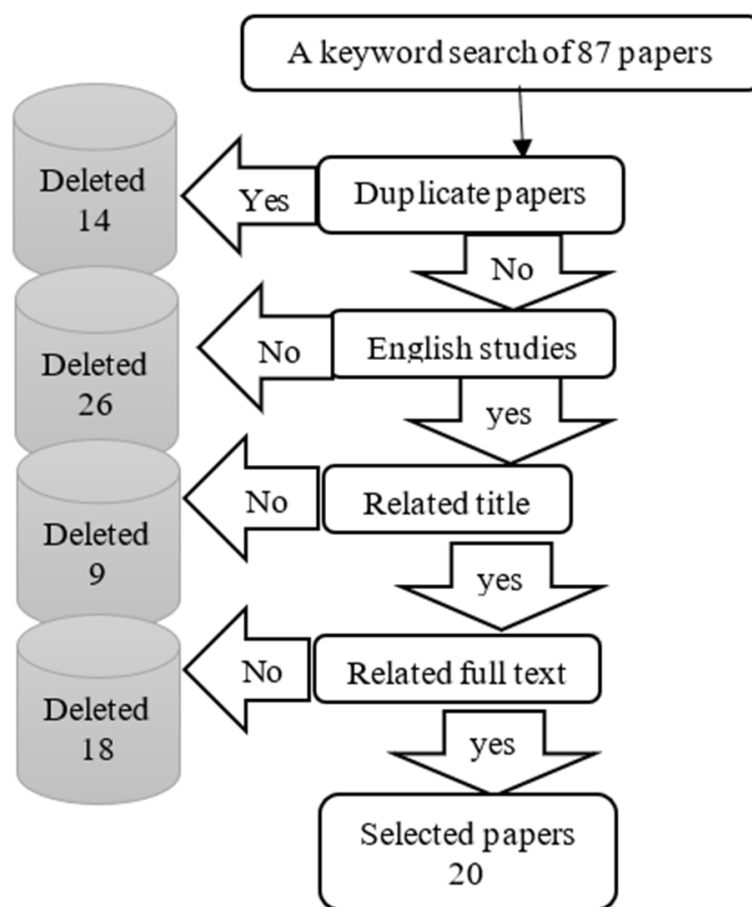


Figure 2. The article selection process.

The obtained 87 articles are shown in Figure 3. As can be seen, most of the articles have been published in IEEE publications. Springer and MDPI are ranked second and third, respectively.

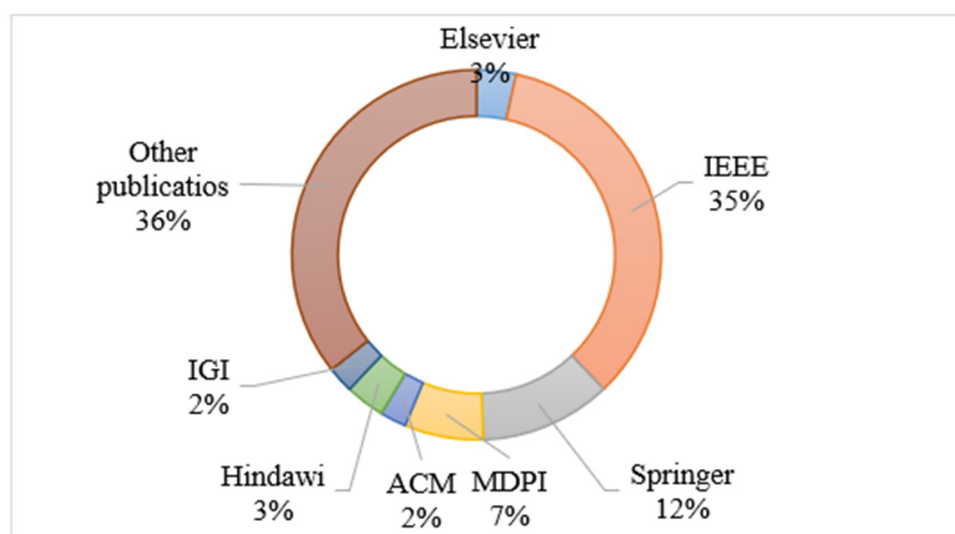


Figure 3. Articles found by the keyword searches.

In addition, we present the articles of the last 8 years in Figure 4 to show that the corpus of research using ML methods and that is related to IIoT-based digitalization is increasing day by day, which shows the importance of this topic among researchers.

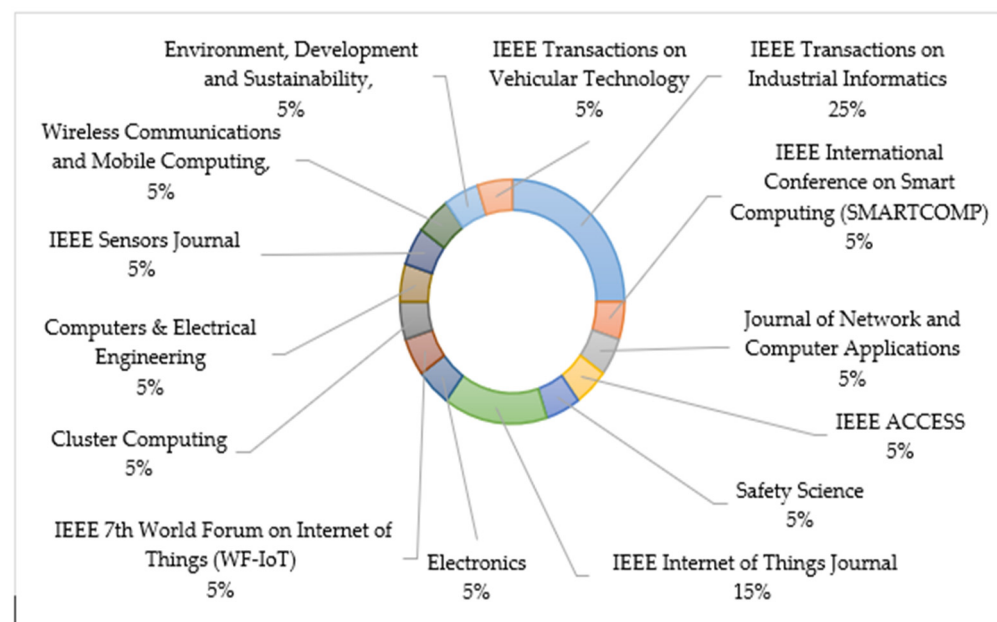


Figure 4. The publications according to year.

The next section will analyze twenty selected articles, based on different filters. The journals of the selected articles are shown in Figure 5. Most of the selected papers are from IEEE publications.

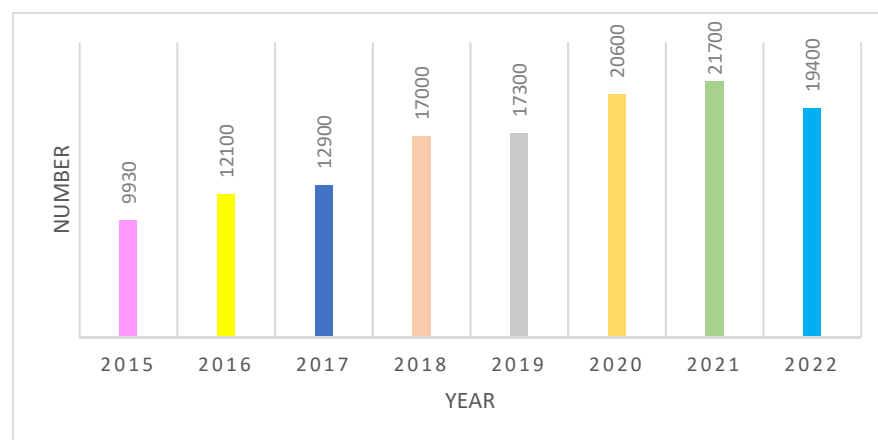


Figure 5. The selected articles for review in this study.

4. Systematic Literature Review

In recent decades, the advent of the IoT has been a crucial development and provided the impetus for numerous additional advancements [30]. The philosophy of the IoT is a crucial component of the next generation of data. Self-regulating, dispersed smart sensor gateways and nodes comprise wireless sensor networking. The various sensors continuously evaluate external physical data, such as sound, vibration, and temperature [31]. New IIoT platforms attempt to solve the manufacturers' most difficult problem: integrating all production systems into a single model [32]. These technologies are utilized in smart cities, in fields such as disaster preparedness, environmental applications, energy, healthcare, logistics, manufacturing control, home automation, farming, and animal husbandry. These items, machines, and tools can produce, gather, and exchange data without involving humans or computers. The IIoT generates a flood of structured and unstructured data from a growing army of sensors that are capable of registering, among other things, locations, voices, faces, sounds, temperature, emotions, and health. There are billions of connected

IoT devices, with an enormous amount of data being produced. Every device incorporates automation to facilitate daily operational planning, management, and decision-making. ML approaches are used to improve the intelligence and capabilities of a particular program. Numerous academics are currently interested in integrating ML with IoT techniques to create superior IoT technology [33]. IIoT devices learn to execute tasks such as prediction, pattern recognition, classification, and clustering by means of ML [34]. To facilitate the learning process, IoT devices are trained by analyzing sample data using various ML and statistical models. Measuring the functional parameters characterizes the various sectors of the datasets. Then, ML algorithms are applied to the data set to discover features, provide output, classify patterns, make decisions, and draw inferences. Without using humans or additional computers, machines and appliances can produce, gather, and distribute data [35]. In the following section, the articles selected in the previous section will be reviewed in the context of these four groups (see Figure 6).

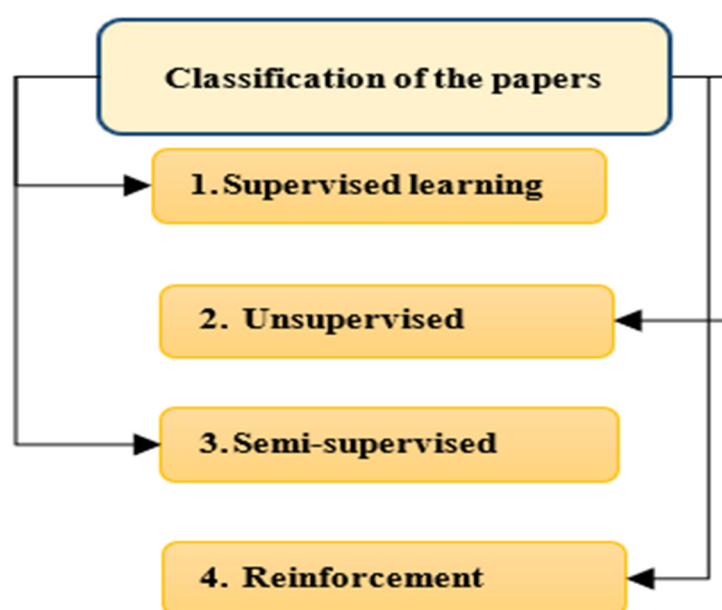


Figure 6. The selected papers.

4.1. Supervised Learning

Real-world applications of supervised learning have been quite successful. The technique is utilized in virtually all domains, including text and web domains. ML also refers to supervised learning as classification or inductive learning. This method of learning is akin to how humans acquire new knowledge through past experiences and use it to enhance their ability to accomplish real-world activities [36]. Mapping across a collection of input variables, X , and an output variable, Y , is established by supervised learning, and this mapping is then used to predict the outcomes for unknown data. This approach, which is the most important ML methodology, is essential for processing multimedia data. Many supervised learning techniques have been used to handle multimedia input, with supervised learning accounting for the majority of ML research. The availability of annotated training datasets supervised learning apart from unsupervised learning. The term “supervisor” conjures up the idea of a “supervisor” who directs the learning system in terms of choosing what labels to apply to training occurrences. In classification problems, these labels are often classification labels. Models that can identify other unlabeled data are created by supervised learning algorithms using these training data [37]. The remaining paragraphs in this section address papers on supervised learning.

Rodriguez, Saed, and Li [38] investigated beverage freshness sensing using WPT/NFC (wireless power transfer/near-field communication) technology that was compatible with smartphones, using supervised ML. The classification performance of features of various

types (such as magnitude, amplitude, and phase) was explored and assessed, using a circuit model for the beverage–coil interaction. Employing supervised ML to classify the freshness of milk resulted in accuracies as high as 96.7 percent when five distinct types of milk were utilized. In addition, the required RF bandwidth for classification was reduced to 10 MHz by means of singular value decomposition and boxplot examination, without impacting the classification performance for two distinct feature extraction approaches.

Gantert et al. [39] addressed corrective maintenance using fault recognition that was based on the sounds created by machine components. Different spectral characteristics were retrieved from industrial sounds and fed into supervised learning algorithms to categorize normal and abnormal activities. The f1 score was used to demonstrate that studies using the dataset for malfunctioning industrial machines investigation and inspection, which includes sound samples from components such as pumps, sliding rails, valves, and fans, have been successful. They also analyzed the impact of the various spectral properties, validating their incremental influence. Lastly, they contrasted the idea with a baseline option from the existing literature that employs unsupervised learning and mel-spectrogram conversion. Their strategy increased the metric of the area under the curve.

Using supervised learning classifiers, Gupta et al. [40] presented an intelligent defense against distributed denial of service (DDoS) attacks in IoT networks. Utilizing local IoT network-specific features, their approach enabled low-cost ML classifiers to detect attacks at the local router. The testing results demonstrated that the proposed method attained the greatest accuracy of 0.99, confirming its robustness and dependability in the context of IoT networks.

Djenouri et al. [41] proposed a method that processes IoT data using DL models and improves the interpretation of the results. They offered an updated Gamian angular technique for converting the time series acquired by the various sensors into visual characteristics that may be conveniently represented by a succession of photographs. This enables the use of a promising visual geometry group architecture for learning sensor data correlations from a set of photos. The authors' framework investigates the relationships between sensor data characteristics and then applies DL to learn prediction and intrusion detection tasks (the most challenging problems in IoT applications). In addition, explainable artificial intelligence (XAI) is used to establish the contribution of each feature to the prediction and detection outputs. Extensive tests were conducted to demonstrate the efficacy of the proposed technology in two unique applications: stream prediction and intrusion detection. In terms of both runtime and precision, the experimental results revealed that the technique is superior to that of the baseline approaches.

To enhance trustworthiness and collaborative communication in smart cities, Haseeb et al. [42] presented a fault-tolerant supervised routing architecture for trust management in the IoT. The IoT nodes assessed their neighbors' behavior in the proposed architecture and built direct trust for a dependable and optimal network structure. In addition, a fault-tolerant relaying system was developed, utilizing supervised ML without incurring additional costs. In addition, it eliminated the burden of calculating the ideal decision and training the IoT system to balance network costs. Finally, a secure technique was presented to protect confidentiality and authentication in the presence of critical key-based assaults. The performance of the proposed technique was superior to that of the existing work.

In this section, five articles are reviewed. Table 2 summarizes the articles' key topics so that readers can access the articles' specifics and compare them to one another. As the results revealed, increasing the accuracy of the proposed system has been one of the most important goals of the researchers. Furthermore, privacy and trust have been incorporated in the next phase of the researchers' attention.

Table 2. The details of selected topics in the supervised learning articles.

Ref/	Year	Evaluation	Keywords	Title	Network/Model/Structure	Achievements
[38]	2020	Implemented	<ul style="list-style-type: none"> Sensors Dairy products Impedance The dielectric constant Couplings Near-field communication Smartphones 	<ul style="list-style-type: none"> A WPT/NFC-based sensing approach for beverage freshness detection using supervised ML 	<ul style="list-style-type: none"> WPT/NFC technology IoT 	<ul style="list-style-type: none"> High level of accuracy Reducing bandwidth
[39]	2021	Implemented	<ul style="list-style-type: none"> Rails Support vector machines Fans Pumps Maintenance engineering Feature extraction Valves 	<ul style="list-style-type: none"> A supervised approach for corrective maintenance using spectral features from industrial sounds 	<ul style="list-style-type: none"> IoT 	<ul style="list-style-type: none"> Better area under the curve performance Improving corrective maintenance
[40]	2022	Simulated	<ul style="list-style-type: none"> Smart defense Distributed service IoT Supervised learning 	<ul style="list-style-type: none"> Smart defense against distributed denial of service attacks in IoT networks using supervised learning classifiers 	<ul style="list-style-type: none"> IoT ML 	<ul style="list-style-type: none"> High level of accuracy Less resource consumption Low computational overhead High level of reliability
[41]	2022	Implemented	<ul style="list-style-type: none"> XAI DL IoT applications Genetic algorithm 	<ul style="list-style-type: none"> When explainable AI meets IoT applications for supervised learning 	<ul style="list-style-type: none"> IoT ML AI DL Evolutionary computing 	<ul style="list-style-type: none"> Reducing runtime High level of accuracy
[42]	2022	Implemented	<ul style="list-style-type: none"> IoT Routing Smart cities Relays Computational modeling Security Fault-tolerant systems 	<ul style="list-style-type: none"> Trust management with fault-tolerant supervised routing for smart cities using IoT 	<ul style="list-style-type: none"> IoT ML 	<ul style="list-style-type: none"> Improving trust management Improving trustworthiness Improving collaborative communication Low cost High level of privacy

4.2. Unsupervised Learning

Recently, self-supervised and unsupervised learning has been proven to offer comparable performance to existing methods while removing manually labeled training processes. Unsupervised learning approaches exhibit self-organization to record patterns as probability densities or as a combination of neural feature preferences [43]. Additionally, this technique reduces the complexity of the training technique in lightweight devices to boost processing speed and effectively detect the health of equipment assets [44]. The selected articles related to unsupervised learning are discussed in the rest of this section.

Bhatia et al. [45] proposed a network-centric and behavior-learning-based anomaly detection technique for securing such vulnerable environments. Using unsupervised ML, they proved that the predictability of transmission control protocol traffic from IoT devices

could be leveraged to identify various sorts of distributed denial of service attacks in real time. The developed ML classifier can distinguish between regular and abnormal traffic from a tiny set of features. Their method can be integrated into a wider system for recognizing compromised endpoints despite IP spoofing, enabling specially designated national-based strategies to block attack traffic near the source. Their unsupervised ML approaches are easier to implement than supervised ML methods and are more effective at detecting new and previously unknown assaults.

Chen et al. [46] offered an online unsupervised anomaly detection method using a variational autoencoder with a convolutional neural network (CNN) structure for an industrial robot. This method utilized a reasonably long sliding window to better identify regular data patterns. The CNN structure was also incorporated into the encoder and decoder of the variational autoencoder model to extract temporal and spatial data. Data were gathered from the robot controller at a relatively low frequency. It learned the typical pattern from standard time series data and discovered anomalies by identifying the unseen data pattern, saving time and effort in terms of fault data collection. In addition, the method can be implemented online without accumulating data, accelerating anomaly detection and resolution. Using a CNN structure, which helps capture the relationships of the input data, this method may also automatically identify useful features that are sensitive to robot failures, as opposed to robot motions. Overall, the experiments demonstrated that their model could detect unknown spatial and temporal irregularities in the industrial robot with reliability.

Using a self-supervised learning approach in a time-series dataset, Tran et al. [44] developed a lightweight method for anomaly detection to improve the model's performance. Considering time-series data augmentation for pseudo-label generation, a classifier employing a one-dimensional convolutional neural network was used to learn the features of standard data. The output of their categorization model accurately indicated the degree of irregularity. The experimental results demonstrated that their proposed strategy outperforms conventional anomaly detection techniques. In addition, the model was deployed in a real testbed to demonstrate the efficacy of the self-supervised learning technique for time-series anomaly detection.

Zhan et al. [47] presented a framework for an intelligent system utilizing the IIoT and digital twin (DT) technologies to design real-time safety monitoring in the warehouse and ensure synchronized cyber-physical spaces for information visibility and traceability. The unsupervised deep neural structure of the stacked auto-encoder was created to differentiate abnormal stationary behavior from human motion status, which was interpreted as a warning sign of an oncoming accident. The model was designed to automatically update online by collaborating with the calibration samples to stay in sync with environmental changes. Using a Bluetooth-based model, indoor localization was achieved so that management could respond rapidly to an occurrence on-site. In addition, various intelligent services were enabled to improve safety management efficacy. A case study was performed at a cold storage warehouse used for air cargo to show the validity and logic of the proposed framework and procedures. This implementation was developed to facilitate efficient duplication and reproduction. The experiments were performed to investigate the impact of distance and vibration-related learning features on anomaly detection performance.

Dinh-Van et al. [48] presented a comprehensive system framework for reconfigurable intelligent surface-enhanced broadcast communications in the IIoT. In the system model, they accounted for the coexistence of various sensor clusters in a smart factory wherein direct connections between these clusters and a central base station were fully barred. In this context, a reconfigurable intelligent surface was used to reflect the signals broadcast from the base station toward cluster heads, which act as a representation of clusters, while the base station has only the statistical channel's state distribution information. Based on these mathematical conclusions, two methods, the Riemannian conjugate gradient method and the deep neural network approach, were developed to govern phase shifts at reconfigurable intelligent surfaces. While the Riemannian conjugate gradient approach employs the

standard iterative method, the deep neural network technique is based on unsupervised DL. According to their numerical findings, both methods achieved satisfactory performance, using only statistical channel state data. In addition, when compared to the Riemannian conjugate gradient technique, the computational delay was lowered by a factor of more than ten, while the total ergodic spectral efficiency was nearly comparable. While the typical Riemannian conjugate gradient method may deliver insufficient latency, the deep neural network technology showed great potential for providing reconfigurable intelligent surfaces in ultra-reliable and low-latency communications.

In this section, five articles related to unsupervised learning are discussed. The important points are summarized in Table 3. The findings show that reducing delays and saving time, energy, and cost are the most important goals of these algorithms.

Table 3. The details of selected articles in the unsupervised learning articles.

Ref/	Year	Evaluation	Keywords	Title	Network/Model/Structure	Achievements
[45]	2019	Implemented	<ul style="list-style-type: none"> Computing methodologies ML Learning settings Semi-supervised learning settings Neural networks 	<ul style="list-style-type: none"> Unsupervised ML for network-centric anomaly detection in IoT 	<ul style="list-style-type: none"> IoT ML 	<ul style="list-style-type: none"> More effective in detecting new and unseen attacks The proposed model is easier
[46]	2020	Simulated	<ul style="list-style-type: none"> Service robots Anomaly detection Time series analysis Mathematical model Real-time systems Robot sensing systems 	<ul style="list-style-type: none"> Unsupervised anomaly detection of industrial robots using a sliding-window convolutional variational autoencoder 	<ul style="list-style-type: none"> CNN IoT 	<ul style="list-style-type: none"> Detecting anomalies in the robot Saving effort and time in collecting fault data
[44]	2022	Implemented	<ul style="list-style-type: none"> Anomaly detection Self-supervised learning Edge computing 	<ul style="list-style-type: none"> Self-supervised learning for time-series anomaly detection in IIoT 	<ul style="list-style-type: none"> IoT Edge computing One-dimensional convolutional neural network 	<ul style="list-style-type: none"> High level of accuracy Improving lightweight method

Table 3. Cont.

Ref/	Year	Evaluation	Keywords	Title	Network/Model/Structure	Achievements
[47]	2022	Implemented	<ul style="list-style-type: none"> Occupational safety management Abnormal stationary detection DL Indoor positioning IoT Digital twin Cold chain logistics 	<ul style="list-style-type: none"> IIoT and unsupervised DL enabled real-time occupational safety monitoring in the cold storage warehouse 	<ul style="list-style-type: none"> IoT DL Unsupervised deep neural structure 	<ul style="list-style-type: none"> Realizing real-time occupational safety monitoring Low energy
[48]	2022	Implemented	<ul style="list-style-type: none"> IIoT Ultra-reliable low latency communication Downlink DL Base stations Wireless sensor networks Smart manufacturing 	<ul style="list-style-type: none"> Unsupervised DL-based reconfigurable intelligent surface-aided broadcasting communications in IIoTs 	<ul style="list-style-type: none"> DL IoT Riemannian conjugate gradient method The deep neural network method 	<ul style="list-style-type: none"> Low latency communications High level of reliability

4.3. Semi-Supervised Learning

With both labeled and unlabeled data, the semi-supervised learning technique investigates how computer programs and natural systems learn. Both the supervised and unsupervised paradigms have traditionally been used to study learning. In the supervised paradigm, all data are labeled. Understanding how the mix of labeled and unlabeled inputs affects learning behavior is the goal of semi-supervised learning, as is creating algorithms that make use of this combination. This form of learning in ML and the role of data mining are intriguing because ML can easily use unlabeled data for better-supervised learning tasks when labeled data are rare or expensive. Additionally, it has promise as a quantitative tool for studying human category learning since most of the inputs are unlabeled. Because semi-supervised learning involves less human effort and provides greater precision, it is of tremendous theoretical and practical relevance [49]. The selected articles related to this section will be analyzed below.

To adopt a CNN on fog-cloud infrastructures for SOD-based applications, Wang et al. [50] presented a semi-supervised adversarial learning technique. A unique concatenated generative adversarial network (GAN) structure with partially shared parameters enabled the SaliencyGAN model. The CNN can select its backbone, based on unique devices and applications. Meanwhile, the authors' training strategy utilized both labeled and unlabeled data from several issue domains. Using a variety of well-known benchmark datasets, they compared state-of-the-art baseline approaches to our SaliencyGAN, trained on 10–100 percent of labeled training data. When the percentage of labeled data reached 30 percent, SaliencyGAN achieved a performance comparable to the supervised baselines and surpassed the weakly supervised and unsupervised baselines. In addition, their ablation analysis revealed that SaliencyGAN was more resistant to the “missing mode” problem

than the other GAN models. The visual representation of the ablation results demonstrated that SaliencyGAN improved its estimation of data distributions.

Hassan et al. [51] suggested adaptive trust boundary protection for the IIoT by means of a deep-learning, feature-extraction-based, semi-supervised technique. The proposed approach does not require any manual effort to update the attack databases and can learn the rapidly changing natures of unknown attack models using unsupervised learning and unlabeled data from the wild. Thus, the suggested technique proved resistant to evolving cyberattacks and their fluid character. The technique was verified using a real IIoT testbed. An empirical analysis of the attack models and findings showed that the recommended technique performs noticeably better in terms of recognizing assaults than conventional security control tactics.

Li, Meng, and Au [52] proposed semi-supervised learning and designed distributed antenna system-collaborative intrusion detection systems by applying disagreement-based semi-supervised learning algorithms for collaborative detection systems. In this study, the performance of distributed antenna system-collaborative intrusion detection systems was evaluated using datasets and real IoT network scenarios to assess detection performance and false alarm reduction. By automatically utilizing unlabeled data, their method was more effective than the typical supervised classifiers at detecting intrusions and lowering false alarms, as determined by the trial results.

De Vita, Bruneo, and Das [53] presented a technique for anomaly detection based on an industrial data collection and monitoring framework. They addressed the dearth of labeled data by developing a semi-supervised anomaly detection algorithm that uses Bayesian Gaussian mixtures to evaluate the plant's operational condition while accounting for uncertainty during the diagnosis process. They then implemented the suggested framework on a scale replica of an assembly plant that served as a real-world IIoT testbed. The experimental results indicated that their anomaly detection system could detect plant functioning conditions with 99.8% accuracy, and the semi-supervised technique outperformed a supervised approach.

Aouedi et al. [54] presented a federated semi-supervised learning system that uses unlabeled and labeled data in a federated manner. On each device, an autoencoder was trained to learn the representative and low-dimensional features. Then, utilizing federated learning, a cloud server combined these models into a global autoencoder. The global encoder was later supplemented with fully connected layers to create a supervised neural network. The resulting model was trained using labeled data that were made available to the public. Their model: (a) guarantees that no local private data is transferred; (b) detects attacks with excellent classification performance; (c) functions even with small amounts of labeled data; (d) has low communication overheads.

In recent years, semi-supervised research has followed the general trends in ML, with a significant focus on neural network-based models and generative learning. Additionally, the literature on the topic has grown in the number of papers and scope, including a broad range of theories, methods, and applications [55]. The results of a review of 5 related papers are shown in Table 4.

4.4. Reinforcement Learning

Reinforcement learning comprises both the science of the adaptive behavior of rational humans in uncertain settings and a computer methodology for discovering optimal behaviors for complex issues in control, optimization, and the adaptive behavior of intelligent entities. The area of reinforcement learning has advanced significantly over the past decade. Reinforcement learning provides both qualitative and quantitative models for comprehending and simulating adaptive decision-making in response to rewards and punishments [56]. Various reinforcement learning studies are reviewed here.

Table 4. The details of selected semi-supervised learning articles.

Ref/	Year	Evaluation	Keywords	Title	Network/ Model/ Structure	Achievements
[50]	2019	Implemented	<ul style="list-style-type: none"> IoT Training Computational modeling DL Data models Gallium nitride Feature extraction 	<ul style="list-style-type: none"> SaliencyGAN: DL semi-supervised salient object detection in the fog of IoT 	<ul style="list-style-type: none"> Fog IoT DL GAN framework 	<ul style="list-style-type: none"> Improving supervised baselines
[51]	2020	Implemented	<ul style="list-style-type: none"> Protocols Informatics IoT Security ML Adaptation models Process control 	<ul style="list-style-type: none"> An adaptive trust boundary protection for IIoT networks using a DL feature-extraction-based semi-supervised model 	<ul style="list-style-type: none"> IoT DL 	<ul style="list-style-type: none"> Improving the identification of attacks over conventional security control techniques High level of flexibility
[52]	2020	Implemented	<ul style="list-style-type: none"> Intrusion detection Semi-supervised learning IoT 	<ul style="list-style-type: none"> Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments 	<ul style="list-style-type: none"> IoT Semi-supervised learning algorithm 	<ul style="list-style-type: none"> Reducing false alarms Improving detecting intrusions
[53]	2021	Implemented	<ul style="list-style-type: none"> Employee welfare Uncertainty Measurement uncertainty Data collection Sensor systems Bayes methods Telemetry 	<ul style="list-style-type: none"> A semi-supervised Bayesian anomaly detection technique for diagnosing faults in IIoT systems 	<ul style="list-style-type: none"> Bayesian Gaussian mixtures IoT 	<ul style="list-style-type: none"> High level of accuracy Improving monitoring performance
[54]	2023	Simulation	<ul style="list-style-type: none"> Data models IIoT Intrusion detection Data privacy Training Radiofrequency Servers 	<ul style="list-style-type: none"> Federated semi-supervised learning for attack detection in IIoT 	<ul style="list-style-type: none"> Cloud server Neural network IoT DL algorithms 	<ul style="list-style-type: none"> Low communication overheads Improving attack detection Improving performance High level of privacy Low cost

Yang et al. [57] presented a DT-enabled IIoT (DTEI) architecture wherein DTs capture the characteristics of industrial equipment for real-time processing and intelligent decision-making. They intended to optimize federated learning, to develop the DTEI model to reduce data transmission overhead and privacy leaks. To address the heterogeneity of IIoT devices, they created the DTEI-assisted deep reinforcement learning approach for selecting IIoT devices in federated learning, particularly for selecting IIoT devices with a high utility rate. In addition, they presented a federated asynchronous learning approach to handle the discrete impacts induced by heterogeneous IIoT devices. Compared to the benchmark, the experimental results demonstrated that the suggested technique provides faster convergence and higher training precision.

Tharewal et al. [58] presented a near-end strategy optimization technique for IIoT intrusion detection, using a deep reinforcement learning algorithm. This technique merged the observation capability of DL with the decision-making capability of reinforcement learning to enable the efficient detection of various types of cyberattacks on the IIoT. When combined with DL algorithms, the DRL-intrusion detection system identified intrusions effectively. Numerous experiments on a publicly accessible data set of the IIoT proved that the proposed intrusion detection system detected 99% of IIoT network attacks. In addition, the rate of accuracy was 0.9%. Based on various models of DL, the intrusion detection system's accuracy, precision, recall rate, and other performance indicators were superior.

In order to address the issue of scalability in deep reinforcement learning algorithms in the context of the transportation domain, Raza et al. [59] suggested a model. The proposed model used a partition-based technique to decrease the complexity of the environment. Their partition-based strategy allowed agents to remain within their working space; this simplified the learning environment and decreased each agent's observations. According to the suggested model, multiple agents in a dynamic environment were trained by means of generative adversarial imitation learning, behavior cloning, and a proximal policy optimization method. They compared the preferred provider organization, the soft actor-critic, and their own model in the context of reward accumulation. The simulation findings demonstrated that their model excels in the symposium on applied computing and preferred provider organization in terms of cumulative incentive accumulation, and the training of many agents was significantly enhanced.

A deep dual-reinforcement learning approach that was based on actor and critic models was suggested by Chang et al. [60]. Dual architectures prevent the network from over-optimizing itself. The actor model continuously acquires the knowledge of recognizing unknown samples through a greedy algorithm. The critic model then dynamically modifies the policy to steer the actor model in the correct training direction. Three bearing datasets were utilized to verify the efficacy of the suggested technique. According to the findings, the recommended strategy enabled agents to identify faults quantitatively and independently. Developing an experience storage unit solved the problem of insufficient samples, preventing the proposed method from being evaluated by trial and error.

Abedin et al. [61] designed an elastic open radio access network (O-RAN) slicing method for the IIoT. First, they formulated the O-RAN slicing problem for real-time industrial monitoring and control. The goal was to lessen the cost of fresh information updates from IIoT devices, working within the restrictions of device power consumption and O-RAN slice isolation. Second, they proposed an intelligent O-RAN framework by means of game theory and ML to reduce the complexity of the problem. In the O-RAN control layer, they suggested a two-sided distributed matching game that captured the IIoT channel characteristics and the IIoT service priorities to generate preference lists for IIoT devices and small-cell base stations (SBS). They used an actor-critic model with a deep deterministic policy gradient (DDPG), which was employed to address the resource allocation problem for optimizing the network slice configuration policy under time-varying requests in the O-RAN service management layer. Additionally, the suggested matching game within the actor-critic model training process enforced long-term policy-based guidance for resource allocation that reflects the trends in customer satisfaction across all IIoT devices and SBSs. Lastly, the simulation findings demonstrated that the suggested method improves performance gains for IIoT services by serving an average of 50% and 43.64% more IIoT devices than the baseline methods.

As the IIoT is a data-centric network, cognitive data processing is required to realize the interconnection between machines. In order to improve the self-monitoring and self-management capabilities of diverse devices, the intelligent development of the IIoT is increasingly reliant on DL-based technologies. Nonetheless, the quantity and quality of data, as well as parameter optimization, severely restrict the features of such methods. Deep reinforcement learning, a breakthrough in AI, give inspiration and direction that combines the benefits of DL and reinforcement learning to build an end-to-end defect diagnosis

system [60]. The results of the 5 reviewed articles are presented in Table 5. The findings showed that improving accuracy and reducing error was one of the most important goals of studies in this department.

Table 5. The important points of the reinforcement learning articles.

Ref/	Year	Evaluation	Keywords	Title	Network/ Model/ Structure	Achievements
[57]	2022	Implemented	<ul style="list-style-type: none"> • IIoT • Training • Data models • Real-time systems • Digital twins • Collaborative work • Task analysis 	<ul style="list-style-type: none"> • Optimizing federated learning with deep reinforcement learning for DT-empowered IIoT 	<ul style="list-style-type: none"> • IoT • DTEI architecture • DL 	<ul style="list-style-type: none"> • Optimizing federated learning • Faster convergence • Higher training accuracy
[58]	2022	Implemented	<ul style="list-style-type: none"> • Intrusion detection system • IIoT • Deep reinforcement learning 	<ul style="list-style-type: none"> • Intrusion detection system for IIoT, based on deep reinforcement learning 	<ul style="list-style-type: none"> • IoT • DL 	<ul style="list-style-type: none"> • High level of accuracy • Detecting 99 percent of different types of IIoT network assaults
[59]	2022	Simulation	<ul style="list-style-type: none"> • Deep reinforcement learning • Multi-agents • Behavior cloning • Dynamic environment • Scalability 	<ul style="list-style-type: none"> • Collaborative multi-agents in dynamic IIoT using deep reinforcement learning 	<ul style="list-style-type: none"> • IoT • Deep reinforcement learning 	<ul style="list-style-type: none"> • High scalability • Reducing complexity
[60]	2022	Implemented	<ul style="list-style-type: none"> • Reinforcement learning • IIoT • Fault diagnosis • Feature extraction • Training • DL • Predictive models 	<ul style="list-style-type: none"> • Intelligent fault quantitative identification for IIoT via a novel deep dual reinforcement learning model, accompanied by insufficient samples 	<ul style="list-style-type: none"> • IoT • DL 	<ul style="list-style-type: none"> • Realizing precise quantitative fault identification • Reducing error
[61]	2022	Simulation	<ul style="list-style-type: none"> • IIoT • Network slicing • Quality of service • Resource management • Monitoring • Energy efficiency • 5G mobile communication 	<ul style="list-style-type: none"> • Elastic O-RAN slicing for industrial monitoring and control: a distributed matching game and deep reinforcement learning approach 	<ul style="list-style-type: none"> • O-RAN • IoT • ML • Actor-critic model 	<ul style="list-style-type: none"> • Low cost • Optimizing the network slice configuration policy under time-varying slicing demand

5. Discussion and Results

A comparative analysis of the management of IoT-based organizational and industrial digitalization using ML methods has been provided in the previous sections. The applied methods included supervised, unsupervised, semi-supervised, and reinforcement learning

approaches. Twenty research articles and five review articles were reviewed in this study, and the results were presented.

The IoT attaches millions of computer devices to each other and has paved the way for future technology in which industrial applications such as smart cities and homes would function with minimal human interaction. The fusion of IoT with emerging technologies such as 5G and blockchain impacts human lives. In order to achieve Industry 4.0, the fast development of the IIoT is accelerating the digitalization of industrial production. An increased reliance on the IoT necessitates attention being paid to its privacy and security issues. Encryption, authentication, access control, and communication security are urgently required to implement security. These requirements can be met most effectively through the application of ML and DL, which facilitate the development of secure intelligent systems [62]. Specifically, ML is the study area dedicated to the formal investigation of learning systems. This highly interdisciplinary field takes and expands upon concepts from statistics, computer science, engineering, cognitive science, optimization theory, and numerous other scientific and mathematical disciplines [63]. Therefore, according to the data, IoT providers wish to host ML in order to obtain greater benefits. In addition, as technology advances, nearly all IIoT applications become more data-driven. Therefore, more modern communication methods are required to conserve energy and efficiently capture vast amounts of data [64]. The most important application areas in which ML and IIoT can contribute are also presented in Figure 7.

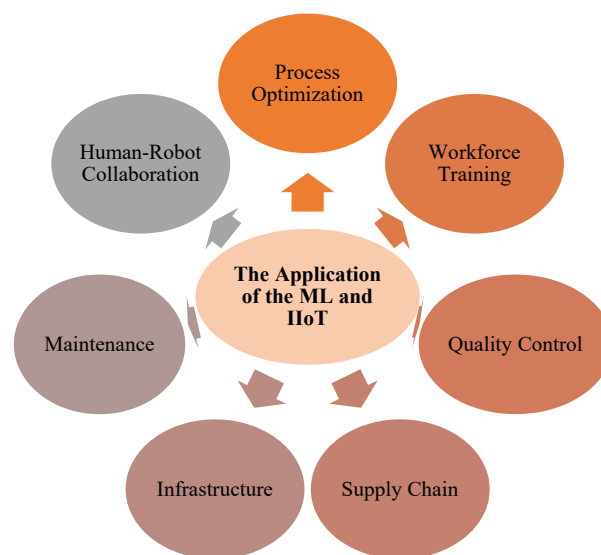


Figure 7. The most important application areas of ML and IIoT.

- **Process Optimization**

The use of factory sensors to monitor process optimization and plant conditions to ensure the factory is running correctly. Besides this, minimizing errors sooner and thereby improving yields and revenues is another area of rapid growth for IIoT [65].

- **Quality control**

Quality control is one area with significant potential in terms of ML benefits. Manufacturers can increase quality inspection at latency, speeds, and prices that are further than the capability of human inspectors because of the usage of smart cameras and the relevant AI-enabled software [66].

- **Maintenance**

The effectiveness of manufacturing lines is significantly influenced by maintenance. Efficient maintenance cuts downtime and can minimize energy use, particularly for equipment that consumes a great deal of power, such as motors, which can waste much energy

when operating improperly. Due to the broad deployment of sensor technologies across plant floors, IIoT provides predictive maintenance by increasing the knowledge of equipment conditions [67]. Additionally, predictive maintenance may be used alone to reduce operating costs and guarantee the vital infrastructure's continuous and uninterrupted functioning [68].

- Workforce training

Companies may promote the development of IIoT knowledge via upskilling their personnel by means of training programs and certifications. Classes on the overall IoT or on particular topics, including IoT security certifications, are available from several institutions, businesses, and charitable groups. Workforce development benefits people's career advancement, productivity, and success while assisting firms in scaling, profiting, and thriving in the long run [69].

- Supply chain

With capabilities to gather, exchange, analyze, and track goods as they move through various businesses and even across international boundaries, the IIoT can greatly broaden the scope of supply-chain monitoring approaches. IoT can potentially reduce counterfeiting, theft, and other crimes by providing real-time information on the location and transit of items [65].

- Human–robot collaboration

Smart manufacturing relies heavily on human–robot collaboration to meet stringent standards for sustainability, human-centricity, and resilience. The advancement of human–robot cooperation is currently focused primarily on a human- or robot-dominant approach, in which human and robotic agents reactively carry out tasks by adhering to pre-established instructions. This approach is a far from compelling fusion of robotic automation and human cognition. These rigid human–robot relationships are unsuitable for complicated production processes and cannot reduce the human operators' physical and mental strain [70].

- Infrastructure

Buildings and intelligent devices may improve the adaptability, dependability, efficiency, and resilience of the civil infrastructure. By enhancing safety, lowering costs, and requiring less labor to maintain and run infrastructure services, these advancements can provide significant economic benefits for industrial users of the intelligent infrastructure [65].

The rest of this section discusses the comparison of the obtained results. The sign (✓) indicates that the study has examined the relevant factor, while the sign (×) indicates that the study has not investigated this relevant factor. Table 6 shows these comparisons.

The results of Table 6 are shown in Figure 8 as a percentage. Figure 8 shows the selected articles' findings, based on the researchers' focus on important parameters. The accuracy is 25%, the cost is 14%, privacy and overheads are 11%, latency, energy, reliability, and error are 7%, and other parameters comprise less than 4% of all parameters. The cost and accuracy attracted more attention, according to the results. There should be more focus on security in the future. Moreover, reducing costs and improving accuracy can be considered the main future goals of industrialization management.

Table 6. The comparisons of the most important factors in the selected papers.

[illegible]

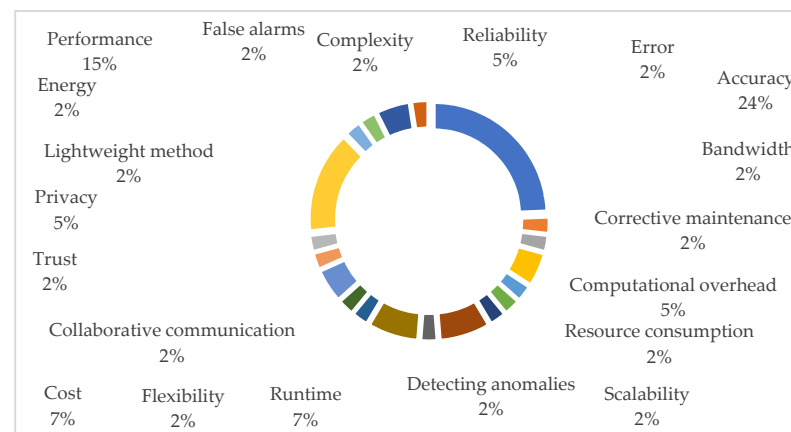


Figure 8. A comparison of the results obtained from reviews of the articles.

6. Challenges and Future Direction

This study on IoT-based organizational and industrial digitalization employing ML techniques for intelligent data analysis and applications raises research questions in the field. Consequently, in this section, we examine and outline the obstacles encountered, as well as future research prospects and initiatives. The most important challenges related to the research topic are presented in Figure 9. Subsequently, we will examine and explain each one.

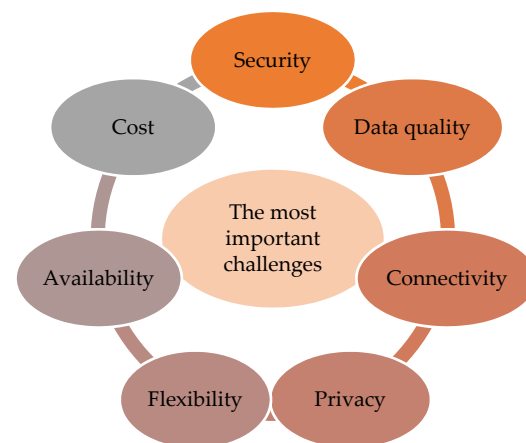


Figure 9. The most important challenges of the IIoT and ML.

- **Cost**

The high investment cost for organizations is one of the first difficulties when integrating IIoT assets. This cost results from implementing IIoT architecture across the sector and all linked devices, which entails maintenance expenses for recruiting employees and monitoring all activities. In order to cut expenses, there is the potential to develop an automated architecture utilizing ML algorithms [71].

- **Security**

Additionally, Industry 4.0 promises higher efficiency and automation and presents new security flaws in critical industrial control systems through unsecured devices and machinery. Industry 4.0-related large-scale complex industrial systems are the focus of extensive research and development, which suggests that reliability and safety concerns present significant hurdles. During online operations, system performance deterioration will result in significant safety risks, in addition to financial losses [72]. Security has emerged as a major issue for Industry 4.0 as a result of the advent of new cyber threats. Industry 4.0 IoT devices generate enormous amounts of data, but accessing labeled data is difficult since

data labeling is expensive and time-consuming; this raises a number of problems for DL techniques that need labeled data. Adopting fresh approaches is important to overcome these difficulties. Networks must adopt a bigger role in stopping attacks before they damage critical infrastructure since host-centric IT security solutions, including anti-virus and software patching, have failed to protect IoT devices from being compromised [45]. It is necessary to upgrade or improve the current preprocessing techniques or to suggest novel data preparation strategies in order to effectively use learning algorithms in the related application field.

The rapid growth of IoT platforms gives numerous crucial answers to the industrial sector. Consequently, the IIoT landscape has moved from static manufacturing processes to dynamic and sustainable manufacturing workflows because of the rapid adoption of the IoT in industrial applications. Unlike the IoT, the IIoT has additional issues, such as a harsh communication environment, changes in network-slice resource consumption, energy consumption, and the need for real-time information updates from IIoT devices throughout industrial production [61]. The increased integration of industrial systems with corporate systems via IIoT networks, for instance, exposes the industrial domain to significant cyber dangers. Conventional IT security is incapable of preventing assaults against IIoT networks due to numerous proprietary layered protocols, restricted upgrade opportunities, heterogeneous communication infrastructures, and a significant trust boundary. For critical reaction-time requirements, current secure protocols, such as the secure distributed network protocol, are restricted to weak hash algorithms [51]. Authentication remains the most critical IoT security measure. To exploit the IoT's diverse applications and services, users must be verified. IoT services and applications typically revolve around data interchange across numerous platforms [31]. Finally, a sustainable IIoT for fulfilling the processes of businesses and industries without negatively impacting the environment, community, or society can be investigated in the near future.

Through the IIoT, it is necessary to have security using the bottom-to-top approach, which means that IIoT applications must adopt a safe booting process, firewalling, access control rules, and device authentication, and must be able to perform security patches and updates. Blockchain can be seen as a security and safety enabler in the IIoT. ML models also have great potential to identify cyber threats and vulnerabilities in IIoT networks. Intrusion detection systems can enhance the network's security by detecting malicious activities. Integrating AI with the IIoT can maintain trust between the different sources and network participants. Once a blockchain-enabled system comes to fruition, IIoT users can monetize their data and crowdsource data to the ML models for IoT services. Publicly available big data repositories that are secured by blockchain technology can improve model training for industrial automation.

- Availability

The absence of readily available and homogeneous data is one of the most significant obstacles to the economically viable application of ML in production. To fully utilize the data, proper data sources, infrastructure, knowledge, and procedures must be used in data collection [73]. A network of interconnected industrial devices known as the IIoT ecosystem exchanges and analyzes the gathered data to provide fresh perspectives on industrial operations. Consequently, this significantly lowers operating costs, eliminates waste, raises quality standards, and boosts the industrial systems' total safety [68].

- Connectivity

To improve the production output, the IIoT must ensure that all industrial machines and gadgets are operational and are linked to one another and to surveillance equipment. As a result, inadequate or subpar connection presents severe issues for IIoT. There may be issues in managing separate IIoT machine units when there is a power outage, an internet outage, or other technical or physical issues [74].

- Data Quality

Although delay-sensitive industrial applications have a long history, there are still numerous obstacles, particularly in the age of IIoT with big data. Using independent manufacturing inspections as an example, handling massive volumes of data in close to real time is required, while tracing any problematic items along the production cycle to enhance product quality. It is well known that surface integration inspection, which uses machine vision and image processing methods, is frequently utilized to find surface flaws for better product quality in manufacturing [75,76]. On the other hand, data collected from IIoT are massive and are derived from multiple sources. On the one hand, massive IIoT datasets bring time and structure complexity; more time-efficient and lightweight future architectures should be designed to handle the voluminous input data and maintain the generation performance. IIoT, when paired with a traditional Internet, enhances the automation of the network by integrating intelligent devices. Most IoT devices are resource-constrained, which creates problems with blockchain-based decentralized architectures. Blockchains can be implemented to store structured and unstructured data over the network. Therefore, they have enough potential to enable interoperability over IoT devices.

- Privacy

In general, ML applications demand a great deal of computing knowledge and resources. IIoT data from manufacturing organizations are typically sent to a cloud system or to a third party with ML capabilities. Decrypted data are required for ML applications to operate effectively. As a result, other parties may be granted access rights to IIoT data that inappropriately depicts the manufacturing process throughout the data processing. IIoT data may have disguised essential elements, causing information leakage for businesses [77]. Due to these issues, companies cannot share their IIoT data with third parties. Users' worries about data privacy are raised by the access to these datasets in the centralized ML algorithms [78]. Hence, it is vital to offer frameworks that safeguard users' privacy in further investigations. Finally, large real-world datasets in IIoT applications are used to generate IIoT data, which unavoidably raises many privacy concerns. Therefore, a privacy protection mechanism should be an indispensable component of privacy preservation, to prevent privacy leakage and maintain the performance of IIoT data generation.

- Flexibility

As there are several IIoT applications, service provisioning to the various IIoT applications according to their demands has been quite challenging. IIoT consumers typically require on-the-move applications that are continuously optimized, personalized, value-added, and autonomous. The best way to design an IIoT solution that expands and helps the organization to integrate different applications is to utilize a flexible architecture that will evolve in the future. The manufacturers or the designers of IoT devices and applications must develop flexibility in their products. Industrial systems must also equip themselves with scalable infrastructures that are ready for expansion. In the future, many devices will be installed that will be mobile and constrained, so any IIoT solution needs to be adaptive and scalable enough to accommodate many devices.

In addition to the above, the IIoT has expanded dramatically during the past few years. While integrating industrial digitalization, automation, and intelligence exposed industries to a multitude of cyber dangers, the complex and diverse IIoT environment presented a new attack surface for network attackers [58]. Therefore, many IoT network difficulties necessitate upgrading the conventional internet infrastructure [79]. In recent years, IoT devices have been fascinating weapons in the arsenals of adversaries attempting to build a large botnet army to launch the most dangerous attack on the Internet, a DDoS strike [80]. A DDoS assault prevents the victim's services from being accessed by genuine Internet users. To achieve this objective, the attacker bombards the target system with many trash packets, causing its processing and storage capacities to become overloaded and eventually resulting in a system crash. The botnet army is the most general approach when conducting attacks on a large scale [81]. The resource limitations of smart items hinder the integration of conventional security solutions, transforming IoT networks into the most enticing target

for an attacker. Most smart things operate in unattended environments, so these gadgets are ideal for constructing botnets [40].

Hundreds of sensor-actuator-enabled devices, including the IIoT, interact and communicate differently with the physical and human worlds due to the Industry 4.0 paradigm. The diagnostics of such systems are essential, due to their complexity. Even though anomaly detection is a valid strategy for preventing unscheduled maintenance and even complete system failure, its application in the IIoT requires the design and implementation of monitoring, data collection, and analysis frameworks. Most existing anomaly detection systems provide a fault diagnosis without taking uncertainty into account. In addition, the absence of ground truth data (a common issue in the industrial context) makes the strategy's implementation considerably more difficult [53].

7. Conclusions and Limitations

This work presents a detailed overview of IoT-based digitalization when utilizing ML for industrialization. According to our objectives, we have reviewed how industrialization might be used to solve a variety of real-world problems. Three research questions were presented, and their answers are given below.

- RQ1: What are the results of an SLR in IIoT-Based digitalization using the ML methods?

Answer to RQ1: The results of an SLR concerning the research topic, according to Figure 3 (which shows the number of articles published in different publications), demonstrated that IEEE publications have the highest number of published articles among other journals. According to Figure 5, which indicates the number of articles published each year, we also found that research related to IIoT-based digitalization using ML methods is increasing daily because the number of published articles has increased every year.

- RQ2: What well-liked algorithms are employed to manage organizational and IIoT-based digitalization using ML methods?

Answer to RQ2: Based on the articles that were obtained in the SLR method and the investigations that were conducted, the results showed that the most popular algorithms for managing organizational and IIoT-based digitalization using ML methods are supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning.

- RQ3: What are the next developments, unresolved problems, and difficulties in using ML methods for organizational and IIoT-based digitalization?

Answer to RQ3: Based on our analysis of the obtained articles and the results in Tables 2–5, the results have been collected in Figure 8. These showed that the most critical challenges in organizational and IIoT-based digitalization using ML methods are security, reproducibility, availability, data quality, governance, and privacy. Security is the most critical challenge, presenting a subject on which many researchers have conducted a great deal of research, and there are still many security-related problems. The investigation revealed that the availability, data quality, and connectivity issues are expected to be resolved within the next three years, and other issues, such as cost, within the next five years. However, other issues, such as security and privacy, may take a little longer.

The results showed that security is the largest obstacle that the IIoT confronts because even the tiniest threat to its architectural components might destroy the entire enterprise. Organizations will not take the risk of using IIoT in their businesses unless a strict security plan is created, due to the higher costs and maintenance needs of fixing security-related IIoT concerns. Prospective security algorithms could assist in overcoming numerous IoT security difficulties and open the path for their application, with new technologies such as 5G, blockchain, edge computing, fog computing, and their uses for constructing intelligent environments. Thus, an ML-based solution's eventual effectiveness depends mainly on the data and the learning algorithms. If the data are unsuitable for learning, such as being unrepresentative, of poor quality, or including irrelevant features, or if there are insufficient data for training, then the ML models may become useless or deliver less accurate results. It

is essential to analyze the data and manage the various learning algorithms for an ML-based solution and, ultimately, for the development of intelligent apps.

From a technical standpoint, we believe that this study on the management of IoT-based organizational and industrial digitalization using ML methods opens up a promising research direction and can be utilized as a reference for future research and applications by academic professionals and industrial decision-makers. The deletion of non-English articles is one of the restrictions of this article. Future academics can thoroughly study this subject by also reviewing non-English papers.

Author Contributions: Conceptualization, A.X., M.D. and S.Y.; methodology, D.J. and A.A.S.; software, A.X., M.D. and D.J.; validation, A.X., M.D., D.J. and A.A.S.; formal analysis, N.J.N. and A.A.S.; investigation, M.D., D.J., N.J.N. and A.A.S.; resources, M.D. and N.J.N.; writing—original draft, A.X. and N.J.N.; writing—review and editing, M.D., D.J., N.J.N. and S.Y.; visualization, A.X., M.D., D.J., N.J.N. and A.A.S.; supervision, A.X., N.J.N. and S.Y.; project administration, N.J.N. and S.Y.; funding acquisition, N.J.N. and N.J.N. All authors have read and agreed to the published version of the manuscript.

Funding: This study is supported via funding from Prince Satam bin Abdulaziz University project number (PSAU/2023/R/1444).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are reported in the paper.

Conflicts of Interest: There is no conflict of interest.

References

1. Syam, N.; Sharma, A. Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. *Ind. Mark. Manag.* **2018**, *69*, 135–146. [CrossRef]
2. Urbach, N.; Röglinger, M. Introduction to digitalization cases: How organizations rethink their business for the digital age. In *Digitalization Cases*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–12.
3. Gruia, L.-A.; Bibu, N.; Nastase, M.; Roja, A.; Cristache, N. Approaches to Digitalization within Organizations. *Rev. Int. Comp. Manag./Rev. De Manag. Comp. Int.* **2020**, *21*, 287–297.
4. Gardas, B.B.; Heidari, A.; Navimipour, N.J.; Unal, M. A fuzzy-based method for objects selection in blockchain-enabled edge-IoT platforms using a hybrid multi-criteria decision-making model. *Appl. Sci.* **2022**, *12*, 8906. [CrossRef]
5. Sharma, A.K.; Singh, P.; Vats, P.; Jain, D. Deep learning and machine intelligence for operational management of strategic planning. In *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*; Springer: Singapore, 2021; pp. 475–485.
6. Mohanta, B.; Nanda, P.; Patnaik, S. Management of VUCA (Volatility, Uncertainty, Complexity and Ambiguity) Using machine learning techniques in industry 4.0 paradigm. In *New Paradigm of Industry 4.0*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–24.
7. Kashyap, P. Industrial applications of machine learning. In *Machine Learning for Decision Makers*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 189–233.
8. van Dinter, R.; Tekinerdogan, B.; Catal, C. Automation of systematic literature reviews: A systematic literature review. *Inf. Softw. Technol.* **2021**, *136*, 106589. [CrossRef]
9. Xiao, Y.; Watson, M. Guidance on conducting a systematic literature review. *J. Plan. Educ. Res.* **2019**, *39*, 93–112. [CrossRef]
10. Cruz-Benito, J. Systematic Literature Review & Mapping. 2016. Available online: https://repositorio.grial.eu/bitstream/grial/685/3/201611_PhD_EKS_SLR-1.pdf (accessed on 1 January 2023).
11. Felizardo, K.R.; Carver, J.C. Automating systematic literature review. In *Contemporary Empirical Methods in Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 327–355.
12. Shahbazi, Z.; Byun, Y.-C. Improving transactional data system based on an edge computing–blockchain–machine learning integrated framework. *Processes* **2021**, *9*, 92. [CrossRef]
13. Attaran, M. The impact of 5G on the evolution of intelligent automation and industry digitization. *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–17. [CrossRef] [PubMed]
14. Bauer, W.; Schlund, S.; Hornung, T.; Schuler, S. Digitalization of industrial value chains—a review and evaluation of existing use cases of Industry 4.0 in Germany. *LogForum* **2018**, *14*, 331–340. [CrossRef]
15. Matt, D.T.; Pedrini, G.; Bonfant, A.; Orzes, G. Industrial digitalization. A systematic literature review and research agenda. *Eur. Manag. J.* **2022**, *41*, 47–78. [CrossRef]

16. Tian, W. Industrial Digitalization in China: Literature Review and Research Prospects. *Acad. J. Bus. Manag.* **2022**, *4*, 34–41.
17. Osipova, N.; Idrisov, R. Review of Organizational and Legal Problems in the Field of Agro-industrial Complex: Public–Private Partnership, Production Digitalization. In *Agriculture Digitalization and Organic Production*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 137–148.
18. Bigliardi, B.; Filippelli, S.; Petroni, A.; Tagliente, L. The digitalization of supply chain: A review. *Procedia Comput. Sci.* **2022**, *200*, 1806–1815. [\[CrossRef\]](#)
19. Tremmel, M.; Gerdtham, U.-G.; Nilsson, P.M.; Saha, S. Economic burden of obesity: A systematic literature review. *Int. J. Environ. Res. Public Health* **2017**, *14*, 435. [\[CrossRef\]](#) [\[PubMed\]](#)
20. Cocchia, A. Smart and digital city: A systematic literature review. In *Smart City*; Springer: Cham, Switzerland, 2014; pp. 13–43.
21. Hussain, M.; Javed, W.; Hakeem, O.; Yousafzai, A.; Younas, A.; Awan, M.J.; Nobanee, H.; Zain, A.M. Blockchain-Based IoT Devices in Supply Chain Management: A Systematic Literature Review. *Sustainability* **2021**, *13*, 13646. [\[CrossRef\]](#)
22. Zhang, G.; Navimipour, N.J. A comprehensive and systematic review of the IoT-based medical management systems: Applications, techniques, trends and open issues. *Sustain. Cities Soc.* **2022**, *82*, 103914. [\[CrossRef\]](#)
23. Fink, A. *Conducting Research Literature Reviews: From the Internet to Paper*; Sage Publications: Newcastle upon Tyne, UK, 2019.
24. Vahdat, S. Clinical profile, outcome and management of kidney disease in COVID-19 patients—A narrative review. *Eur. Rev. Med. Pharmacol. Sci.* **2022**, *26*, 2188–2195. [\[CrossRef\]](#)
25. Doewes, R.I.; Gharibian, G.; Zadeh, F.A.; Zaman, B.A.; Vahdat, S.; Akhavan-Sigari, R. An updated systematic review on the effects of aerobic exercise on human blood lipid profile. *Curr. Probl. Cardiol.* **2022**, *48*, 101108. [\[CrossRef\]](#)
26. Zadeh, F.A.; Bokov, D.O.; Yasin, G.; Vahdat, S.; Abbasalizad-Farhangi, M. Central obesity accelerates leukocyte telomere length (LTL) shortening in apparently healthy adults: A systematic review and meta-analysis. *Crit. Rev. Food Sci. Nutr.* **2021**, 1–10. [\[CrossRef\]](#)
27. Esmailiyan, M.; Amerizadeh, A.; Vahdat, S.; Ghodsi, M.; Doewes, R.I.; Sundram, Y. Effect of different types of aerobic exercise on individuals with and without hypertension: An updated systematic review. *Curr. Probl. Cardiol.* **2021**, *48*, 101034. [\[CrossRef\]](#)
28. Vahdat, S.; Shahidi, S. D-dimer levels in chronic kidney illness: A comprehensive and systematic literature review. *Proc. Natl. Acad. Sci. USA India Sect. B Biol. Sci.* **2020**, *90*, 911–928. [\[CrossRef\]](#)
29. Vahdat, S. The role of IT-based technologies on the management of human resources in the COVID-19 era. *Kybernetes* **2021**, *51*, 2065–2088. [\[CrossRef\]](#)
30. Lakshmana, K.; Subramani, N.; Alotaibi, Y.; Alghamdi, S.; Khalafand, O.I.; Nanda, A.K. Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks. *Sustainability* **2022**, *14*, 7712. [\[CrossRef\]](#)
31. Haldorai, A.; Ramu, A.; Suriya, M. Organization internet of things (IoTs): Supervised, unsupervised, and reinforcement learning. In *Business Intelligence for Enterprise Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 27–53.
32. Zambouri, K.; Razoughi Bastak, M.; Alizadeh, S.M.; Jafari Navimipour, N.; Yalcin, S. A New Energy-Aware Method for Gas Lift Allocation in IoT-Based Industries Using a Chemical Reaction-Based Optimization Algorithm. *Electronics* **2022**, *11*, 3769. [\[CrossRef\]](#)
33. Islam, U.; Muhammad, A.; Mansoor, R.; Hossain, M.S.; Ahmad, I.; Eldin, E.T.; Khan, J.A.; Rehman, A.U.; Shafiq, M. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. *Sustainability* **2022**, *14*, 8374. [\[CrossRef\]](#)
34. Heidari, A.; Jabraeil Jamali, M.A.; Jafari Navimipour, N.; Akbarpour, S. Deep Q-learning technique for offloading offline/online computation in blockchain-enabled green IoT-edge scenarios. *Appl. Sci.* **2022**, *12*, 8232. [\[CrossRef\]](#)
35. Dhanaraj, R.K.; Rajkumar, K.; Hariharan, U. Enterprise IoT modeling: Supervised, unsupervised, and reinforcement learning. In *Business Intelligence for Enterprise Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 55–79.
36. Liu, B. Supervised learning. In *Web Data Mining*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 63–132.
37. Cunningham, P.; Cord, M.; Delany, S.J. Supervised learning. In *Machine Learning Techniques for Multimedia*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 21–49.
38. Rodriguez, D.; Saed, M.A.; Li, C. A WPT/NFC-based sensing approach for beverage freshness detection using supervised machine learning. *IEEE Sens. J.* **2020**, *21*, 733–742. [\[CrossRef\]](#)
39. Gantert, L.; Sammarco, M.; Detyniecki, M.; Campista, M.E.M. A supervised approach for corrective maintenance using spectral features from industrial sounds. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14 June–31 July 2021; pp. 723–728.
40. Gupta, B.; Chaudhary, P.; Chang, X.; Nedjah, N. Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Comput. Electr. Eng.* **2022**, *98*, 107726. [\[CrossRef\]](#)
41. Djenouri, Y.; Belhadi, A.; Srivastava, G.; Lin, J.C.-W. When explainable AI meets IoT applications for supervised learning. *Clust. Comput.* **2022**, 1–11. [\[CrossRef\]](#)
42. Haseeb, K.; Saba, T.; Rehman, A.; Ahmed, Z.; Song, H.H.; Wang, H.H. Trust management with fault-tolerant supervised routing for smart cities using internet of things. *IEEE Internet Things J.* **2022**, *9*, 22608–22617. [\[CrossRef\]](#)
43. Hinton, G.; Sejnowski, T.J. *Unsupervised Learning: Foundations of Neural Computation*; MIT Press: Cambridge, MA, USA, 1999.
44. Tran, D.H.; Nguyen, V.L.; Nguyen, H.; Jang, Y.M. Self-Supervised Learning for Time-Series Anomaly Detection in Industrial Internet of Things. *Electronics* **2022**, *11*, 2146. [\[CrossRef\]](#)

45. Bhatia, R.; Benno, S.; Esteban, J.; Lakshman, T.; Grogan, J. Unsupervised machine learning for network-centric anomaly detection in IoT. In Proceedings of the 3rd Acm Conext Workshop on Big Data, Machine Learning and Artificial Intelligence for Data Communication Networks, Orlando, FL, USA, 9 December 2019; pp. 42–48.
46. Chen, T.; Liu, X.; Xia, B.; Wang, W.; Lai, Y. Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder. *IEEE Access* **2020**, *8*, 47072–47081. [\[CrossRef\]](#)
47. Zhan, X.; Wu, W.; Shen, L.; Liao, W.; Zhao, Z.; Xia, J. Industrial internet of things and unsupervised deep learning enabled real-time occupational safety monitoring in cold storage warehouse. *Saf. Sci.* **2022**, *152*, 105766. [\[CrossRef\]](#)
48. Dinh-Van, S.; Hoang, T.M.; Trestian, R.; Nguyen, H.X. Unsupervised deep learning-based reconfigurable intelligent surface aided broadcasting communications in industrial IoTs. *IEEE Internet Things J.* **2022**, *9*, 19515–19528. [\[CrossRef\]](#)
49. Zhu, X.J. *Semi-Supervised Learning Literature Survey*; University of Wisconsin-Madison Department of Computer Sciences: Madison, WI, USA, 2005.
50. Wang, C.; Dong, S.; Zhao, X.; Papanastasiou, G.; Zhang, H.; Yang, G. SaliencyGAN: Deep learning semisupervised salient object detection in the fog of IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 2667–2676. [\[CrossRef\]](#)
51. Hassan, M.M.; Huda, S.; Sharmeen, S.; Abawajy, J.; Fortino, G. An adaptive trust boundary protection for IIoT networks using deep-learning feature-extraction-based semisupervised model. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2860–2870. [\[CrossRef\]](#)
52. Li, W.; Meng, W.; Au, M.H. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments. *J. Netw. Comput. Appl.* **2020**, *161*, 102631. [\[CrossRef\]](#)
53. De Vita, F.; Bruneo, D.; Das, S.K. A Semi-Supervised Bayesian Anomaly Detection Technique for Diagnosing Faults in Industrial IoT Systems. In Proceedings of the 2021 IEEE International Conference on Smart Computing (SMARTCOMP), Irvine, CA, USA, 23–27 August 2021; pp. 31–38.
54. Aouedi, O.; Piamrat, K.; Muller, G.; Singh, K. Federated Semi-Supervised Learning for Attack Detection in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *19*, 286–295. [\[CrossRef\]](#)
55. Van Engelen, J.E.; Hoos, H.H. A survey on semi-supervised learning. *Mach. Learn.* **2020**, *109*, 373–440. [\[CrossRef\]](#)
56. Dayan, P.; Niv, Y. Reinforcement learning: The good, the bad and the ugly. *Curr. Opin. Neurobiol.* **2008**, *18*, 185–196. [\[CrossRef\]](#)
57. Yang, W.; Xiang, W.; Yang, Y.; Cheng, P. Optimizing federated learning with deep reinforcement learning for digital twin empowered industrial IoT. *IEEE Trans. Ind. Inform.* **2022**, *19*, 1884–1893. [\[CrossRef\]](#)
58. Tharewal, S.; Ashfaq, M.W.; Banu, S.S.; Uma, P.; Hassen, S.M.; Shabaz, M. Intrusion detection system for industrial Internet of Things based on deep reinforcement learning. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9023719. [\[CrossRef\]](#)
59. Raza, A.; Shah, M.A.; Khattak, H.A.; Maple, C.; Al-Turjman, F.; Rauf, H.T. Collaborative multi-agents in dynamic industrial internet of things using deep reinforcement learning. *Environ. Dev. Sustain.* **2022**, *24*, 9481–9499. [\[CrossRef\]](#)
60. Chang, Y.; Chen, J.; Wu, W.; Pan, T.; Zhou, Z.; He, S. Intelligent Fault Quantitative Identification for Industrial Internet of Things (IIoT) via a Novel Deep Dual Reinforcement Learning Model Accompanied with Insufficient Samples. *IEEE Internet Things J.* **2022**, *9*, 19811–19822. [\[CrossRef\]](#)
61. Abedin, S.F.; Mahmood, A.; Tran, N.H.; Han, Z.; Gidlund, M. Elastic O-RAN slicing for industrial monitoring and control: A distributed matching game and deep reinforcement learning approach. *IEEE Trans. Veh. Technol.* **2022**, *71*, 10808–10822. [\[CrossRef\]](#)
62. 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. [\[CrossRef\]](#)
63. Ghahramani, Z. Unsupervised learning. In *Summer School on Machine Learning*; Springer: Berlin/Heidelberg, Germany, 2003.
64. Kherbache, M.; Sobirov, O.; Maimour, M.; Rondeau, E.; Benyahia, A. Reinforcement Learning TDMA-Based MAC Scheduling in the Industrial Internet of Things: A Survey. *IFAC-PapersOnLine* **2022**, *55*, 83–88. [\[CrossRef\]](#)
65. Saptana, C.M.; Susilowati, S.H.; Simchi-Levi, D.; Kaminsky, P. *Designing, and Managing the Supply Chain: Concepts, Strategies and Case Studies*; Sofanudin, A., Budiman, E.K., Eds.; McGraw-Hill: New York, NY, USA, 2017.
66. Gopalakrishnan, S.; Kumaran, M.S. IIoT Framework Based ML Model to Improve Automobile Industry Product. *Intell. Autom. Soft Comput.* **2022**, *31*, 1435–1449. [\[CrossRef\]](#)
67. Bloom, G.; Alsulami, B.; Nwafor, E.; Bertolotti, I.C. Design patterns for the industrial Internet of Things. In Proceedings of the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, Italy, 13–15 June 2018; pp. 1–10.
68. Gardašević, G.; Berbakov, L.; Mastilović, A. Cybersecurity of industrial internet of things. In *Cyber Security of Industrial Control Systems in the Future Internet Environment*; IGI Global: Hershey, PA, USA, 2020; pp. 47–68.
69. Behravan, A.; Bogonikolos, N.; Bohlouli, M.; Cachero, C.; Kaklatzis, P.; Kiamanesh, B.; Luján-Mora, S.; Meliá, S.; Mirhaj, M.; Obermaier, R. Empowering the European Workforce through Virtual Skills Training on Industrial Iot: The Skops Project. In Proceedings of the EDULEARN22 Proceedings, 14th International Conference on Education and New Learning Technologies, Palma, Spain, 4–6 July 2022; pp. 7165–7174.
70. Li, S.; Zheng, P.; Liu, S.; Wang, Z.; Wang, X.V.; Zheng, L.; Wang, L. Proactive human–robot collaboration: Mutual-cognitive, predictable, and self-organising perspectives. *Robot. Comput.-Integr. Manuf.* **2023**, *81*, 102510. [\[CrossRef\]](#)
71. Joudat, B.; Lighvan, M.Z. The Role of Machine Learning in IIoT Through FPGAs. In *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 121–137.
72. Jiang, Y.; Yin, S.; Kaynak, O. Performance supervised plant-wide process monitoring in industry 4.0: A roadmap. *IEEE Open J. Ind. Electron. Soc.* **2020**, *2*, 21–35. [\[CrossRef\]](#)
73. Kletti, J. *Manufacturing Execution Systems—MES*; Springer: Berlin/Heidelberg, Germany, 2007.

74. Park, H.; Kim, H.; Joo, H.; Song, J. Recent advancements in the Internet-of-Things related standards: A oneM2M perspective. *Ict Express* **2016**, *2*, 126–129. [[CrossRef](#)]
75. Wuest, T.; Irgens, C.; Thoben, K.-D. An approach to monitoring quality in manufacturing using supervised machine learning on product state data. *J. Intell. Manuf.* **2014**, *25*, 1167–1180. [[CrossRef](#)]
76. Yang, B.; Cao, X.; Li, X.; Zhang, Q.; Qian, L. Mobile-edge-computing-based hierarchical machine learning tasks distribution for IIoT. *IEEE Internet Things J.* **2019**, *7*, 2169–2180. [[CrossRef](#)]
77. Hindistan, Y.S.; Yetkin, E.F. A Hybrid Approach with GAN and DP for Privacy Preservation of IIoT Data. *IEEE Access* **2023**, *11*, 5837–5849. [[CrossRef](#)]
78. Shojafar, M.; Mukherjee, M.; Piuri, V.; Abawajy, J. Guest editorial: Security and privacy of federated learning solutions for industrial IoT applications. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3519–3521. [[CrossRef](#)]
79. Giotis, K.; Argyropoulos, C.; Androulidakis, G.; Kalogeras, D.; Maglaris, V. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Comput. Netw.* **2014**, *62*, 122–136. [[CrossRef](#)]
80. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [[CrossRef](#)]
81. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [[CrossRef](#)]

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