A Survey of Internet of Things and Cyber-Physical Systems: Standards, Algorithms, Applications, Security, Challenges, and Future Directions

Published in:
Information

Publication Status:
Published online: 08/07/2023

DOI:
10.3390/info14070388

Document Version
Publisher's PDF, also known as Version of record

information

MDPI

Review

A Survey of Internet of Things and Cyber-Physical Systems: Standards, Algorithms, Applications, Security, Challenges, and Future Directions

Kwok Tai Chui [1,*], Brij B. Gupta [2,3,4,5,6,*], Jiaqi Liu [1], Varsha Arya [7,8], Nadia Nedjah [9], Ammar Almomani [6,10] and Priyanka Chaurasia [11]

1 Department of Electronic Engineering and Computer Science, School of Science and Technology, Hong Kong Metropolitan University, Hong Kong, China; s1304012@live.hkmu.edu.hk
2 Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
3 Symbiosis Centre for Information Technology (SCIT), Symbiosis International University, Pune 412115, India
4 Lebanese American University, Beirut 1102, Lebanon
5 Center for Interdisciplinary Research at University of Petroleum and Energy Studies (UPES), Dehradun 248007, India
6 School of Computing, Skyline University College, Sharjah P.O. Box 1797, United Arab Emirates; ammarnav6@bau.edu.jo
7 Department of Business Administration, Asia University, Taichung 41354, Taiwan; 111231027@live.asia.edu.tw
8 UCRD, Chandigarh University, Chandigarh 140413, India
9 Department of Electronics Engineering and Telecommunications, Faculty of Engineering, State University of Rio de Janeiro, R. São Francisco Xavier, 524, Maracanã, Rio de Janeiro 20550-900, Brazil; nadia@eng.uerj.br
10 IT-Department, Al-Huson University College, Al-Balqa Applied University, Al-Salt 19117, Jordan
11 School of Computing, Ulster University, Londonderry BT48 7JL, UK; p.chaurasia@ulster.ac.uk
* Correspondence: jktchui@hkmu.edu.hk (K.T.C.); bbgupta@asia.edu.tw (B.B.G.)

Abstract: The smart city vision has driven the rapid development and advancement of interconnected technologies using the Internet of Things (IoT) and cyber-physical systems (CPS). In this paper, various aspects of IoT and CPS in recent years (from 2013 to May 2023) are surveyed. It first begins with industry standards which ensure cost-effective solutions and interoperability. With ever-growing big data, tremendous undiscovered knowledge can be mined to be transformed into useful applications. Machine learning algorithms are taking the lead to achieve various target applications with formulations such as classification, clustering, regression, prediction, and anomaly detection. Notably, attention has shifted from traditional machine learning algorithms to advanced algorithms, including deep learning, transfer learning, and data generation algorithms, to provide more accurate models. In recent years, there has been an increasing need for advanced security techniques and defense strategies to detect and prevent the IoT and CPS from being attacked. Research challenges and future directions are summarized. We hope that more researchers can conduct more studies on the IoT and on CPS.

Keywords: big data; cyber-physical systems; cybersecurity; data generation; deep learning; internet of things; machine learning; smart city; transfer learning

check for updates

Citation: Chui, K.T.; Gupta, B.B.; Liu, J.; Arya, V.; Nedjah, N.; Almomani, A.; Chaurasia, P. A Survey of Internet of Things and Cyber-Physical Systems: Standards, Algorithms, Applications, Security, Challenges, and Future Directions. *Information* **2023**, *14*, 388. https://doi.org/10.3390/info14070388

Academic Editor: Libing Wu

Received: 29 May 2023
Revised: 3 July 2023
Accepted: 6 July 2023
Published: 8 July 2023

1. Introduction

A cyber-physical system (CPS) is an embedded computing and communication system that combines virtual and physical spaces and connects the digital and physical worlds [1,2]. In today's digital era, the Internet of Things (IoT) is a promising network of physical objects, embedding sensors, devices, servers, and platforms connected to the Internet for data communication, exchange, storage, and analysis [3,4]. Various recent review-type articles have brought attention to the synergy between CPS and IoT, such as in the aspects of Industry 4.0 [5], security [6], artificial intelligence [7], and smart grids [8]. In addition, smart city initiatives [9] and sustainable development goals [10] have driven the development of

CPS and the IoT as key enablers to offer tremendous and useful applications. To study the trends of the CPS and IoT, advanced queries were made on Scopus. Figure 1 summarizes the trends of topics about CPS and the IoT in the past decade (2014 to 16 May 2023, the time of preparation of this paper). Individual CPS and IoT research areas are receiving significant attention. However, fewer studies covered both CPS and IoT. The annual number of publications increased from 913 to 3690 (38.0% yearly growth rate) for CPS, from 2844 to 30,306 (121% annual growth rate) for IoT, and from 71 to 752 (120% annual growth rate) for both CPS and IoT between 2014 and 2022.

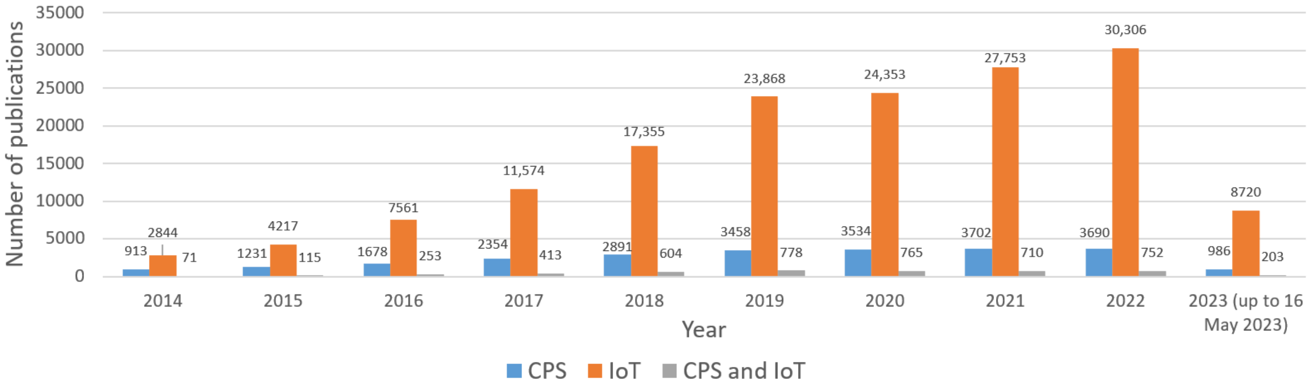

Figure 1. Trends in the number of publications on CPS and IoT.

Table 1 summarizes the scope of recent review-type articles [5–8,11–14] on the research topics of CPS and IoT toward their standards, algorithms, applications, security, challenges, and future directions. In this paper, a comprehensive discussion is presented on all categories. Particularly, more discussion is held on standards and algorithms (traditional and advanced machine learning algorithms). Only research works including both CPS and IoT will be discussed to ensure relevant discussions.

Table 1. Summary of the scope of recent review-type articles.

Work	Standards	Algorithms	Applications	Security	Challenges	Future Directions
[5]	X	X	✓	✓	✓	✓
[6]	X	X	✓	✓	✓	✓
[7]	X	✓	✓	X	✓	✓
[8]	✓	X	✓	✓	✓	✓
[11]	X	X	✓	X	✓	✓
[12]	X	X	✓	✓	✓	✓
[13]	X	X	✓	✓	✓	✓
[14]	X	X	✓	X	✓	✓
Our work	✓	✓	✓	✓	✓	✓

Organization of the Article

Figure 2 presents the structure of this paper and summarizes the number of standards, algorithms, applications, security threats, security tools, and open challenges presented. First, Section 2 introduces 31 standards of CPS and IoT. Traditional machine learning algorithms are briefly discussed, with more efforts devoted to the latest developments of advanced algorithms in Section 3. The following section, Section 4, presents various CPS and IoT applications and summarizes their methodologies and results. Security threats and tools are investigated in Section 5 for safe CPS and IoT environments. The open challenges of these fields are outlined in Section 6. At last, a conclusion is drawn along with future research directions in Section 7.

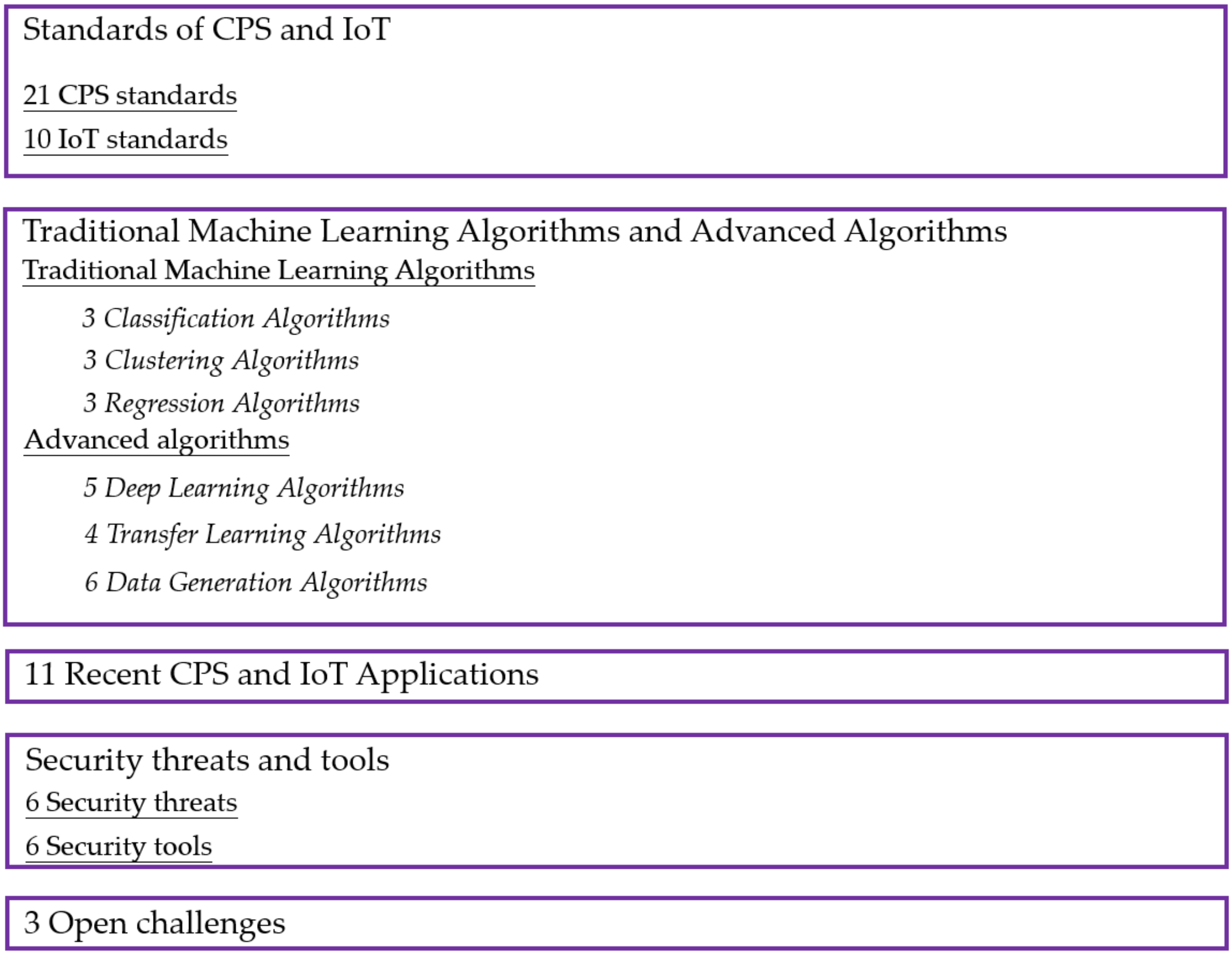

Figure 2. Structure of the article.

2. Standards of CPS and IoT

Twenty-one standards of CPS [15–35] are summarized in Table 2 with their launch years and descriptions. It is noted that some standards have been updated with newer versions to expand their functionality and meet the latest technological requirements. Various organizations, such as the International Electrotechnical Commissions (IEC), PRIME Alliance, the Institute of Electrical and Electronics Engineers (IEEE), the American National Standards Institute (ANSI), the European Union Agency for Cybersecurity (ENISA), the International Society of Automation (ISA), the International Organization for Standardization (ISO), and the Society of Automotive Engineers (SAE), contribute to the establishment of standards for CPS. These standards are widely applied to various applications, such as wide area monitoring control systems, supervisory control and data acquisition, advanced metering infrastructure, smart grids, electric power systems, and protective systems.

Table 2. Typical standards of CPS.

Work	Name of Standard	Launch Year	Descriptions
[15]	IEC 60870-5	1990	A transmission protocol that manages the communication profile for information exchange.
[16]	IEC 60870-6	1992	A standard for data acquisition and control of supervision.
[17]	IEC 60834	1999	A standard for the protection of equipment and command systems. It specifies the maximum latency of the control signal for protective action to be 10 ms.

Table 2. *Cont.*

Work	Name of Standard	Launch Year	Descriptions
[18]	IEC 62056	2002	A standard for supporting advanced metering infrastructure. Typical applications are demand response, tariffs, and automatic meter reading.
[19]	IEC 61850	2003	A standard that specifies the requirement for communication between substations and three-layer architectures (station, bay, and process levels).
[20]	IEC 61970	2005	A standard for managing the interoperability between energy management systems with different environments and interfaces.
[21]	IEC 62351-6	2007	Security support for IEC 61850.
[22]	IEC 61968	2008	A standard that defines the information exchange between applications with different environments and interfaces.
[23]	PRIME	2008	A standard that specifies the interoperability of narrow band powerline communications, mainly adopted in advanced metering infrastructure.
[24]	IEEE 1815	2010	A standard for distributed network protocols that specifies the structure, functionality, and interoperability of devices for electrical systems.
[25]	IEEE 2030	2011	A standard for smart grid interoperability between energy technologies and IT operation with electric power systems.
[26]	IEEE C37.118	2011	A standard for the measurement of the rates of change of frequency and synchrophasors in different environments and situations.
[27]	ANSI C12	2012	A standard for supporting advanced metering infrastructure, with a stronger focus on the application and transportation layers.
[28]	ENISA	2014	A standard for promoting a typical level of information and network security.
[29]	ISA-62443-4-2	2018	Technical requirements for cybersecurity for industrial automation and control systems.
[30]	ISO/IEC 27014	2020	Guidelines for processes of information security.
[31]	IEC TR 60601-4-5	2021	Requirements for the cybersecurity of medical devices and systems.
[32]	IEC 81001-5-1	2021	A standard for the security, effectiveness, and safety of health software and systems.
[33]	IEEE 2418.7	2021	A standard for blockchain use in supply chain management, procedures, and implementations.
[34]	SAE JA7496	2022	A standard for accessing and managing security risks of cyber-physical systems.
[35]	IEEE 2883	2022	A standard for conformance and sanitizing storage.

Additionally, ten standards of IoT [36–45] are summarized in Table 3. The organizations involved include but are not limited to the IEEE, the ANSI, the ISA, the ISO, and the IEC. It can be seen from Tables 2 and 3 that these standards are not designed to bridge between CPS and IoT. However, the standards apply to CPS and IoT systems because interoperability is guaranteed.

Table 3. Crucial IoT standards.

Work	Name of Standard	Launch Year	Descriptions
[36]	IEEE 1451	1999	A standard approach for message security, interoperability, and data sharing in IoT networks. Networks with different communication protocols can be supported.
[37]	ANSI/ISA-95	2005	A standard that provides automation for interfaces in control and IoT systems.
[38]	IEEE P2510	2017	A standard that defines the definitions, parameters, controls, and quality testing methods for IoT data.
[39]	ISO/IEC 20924	2018	A standard that provides definitions and terminologies for IoT systems.

Table 3. *Cont.*

Work	Name of Standard	Launch Year	Descriptions
[40]	ISO/IEC 30141	2018	A standard that defines the best practices, reusable designs, and architectures for IoT systems.
[41]	IEEE P2413	2020	A standard that summarizes descriptions, definitions, and commonalities between IoT domains. It helps promote compatibility and interoperability between IoT systems.
[42]	ISO/IEC 30161-1	2020	A standard that specifies guidelines for IoT data exchange platforms, service communication networks, functionalities, end-point performance, and middleware components.
[43]	ISO/IEC TR 30166	2020	A standard that outlines standardization, functionality, technical aspects, and characteristics for IoT systems.
[44]	ISO/IEC 30162	2022	A standard that covers the best guidance and practices for network connectivity, transportation connectivity, framework connectivity, data management, data interoperability, and interaction between data transmission protocols used in industrial IoT systems.
[45]	ISO/IEC 27400	2022	A guideline on the controls, principles, and risks to privacy and security of IoT systems.

3. Traditional Machine Learning Algorithms and Advanced Algorithms

Success stories of machine learning algorithms in many applications using various formulations, such as classification, clustering, and regression, can be witnessed. In this section, traditional machine learning algorithms are briefly discussed. Attention is drawn to the latest advanced algorithms, which are breakthroughs of advanced applications.

3.1. Traditional Machine Learning Algorithms

3.1.1. Classification Algorithms

Given a dataset comprising some samples, each sample is assigned a class label (single label) or more than one class label (multi-label). Generally, there are two types of formulations: (i) binary classification, which classifies a sample as one of two classes; (ii) multi-class classification, which classifies a sample as one of more than two classes. Classification algorithms usually aim to find decision boundaries or hyperplanes between classes. Mainly, the challenges are that there are many solutions for boundaries or hyperplanes, the generalizability of models, robustness to noise, imbalanced class labels, etc. [46–48]. Examples of typical classification algorithms are neural networks (NNs), support vector machines (SVMs), and decision trees (DTs).

- NNs: Neural networks are computing processes inspired by human brains. They form the foundation of many deep learning algorithms. Each NN comprises an input layer, a hidden layer, and an output layer. The general principle is to assign weights between nodes (representing the connection of neurons). Commonly, negative weights refer to inhibitory connections, whereas positive weights refer to excitatory connections. There are two types of NNs: feed-forward NNs and feed-backward NNs [49]. The former type includes radial basis function networks, multi-layer perceptrons, and single-layer perceptrons. The latter contains arts models, competitive networks, Hopfield networks, Kohonen's self-organizing map, and Bayesian regularized neural networks. The advantages of NNs are their good generalization ability, fault tolerance, non-linear relationships, and good learning ability [50]. The disadvantages are that these models are noise-sensitive, require sufficient training samples, have large computing complexity, and are prone to model overfitting.
- SVMs: Support vector machines map input samples to a feature space of higher dimensions using kernel mapping. A hard-margin formulation is used if the data are linearly separable, whereas a soft-margin formulation is utilized if the data are non-linearly separable. Typical kernel functions for general applications are linear functions, radial basis functions, polynomial functions, sigmoid functions, and Gaussian kernels. To

enhance mapping ability, customized kernels (kernels fulfilling Mercer's Theorem) can be designed for desired applications [51]. The advantages of SVMs are the flexibility of kernel tricks to separate between classes, higher memory efficiency to work in high-dimensional feature spaces, and fewer convex optimization problems [52]. Their disadvantages are that they are vulnerable to noisy environments, unsuitable for large-scale datasets, and have high model complexity with more features.

- DTs: Decision trees are tree-based hierarchical structures. The members of a tree are its leaf nodes, internal nodes, branches, and one root node. The rationale is related to decisions and outcomes, which can be quantified using their utility, resource costs, and event outcomes. Attributed to their ease of interpretation, DTs are widely used in operations management and research for decision-making [53]. Their advantages are their ability to handle missing samples, tackle numerical and categorical samples, and determine representative features [54]. Their disadvantages are that they are prone to overfitting and that their models are sensitive to minor changes in sample distribution and are biased towards outcomes.

3.1.2. Clustering Algorithms

Clustering usually aims to group unlabeled samples into several clusters (groups) via unsupervised clustering. However, a small portion of research is focused on semi-supervised clustering [55] or supervised learning clustering [56]. The major tasks of clustering algorithms are to analyze data statistically and exploratorily. The challenges of clustering algorithms include determining the number of clusters, having no unique solutions, difficulty evaluating the clusters' correctness, and clusters' sensitivity to outliers. Typical clustering algorithms are k-means clustering, mean shift clustering, and affinity propagation clustering.

- k-means clustering: As one of the most classic algorithms, it groups samples into k-clusters. Each sample is assigned to a cluster with the nearest mean. In other words, the algorithm aims to minimize within-cluster variance. Commonly, the k-means clustering algorithm assumes that features are equally important. To choose the value of k, different indexes have been proposed, such as the Calinski–Harabasz (CH), Davies–Bouldin (DB), Silhouette (SH), and Consensus (CI) indices [57]. The advantages of the algorithm include convergence being guaranteed, good adaptation to new samples, and scalability to large-scale datasets [58]. Challenges experienced by the algorithm include the initialization of the centroids and the number of clusters.
- Mean shift clustering: This algorithm is an iterative process for the convergence of the weighted means of kernel densities. Equivalently, the probability density function of the random variables is estimated. Weighting factors are linked with samples. Standard kernels include the generalized Epanechnikov, Cauchy, and Gaussian kernels [59]. Similar to the kernel-based SVM, a customized kernel is a promising solution if the best performance is desired. The advantages of mean shift clustering are its robustness to outliers, its ability to handle any feature space, and no assumptions on the shapes of clusters [60]. Its challenges are performance degradation in high-dimensional feature spaces and difficulty in window size selection.
- Affinity propagation clustering: This algorithm is an iterative process to update two matrices: the availability matrix and the responsibility matrix. The algorithm takes advantage of free initialization of a number of clusters. Messages are sent between samples to group samples with the same exemplar in the cluster. An extended version of the affinity propagation algorithm is multi-exemplar [61]. The termination condition is that either the maximum number of iterations has been reached or the cluster boundary is unchanged. The advantages of the affinity clustering algorithm are its lack of assumptions of initial cluster centroids and a number of clusters and flexible data shapes [62]. Regarding disadvantages, the algorithm requires high computing power for large-scale datasets.

3.1.3. Regression Algorithms

Regression (also called regression analysis) is a common technique in statistical modeling. In recent years, some researchers have linked regression closely to and compared it with machine learning algorithms [63]. The regression formulation aims to determine the relationship between a dependent variable and at least one independent variable. There are various types of regression, such as stepwise, robust, nonparametric, nonlinear, logistic, and linear regressions [64]. Three types of regression algorithms, linear, logistic, and nonparametric regressions, are briefly discussed.

- Linear regression: A linear predictor function is used as a linear regression formulation to model the relationship between a dependent variable and one independent variable. When the problem is extended to multiple linear regression, more than one independent variable is expected. The advantages of regression algorithms include the prediction of continuous variables and quick analysis of the relationships of the variables [65]. However, the algorithms may experience difficulty in highly non-linear formulations between variables, and they are vulnerable to noise and model overfitting.
- Logistic regression: This algorithm aims to model the probability of events, which includes a linear combination of at least one independent variable using the log odds. Attributed to its characteristics, logistic regression can be applied to prediction and classification problems [66]. A recent systematic review revealed that logistic regression and machine learning algorithms perform similarly well when used for prediction in medical research [67]. It can be extended to probabilistic-based or multinomial regression models. The advantages of the logistic regression algorithm are the direction (negative or positive) of association for the predictor and no assumptions of data distribution in the feature space [68]. Nevertheless, it can be applied to variables with a log odds relationship, requiring no or average multicollinearity between independent variables.
- Nonparametric regression: Unlike parametric-based regression algorithms, i.e., linear and logistic regression algorithms, the nonparametric regression algorithm does not assume any relationships between dependent and independent variables. In other words, the predictor is implemented based on the features extracted from the data distribution. The nonparametric regression algorithm takes advantage of the ability to tackle outlying and unexpected samples and is flexible to different data distributions [69]. However, it is challenging to utilize in small-scale datasets. In addition, the issue of tied values leads to the failure of a nonparametric regression algorithm.

3.2. Advanced Algorithms

Traditional machine learning algorithms may not be sufficiently accurate to fulfill the requirements of some applications, particularly mission-critical and zero-fault tolerance applications. The technological advancement of algorithms has driven the utilization of advanced algorithms, including deep learning, transfer learning, and data generation algorithms.

3.2.1. Deep Learning

Generally, deep learning algorithms require sufficient training data and high-performance computing services [70,71]. These algorithms can learn more high-level features to build more accurate models with a tradeoff of increasing model complexity (more hyperparameters and higher dimensionality).

Deep learning extends artificial neural networks and feature learning with at least three layers. Many deep learning algorithms have been proposed, including deep neural networks, convolutional neural networks, deep belief networks, gated recurrent units, and long short-term memory [72–74]. Table 4 compares the advantages and disadvantages of these deep learning algorithms. Although the CNN algorithm has received the most significant adoption, attributable to its superiority in automatic feature extraction to build deep learning models without a complete understanding of domain knowledge, it has several disadvantages that bring up the need for other deep learning algorithms. Different algorithms may be selected for other applications, with no best general applications for algorithm fitting. The uniqueness of different deep learning algorithms leads to vigorous performance evaluation and comparison procedures such that ablation studies, extensive analyses of hyperparameter fine-tuning, and verification of multiple types of deep learning algorithms are often presented in the literature. The general idea for choosing an appropriate algorithm is that it depends on the problem formulation, the size of the dataset, the complexity and performance requirements for the models, and the availability of computing power.

Table 4. Advantages and disadvantages of common deep learning algorithms.

Deep Learning Algorithms	Advantages	Disadvantages
Deep neural networks	Good self-learning ability to extract deep features; can capture non-linear knowledge, particularly from images	Vanishing gradient issue; generally possess higher dimensionality
Convolutional neural networks	Shared biases and weights for hidden neurons; reduce dimensionality without information loss	Variance in images with different orientations and positions; longer training time due to computationally intensive max pooling operations
Deep belief networks	Good for tackling images with different orientations and positions; good for managing unlabeled data for better generalization	Slow convergence rate; becomes stuck in local solutions
Gated recurrent units	Good memory capacity; prevent gradient vanishing issue	No exploration of the importance of elements in sequences; challenging to train the model with long-term sequences
Long short-term memory	Good at handling long-term sequences; prevents gradient vanishing issue	Difficultly supporting online learning; higher risk of model overfitting

3.2.2. Transfer Learning

Regarding the application of deep learning, there are various challenges, including the following: (i) training a deep learning model from scratch is time-consuming, particularly when processing big and high-dimensional data; (ii) large-scale datasets may not be available in many applications due to the small-scale nature of some classes of data and expensive data collection process (as mentioned in Section 3.2.1, deep learning algorithms do not natively perform in small-scale datasets); (iii) insufficient seen data in the model, as any machine learning model is trained with relatively few samples compared to the global data pool.

The general idea of transfer learning is to transfer knowledge from a pre-trained model (usually trained with a large-scale dataset) to a target model (usually trained with a small-scale dataset). There are many variants of transfer learning that bring extensions to the basic idea. Figure 3 summarizes the categories of transfer learning [75,76]. Transfer learning can be divided into four categories:

- Unsupervised learning [77]: In this category, transfer learning is conducted with unlabeled source and target domains. Learning good representation is challenging because the domains need not be similar (i.e., domains can be heterogeneous);
- Transductive learning [78]: This category considers the same task in the source and target domains. The source and target domains can be similar or different. The source domain is labeled data, whereas the target domain is unlabeled data;
- Inductive learning [79]: This category considers different tasks in the source and target domains. Similarity between the source and target domains is not a prerequisite. Labeled data is usually required in the target domain, whereas it is optional in the source domain;

- Cross-modality learning [80]: This is one of the most challenging categories of transfer learning, and it considers source and target domains of different modalities (from text to audio, from text to image, etc.). Knowledge transfer from any pre-trained models to any target models becomes feasible if this can be achieved. However, negative learning exists for any transfer learning category, which lowers the performance of the target model.

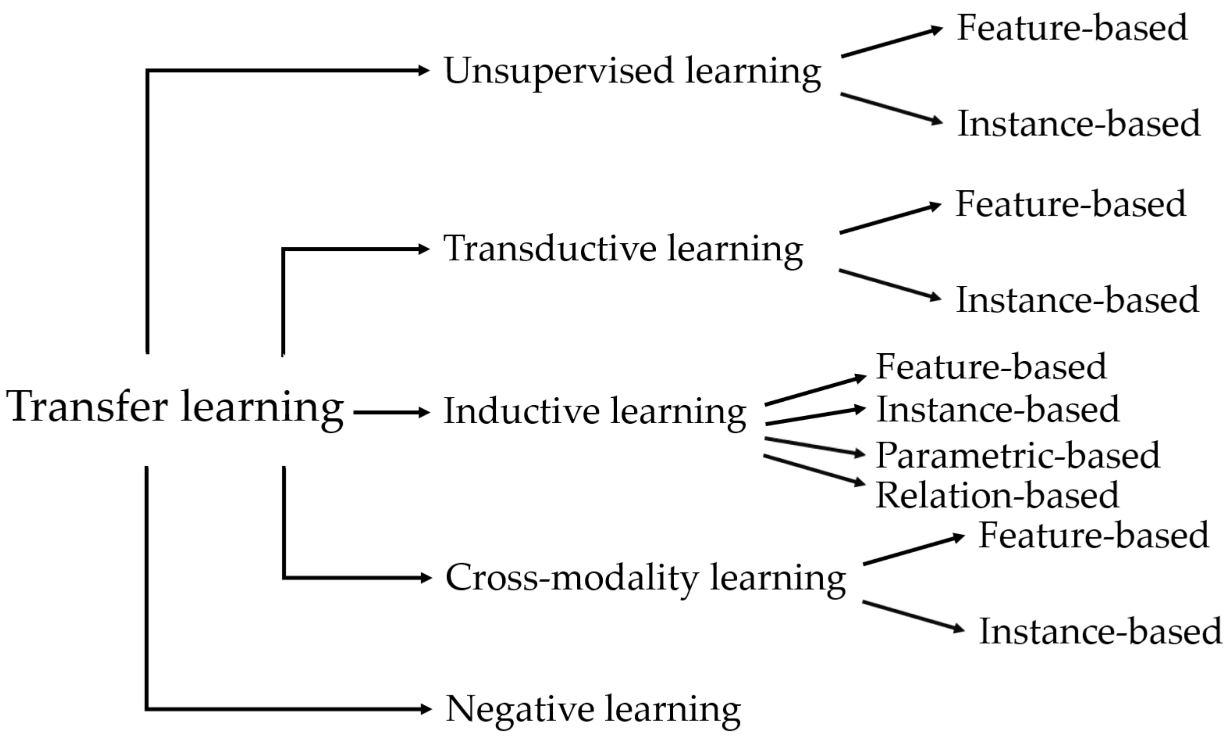

Figure 3. Categories of transfer learning.

The research of transfer learning via multiple source datasets has become an emergent solution to tackle negative transfer by introducing multi-round transfer learning, which slows down the knowledge transfer process [81–83]. In addition, this facilitates the enhancement of model performance with more source datasets (more unseen data from the perspective of the target domain). On the other hand, multi-round transfer learning can be formulated with auxiliary domains [84,85], which serve as intermediate domains between the source and target domains. The intermediate domains are often chosen to reduce the dissimilarity between the source and target domains so that the extent of negative transfer can be reduced.

3.2.3. Data Generation

In the literature, many studies have revealed the contribution of additional training samples toward enhancing the performance of the models. Some studies [86,87] have estimated that synthetic data will overtake ground truth data by 2030. Traditionally, data augmentation is adopted, for example, by resizing, rescaling, and rotating images [88–90]. Moreover, it takes advantage of simple implementation and fast outputs. In recent years, generative artificial intelligence applications, such as chatbots [91,92], variational autoencoders [93,94], and generative adversarial networks (GANs) [95,96], have been proposed to generate valuable data.

Attention has been drawn to the field of GANs, where researchers have proposed many variants, such as the deep convolutional GAN [97], conditional GAN [98], information-maximizing GAN [99], auxiliary classifier GAN [100], bidirectional GAN [101], and loss-sensitive GAN [102]. Table 5 presents the characteristics of these data generation algorithms. Table 6 summarizes recent studies on CPS and IoT applications using these data generation algorithms.

Table 5. Characteristics of common data generation algorithms.

Deep Learning Algorithms	Characteristics
Deep convolutional GAN	Convolutional stride is used instead of max pooling; up-sampling is achieved using transposed convolution; batch normalization is used in all layers except the output layer; the activation function leaky rectified linear unit is introduced.
Conditional GAN	Introduces conditions to the generator and discriminator to control the generated outputs; supports the learning of multi-modal models.
Information-maximizing GAN	Introduces control variables, which are automatically updated to control the generated outputs; the loss function is updated to include mutual information to maximize the information between a small subset of the latent variables.
Auxiliary classifier GAN	The discriminator is assigned to predict the class label instead of using it as an input so that learning is independent of the class label; allows separation of a dataset into subsets to train the generator and discriminator.
Bidirectional GAN	Introduces an encoder to map data to the latent representation; the encoder and generator cannot communicate, but they are designed to invert one another.
Loss-sensitive GAN	The generator learns to generate real samples; the loss function is regularized using the Lipschitz regularity condition.

Table 6. Recent research works on CPS and IoT applications using data generation algorithms.

Works	Applications	Methodologies	Results
[103]	Intrusion detection	Deep convolutional GAN; fuzzy rough set	Accuracies of 95.2–98.6% using two benchmark datasets
[104]	Cyber–physical–social detection system	Deep convolutional GAN; blockchain	Accuracies of 95–100% using the Cifar10 dataset
[105]	Intrusion detection	Conditional GAN; convolutional neural networks	An average accuracy of 74.3%
[106]	Cross-site scripting attacks detection	Conditional GAN; gradient penalty	Recall rates of 96.7–99.0%
[107]	Security analysis	Information-maximizing GAN	Accuracy of 51.9%
[108]	Web traffic estimation	Information-maximizing GAN; long short-term memory	Root-mean-square error of 40.6
[109]	Controller area network bus intrusion detection	Auxiliary classifier GAN; binary real–fake classifier	F1-scores of 97.5–99.8%
[110]	Cyber-attacks and faults detection	Auxiliary classifier GAN; multilayer perceptron	F1-scores of 88.2–99.7% in 45 scenarios
[111]	Network intrusion detection	Bidirectional GAN; encoder–discriminator	Accuracies of 99.1–99.7% using two benchmark datasets
[112]	Network anomaly detection	Bidirectional GAN	F1-scores of 83.5–94.9% using two benchmark datasets
[113]	Automated surface inspection	Loss-sensitive GAN; wavelet fusion	Accuracies of 90.8–95.7%
[114]	Membership inference attacks detection	Loss-sensitive GAN	Accuracies of 50.8–90.8%

It is noted that the GAN family may experience challenges that include (i) difficulty in model training, as the convergence of a GAN is not guaranteed and small sample sizes often exist (as a major reason to generate additional training data); (ii) mode collapse, as GAN is prone to generate a subset of outputs with a narrow variety of samples, and it requires good knowledge of the design of the loss function to produce a good variety of outputs; (iii) computational requirements, as the additional data generation step using GAN increases the need for computing power to build a machine learning model, i.e., the total time taken for data generation, feature extraction, and model construction is lengthy and requires enormous computing power; (iv) overtraining, as the generator achieves high accuracy, but the generated samples deviate to a large extent from the ground truth data distribution.

4. Recent CPS and IoT Applications

Recent research on CPS and IoT applications is discussed here. We have only included studies (including technical articles and excluding review-type articles) focused on both areas. Table 7 summarizes the methodologies and results of the applications [115–127]. To ensure an up-to-date discussion, only works published in 2023 were included in Table 7. In general, existing works have tackled CPS and IoT applications using classification [115,118–124,127], regression [125], and deep learning [118–122,126] approaches. More investigations can be conducted using clustering, transfer learning, and data generation algorithms. Attention is also drawn to the satellite-based IoT systems driven by the development of 5G and 6G networks [128]. Examples of applications are maritime transportation services [129] and remote monitoring and asset tracking in marine environments [130].

Table 7. Recent research on CPS and IoT applications using classification, regression, and deep learning algorithms.

Works	Applications	Methodologies	Results
[115]	Open network connections for real-time packet reception	Soft early demultiplexing with packet classification and lazy cache invalidation; priority inheritance scheme to facilitate the communication process; rate limitation scheme to protect the system from unexpected high traffic	The network traffic load was increased by seven times
[116]	Attack detection and mitigation using a threat modeling framework	Center for threat-informed defense techniques with threat lists and mapped controls	Only theoretical discussions were shared
[117]	An authentication scheme preserving light computational load, privacy, and security	Secured data exchange via GaggleBridge and Gaggle; seven-phase privacy-preserving approach, including server registration and system initialization, application server, client registration, system login, network ID and device verification, system authentication and key agreement, and service-ware verification phases	Reduced the total number of transmission bits by 33–70% and energy consumption by 97–159%
[118]	Network intrusion detection systems	Semi-supervised stacked autoencoder with a threshold selection algorithm	Recall rate of 94.9–100% and precision of 96.1–99.9% using six benchmark datasets
[119]	A prediction system for energy production and consumption	Bidirectional long short-term memory network with an attention mechanism	Root-mean-square error of 0.011 and a mean average error of 0.002
[120]	Anomaly detection for network incursions	Federated deep neural network	True negative rate of 97.9%, true positive rate of 99.7%, and accuracy of 99.7%

Table 7. *Cont.*

Works	Applications	Methodologies	Results
[121]	Network intrusion detection systems	Self-learning ability-basedfeature extraction and an enhanced chicken swarm optimization for the enhancement of recurrent neural networks	Error rate of 8.16%
[122]	Malware detection systems	Snake optimization-based feature extraction approach for the enhancement of graph convolutional network	Precision of 98.7%, recall rate of 98.5%, and F1-score of 98.5%
[123]	Attack path detection systems	Depth-first search algorithm for the identification of all paths between sources and target nodes; Floyd–Warshall algorithm for detection of attack path risk level	Running time of 7–18 ms with varying target nodes of 7–10, and running time of 6–130 ms with varying source nodes of 0–15
[124]	Network intrusion detection systems under the presence of label-flipping poisoning attacks	Ensemble equalization and normalization of Kitsune's core algorithm to self-reproduce data; one-class support vector machine for network anomaly detection	Partial area under the ROC curve of 97.1%
[125]	Blasting parameters and fragmentation prediction model for open pit mines	Evolutionary particle swarm optimization-based support vector regression	Relative errors ranging from 0.76% to 10.82%
[126]	Real-time denoising of IoT data	Noise contrastive estimation; autoencoder and denoising autoencoder	Reduced root-mean-square error from 2.165–4.277 to 0.276–0.542
[127]	Anomaly detection of engines	Three-layer correlation graph; decision tree	Average accuracy of 98.4%

Many studies have considered applications to detect security threats such as network attacks [116], network intrusion [118], anomaly [120,127], network intrusion [121,124], malware [122], and attack paths [123]. More discussion is presented on security threats and common tools in Section 5.

5. Security Threats and Tools

Cybersecurity threats have worsened with the rapid growth of the internet and its usage. The severity of the problem peaked in the recent pandemic because workers were working from home using the internet. A survey (264 respondents) suggested a need for security culture evolution [131].

Here, six common cybersecurity threats are discussed:

- Social engineering: This threat is related to human interaction-based malicious activity; the victims are usually tricked into making security mistakes. The issue is generally described as a social engineering lifecycle [132], which comprises four steps: (i) investigation, in which attackers identify targets, gather information, and select potential attack approaches; (ii) hook, in which attackers interact with the targets, tell a story, and take control of the interaction; (iii) play, in which attackers execute the attack; (iv) exit, in which attackers close the interaction with the victims and remove traces of their attack.
- Third-party exposure: Third-party breaches are usually passive because sensitive and private data are stolen from third-party vendors, or because attackers access the information via the vendors' systems. According to a report, the average loss caused by data breaches was over 8.6 million USD in 2020 [133]. For some companies (e.g., logistics) that outsource their operations to other suppliers, this potentially leads to fourth-party risks [134].
- Configuration mistakes: Users often need to pay more attention to misconfigurations, as they put users at risk of malware. Typical misconfigurations [135] include (i) delayed

software patching, as it is common for users to delay (even skip) updating their systems and servers, and breaches become more accessible via old versions of software; (ii) password reuse, as users may keep using the same password for multiple devices, and the leakage of a password in one device will affect other devices; (iii) default credentials, described as retaining the default usernames and passwords used to set up network devices, including operating systems, routers, and firewalls.

- Poor cyber hygiene: Technology use requires good practices to protect Wi-Fi networks, accounts, etc. Nowadays, two-factor authentication is often used for highly secure applications (e.g., bank transactions). Cyber hygiene is related to the habits of users; education is required to change the mindset and behavior of users [136].
- Cloud vulnerabilities: Cloud storage is taking the lead role for file storage and backup purposes instead of local computing devices. Cloud computing is also a superior tool for providing low-cost and high computing power services. Hackers may get access to and steal cloud data. Worrying about cloud vulnerabilities can be minimized when users follow the user guidelines established by the cloud providers [137]. Cloud infrastructures are designed to provide robust and secure cloud services.
- Mobile vulnerabilities: The vulnerabilities of mobile devices have become essential issues because of the rapid development of mobile applications. Vulnerabilities include code tampering, client code quality, weak authorization, poor authentication, insecure communication, data storage, and improper platform usage. In addition, mobile computing has increased the risk of threats because valuable data is sent and shared with the computing platform [138].

To tackle security threats, automatic detection via machine learning algorithms [116,118,120–124,127] is one promising solution. There are various cybersecurity tools to protect systems from cyber-attacks:

- Network security monitoring tools: Monitoring networks helps examine their downtime and helps to address problems via network optimization schemes. Generally, factors to be monitored are errors, traffic, memory, CPU, and availability [139]. To thoroughly study and analyze network performance, reading the monitoring report is crucial.
- Network defense wireless tools: The ease of use of wireless networks everywhere increases the risk of threats [140]. These tools help obtain secure Wi-Fi connections, detect unauthorized access points, detect reasons for wireless interference, search for areas with poor coverage in wireless local area networks, and reveal SSIDs.
- Web vulnerability scanning tools: These tools help scan for vulnerabilities, test penetration capabilities, test servers, analyze traffic between the server and browsers, discover networks, audit security, and identify open ports [141]. Different web applications are typically tested with threats such as cross-site request forgeries, cross-site scripting, and SQL injections.
- Antivirus software: An antivirus is a three-level computer program that ensures malware prevention, detection, and removal [142]. Being the most famous cybersecurity tool, antivirus software is commonly a built-in software application in operating systems. Users usually uninstall the built-in antivirus software and replace it with other software for more attractive functions.
- Encryption tools: Cryptography protects digital information stored in devices or transmitted over the internet. The best practices of encryption key management are encryption algorithms, key size, centralization, secure storage, automatic generation, access logs, audit logs, backup, life cycle management, third-party integration, and end of keys [143].
- Firewall: Untrusted and trusted networks are separated by a firewall. It is a network security system to monitor and I/O control network traffic. The development of firewalls starts from packet filters to circuit-level gateways to the application layer (the next-generation firewall) [144]. Because of the varying environments of applications, proper and solid configuration of firewalls is required.

6. Open Challenges

Key open challenges are shared in this section, calling for more research and development efforts.

- Many CPS and IoT standards are not yet ready: Standards are official documents that define the guidelines and specifications that enhance the performance of services, methods, products, and/or materials. These also help to achieve replicable results. Generally, dedicated working groups (involving different parties, such as government officials, industry representatives, and consumers) take several years to publish a standard. Tables 2 and 3 share 31 published standards in CPS and IoT. Other CPS and IoT standards are under development. Examples of developing CPS standards include (i) IEEE P1547.3 (interconnection between electric power systems and distributed energy resources); (ii) IEEE P2658 (testing of electric power systems); (iii) IEEE P2808: (function designations of electrical power systems); (iv) IEEE P2968.2 (threat modeling for decentralized clinical trials); (v) IEEE P9274.4.2 (implementation of the Experience Application Programming Interface). Examples of developing IoT standards include (i) IEEE P1912 (security and privacy for wireless devices); (ii) IEEE P2303 (adaptive management of cloud computing); (iii) IEEE P3333.1.1 (visual comfort assessment and quality of experience of 3D content); (iv) IEEE P21451-1-6 (message queue telemetry transport for networked device communication); (v) IEC/IEEE P62704-4 (finite element method for specific absorption rate calculation in the human body from wireless devices). Without the aid of standards, things become highly heterogeneous, which leads to interoperability issues. In reality, it is time-consuming to phase out existing gadgets and migrate to new versions that follow standards. Further resistance to adopting standards is due to the fact that laws may not enforce regulation of the systems and products to follow these standards, which is mainly due to a longer timeframe in law legislation than that of standard publication.
- Open data is not widely available: Open data policies have been receiving resistance from government officials [145], the general public [146], and companies [147]. Typical reasons for opposing open data include the following: (i) new laws to regulate the release and use of open data are difficult to create because there is poor acceptability across different stakeholders; (ii) ensuring data privacy is important because data often contains personal and sensitive information that, if misused or stolen, will lead to threats; (iii) data analysis turns data into valuable information that potentially brings benefits and income (for example, if sufficient samples are shared with a marketing company, it is unclear who should pay for the data because data collection is costly); (iv) collecting and storing ever-growing data is expensive, and as a result, consumer-grade products usually ignore data collection and storage. It is important to recognize that open data plays a crucial role in providing a substantial amount of data to train machine learning models. This is especially true in situations where various small-scale and diverse open datasets must be combined to create the models. Although generational algorithms can create more training data, it is not effective for classes with very few samples. In recent years, an open data working group was established under the United Nations that comprised 12 country representatives (New Zealand, Mauritius, Argentina, Poland, Australia, Suriname, Egypt, Sweden, Italy, the UK, Jordan, and Malaysia), international organizations, and agencies. It is willing to attract and invite representatives to join the working group from the rest of the member states (181) of the United Nations.
- Availability of computing power for model training and data analysis: Analyzing big data and training models using advanced algorithms requires immense computing power. Mobile devices and local computers (embedded with GPUs) are limited in many applications. The availability of edge, fog, and cloud computing offers more computing power with latency tradeoffs between edge, fog, and cloud computing [148]. There is an increasing trend toward subscribing to cloud GPUs, which usually charge based on usage each hour. Therefore, purchasing multiple GPUs for use in local com-

puters is not necessary, which also relieves the local computing bandwidth. However, the bottleneck of the availability of computing power is that the growth rate of data is much higher than that of the processing units' power. Only a limited number of users can rely on the computing services that lead to suitable latency in data analysis and decision-making. An alternative solution is to prioritize resources to more critical applications (i.e., those that can benefit a wider group of people).

7. Conclusions and Future Research Directions

In this paper, we surveyed the standards, algorithms, applications, security, challenges, and future directions for the IoT and CPS. The IoT and CPS have witnessed rapid development and many success stories in recent years. As the IoT becomes a dominant network architecture, it will play a more critical role in CPS development. Future research directions could address three crucial open challenges discussed in Section 6 and adopt advanced algorithms on IoT and CPS applications. In addition, extensive performance evaluations of advanced algorithms and comparisons with traditional machine learning algorithms are required to verify the effectiveness of the advanced algorithms. It is hoped that there will be more research on the IoT and CPS in the near future.

Author Contributions: Formal analysis, K.T.C., B.B.G., J.L., V.A., N.N., A.A. and P.C.; investigation, K.T.C., B.B.G., J.L., V.A., N.N., A.A. and P.C.; visualization, K.T.C. and B.B.G.; writing—original draft, K.T.C., B.B.G., J.L., V.A., N.N., A.A. and P.C.; writing—review and editing, K.T.C., B.B.G., J.L., V.A., N.N., A.A. and P.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Ammi, M.; Adedugbe, O.; Alharby, F.M.; Benkhelifa, E. Taxonomical challenges for cyber incident response threat intelligence: A review. *Int. J. Comput. Appl.* **2022**, *12*, 1–14.
2. Nguyen, G.N.; Le Viet, N.H.; Elhoseny, M.; Shankar, K.; Gupta, B.B.; Abd El-Latif, A.A. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *J. Parallel Distrib. Comput.* **2021**, *153*, 150–160.
3. Gaurav, A.; Psannis, K.; Peraković, D. Security of cloud-based medical internet of things (miots): A survey. *Int. J. Softw. Sci. Comput. Intell.* **2022**, *14*, 1–16.
4. Singh, A.; Gupta, B.B. Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions. *Int. J. Semant. Web Inf. Syst.* **2022**, *18*, 1–43.
5. Pivoto, D.G.; de Almeida, L.F.; da Rosa Righi, R.; Rodrigues, J.J.; Lugli, A.B.; Alberti, A.M. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *J. Manuf. Syst.* **2021**, *58*, 176–192.
6. Franco, J.; Aris, A.; Canberk, B.; Uluagac, A.S. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2351–2383.
7. Sharma, R.; Sharma, T.P.; Sharma, A.K. Detecting and preventing misbehaving intruders in the internet of vehicles. *Int. J. Comput. Appl.* **2022**, *12*, 1–21.
8. Liu, Y.; Yang, X.; Wen, W.; Xia, M. Smarter grid in the 5G Era: A framework integrating power internet of things with a cyber physical system. *Front. Commun. Netw.* **2021**, *2*, 689590.
9. Rani, S.; Kataria, A.; Chauhan, M.; Rattan, P.; Kumar, R.; Sivaraman, A.K. Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: State-of-art work. *Mater. Today Proc.* **2022**, *62*, 4671–4676.
10. Barroso, S.; Bustos, P.; Núñez, P. Towards a cyber-physical system for sustainable and smart building: A use case for optimizing water consumption on a SmartCampus. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 6379–6399.
11. Lesch, V.; Züfle, M.; Bauer, A.; Iffländer, L.; Krupitzer, C.; Kounev, S. A literature review of IoT and CPS—What they are, and what they are not. *J. Syst. Softw.* **2023**, *200*, 111631.
12. Radanliev, P.; De Roure, D.; Nicolescu, R.; Huth, M.; Santos, O. Digital twins: Artificial intelligence and the IoT cyber-physical systems in Industry 4.0. *Int. J. Intell. Robot. Appl.* **2022**, *6*, 171–185.
13. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-li, F.W.; Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2022**, *181*, 274–283.
14. Fatima, I.; Malik, S.U.; Anjum, A.; Ahmad, N. Cyber physical systems and IoT: Architectural practices, interoperability, and transformation. *IT Prof.* **2020**, *22*, 46–54. [CrossRef]

15. Kwon, Y.; Lee, S.; King, R.; Lim, J.I.; Kim, H.K. Behavior analysis and anomaly detection for a digital substation on cyber-physical system. *Electronics* **2019**, *8*, 326. [CrossRef]
16. Gaggero, G.B.; Rossi, M.; Girdinio, P.; Marchese, M. Cybersecurity Issues in Communication-Based Electrical Protections. In Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies, Prague, Czech Republic, 20–22 July 2022.
17. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and research trends in microgrids cybersecurity. *Appl. Sci.* **2021**, *11*, 7363.
18. Hinkel, G. The TTC 2017 Outage System Case for Incremental Model Views. In Proceedings of the 10th Transformation Tool Contest, Marburg, Germany, 21 July 2017.
19. Nweke, L.O.; Weldehawaryat, G.K.; Wolthusen, S.D. Threat modelling of cyber–physical systems using an applied π-calculus. *Int. J. Crit. Infrastruct. Prot.* **2021**, *35*, 100466.
20. Balijepalli, V.M.; Sielker, F.; Karmakar, G. Evolution of power system cim to digital twins-a comprehensive review and analysis. In Proceedings of the 2021 IEEE PES Innovative Smart Grid Technologies Europe, Espoo, Finland, 18–21 October 2021.
21. Esiner, E.; Tefek, U.; Erol, H.S.; Mashima, D.; Chen, B.; Hu, Y.C.; Kalbarczyk, Z.; Nicol, D.M. LoMoS: Less-online/more-offline signatures for extremely time-critical systems. *IEEE Trans. Smart Grid* **2022**, *13*, 3214–3226. [CrossRef]
22. Georg, H.; Müller, S.C.; Rehtanz, C.; Wietfeld, C. Analyzing cyber-physical energy systems: The INSPIRE cosimulation of power and ICT systems using HLA. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2364–2373. [CrossRef]
23. Becejac, T.; Eppinger, C.; Ashok, A.; Agrawal, U.; O'Brien, J. Prime: A real-time cyber-physical systems testbed: From wide-area monitoring, protection, and control prototyping to operator training and beyond. *IET Cyber-Phys. Syst. Theory Appl.* **2020**, *5*, 186–195. [CrossRef]
24. Yoo, H.; Shon, T. Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. *Future Gener. Comput. Syst.* **2016**, *61*, 128–136.
25. Awadid, A. Reference Architectures for Cyber-Physical Systems: Towards a Standard-Based Comparative Framework. In *Advances in Information and Communication, Proceedings of the 2022 Future of Information and Communication Conference, San Francisco, CA, USA, 3–4 March 2022*; Springer International Publishing: Cham, Switzerland, 2022.
26. Chawla, A.; Aftab, M.A.; Hussain, S.S.; Panigrahi, B.K.; Ustun, T.S. Cyber–physical testbed for Wide Area Measurement System employing IEC 61850 and IEEE C37. 118 based communication. *Energy Rep.* **2022**, *8*, 570–578. [CrossRef]
27. Rana, S.; Zhu, H.; Lee, C.W.; Nicol, D.M.; Shin, I. The Not-So-Smart grid: Preliminary work on identifying vulnerabilities in ANSI C12.22. In Proceedings of the 2012 IEEE Globecom Workshops, Anaheim, CA, USA, 3–7 December 2012.
28. Rosado, D.G.; Santos-Olmo, A.; Sánchez, L.E.; Serrano, M.A.; Blanco, C.; Mouratidis, H.; Fernández-Medina, E. Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Comput. Ind.* **2022**, *142*, 103715.
29. Weiss, J.; Hood, M.; Miller, N.; Potorieko, C.; Michael, J.B. Using Machine Learning to Work Around the Operational and Cybersecurity Limitations of Legacy Process Sensors. *Computer* **2022**, *55*, 106–111. [CrossRef]
30. Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics* **2022**, *11*, 2181.
31. Arandia, N.; Garate, J.I.; Mabe, J. Embedded Sensor Systems in Medical Devices: Requisites and Challenges Ahead. *Sensors* **2022**, *22*, 9917. [PubMed]
32. Puder, A.; Henle, J.; Sax, E. Threat Assessment and Risk Analysis (TARA) for Interoperable Medical Devices in the Operating Room Inspired by the Automotive Industry. *Healthcare* **2023**, *11*, 872.
33. Chen, X.; Zhang, Q.; Zhang, L.; Jia, X.; Zheng, P.; Yang, X. Standardization of Financial Blockchain: Technologies, Challenges, and Future. In Proceedings of the 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud, Xi'an, China, 25–27 June 2022.
34. David, A. *Unsettled Topics Concerning Airport Cybersecurity Standards and Regulation*; No. EPR2021020; SAE Technical Paper: Warrendale, PA, USA, 2021.
35. Hands, J.; Coughlin, T. New IEEE Media Sanitization Specification Enables Circular Economy for Storage. *Computer* **2023**, *56*, 111–116.
36. Da Rocha, H.; Abrishambaf, R.; Pereira, J.; Espirito Santo, A. Integrating the IEEE 1451 and IEC 61499 standards with the industrial internet reference architecture. *Sensors* **2022**, *22*, 1495. [CrossRef]
37. Rajendran, T.; Surya, S.; Babu, N. Big Data Analytics in Industrial IoT and Cybertwin. In *New Approaches to Data Analytics and Internet of Things Through Digital Twin*; IGI Global: Hershey, PA, USA, 2023; pp. 191–210.
38. Khalil, R.A.; Saeed, N.; Babar, M.I.; Jan, T. Toward the internet of underwater things: Recent developments and future challenges. *IEEE Consum. Electron. Mag.* **2020**, *10*, 32–37. [CrossRef]
39. Karale, A. The challenges of IoT addressing security, ethics, privacy, and laws. *Internet Things* **2021**, *15*, 100420.
40. Lee, C.; Kim, N.; Hong, S. Toward industrial IoT: Integrated architecture of an OPC UA synergy platform. *IEEE Access* **2021**, *9*, 164720–164731. [CrossRef]
41. Mukhopadhyay, S.C.; Tyagi, S.K.S.; Suryadevara, N.K.; Piuri, V.; Scotti, F.; Zeadally, S. Artificial intelligence-based sensors for next generation IoT applications: A review. *IEEE Sens. J.* **2021**, *21*, 24920–24932.
42. Shang, K.; McDonald, S.; Buticchi, G.; Brusic, V. The development of ethically informed standards for intelligent monitoring systems of electric machines. In Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference, Los Alamitos, CA, USA, 27 June–1 July 2022.

43. Sousa, J.; Mendonça, J.P.; Machado, J. A generic interface and a framework designed for industrial metrology integration for the Internet of Things. *Comput. Ind.* **2022**, *138*, 103632.
44. Zachila, K.; Kotis, K.; Paparidis, E.; Ladikou, S.; Spiliotopoulos, D. Facilitating Semantic Interoperability of Trustworthy IoT Entities in Cultural Spaces: The Smart Museum Ontology. *IoT* **2021**, *2*, 741–760. [CrossRef]
45. Liu, D.; Wu, C.; Yang, L.; Zhao, X.; Sun, Q. The Development of Privacy Protection Standards for Smart Home. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9641143.
46. Abramovich, F.; Pensky, M. Classification with many classes: Challenges and pluses. *J. Multivar. Anal.* **2019**, *174*, 104536. [CrossRef]
47. Gibert, D.; Mateu, C.; Planes, J. The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *J. Netw. Comput. Appl.* **2020**, *153*, 102526.
48. Mukhamediev, R.I.; Popova, Y.; Kuchin, Y.; Zaitseva, E.; Kalimoldayev, A.; Symagulov, A.; Levashenko, V.; Abdoldina, F.; Gopejenko, V.; Yakunin, K.; et al. Review of Artificial Intelligence and Machine Learning Technologies: Classification, Restrictions, Opportunities and Challenges. *Mathematics* **2022**, *10*, 2552.
49. Abiodun, O.I.; Jantan, A.; Omolara, A.E.; Dada, K.V.; Mohamed, N.A.; Arshad, H. State-of-the-art in artificial neural network applications: A survey. *Heliyon* **2018**, *4*, e00938.
50. Peng, J.; Yang, B.; Gupta, B.B.; Abd El-Latif, A.A. A biometric cryptosystem scheme based on random projection and neural network. *Soft Comput.* **2021**, *25*, 7657–7670.
51. Chui, K.T.; Gupta, B.B.; Torres-Ruiz, M.; Arya, V.; Alhalabi, W.; Zamzami, I.F. A Convolutional Neural Network-Based Feature Extraction and Weighted Twin Support Vector Machine Algorithm for Context-Aware Human Activity Recognition. *Electronics* **2023**, *12*, 1915.
52. Srivastava, D.; Chui, K.T.; Arya, V.; Peñalvo, F.J.G.; Kumar, P.; Singh, A.K. Analysis of Protein Structure for Drug Repurposing Using Computational Intelligence and ML Algorithm. *Int. J. Softw. Sci. Comput. Intell.* **2022**, *14*, 1–11. [CrossRef]
53. Chou, Y.C.; Chuang, H.H.C.; Chou, P.; Oliva, R. Supervised machine learning for theory building and testing: Opportunities in operations management. *J. Oper. Manag.* **2023**, *2023*, 643–675.
54. Almomani, A.; Alauthman, M.; Shatnawi, M.T.; Alweshah, M.; Alrosan, A.; Alomoush, W.; Gupta, B.B. Phishing website detection with semantic features based on machine learning classifiers: A comparative study. *Int. J. Semant. Web Inf. Syst.* **2022**, *18*, 1–24.
55. Cai, J.; Hao, J.; Yang, H.; Zhao, X.; Yang, Y. A review on semi-supervised clustering. *Inf. Sci.* **2023**, *632*, 164–200.
56. Chui, K.T. Driver stress recognition for smart transportation: Applying multiobjective genetic algorithm for improving fuzzy c-means clustering with reduced time and model complexity. *Sustain. Comput. Inform. Syst.* **2022**, *35*, 100668.
57. Chui, K.T.; Tsang, K.F.; Chung, S.H.; Yeung, L.F. Appliance signature identification solution using K-means clustering. In Proceedings of the IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society, Vienna, Austria, 10–13 November 2013.
58. Ikotun, A.M.; Ezugwu, A.E.; Abualigah, L.; Abuhaija, B.; Heming, J. K-means Clustering Algorithms: A Comprehensive Review, Variants Analysis, and Advances in the Era of Big Data. *Inf. Sci.* **2023**, *622*, 178–210.
59. Beck, G.; Duong, T.; Lebbah, M.; Azzag, H.; Cérin, C. A distributed approximate nearest neighbors algorithm for efficient large scale mean shift clustering. *J. Parallel Distrib. Comput.* **2019**, *134*, 128–139.
60. Ranjbarzadeh, R.; Saadi, S.B. Automated liver and tumor segmentation based on concave and convex points using fuzzy c-means and mean shift clustering. *Measurement* **2020**, *150*, 107086.
61. Wang, C.D.; Lai, J.H.; Suen, C.Y.; Zhu, J.Y. Multi-exemplar affinity propagation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2013**, *35*, 2223–2237. [CrossRef] [PubMed]
62. Rahman, M.R.; Arefin, M.S.; Rahman, S.; Ahmed, A.; Islam, T.; Dhar, P.K.; Kwon, O.J. A Comprehensive Survey on Affinity Analysis, Bibliomining, and Technology Mining: Past, Present, and Future Research. *Appl. Sci.* **2022**, *12*, 5227. [CrossRef]
63. Pentoś, K.; Mbah, J.T.; Pieczarka, K.; Niedbała, G.; Wojciechowski, T. Evaluation of multiple linear regression and machine learning approaches to predict soil compaction and shear stress based on electrical parameters. *Appl. Sci.* **2022**, *12*, 8791. [CrossRef]
64. Zuur, A.F.; Ieno, E.N. A protocol for conducting and presenting results of regression-type analyses. *Methods Ecol. Evol.* **2016**, *7*, 636–645. [CrossRef]
65. Fernández-Delgado, M.; Sirsat, M.S.; Cernadas, E.; Alawadi, S.; Barro, S.; Febrero-Bande, M. An extensive experimental survey of regression methods. *Neural Netw.* **2019**, *111*, 11–34. [CrossRef] [PubMed]
66. Zhou, Y.; Song, L.; Liu, Y.; Vijayakumar, P.; Gupta, B.B.; Alhalabi, W.; Alsharif, H. A privacy-preserving logistic regression-based diagnosis scheme for digital healthcare. *Future Gener. Comput. Syst.* **2023**, *144*, 63–73. [CrossRef]
67. Christodoulou, E.; Ma, J.; Collins, G.S.; Steyerberg, E.W.; Verbakel, J.Y.; Van Calster, B. A systematic review shows no performance benefit of machine learning over logistic regression for clinical prediction models. *J. Clin. Epidemiol.* **2019**, *110*, 12–22.
68. Shipe, M.E.; Deppen, S.A.; Farjah, F.; Grogan, E.L. Developing prediction models for clinical use using logistic regression: An overview. *J. Thorac. Dis.* **2019**, *11*, S574. [CrossRef]
69. Čížek, P.; Sadıkoğlu, S. Robust nonparametric regression: A review. *Wiley Interdiscip. Rev. Comput. Stat.* **2020**, *12*, e1492. [CrossRef]
70. Abrol, A.; Fu, Z.; Salman, M.; Silva, R.; Du, Y.; Plis, S.; Calhoun, V. Deep learning encodes robust discriminative neuroimaging representations to outperform standard machine learning. *Nat. Commun.* **2021**, *12*, 353. [CrossRef]
71. Janiesch, C.; Zschech, P.; Heinrich, K. Machine learning and deep learning. *Electron. Mark.* **2021**, *31*, 685–695. [CrossRef]

72. Lakshmanna, K.; Kaluri, R.; Gundluru, N.; Alzamil, Z.S.; Rajput, D.S.; Khan, A.A.; Haq, M.A.; Alhussen, A. A review on deep learning techniques for IoT data. *Electronics* **2022**, *11*, 1604. [CrossRef]
73. Dubey, S.R.; Singh, S.K.; Chaudhuri, B.B. Activation functions in deep learning: A comprehensive survey and benchmark. *Neurocomputing* **2022**, *503*, 92–108.
74. Zhang, Q.; Guo, Z.; Zhu, Y.; Vijayakumar, P.; Castiglione, A.; Gupta, B.B. A deep learning-based fast fake news detection model for cyber-physical social services. *Pattern Recognit. Lett.* **2023**, *168*, 31–38. [CrossRef]
75. Niu, S.; Liu, Y.; Wang, J.; Song, H. A decade survey of transfer learning (2010–2020). *IEEE Trans. Artif. Intell.* **2020**, *1*, 151–166.
76. Yao, S.; Kang, Q.; Zhou, M.; Rawa, M.J.; Abusorrah, A. A survey of transfer learning for machinery diagnostics and prognostics. *Artif. Intell. Rev.* **2023**, *56*, 2871–2922. [CrossRef]
77. Zhao, Z.; Zhang, Q.; Yu, X.; Sun, C.; Wang, S.; Yan, R.; Chen, X. Applications of unsupervised deep transfer learning to intelligent fault diagnosis: A survey and comparative study. *IEEE Trans. Instrum. Meas.* **2021**, *70*, 1–28. [CrossRef]
78. Luo, Y.; Zhang, Z.; Zhang, L.; Han, J.; Cao, J.; Zhang, J. Developing High-Resolution Crop Maps for Major Crops in the European Union Based on Transductive Transfer Learning and Limited Ground Data. *Remote Sens.* **2022**, *14*, 1809. [CrossRef]
79. Zhang, Y.; Xia, K.; Jiang, Y.; Qian, P.; Cai, W.; Qiu, C.; Wee, L.K.; Wu, D. Multi-modality fusion & inductive knowledge transfer underlying non-sparse multi-kernel learning and distribution adaption. *IEEE ACM Trans. Comput. Biol. Bioinform.* **2022**. [CrossRef]
80. Song, Y.; Li, J.; Gao, P.; Li, L.; Tian, T.; Tian, J. Two-stage cross-modality transfer learning method for military-civilian SAR ship recognition. *IEEE Geosci. Remote Sens. Lett.* **2022**, *19*, 1–5. [CrossRef]
81. Liu, X.; Li, Y.; Chen, L.; Chen, G.; Zhao, B. Multiple source partial knowledge transfer for manufacturing system modelling. *Robot. Comput. Integr. Manuf.* **2023**, *80*, 102468. [CrossRef]
82. Chui, K.T.; Gupta, B.B.; Jhaveri, R.H.; Chi, H.R.; Arya, V.; Almomani, A.; Nauman, A. Multiround transfer learning and modified generative adversarial network for lung cancer detection. *Int. J. Intell. Syst.* **2023**, *2023*, 6376275. [CrossRef]
83. Kang, Z.; Nielsen, M.; Yang, B.; Ghazi, M.M. Partial feedback online transfer learning with multi-source domains. *Inf. Fus.* **2023**, *89*, 29–40. [CrossRef]
84. Li, C.; Li, S.; Wang, H.; Gu, F.; Ball, A.D. Attention-based deep meta-transfer learning for few-shot fine-grained fault diagnosis. *Knowl.-Based Syst.* **2023**, *264*, 110345. [CrossRef]
85. Qian, Q.; Zhou, J.; Qin, Y. Relationship Transfer Domain Generalization Network for Rotating Machinery Fault Diagnosis Under Different Working Conditions. *IEEE Trans. Ind. Inform.* **2023**. [CrossRef]
86. Arora, A.; Arora, A. Synthetic patient data in health care: A widening legal loophole. *Lancet* **2022**, *399*, 1601–1602. [CrossRef]
87. Matuzevičius, D. Synthetic Data Generation for the Development of 2D Gel Electrophoresis Protein Spot Models. *Appl. Sci.* **2022**, *12*, 4393. [CrossRef]
88. Shorten, C.; Khoshgoftaar, T.M. A survey on image data augmentation for deep learning. *J. Big Data* **2019**, *6*, 1–48. [CrossRef]
89. Chlap, P.; Min, H.; Vandenberg, N.; Dowling, J.; Holloway, L.; Haworth, A. A review of medical image data augmentation techniques for deep learning applications. *J. Med. Imaging Radiat. Oncol.* **2021**, *65*, 545–563. [CrossRef]
90. Xu, M.; Yoon, S.; Fuentes, A.; Park, D.S. A comprehensive survey of image augmentation techniques for deep learning. *Pattern Recognit.* **2023**, *137*, 109347.
91. Kuhail, M.A.; Alturki, N.; Alramlawi, S.; Alhejori, K. Interacting with educational chatbots: A systematic review. *Educ. Inf. Technol.* **2023**, *28*, 973–1018. [CrossRef]
92. Lin, C.C.; Huang, A.Y.; Yang, S.J. A review of ai-driven conversational chatbots implementation methodologies and challenges (1999–2022). *Sustainability* **2023**, *15*, 4012. [CrossRef]
93. Singh, A.; Ogunfunmi, T. An overview of variational autoencoders for source separation, finance, and bio-signal applications. *Entropy* **2022**, *24*, 55. [CrossRef] [PubMed]
94. Figueira, A.; Vaz, B. Survey on synthetic data generation, evaluation methods and GANs. *Mathematics* **2022**, *10*, 2733. [CrossRef]
95. Brophy, E.; Wang, Z.; She, Q.; Ward, T. Generative adversarial networks in time series: A systematic literature review. *ACM Comput. Surv.* **2023**, *55*, 1–31. [CrossRef]
96. AlAmir, M.; AlGhamdi, M. The Role of generative adversarial network in medical image analysis: An in-depth survey. *ACM Comput. Surv.* **2022**, *55*, 1–36. [CrossRef]
97. Suárez, P.L.; Sappa, A.D.; Vintimilla, B.X. Infrared image colorization based on a triplet dcgan architecture. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Honolulu, HI, USA, 21–26 July 2017.
98. Mirza, M.; Osindero, S. Conditional generative adversarial nets. *arXiv* **2014**, arXiv:1411.1784.
99. Chen, X.; Duan, Y.; Houthooft, R.; Schulman, J.; Sutskever, I.; Abbeel, P. Infogan: Interpretable representation learning by information maximizing generative adversarial nets. In Proceedings of the Annual Conference on Neural Information Processing Systems 2016, Barcelona, Spain, 5–10 December 2016.
100. Odena, A.; Olah, C.; Shlens, J. Conditional image synthesis with auxiliary classifier gans. In Proceedings of the International Conference on Machine Learning, Sydney, Australia, 6–11 August 2017.
101. Donahue, J.; Krähenbühl, P.; Darrell, T. Adversarial feature learning. *arXiv* **2016**, arXiv:1605.09782.
102. Qi, G.J. Loss-sensitive generative adversarial networks on lipschitz densities. *Int. J. Comput. Vis.* **2020**, *128*, 1118–1140. [CrossRef]
103. Wu, Y.; Nie, L.; Wang, S.; Ning, Z.; Li, S. Intelligent intrusion detection for internet of things security: A deep convolutional generative adversarial network-enabled approach. *IEEE Int. Things J.* **2023**, *10*, 3094–3106. [CrossRef]

104. Feng, J.; Yang, L.T.; Zhu, Y.; Gati, N.J.; Mo, Y. Blockchain-enabled tensor-based conditional deep convolutional GAN for Cyber-physical-Social systems. *ACM Trans. Internet Technol.* **2021**, *21*, 1–17. [CrossRef]
105. Le, K.H.; Nguyen, M.H.; Tran, T.D.; Tran, N.D. IMIDS: An intelligent intrusion detection system against cyber threats in IoT. *Electronics* **2022**, *11*, 524. [CrossRef]
106. Mokbal, F.M.M.; Wang, D.; Wang, X.; Fu, L. Data augmentation-based conditional Wasserstein generative adversarial network-gradient penalty for XSS attack detection system. *PeerJ Comput. Sci.* **2020**, *6*, e328. [CrossRef]
107. Cheng, K.; Tahir, R.; Eric, L.K.; Li, M. An analysis of generative adversarial networks and variants for image synthesis on MNIST dataset. *Multimed. Tools Appl.* **2020**, *79*, 13725–13752. [CrossRef]
108. Zhou, K.; Wang, W.; Huang, L.; Liu, B. Comparative study on the time series forecasting of web traffic based on statistical model and Generative Adversarial model. *Knowl.-Based Syst.* **2021**, *213*, 106467. [CrossRef]
109. Zhao, Q.; Chen, M.; Gu, Z.; Luan, S.; Zeng, H.; Chakrabory, S. CAN bus intrusion detection based on auxiliary classifier GAN and out-of-distribution detection. *ACM Trans. Embed. Comput. Syst.* **2022**, *21*, 1–30. [CrossRef]
110. Farajzadeh-Zanjani, M.; Hallaji, E.; Razavi-Far, R.; Saif, M. Generative-adversarial class-imbalance learning for classifying cyber-attacks and faults-a cyber-physical power system. *IEEE Trans. Dependable Secure Comput.* **2022**, *19*, 4068–4081. [CrossRef]
111. Xu, W.; Jang-Jaccard, J.; Liu, T.; Sabrina, F.; Kwak, J. Improved Bidirectional GAN-Based Approach for Network Intrusion Detection Using One-Class Classifier. *Computers* **2022**, *11*, 85. [CrossRef]
112. Liao, J.; Teo, S.G.; Kundu, P.P.; Truong-Huu, T. ENAD: An ensemble framework for unsupervised network anomaly detection. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, Rhodes, Greece, 26–28 July 2021.
113. Liu, L.; Cao, D.; Wu, Y.; Wei, T. Defective samples simulation through adversarial training for automatic surface inspection. *Neurocomputing* **2019**, *360*, 230–245. [CrossRef]
114. Chen, J.; Wang, W.H.; Gao, H.; Shi, X. PAR-GAN: Improving the generalization of generative adversarial networks against membership inference attacks. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining, Singapore, 14–18 August 2021.
115. Behnke, I.; Blumschein, C.; Danicki, R.; Wiesner, P.; Thamsen, L.; Kao, O. Towards a real-time IoT: Approaches for incoming packet processing in cyber-physical systems. *J. Syst. Archit.* **2023**, *140*, 102891. [CrossRef]
116. Zahid, S.; Mazhar, M.S.; Abbas, S.G.; Hanif, Z.; Hina, S.; Shah, G.A. Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. *Internet Things* **2023**, *22*, 100766.
117. Bakkiam Deebak, D.; AL-Turjman, F. Lightweight privacy-aware secure authentication scheme for cyber-physical systems in the edge intelligence era. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e6510. [CrossRef]
118. Catillo, M.; Pecchia, A.; Villano, U. CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders. *Comput. Secur.* **2023**, *129*, 103210. [CrossRef]
119. Cicceri, G.; Tricomi, G.; D'Agati, L.; Longo, F.; Merlino, G.; Puliafito, A. A Deep Learning-Driven Self-Conscious Distributed Cyber-Physical System for Renewable Energy Communities. *Sensors* **2023**, *23*, 4549. [CrossRef] [PubMed]
120. Wang, X.; Wang, Y.; Javaheri, Z.; Almutairi, L.; Moghadamnejad, N.; Younes, O.S. Federated deep learning for anomaly detection in the internet of things. *Comput. Electr. Eng.* **2023**, *108*, 108651. [CrossRef]
121. Alohali, M.A.; Elsadig, M.; Al-Wesabi, F.N.; Al Duhayyim, M.; Hilal, A.M.; Motwakel, A. Swarm intelligence for IoT attack detection in fog-enabled cyber-physical system. *Comput. Electr. Eng.* **2023**, *108*, 108676. [CrossRef]
122. Daniel, A.; Deebalakshmi, R.; Thilagavathy, R.; Kohilakanagalakshmi, T.; Janakiraman, S.; Balusamy, B. Optimal feature selection for malware detection in cyber physical systems using graph convolutional network. *Comput. Electr. Eng.* **2023**, *108*, 108689. [CrossRef]
123. Arat, F.; Akleylek, S. Attack Path Detection for IIoT Enabled Cyber Physical Systems: Revisited. *Comput. Secur.* **2023**, *128*, 103174. [CrossRef]
124. Bovenzi, G.; Aceto, G.; Ciuonzo, D.; Montieri, A.; Persico, V.; Pescapé, A. Network anomaly detection methods in IoT environments via deep learning: A Fair comparison of performance and robustness. *Comput. Secur.* **2023**, *128*, 103167. [CrossRef]
125. Bai, R.; Zhang, P.; Zhang, Z.; Sun, X.; Fei, H.; Bao, S.; Hu, G.; Li, W. Optimization of blasting parameters and prediction of vibration effects in open pit mines based on deep neural networks. *Alex. Eng. J.* **2023**, *70*, 261–271. [CrossRef]
126. Langarica, S.; Núñez, F. Contrastive blind denoising autoencoder for real time denoising of industrial IoT sensor data. *Eng. Appl. Artif. Intell.* **2023**, *120*, 105838. [CrossRef]
127. Wang, Y.; Kong, L.; Lin, S.; He, L. Detecting Engine Anomalies Using Batteries. *IEEE Trans. Mob. Comput.* **2023**, *22*, 2069–2083. [CrossRef]
128. Sadek, R.A.; Elbadawy, H.M. Towards IoT Era with current and Future Wireless Communication Technologies: An Overview. In Proceedings of the 2022 39th National Radio Science Conference, Cairo, Egypt, 29 November–1 December 2022.
129. Monzon Baeza, V.; Ortiz, F.; Herrero Garcia, S.; Lagunas, E. Enhanced communications on satellite-based iot systems to support maritime transportation services. *Sensors* **2022**, *22*, 6450. [CrossRef] [PubMed]
130. Fort, A.; Mugnaini, M.; Peruzzi, G.; Pozzebon, A. Reliability Analysis of an IoT Satellite Facility for Remote Monitoring and Asset Tracking within Marine Environments. In Proceedings of the 2022 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters, Milazzo, Italy, 24 November 2022.
131. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Secur. J.* **2022**, *35*, 486–505. [CrossRef]

132. Chetioui, K.; Bah, B.; Alami, A.O.; Bahnasse, A. Overview of social engineering attacks on social networks. *Procedia Comput. Sci.* **2022**, *198*, 656–661. [CrossRef]
133. Ponemon Institute. *Cost of Data Breach Report (2020)*; Ponemon Institute: Traverse City, MI, USA, 2020.
134. Wang, H.; Huang, M.; Feng, X.; Zhou, Y. Contract design for the fourth party logistics considering tardiness risk. *Int. J. Ind. Eng. Comput.* **2022**, *13*, 13–30. [CrossRef]
135. Angelogianni, A.; Politis, I.; Mohammadi, F.; Xenakis, C. On identifying threats and quantifying cybersecurity risks of mnos deploying heterogeneous rats. *IEEE Access* **2020**, *8*, 224677–224701. [CrossRef]
136. Neigel, A.R.; Claypoole, V.L.; Waldfogle, G.E.; Acharya, S.; Hancock, G.M. Holistic cyber hygiene education: Accounting for the human factors. *Comput. Secur.* **2020**, *92*, 101731. [CrossRef]
137. Achar, S. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. *Int. J. Comput. Syst. Eng.* **2022**, *16*, 379–384.
138. Liao, B.; Ali, Y.; Nazir, S.; He, L.; Khan, H.U. Security analysis of IoT devices by using mobile computing: A systematic literature review. *IEEE Access* **2020**, *8*, 120331–120350. [CrossRef]
139. Du, M. Application of information communication network security management and control based on big data technology. *Int. J. Commun. Syst.* **2022**, *35*, e4643. [CrossRef]
140. Sheikh, A. Hacking Wireless Networks. In *Certified Ethical Hacker (CEH) Preparation Guide: Lesson-Based Review of Ethical Hacking and Penetration Testing*; Apress: Berkeley, CA, USA, 2021.
141. Tundis, A.; Mazurczyk, W.; Mühlhäuser, M. A review of network vulnerabilities scanning tools: Types, capabilities and functioning. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018.
142. Garba, F.A.; Kunya, K.I.; Ibrahim, S.A.; Isa, A.B.; Muhammad, K.M.; Wali, N.N. Evaluating the state of the art antivirus evasion tools on windows and android platform. In Proceedings of the 2019 2nd International Conference of the IEEE Nigeria Computer Chapter, Zaria, Nigeria, 14–17 October 2019.
143. Gupta, B.B.; Li, K.C.; Leung, V.C.; Psannis, K.E.; Yamaguchi, S. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. *IEEE CAA J. Autom. Sin.* **2021**, *8*, 1877–1890.
144. Anwar, R.W.; Abdullah, T.; Pastore, F. Firewall best practices for securing smart healthcare environment: A review. *Appl. Sci.* **2021**, *11*, 9183. [CrossRef]
145. Ansari, B.; Barati, M.; Martin, E.G. Enhancing the usability and usefulness of open government data: A comprehensive review of the state of open government data visualization research. *Gov. Inf. Q.* **2022**, *39*, 101657. [CrossRef]
146. Gao, Y.; Janssen, M. The open data canvas–Analyzing value creation from open data. *Digit. Gov. Res. Prac.* **2022**, *3*, 1–15. [CrossRef]
147. Kamariotou, M.; Kitsios, F. Bringing Digital Innovation Strategies and Entrepreneurship: The Business Model Canvas in Open Data Ecosystem and Startups. *Future Internet* **2022**, *14*, 127. [CrossRef]
148. Kar, B.; Yahya, W.; Lin, Y.D.; Ali, A. Offloading using traditional optimization and machine learning in federated cloud-edge-fog systems: A survey. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1199–1226. [CrossRef]