electronics

MDPI

Article

A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems

Nicholas Jeffrey [1,*], Qing Tan [2] and José R. Villar [1]

[1] Faculty of Computer Science, University of Oviedo, 33003 Oviedo, Spain; villarjose@uniovi.es
[2] Faculty of Science and Technology, Athabasca University, Athabasca, AB T9S 3A3, Canada; qingt@athabascau.ca
[*] Correspondence: uo292630@unovi.es

Abstract: Cyber-Physical Systems (CPS) are integrated systems that combine software and physical components. CPS has experienced rapid growth over the past decade in fields as disparate as telemedicine, smart manufacturing, autonomous vehicles, the Internet of Things, industrial control systems, smart power grids, remote laboratory environments, and many more. With the widespread integration of Cyber-Physical Systems (CPS) in various aspects of contemporary society, the frequency of malicious assaults carried out by adversaries has experienced a substantial surge in recent times. Incidents targeting vital civilian infrastructure, such as electrical power grids and oil pipelines, have become alarmingly common due to the expanded connectivity to the public internet, which significantly expands the vulnerability of CPS. This article presents a comprehensive review of existing literature that examines the latest advancements in anomaly detection techniques for identifying security threats in Cyber-Physical Systems. The primary emphasis is placed on addressing life safety concerns within industrial control networks (ICS). A total of 296 papers are reviewed, with common themes and research gaps identified. This paper makes a novel contribution by identifying the key challenges that remain in the field, which include resource constraints, a lack of standardized communication protocols, extreme heterogeneity that hampers industry consensus, and different information security priorities between Operational Technology (OT) and Information Technology (IT) networks. Potential solutions and/or opportunities for further research are identified to address these selected challenges.

Keywords: anomaly detection in {CPS, IoT, IIoT, SCADA}; security threats to {CPS, IoT, IIOT, SCADA}; AI/ML in CPS; machine learning in IoT security

check for updates

Citation: Jeffrey, N.; Tan, Q.; Villar, J.R. A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electronics* **2023**, *12*, 3283. https://doi.org/10.3390/electronics12153283

Academic Editor: Andrei Kelarev

Received: 20 June 2023
Revised: 28 July 2023
Accepted: 29 July 2023
Published: 30 July 2023

1. Introduction

Cyber-Physical Systems (CPS) are integrated systems that combine cyber components, such as software (embedded) programmed computational algorithms, and physical components, such as sensors and actuators, into a unified real-time control system [1], where all the components are interconnected through communication links, such as computer networks and the Internet, with shared communication protocols and are interacted with and function based on their system architecture to serve particular applications. CPS is a broad field, encompassing traditional Industrial Control Systems (ICS), Supervisory Control And Data Acquisition (SCADA), and the more modern Internet of Things (IoT)-based smart systems.

The term "Cyber-Physical System" is commonly utilized in academic circles, whereas the industry predominantly employs "IoT" when referring to consumer-grade devices and "IIoT" (Industrial Internet of Things) for industrial control systems encompassing manufacturing, process control, and related domains.

The exponential expansion [2] of Cyber-Physical Systems (CPS) has surpassed the progress made in cybersecurity, leading to the emergence of novel threat models and security challenges. Unfortunately, there is a lack of a unified framework for ensuring secure design, resistance against malware, and effective risk mitigation. The majority of attention from both academia and industry is primarily focused on consumer-grade IoT devices, such as smart home automation. Regrettably, there seems to be comparatively less emphasis on industrial-grade IoT from both academia and industry, despite the fact that the consequences of IIoT failures can be significantly more severe, encompassing scenarios such as power grid failures, oil pipeline shutdowns, and transportation network interruptions [2].

The field of threat detection and prevention has reached a mature stage within enterprise networks, supported by established vendors (Cisco, Crowdstrike, FortiNet, Palo Alto, etc.) offering robust host-based and network-based Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS). However, CPS currently lacks equivalent IDS/IPS capabilities [3].

Legacy ICS and SCADA environments have not fully adapted to the pervasive connectivity brought by Industry 4.0 [4]. Moreover, security measures in ICS often tend to be an afterthought or low-priority feature set. This can be attributed to the outdated belief that the ICS environment remains isolated from an air-gapped and trusted network [5], which is no longer accurate. As a consequence of heightened connectivity to hostile networks, Cyber-Physical Systems (CPS) have witnessed a rapid surge in malicious intrusions, leading to substantial economic losses and posing risks to life safety.

Academic research on ICS/SCADA systems used for industrial process control has been subsumed into the larger body of CPS, with active collaboration [6] between industry and academia enabling rapid enhancements, particularly in the areas of security and reliability engineering.

There is a gap in academic research and industry practice in the area of anomaly detection/intrusion detection/intrusion prevention. This paper aims to summarize the existing efforts in this area, which will enable the identification of gaps and weaknesses as well as opportunities for additional research.

As a systematic review, this paper is intended to be useful as a form of secondary study, providing a summation of existing literature in the field, identifying gaps or areas with limited existing research, and identifying opportunities for future works in the research area. A five-step methodology was used to develop this review, beginning with the framing of the research question and followed by an exhaustive search to identify relevant works. The identified works were then assessed to determine quality and relevance, followed by a summarization of the existing works and interpretations of the existing findings, with the goal of identifying gaps in the existing research for future development.

The remainder of this paper is organized as follows: Section 2 provides historical background on CPS as well as the rationale for the safe and secure operation of these increasingly critical infrastructures. In Section 3, a statistical analysis of the areas covered in the existing literature is presented, enabling the identification of gaps in current research. In Section 4, a literature analysis is conducted for each category that has been identified. Section 5 showcases the existing challenges and identifies potential solutions to advance the state of the art. Lastly, in Section 6, this paper discusses the conclusions drawn and highlights opportunities for future research.

2. Background and Rationale

In years past, the paramount objective in ICS design was to achieve utmost reliability and predictability. As a result, fundamental cybersecurity practices such as implementing complex passwords or enforcing stringent authentication requirements were perceived as hindrances to system accessibility. Consequently, designers and operators of these systems deliberately avoided such measures [7]. Similarly, traditional anti-malware programs like signature-based antivirus tools were eschewed to mitigate the risk of false positives mistakenly quarantining or disabling crucial system operations. These legacy systems were commonly operated on completely trusted and isolated networks, devoid of any connections to corporate networks and certainly without any link to the public Internet.

Furthermore, the absence of standardization in the early years of ICS design gave rise to a wide variety of proprietary communication protocols, which often relied on the principle of "security by obscurity" [8]. This approach was due to the lack of a rigorous peer review process. Moreover, system vendors typically lacked mechanisms for delivering updates or bug fixes, which meant that newly discovered vulnerabilities would persist throughout the lifespan of the system. In such cases, sole reliance was placed on network isolation as a means of protection against threats.

With the evolution from legacy ICS to modern CPS environments, the previously held design principles became unsustainable. The widespread adoption of wireless networks and the swift abandonment of isolated air-gapped network environments made the historical design considerations impractical in the face of the requirements for standardized communication protocols used on the public internet.

Legacy communication protocols employed by ICS, such as Modbus, DNP, Fieldbus, HART, and others [9], are gradually being replaced by TCP/IP protocols used in Cyber-Physical Systems (CPS). This shift is predominantly motivated by commercial interests to enable communication with business networks and the wider Internet.

The current landscape of CPS reflects a highly interconnected world where the presence of threat actors is pervasive, necessitating the assumption of a hostile network environment. As CPS becomes more extensively integrated with various corporate and public networks, the attack surface has exponentially expanded. Consequently, breaches targeting critical national infrastructure (CNI), including power grids [10] and more, have become increasingly frequent.

As a result of the historical design objectives in ICS, the level of observability of the system state [10] has traditionally been confined to the real-time status of individual sensors or actuators, accompanied by straightforward threshold-based alerts for system operators. The assumption that ICS would operate within isolated and completely trusted networks meant that IDS/IPS were not prioritized during the design phase. Consequently, there is a deficiency in observability within the increasingly hostile network layer of CPS, making it challenging to detect threats and malicious activities in an increasingly interconnected world.

Perhaps the most notorious example of a blended or integrated threat is the Stuxnet [11] malware that attacked the Natanz nuclear enrichment facility, using a combined suite of attacks against both the Cyber and the Physical components of the system. In what is widely considered the first large-scale attack on a CPS, the Stuxnet malware used zero-day exploits developed specifically for the Information Technology (IT) components of the CPS, which were then leveraged to run the Operational Technology (OT) components of the CPS slightly outside the operational tolerances of speed and pressure, resulting in the physical destruction of precision equipment.

Anomaly detection of security threats to CPS has become more urgent and critical to industry and life safety as CNI becomes increasingly interconnected with public networks. Therefore, further study is needed to advance the state of academic research on the issue and to develop and apply preventative solutions for industry to ensure safe and secure implementations of CPS.

Serpanos [2] identifies how CPS differs from traditional computational systems due to the integration of a wide range of heterogenous technologies in the sensors and actuators and discusses how interaction with the physical world raises key issues around resilience, fault tolerance, and life safety issues. The integration challenges of combining IT and OT [12] are significant, as the design goals are often at odds, in part due to IT networks being approached from a Computer Science perspective while OT networks are approached from an industrial operations management perspective, each of which has differing goals and objectives.

3. Statistical Analysis

The search terms described in the Keywords section were used to identify relevant literature sources from assorted search engines, including the ACM Digital Library, Google Scholar, IEEE Xplore, Semantic Scholar, SpringerOpen, and Web of Science. Search results were further filtered by year, excluding references older than 5 years. Exclusions were performed by manual review to ensure relevancy. Additional inclusions were identified through manual review of the results returned by the above search engines and through use of the "Cited by" functionality of Google Scholar to identify related references. A total of 296 sources of literature have been selected and reviewed for this research. As a literature review, this section is designed not only to summarize the existing research in the field but also to be of use to future researchers. As such, this section will categorize the existing research literature reviewed in this paper by country of origin (based on the first author's institutional affiliation), publication type, publisher, and publication year. As shown in Table 1, The top two academic publishers comprise more than half of the available literature, resulting in an effective oligopoly in academic publishing in this specific research area.

Table 1. Academic Publishers.

Publisher	**Articles**
IEEE	114 (39%)
Springer	47 (16%)
ScienceDirect	44 (15%)
MDPI	16 (5%)
ACM	12 (4%)
Other	63 (21%)
Total	296 (100%)

The majority of available research in this field is contributed by the top five publishers, all of which are well-established academic publishers known for their rigorous peer review and high level of quality assurance processes. The so-called "network effect" of the overwhelming majority of available research being concentrated in such a small number of publishers makes it difficult for new or niche publishers to gain critical mass, as researchers gravitate to the publishers with the highest reputations and impact factors.

As shown in Table 2, Academic journals account for the majority of research publications in this area, with academic conferences being a distant second and other publications (i.e., industry whitepapers, trade association standards) ranking as nearly insignificant.

Table 2. Publication Types.

Publication Type	**Articles**
Journal	182 (61%)
Conference	72 (24%)
Other	43 (15%)
Total	296 (100%)

The realm of CPS security is significantly shaped by industry, although the focus of these efforts is often geared towards immediate tactical measures to address current market threats and opportunities. Industry-driven initiatives, motivated by competitive advantage and the need to protect trade secrets, are seldom disclosed to the wider community. Consequently, the practice of "security by obscurity" remains prevalent in the industry. This situation highlights a distinct absence of collaboration between industry and academia in the field of CPS security, presenting a valuable opportunity for enhancement and progress.

In order to remain up-to-date in a swiftly evolving domain, the literature examined in this paper encompasses the past decade, primarily focusing on articles published within the last three years, as shown in Table 3. The term "Cyber-Physical Systems" was introduced by the US-based National Science Foundation (NSF) in 2006 [13], resulting in limited pre-existing research prior to that timeframe. Earlier investigations pertaining to CPS were conducted within the domains of industrial process control, cybernetics, control logic, and engineering.

Table 3. Publications by Year.

Publication Year	Articles
2022	68 (23%)
2021	69 (23%)
2020	73 (25%)
2011–2019	86 (29%)
Total	296 (100%)

As shown in Table 4, the largest single contributor of research in this domain is the USA, generating one-fifth of the available literature, and the top four countries generate as much research as all other countries combined.

Table 4. Publications by Country.

Country	Articles
USA	59 (19.9%)
China	34 (11.5%)
India	28 (9.5%)
UK	25 (8.4%)
Other	150 (50.7%)
Total	296

4. Literature Analysis

The existing research in the area of anomaly detection on CPS can be broadly classified into the following categories, each of which will be discussed further: Table 5 shows the statistical numbers of the literature reviewed in this paper by topic.

Table 5. Publications by Category.

Category	Articles
Comparison of Anomaly Detection Strategies	60
Using IDS/IPS for Anomaly Detection	63
Using AI/ML for Anomaly Detection	92
Improving Anomaly Detection with Simulators/Testbeds	27
Anomaly Detection at the Network Edge	20
Trusted Systems vs Zero-Trust Architecture	21

The categories shown in Table 5 should be considered broad in nature, and many of the sources in the existing literature have minor degrees of overlap in more than one category, but all sources will have a primary focus on a single category. In addition to the above publications, there are 13 sources referenced in the Introduction section of this paper that provide supporting historical references but are not included in the above table due to their inconsequential relation to the analysis performed in this paper. Table 6 provides a brief summary of each category, with more detailed analysis to follow in the subsequent sections.

Table 6. Category Overview.

Category	Overview
Comparison of Anomaly Detection Strategies	Each AD strategy can be classified as signature-based, threshold-based, or behavior-based, each of which has different advantages and disadvantages.
Using IDS/IPS for Anomaly Detection	IDS/IPS are mature strategies in IT networks, but still struggle in OT networks due to the much higher cost of false positives.
Using AI/ML for Anomaly Detection	AI/ML strategies are primarily leveraged for behavior-based AD strategies, with learning algorithms designed to distill big data problems into actionable intelligence.
Improving Anomaly Detection with Simulators/Testbeds	The physical components of large-scale CPS environments are economically infeasible to duplicate for dev/test, making simulations or small-scale testbeds an attractive alternative.
Anomaly Detection at the Network Edge	As IoT/IIoT sensor networks proliferate, performing initial data filtering and pre-processing at the network edge becomes necessary to avoid network saturation.
Trusted Systems vs Zero-Trust Architecture	For historical reasons, industrial networks were designed to be isolated and fully trusted, but with increasing connectivity to public networks, adoption of ZTA becomes increasingly important.

4.1. Comparison of Anomaly Detection Strategies

This is the third-largest category of research articles [14–72] covered in this review and discusses all the references that describe multiple strategies for performing effective anomaly detection for CPS. Due to the rapid rate of change and extreme heterogeneity of CPS, there are multiple competing recommendations and proposals, with no clear leader in industry or academia.

Threat detection methodologies can be categorized into three main groups [14]: signature-based, threshold-based, and behavior-based. A signature-based approach, like that used in traditional antivirus programs, relies on a centralized and regularly updated database of signatures to identify malicious files or traffic. When a match is found, it triggers an alarm on an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS). Signature-based detection performs effectively on IT networks due to uniform communication protocols and relatively high homogeneity. However, it encounters challenges in OT networks, characterized by proprietary communication protocols and diverse physical components, resulting in higher rates of false negatives.

Threshold-based methodologies depend on established acceptable operational ranges, which are relatively straightforward to define in IT networks. These can include metrics such as network latency, link saturation, and levels of CPU utilization. However, accurately defining known ranges of acceptable operation in OT networks has proven more challenging due to the influence of real-world environmental fluctuations [15]. For instance, in a smart city setting, a network of air quality sensors utilizing wi-fi or cellular networks may experience variations in communication latency caused by factors like fog or rain. This unpredictability makes it difficult to establish consistent thresholds of acceptable operation, as they can differ based on the prevailing weather conditions.

Behavior-based methodologies pose considerable difficulties for accurate detection on IT networks, and these challenges are further magnified when applied to OT networks [16]. Establishing a precise benchmark or reference point for normal behavior on an IT network necessitates a profound level of comprehension of what constitutes typical system activity. However, it is uncommon for IT networks to remain unchanged throughout their entire lifecycle, making the definition of normal behavior a constantly moving target at best. These challenges are amplified on OT networks, which tend to be even more dynamic due to environmental factors such as weather-related variations in temperature, humidity, and ambient light, among others. Furthermore, the repercussions of false positive or false negative detections on OT networks are notably more significant. They can lead to physical equipment damage and pose serious life-safety concerns.

Signature-based anomaly detection provides excellent detection accuracy against known threats but suffers from excessive false negatives for unknown threats. To contrast, behavior-based anomaly detection excels in the detection of unknown threats but suffers from high false positives for known threats. Much of the existing literature describes methodologies to improve on the weaknesses of each method or combine both signature-based and behavior-based anomaly detection into a hybrid system for better accuracy.

Altunay et al. [17] focus on AI/ML methods for optimizing behavior-based anomaly detection by building a large data model of historical performance measurements and enhancing the machine learning model by correlating it with a signature-based database of known threats. This hybrid model of anomaly detection slowly grows in accuracy as more information is added to the learning model, but decreases in real-time performance as the amount of historical data grows.

Rubio et al. [18] focus on the emerging risks posed by Advanced Persistent Threats (APT), a specialized type of malware designed to exploit a specific organization or specific model of CPS. APTs are typically deployed against a high-value target, such as Critical National Infrastructure (CNI), by a highly skilled threat actor. Because the APT is often customized for a specific target, traditional signature-based anomaly detection strategies have limited accuracy due to the zero-day exploits used by the APT. For this reason, an intrusion detection system (IDS) can only be considered the first layer of a multilayered defense and should be used with other mitigation techniques, including network segmentation to minimize risks of lateral exploitation, threshold-based detection methods for observing performance metrics that fall outside of defined boundaries, and behavior-based anomaly detection of traffic patterns with other network hosts.

4.2. Using IDS/IPS for Anomaly Detection

This is the second-largest category of research articles [73–135] covered in this review and discusses all the references that propose novel methods of anomaly detection in CPS, with particular focus on IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems).

As discussed in previous sections of this paper, a CPS can be viewed as a fusion of IT and OT environments. The field of IT networks has mature and robust solutions for threat detection using IDS/IPS, but there have been significant challenges [73] in effective threat detection on OT networks.

Seng et al. [74] focus on the stark divide between industry and academia in the design and operation of IDS/IPS for industrial networks. The oldest and most common method of intrusion detection on both IT and OT networks is signature-based, which uses a database of known malicious patterns to recognize malicious traffic. Signature-based IDS are the oldest and most commonly used method for intrusion detection. They are extremely effective at detecting known attacks but are typically unable to detect novel or zero-day attacks, which means the signature database must be frequently updated. To contrast, anomaly-based detection is typically based on using AI/ML to model normal behavior, then classifying any behavior that falls outside those parameters as anomalous and therefore a potential threat. A simplistic method of anomaly-based detection is to use predefined thresholds to define normal behavior. In IT networks, these thresholds would apply to metrics such as processor or memory utilization, while OT networks would use physical environmental measurements such as temperature, pressure, voltage, etc.

While threshold-based detection methodologies do not require the same frequent database updates as signature-based detection methods, they still share the same high levels of accuracy and a relatively low administrative burden on the part of the system operator to maintain the IDS. This combination of minimal administrative requirements and high levels of accuracy for known threats has resulted in high levels of industry acceptance and adoption of this type of IDS/IPS.

Seng et al. report that while the overwhelming majority of industry adoption of IDS/IPS in industrial environments uses signature-based and threshold-based strategies, the academic community focuses almost entirely (97%) on behavior-based detection strategies using AI/ML, which have very little uptake in industry. AI/ML algorithms are able to achieve very high accuracy rates (typically >95%), but despite achieving high detection rates of both known and unknown threats, the proposed methods rarely progress from academia to industry. The extreme heterogeneity of IIoT environments is particularly challenging, as AI/ML models will typically have low applicability to other environments, making wide adoption difficult. The availability of representative datasets is another significant challenge, with most of the available research datasets being artificially generated by researchers with varying levels of fidelity to real-world IIoT environments. These limitations translate to a high administrative cost in terms of time and expertise on the part of the system operator, which significantly hinders widespread adoption. The primary challenges identified by Seng et al. with behavior-based IDS are the availability of exhaustive datasets containing accurately labeled data and the ongoing ease of administrative maintenance, both of which are currently unsolved problems.

Khraisat et al. [75] further develop the works of Seng by building a taxonomy of current IDS/IPS techniques and comparing the different AI/ML techniques common in academic literature. Systematic comparisons of several ML algorithms are provided, each with varying advantages and disadvantages, with a common theme being that an ensemble method that combines multiple ML algorithms to leverage synergies to improve overall accuracy by stacking different algorithms to achieve higher accuracy levels than can be achieved with a single algorithm. A disadvantage of this method is its higher complexity and additional time and expertise requirements on the part of the system operator, which have hampered industry adoption.

Vasan et al. [76] further develop the work of Khraisat on ensemble learning models to improve IDS/IPS accuracy in IIoT environments with a novel approach for feature selection by stacking heterogeneous features, achieving very high classification accuracy (99.98%) with low computational overheads that can be handled by resource-constrained IoT devices. This ensemble learning model focuses on cross-platform malware due to the rapid growth in IoT attacks against diverse processor architectures, driven by malicious actors refining their own adversarial capabilities. The proposed ensemble model is referred to as MTHAEL (Malware Threat Hunting based on Advanced Ensemble Learning) and combines multiple weak learner algorithms to train a strong learner to generate enhanced predictions based on the multiple predictions from the weak learner models.

MTHAEL generates a normal baseline through disassembly of the executable binary files on the IoT devices to determine the OpCode instructions (i.e., machine code, one level lower than assembly language) to determine which operations occur during normal operation. This extremely low level of instruction provides cross-platform compatibility for intrusion detection, which is advantageous in the highly heterogeneous market of IoT devices. The primary advantage of this methodology is the ability to leverage the same IDS/IPS across a broad range of IoT devices, which helps reduce the administrative burden on the system operator by making the IDS/IPS available to a wider audience without additional customization. However, the initial disassembly of all application binaries is a laborious process that requires high levels of expertise, which is not common outside of academia, thereby limiting broad industry adoption. This type of IDS would best be deployed as a SaaS (Software as a Service) offering, offloading the ongoing maintenance of the IDS to a centralized subject matter expert that can leverage a federated dataset to provide rapid intrusion detection of both known and unknown threats.

Abid et al. [77] propose a novel method of using a distributed IDS, defining the challenges as a big data problem, and using machine learning to sift through both legitimate and attack data from disparate sources in a centralized cloud-based environment, then feeding the analyzed/classified data back to the distributed nodes in the IDS to be acted upon. The value proposition of this method is to provide the Machine Learning (ML) model with richer data sources than can be obtained from a single viewpoint on the network, thus improving the classification accuracy of the IDS. While this approach is useful for a homogenous IIoT environment, it has limited applicability outside of a single organization due to the wide variation in IIoT architectures. This contrasts with IDS/IPS implementations in traditional enterprise networks, which tend to be more monocultural and thus better able to leverage distributed IDS/IPS learning models.

Bai et al. [78] propose an instruction-level methodology for malware detection in CPS/IIoT environments through the use of an out-of-band circuit board that collects power consumption details from the sensors and actuators in the CPS and performs offline analysis to determine if the components in the CPS are operating normally. This methodology avoids the more traditional signature-based detection of malware, opting for behavior-based anomaly detection by using side-channel characteristics such as power consumption, acoustics, response time fluctuations, etc. Analysis of side-channel characteristics essentially turns the entire CPS into a deterministic finite state machine, with the IDS/IPS considering any non-deterministic behavior as malicious. While this is a novel idea, requiring additional out-of-band hardware solely for behavioral monitoring adds significant complexity to a CPS, which is a significant barrier to industry adoption. Additionally, this method suffers from low detection accuracy if the CPS experiences normal load-based variation due to changing operational parameters being incorrectly classified as non-deterministic behavior, so this methodology is best suited to relatively small and static CPS/IIoT environments.

Chavez et al. [79] propose a hybrid IDS that treats the cyber and physical portions of the CPS as distinct environments with different threat profiles, using a signature-based IDS for the cyber components and a behavior-based IDS for the physical components. The objective of this hybrid model is to increase detection accuracy by increasing the level of difficulty for a malicious actor to bypass the IDS on both the cyber and physical portions of the CPS. Additionally, by separating the detection methodologies for the IT and OT portions of the network, the update frequency of intrusion signatures can be independent, which is advantageous for the typically higher velocity of updates on the IT portion of the CPS. Additionally, the detection methodology for the OT portion of the CPS tends to be primarily threshold-based fault detections (i.e., voltages or temperatures outside of defined ranges) rather than intrusion detections. This clear delineation between the IT and OT portions of the CPS allows for more precise tuning of the alert thresholds to minimize false positives, which can have significant economic and life safety issues in IIoT environments.

Gu et al. [80] propose a classification framework that uses Convolutional Neural Networks (CNN) to learn representative attack characteristics from raw network traffic to train a network-based IDS. This methodology is designed to counter the common ML challenge of having insufficient training data in an ML model due to the scarcity of malicious activity, as well as the heterogeneity of different IIoT environments preventing meaningful transfer of ML models between organizations. The proposed method attempts to minimize the data preprocessing by automatically transforming the data into fixed formats that are transferable across different data types, then using a discriminator to determine if the traffic is benign or malicious. The proposed use of CNN for automated feature extraction improves the accuracy of the ML model by mitigating the reduced accuracy typically introduced by unbalanced datasets, but still suffers from relatively high false positives and false negatives for previously unknown attacks.

Rakas et al. [81] suggest that many CPS environments are well-suited to anomaly detection via pattern recognition of a narrowly defined set of traffic patterns between specific hosts using specific communication protocols, with anything outside these narrowly defined boundaries defined as anomalous. This is essentially a threshold-based anomaly detection strategy, that works well for static environments in which all communication patterns are known in advance. This strategy suffers when the consumers of sensor data are dynamic or the amount of communication between nodes on the network varies due to external events that may be semi-random, such as weather fluctuations or human client behavior.

Ravikumar et al. [82] build on the work of Rakas by proposing a distributed IDS for federated CPS environments such as interconnected smart power grids. The proposed distributed IDS uses Ethernet switch port mirroring to capture network traffic flow data and consolidate that data in a centralized or cloud-based IDS environment for enhanced situational awareness of activity in a distributed and/or loosely coupled CPS. This allows IDS rules to be dynamically generated based on activity across a loosely coupled or distributed IDS, such as a smart power grid, to provide faster anomaly detection and greater protection against cascading failures. On test datasets, the accuracy of simulated anomaly events was very high, but it requires further development to be applicable to more dynamic live environments.

Sheng et al. [83] suggest that existing IDS are capable of detecting anomalies but cannot meaningfully describe the overall risk or impact on the CPS and propose a generalized model that characterizes the network environment and CPS processes through event correlation and activity patterns of the nodes on the network, with any violations of the model being considered abnormal behavior and thus an anomalous event. This proposed methodology has had some success when tested against public datasets, but suffers from high false positives on live systems.

Hwang and Lee [84] focus on improvements in anomaly detection from the perspective of minimizing false alarms from sensors by adding an interpretation layer to AI predictions that are opaque to the system operators, providing a higher quality of information to the human security analysts. This combines unsupervised machine learning with supervised machine learning by automatically adding data labels based on statistical mean prediction errors. Data labeling is typically a high-cost effort in terms of human time and expertise, which this proposal attempts to mitigate by automatically applying labels based on statistical analysis, with the intent of the IDS suffering from fewer false positive alerts.

4.3. Using AI/ML for Anomaly Detection

This is the largest category of research articles [136–227] covered in this review and discusses all the references that propose novel methods for using AI/ML for anomaly detection.

As sensors become more powerful and more numerous in CPS, transforming increasingly large amounts of raw data into actionable information becomes increasingly challenging, with AI/ML being used for data ingest, data pre-processing, pattern recognition, and analysis [136]. Along with increases in device processing power, both wired and wireless network technologies have tremendously increased in speed over the years, making the amount of data that can be feasibly retrieved from CPS sensors grow dramatically. As the amount of sensor data reaches so-called "Big Data" levels, the need for automated data processing has made AI increasingly popular for leveraging data from CPS.

The resulting wealth of data from CPS sensors has outstripped human capabilities to effectively process it, with AI/ML increasingly being employed [136–227] to process the large datasets produced from CPS sensors. AI/ML usage in CPS is typically used for data mining/analytics purposes, with the goal of extracting actionable insights from the raw data.

Individual sensors in a CPS are typically resource-constrained [137] and are only aware of the sensor readings from a single device. By having multiple sensors in the CPS feeding an AI learning model, a fuller understanding of the CPS as a cohesive whole can be achieved, including hostile activity such as a DDoS attack that would not be detected by individual sensors.

The adoption of AI in CPS has been notably rapid, particularly in the context of manufacturing processes within the realm of "Industry 4.0". The utilization of AI in CPS serves two primary purposes: enhancing protection against cybersecurity attacks and improving operational efficiency. In their work, Alhaidari and AL-Dahasi [4] develop an enhanced framework that utilizes AI to detect Distributed Denial of Service (DDoS) attacks by employing multiple machine learning algorithms. The research involved analyzing different datasets using machine learning algorithms to enable swift detection of DDoS attacks. Preprocessing of raw data was employed to reduce the amount of data used for training the model, which proved instrumental in enhancing the mean time required to detect an attack. A noteworthy finding drawn from the study emphasized the necessity for increased collaboration between CPS operators and the broader industry to facilitate the sharing of vulnerability information.

Tsochev and Sharabov [138] approach the use of AI in CPS as a means for maximizing production efficiency in a manufacturing-based environment. By using AI as an expert system for near-real-time decision making based on all sensor inputs from the CPS, downtime can be minimized through predictive failure analysis to proactively schedule maintenance activities, which helps enhance life safety precautions. The overall efficiency of the CPS is improved due to machine learning algorithms that extract actionable intelligence from the big data sets generated by the sensors in the CPS.

Altunay et al. [16] propose an approach based on deep learning for training a behavior-based IDS, which shows some promise but is ultimately limited by the quality and breadth of the training data, which is notoriously difficult to gather and accurately label for OT networks owing to their lack of standardized communication protocols and high levels of heterogeneity.

Fatani et al. [139] expand on this concept by proposing an AI-based mechanism for behavior-based IDS using deep learning and metaheuristic algorithms to extract actionable threat intelligence from raw sensor data and network telemetry, leading to improved accuracy in threat detection.

Hindy et al. [140] propose the integration of SIEM (Security Information and Event Management) tools that are already commonly leveraged in IT networks to be more fully integrated into OT networks. The authors recognize the differing information security postures and priorities between IT networks and OT networks, so they customize the event correlation techniques used to build a machine learning model that is optimized for OT networks, focusing on the lack of open standards for CPS communication protocols and the lack of network segmentation in a typical CPS that enables lateral network exploitation.

Shahriar et al. [141] propose an IDS based on a Generative Adversarial Network (GAN) to train an AI model with automatically generated training data to predict anomalous events that have not yet been observed. The intent is to produce a generalized model of anomaly detection that is applicable to heterogeneous CPS environments without the extensive site-specific customization that is typically required.

Yadav et al. [142] build on the work of Shahriar et al. by further developing GAN as a method of improving accuracy in an IDS. GAN uses two opposing neural networks, with a generative model attempting to predict what a previously unseen anomaly might look like, while the opposing discriminatory model is used to determine if the prediction of the generative model is valid. The use of GAN can rapidly accelerate the detection of anomalous events by the IDS while reducing false alarms.

Chen et al. [143] further develop methods of GAN, focusing on hostile actors deliberately introducing slight variations to malicious payloads in order to evade both signature-based and behavior-based IDP/IPS. These evasive strategies from malware authors have long existed as polymorphic computer viruses in IT networks but have traditionally been mitigated by signature-based detection methods. Chen et al. build upon these counter-measures by employing GAN techniques to train a behavior-based detection system to recognize malicious traffic that has been intentionally obfuscated to evade signature-based detection algorithms. This is a novel implementation that provides defensive capabilities against polymorphic attacks using the same techniques as hostile actors by training an ML model with an expansive description of all potential mutations of a particular malicious payload.

Long Short-Term Memory (LSTM) is another promising ML algorithm for intrusion detection. Alsaedi et al. [144] propose a novel framework for detection of malicious behavior in CPS environments through a framework that uses Deep Neural Networks (DNN) to train a ML model to recognize the expected behavior of a complex multi-sensor industrial network. LSTM is used to model temporal sequences from time-series sensor data to capture long-term dependencies and is combined with a novel method of applying different weighting values to focus on the most relevant characteristics in the complex dataset, which improves prediction accuracy by reducing noise in complex datasets.

Al-Shabi et al. [145] further build upon LSTM methods for anomaly detection in IIoT environments by adapting Recurrent Neural Networks (RNN), a subset of DNN that provides better performance and accuracy. The use of RNN combined with LSTM allows the ML model to preserve knowledge about previous iterations of time-series sensor data in the IIoT network, making the model more efficient than typical neural networks that assume each input and output are independent of previous iterations. Utilizing RNN to develop iterative predictions typically suffers from low accuracy due to increasing entropy through fading gradients, but Al-Shabi et al. propose a method to counter this shortcoming with LSTM in order to achieve high accuracy levels with significantly reduced computing time compared to other DNN models.

A frequently cited shortcoming of existing intrusion detection methods that leverage AI/ML is the difficulty in enabling the human operators of IIoT networks to understand the predictive decisions reached by AI-based IDS/IPS, which is crucial for industrial networks that require human intervention for operations with significant economic or life safety considerations. The nascent field of Explainable Artificial Intelligence (XAI) is beginning to see more research interest in IIoT environments.

Borcherding et al. [146] propose a novel method that differentiates linear and non-linear ML models, starting from the hypothesis that linear models are less likely to learn dependencies between features, and this difference can be determined through statistical analysis in order to further tune the ML models with optimized algorithms, specifically Logistic Regression (LR) and Support Vector Machine (SVM) for linear models, while non-linear models are further trained using Neural Networks (NN) and Random Forest (RF). This method is somewhat similar to ensemble learning through its application of multiple ML algorithms, with the appropriate algorithm dynamically selected based on the contents of the particular dataset.

Ha et al. [147] further develop strategies for leveraging XAI in IIoT environments by proposing an extension to existing One-Class Support Vector Machine (OCSVM) and LSTM algorithms that solve the human comprehension issue by integrating XAI into the model and generating human-readable explanations of predictive decisions reached by anomaly detection methods using OCSVM and LSTM. The integrated XAI modules interpret the ML predictions for the human operator of the CPS, reducing maintenance costs and accelerating decisions that require human intervention. The proposed model uses streaming sensor data to feed an LStM autoencoder, which is then further processed via OCSVM and simultaneously filtered through an XAI model that visualizes a human-readable explanation for any detected anomalies. LSTM is particularly effective when used with time-series data, which maps well to sensor data from an IIoT environment, but LSTM suffers from poor performance with large datasets. Ha et al. propose overcoming this limitation by streaming incoming sensor data through OCSVM, which is optimized for rapidly classifying data as normal or anomalous.

Huong et al. [148] focus on improving XAI through the use of federated learning, approaching the existing challenges as a Big Data problem with low-powered edge devices feeding a centralized model called FedEX (Federated learning-based Explainable Anomaly Detection for Industrial Control Systems). This allows geographically distributed IIoT environments to leverage the resource-constrained sensor nodes to collect data, which undergoes local pre-processing on a moderately powerful edge node, with those pre-processed readings then forwarded to a more powerful centralized host for further processing and model training based on data aggregated from all the distributed edge nodes of the highly distributed control system. This two-stage processing allows for rapid anomaly detections in isolated segments of the distributed ICS, which allows distant nodes in the highly distributed environment to eventually learn of localized zero-day attacks through federated learning. This two-stage process is essentially a trade-off between rapid detection and accuracy, optimized by the judicious placement of edge nodes that feed back to the centralized federated learning system.

4.4. Improving Anomaly Detection with Simulators/Testbeds

Within a conventional corporate computer network, it is customary to have both a production environment, which facilitates the operational functions of the organization, and a parallel dev/test environment, specifically designed for testing changes and upgrades. However, when it comes to Cyber-Physical Systems (CPS), the presence of dev/test environments is less prevalent. This is primarily due to the considerable costs and complexities associated with maintaining a parallel version of all the physical components within the CPS [228].

To meet this challenge, numerous simulation platforms [228–254] have been developed to enable researchers and practitioners to test various aspects of a CPS in a controlled, non-production environment. These platforms offer a solution that mitigates the significant economic costs and potential risks to life safety associated with testing on live systems.

Simulated CPS environments find common application in vulnerability assessments, involving activities such as input fuzzing, man-in-the-middle (MitM) attacks, Distributed Denial of Service (DDoS), False Data Injection (FDI), and more. Performing such activities directly on a live CPS could result in substantial financial and/or life-safety consequences, making simulated environments highly appealing for testing purposes [229]. Additionally, these simulated environments are frequently employed for non-disruptive user training, either through parallel virtualized CPS setups or through Augmented Reality/Virtual Reality (AR/VR) simulations.

Simulated or test environments are prevalent in software-only domains, primarily because server virtualization technologies allow cost-effective simulation of extensive networks and applications. However, when it comes to CPS environments, which consist of customized and distinct combinations of cyber and physical devices, the quest for a universal testbed or simulator has proven challenging. The multitude of hardware sensors and actuators available in the marketplace has contributed to the elusive nature of achieving a one-size-fits-all solution.

AL-Hawawreh and Sitnikova [230] take a unique approach, recognizing that the existing installed base of ICS has lifespans that measure into decades, so there are many ICS still in use that were originally deployed in an era prior to ubiquitous connectivity, when networks were much less hostile than they are today. This large installed base of critical infrastructure typically lacks any method of bolting on security functionality after the fact, resulting in a proposal for a generic end-to-end security testbed for ICS environments using legacy protocols with the objective of facilitating cybersecurity testing. A generalized prototype was used, allowing modular plug-ins for assorted sensors, actuators, and other control devices. To allow for interconnection between legacy ICS protocols and modern CPS environments, an IIoT edge gateway is used to translate non-routable legacy protocols into modern TCP/IP protocols with integrated encryption.

The RITICS (Research Institute in Trustworthy Inter-connected Cyber-physical Systems, London, UK) organization [231] is perhaps the leader in academic research in this area, a consortium of universities and industry partners that collaboratively develop simulators and testbeds for a broad range of CPS, with a focus on Industrial Control Networks (ICS) and their interactions with external corporate networks and the public internet.

RITICS has a particular focus on developing simulated environments with a high level of fidelity to the real-world system being emulated, as well as the repeatability and accuracy of test runs. This high degree of fidelity to the real-world counterpart leads to higher levels of confidence in the simulator as being reflective of the real world, which is often lacking in other implementations.

Craggs et al. [232] build on the research conducted at RITICS, proposing a reference architecture for IIoT/ICS testbeds with a focus on cybersecurity issues rather than the real-world fidelity focus of RITICS. The proposed reference architecture generally follows the Purdue model [233], classifying the different attack surfaces of the CPS based on the six different zones defined in the Purdue Reference Architecture [233], plus the addition of a new zone called the Experimental Zone, which is specific to testbed environments.

Waraga et al. [234] propose an extensible open source platform for automated identification of security issues in IoT/CPS, with the goals of accelerating time to market and rapid identification of security vulnerabilities by minimizing human intervention through automated security testing of the CPS using a testbed. The existing testbed implementations have limited scalability for vulnerability analysis, and this modular and automated testbed environment aims to allow researchers to add new test cases through a plug-in architecture. This does provide a novel method that allows other researchers to extend the platform functionality to include new IoT devices that appear on the market, but the platform is heavily slanted towards the cyber portion, and very little coverage is provided for the physical portion of the CPS. This makes the platform most appropriate for the detection of network-based attacks that seek to exploit protocol vulnerabilities, but it has very little coverage for physical vulnerabilities caused by False Command Injection (FCI) attacks that seek to exploit the physical components of a CPS.

To avoid the limitations inherent in the testbed proposed by Waraga, Ani et al. [235] propose a testbed framework with greater real-world fidelity by modeling the physical components of the CPS with emulated hardware. This approach provides researchers with greater confidence that their testbed environments will produce higher quality results, but increases the level of effort, expense, and expertise required to build the testbed environment. A significant challenge with building testbeds that include emulated or simulated physical components is the researcher's understanding of the behavior of the physical components at the edges of the operational thresholds, such as temperature, pressure, vibration, etc. Accurate modeling of edge-case behavior by emulated hardware is a significant design challenge and affects the real-world fidelity of the security testbed.

4.5. Anomaly Detection at the Network Edge

With the throughput of data communication networks and microprocessor speeds increasing exponentially over the past decades, it has become attractive to move certain functions to the network edge [255–274]. In decades past, early CPS were constrained [255] by the state of the art of microprocessor technology and network bandwidth, resulting in low-frequency, low-resolution data sampling from the sensors of the CPS. For example, a typical CPS in the 1990s may have only had sufficient processing power and network bandwidth to sample temperature and pressure sensors once every few minutes, while a modern system has sufficient processing power for continuous, real-time, high-resolution data sampling from sensors. Network throughput has also increased exponentially over the past few decades, but not nearly as quickly as improvements in microprocessor technology, so there is still a bottleneck in the collection of sensor data in a CPS. This bottleneck can be alleviated by pre-processing data at the network edge, close to where the sensor data is collected, and then sending a groomed or compressed subset of the data across the constrained network link, as illustrated in Figure 1.

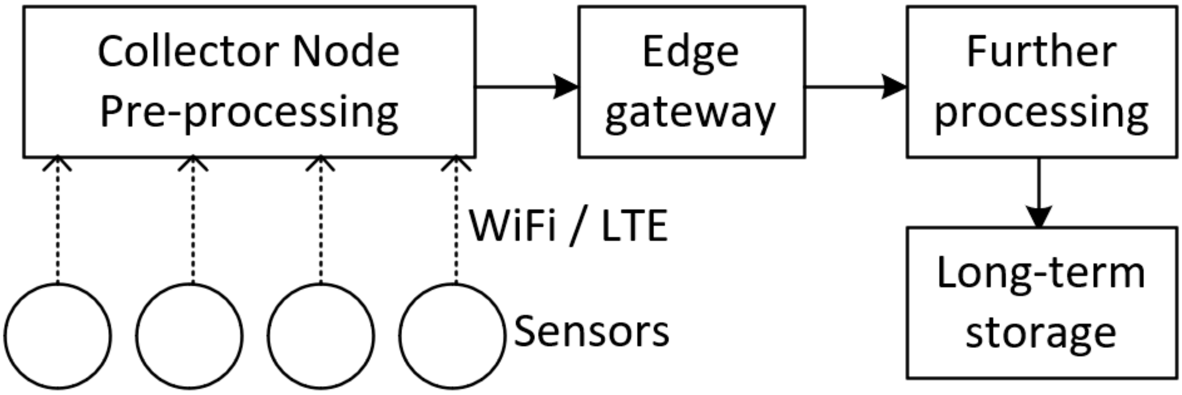

Figure 1. Pre-processing collected data at the network edge.

An et al. [256] propose a lightweight HTTP-based method of anomaly detection using a distributed architecture at the network edge. Rather than traditional signature-based malware detection techniques that use a centralized or choke-point scanner that looks for specific binary strings in the payload section of the TCP packet, the proposed framework uses a distributed scanning architecture at the network edge that ignores the payload section of the TCP packet and only scans the HTTP header information. This moves the detection logic up from the transport layer to the application layer of the TCP/IP networking model, based on the concept that higher layers of the TCP/IP networking model contain richer information. The proposed framework has performance advantages over the more traditional signature-based detection strategies, and its distributed model allows for multiple nodes to perform anomaly detection closer to the sensors and actuators in the CPS, relieving congestion on the network code by processing data closer to the edge. Classification and data pruning occur at the network edge, with the resource-constrained distributed edge nodes forwarding a digest version of the data to a more powerful system at the network core for ingestion into a machine learning model. This hybrid model of performing pre-processing at the resource-constrained network edge plus more detailed processing of aggregate data in the network core shows promise but is limited to the inspection of HTTP traffic. While HTTP is a commonly used protocol in IoT/CPS networks, it is by no means universal, and as lightweight protocols such as MQTT and MATTER specifically optimized for resource-constrained environments continue to gain popularity, HTTP usage in IoT/CPS networks is likely to diminish in the coming years, making this proposed framework somewhat limited. However, due to its modular architecture, a potential future use for this framework would be to add extensions for other protocols.

Recognizing the limitations of being restricted to a single protocol, Huong et al. [257] propose a more generalized framework for distributed anomaly detection at the network edge using a protocol agnostic approach. Similar to An et al., this framework concentrates on higher layers of the TCP/IP networking model, using a distributed cluster of nodes for anomaly detection, placed as close as possible to the data generated by the sensors and actuators of the CPS in order to minimize bandwidth requirements on the resource-constrained network edge. Time series data is aggregated and normalized on the distributed edge nodes and then forwarded to the network core for deeper analysis of the aggregated data from all the distributed nodes. This allows all of the resource-constrained edge nodes to benefit from the compute capacity available in the network core and uses a federated deep learning approach to perform anomaly detection. This anomaly detection method is behavior-based rather than signature-based, so it excels at the detection of previously unknown threats.

Wang et al. [258] propose the insertion of an edge computing platform between the sensors and data consumers of the CPS, with the edge devices acting as a broker between the incoming requests for sensor data and the sensors themselves. This allows inline IDS/IPS functionality to be performed on a more powerful device than the resource-constrained sensors, as well as load balancing and caching of incoming requests and resource availability.

Javed et al. [259] propose a middleware solution based on the microservices architecture popularized by container-based workloads running on cloud computing platforms such as Kubernetes. By inserting a microservices abstraction layer at the network edge, one layer upstream of the CPS sensors, the proprietary communication protocols frequently used by CPS can be translated or encapsulated into open TCP/IP protocols by the microservices layer. This also allows for normalization of incoming client requests, which simplifies anomaly detection by tightly controlling the format of the incoming requests based on a publish/subscribe data broker model. In addition to simplifying anomaly detection, the publish/subscribe model allows for more efficient use of the constrained network bandwidth and processing power available to the sensors by allowing aggregation at the network edge, allowing multiple clients to subscribe to the cached output of a single sensor at the microservices layer.

Das et al. [260] focus on real-time intrusion prevention of edge devices, starting with the rationale that the sensors and actuators in a CPS were designed to operate in harsh environmental conditions but have limited emphasis on resilience in the face of cyberattack. Das et al. propose a generic framework for detection and prevention of Denial of Service (DoS) attacks on Programmable Logic Controllers (PLC) through the use of a novel IPS running at the network edge between the resource-constrained PLC devices and potentially malicious traffic. Recognizing that the physical components of the ICS will typically lack sufficient processing power to perform local intrusion detection, the IPS functionality runs on an inline perimeter device that functions as a TCP proxy server, inspecting traffic destined for a PLC and making real-time decisions to pass or block the traffic. This proposed framework is highly effective in detecting DoS attacks but has limited efficacy in preventing more subtle false command injection or false data injection attacks, limiting its use case to a small subset of threats to CPS.

Eskandari et al. [261] build on the work of Das et al., employing the same edge-based inline IPS but extending the functionality to cover more than simple DoS attacks by training a ML model using the Isolation Forest (IF) and Local Outlier Factor (LOF) algorithms to learn the normal behavior of the CPS and effectively classify anomalous data for multiple attack types, including DoS, port scans, HTTP brute force, and SSH brute force. The proposed framework uses unsupervised learning to autonomously train the model with one-class classification techniques, which can be achieved with relatively low computational effort on moderately powered edge devices but suffers from low performance when scaled to large sensor networks and is still limited to rather rudimentary threshold-based measurements that may be more suited to a centralized SIEM that receives telemetry feeds from edge devices.

Tsukada et al. [262] further develop the concepts of on-device anomaly detection using edge devices with a semi-supervised learning model for anomaly detection using Backpropagation Neural Networks (BP-NN). The use of BP-NN allows for the normal distribution of data in the learning model to change over time as new data is streamed from the edge devices to the centralized IDS. Unlike the binary classification model in supervised learning algorithms, this semi-supervised learning algorithm trains the model with normal, non-anomalous data in order to learn the distribution of the data samples. Semi-supervised learning models often suffer if the distribution of normal data changes over time, a phenomenon referred to as “concept drift.” The time-series sensor data in IIoT environments will commonly experience distribution shifts due to environmental changes (i.e., seasonal variations in usage or power consumption), which can cause the accuracy of a trained model to become quickly obsolete. Tsukada et al. propose a method to overcome this problem via BP-NN, using relatively low-powered edge devices to perform lightweight inference computations while feeding data back to a more powerful centralized host for the more computationally intensive BP-NN calculations that iteratively update the ongoing distribution shifts of normal data. After each training loop of BP-NN calculations is performed on the powerful centralized host, the results are returned to the relatively low-powered edge devices, which use the updated learning model to perform lightweight anomaly detection calculations on-device. This approach allows the edge devices to make rapid decisions on real-time traffic while leveraging a centralized IDS to iteratively account for concept drift over time, maintaining a high level of accuracy with streaming time-series data.

Xu et al. [263] propose that rule-based or signature-based detection strategies are increasingly unable to scale to the rapid growth of IoT/IIoT devices, and ML approaches are required at the network edge. Edge gateways serve to acquire telemetry data from the end nodes, perform preliminary processing and aggregation, and then forward a pre-trained subset of the collected data to a centralized server for further processing. With the number of IoT devices growing faster than the increase in network speeds, performing robust pre-processing of data at the network edge becomes increasingly necessary to avoid overloading the communication bandwidth of the network. Xu et al. propose that as the computing power at the network edge increases due to advances in microprocessor power, it becomes increasingly feasible to shift more computational efforts in ML closer to the data collection points at the network edge. The proposed framework for intelligent edge computing leverages the increased processing power on edge devices to use an ensemble learning model to combine multiple ML algorithms in order to achieve higher accuracy than can be obtained from a single algorithm.

4.6. Trusted Systems vs. Zero-Trust Architecture

The field of CPS encompasses a wide range of applications, and within this domain, there exists a notable division between the conventional ICS environments employed for the control of industrial processes (now commonly known as IIoT) and the more consumer-focused IoT industry. This schism can be broadly defined as trusted systems vs. zero-trust [275–295] and affects the strategies used for anomaly detection.

Due to the extended product lifecycles spanning years or even decades [17] and the historical design assumptions of operating within fully trusted and air-gapped isolated environments, traditional ICS exhibit slower adoption of new technologies compared to their more flexible counterparts in consumer-focused Internet of Things (IoT) devices.

The consumer-focused IoT industry, unlike its IIoT-based counterparts, emerged during an era where ubiquitous connectivity to an increasingly hostile Internet was presumed. This environment drove the adoption of standardized communication protocols centered around TCP/IP, incorporating integrated authentication and encryption functionalities [78]. These protocols were specifically designed for lightweight messaging protocols, taking into account the limitations of devices with constrained processing power, limited battery life, and potentially inconsistent network connectivity.

Due to their long product lifecycles, there are many IIoT-based systems in use today that were originally designed with the assumption of an entirely isolated and trusted environment, meaning that network security was not a design consideration [10]. Those systems have adapted poorly to industry pressures for connectivity and interoperability with corporate networks and the public Internet, with varying levels of success in adding security functionality to a system not designed with security in mind.

When it comes to security design in ICS and IIoT, the predominant focus has traditionally been on implementing a robust perimeter firewall to protect the CPS from other potentially hostile networks. However, once inside the trusted network, there is limited protection, resembling the “hard shell, soft center” security posture observed in enterprise networks in the past [275]. The historical assumptions of an entirely trusted environment have resulted in significant resistance to the active deployment of IPS in CPS, primarily due to the high costs associated with false positives. While passive IDS are gaining acceptance in CPS, the extreme heterogeneity [143] poses a challenge, leading to false positives that make it difficult for CPS operators to distinguish genuine hostile network activity.

The more contemporary consumer-focused IoT industry has embraced a zero-trust model of information security. Recognizing the potentially hostile network environment they operate in, they prioritize incorporating strong authentication and encryption protocols by default [18]. Unfortunately, the rapid pace of IoT advancements means that product lifecycles are notably short, resulting in devices quickly becoming obsolete. This leaves numerous devices "orphaned" without ongoing vendor support or upgrades to address emerging security threats. While some vendors have implemented trusted over-the-air update functionality to counter newly discovered threats, there are still many IoT devices that lack any form of update capability, rendering them permanently vulnerable to emerging threats.

The net effect is that the more modern IoT environments have integrated functionality for telemetry and health monitoring that is designed to feed into Security Information and Event Management (SIEM) systems for anomaly detection, while the longer-lived legacy ICS environments have been forced to bolt on this functionality.

Perez et al. [144] explore the ramifications of continued use of legacy protocols that were designed in the era of fully air-gapped CPS environments and how they can be securely operated in the age of ubiquitous connectivity. Many risks can be mitigated through network segmentation, as described by the Purdue model [233], but the continued use of legacy protocols that operate without encryption or replay resistance against false data injection attacks will leave CPS vulnerable to exploitation. Perez et al. propose a machine learning model that ingests network traffic flow data to and from the sensors and actuators in the CPS to build a model of normal behavior without needing to communicate directly with the legacy devices themselves or even understand the proprietary communication protocols. By using traffic flow patterns as the basis of the machine learning model, anomaly detection is achieved using a behavior-based strategy rather than the more common signature-based detection techniques used by traditional IDS/IPS.

Szymanski [276] proposes a novel method for protecting CPS by using Software Defined Networking (SDN) to create deterministic data flows between the components in a CPS, with any deviation classified as an anomaly. Network communications between nodes have traditionally been considered non-deterministic, as Ethernet-based communications using a shared communication medium may need to wait until the channel is free to send data, and complex networks such as the Internet use dynamic routing protocols that can change based on network conditions. Szymanski proposes the use of Quantum Safe encryption to allow the SDN to embed millions of isolated Deterministic Virtual Private Networks (DVPNs) to hide the underlying complexities of the network from the CPS endpoint nodes, making each path between nodes deterministic. This proposed method is most useful for distributed CPS environments that use untrusted networks such as the Internet, but has limited value for physically airgapped environments that make use of more traditional network security models such as default deny.

Ameer et al. [277] propose a combination of Zero Trust (ZT) architecture with the 3-layer PEI (Policy, Enforcement, Implementation) model for providing access control and authentication for users and devices in IoT/CPS environments. Similar to the manner in which anti-spam filters use scoring to determine if a message is legitimate or not, the proposed model assigns scores to endpoint devices that are based on formally provable mathematical models defined by the PEI. By enforcing continuous mutual authentication along with end-to-end encryption, ZT can ensure that any unauthorized access attempts are automatically denied and flagged as anomalies for further investigation. Anomalies are detected by the score of a particular data flow, which uses a combination of RBAC (Role Based Access Control), MAC (Mandatory Access Control), location, time, and any other characteristics defined in the PEI. This avoids the shortcomings of the more traditional

DAC (Discretionary Access Control) security models and avoids privilege abuse or lateral compromise through the use of continuous mutual authentication.

Federici et al. [278] focus on secure remote access to IIoT environments by implementing a ZT architecture to avoid the perimeter-based security approach that is common in CPS, which assumes all traffic that has been passed through the border firewall can be considered trusted. As modern CPS environments make greater use of collaboration and data exchange with other systems, this perimeter-based security model becomes less useful in protecting against threats of lateral compromise. This work builds on the NIST reference architecture [279] for ZT by proposing a dual-layered access control architecture that leverages a Policy Engine (PE) to automate the creation of rules to allow or deny remote connection requests. This methodology leverages recent developments in Edge Computing, using the concept of an Industrial Gateway as a policy enforcement point that makes authentication decisions, coupled with a resource mediator that makes more detailed access control decisions for each read or write request in the data stream. By dividing authentication and authorization into separate layers, this proposed ZT architecture simplifies some of the complexity of more monolithic architectures, making it easier to secure the overall environment.

Alshomrani and Li [280] propose a novel method for performing continuous authentication of endpoint devices in IoT environments, with the intent of avoiding device impersonation attacks such as address spoofing and false command injection. The proposed model uses physical unclonable function-based device continuous authentication (PUFDCA), which leverages device fingerprinting based on immutable hardware characteristics combined with network path details and WiFi signal characteristics to add location definitions to the device signature. These PUFDCA fingerprints are then used for continuous mutual authentication, which mitigates replay and MiTM attacks. This authentication protocol uses SHA-3 hash functions, which are lightweight enough for the resource-constrained devices typically found in CPS environments while sufficiently strong to resist brute-force decryption attempts.

5. Discussion of Selected Challenges

The field of CPS is still quite young, with the term first defined in 2006 by the US-based National Science Foundation [13]. CPS has grown in leaps and bounds over the past few decades, largely mirroring advancements in microprocessor technology and the increased availability of high-speed wired and wireless networks. Due to the rapid rate of change, CPS has a number of outstanding challenges, a selection of which are described below.

A present-day CPS can be viewed as a fusion of IT and legacy OT environments, each with distinct priorities. Traditional IT networks adhere to the C-I-A (Confidentiality, Integrity, Availability) triad to define their security posture, prioritizing confidentiality, integrity, and availability in that order. Confidentiality ensures that data is only made available to authorized parties and is not available to anyone else. This is closely linked with the principle of least privilege, which provides the lowest amount of access (none, read-only, or read-write) in order to meet organizational requirements. Integrity means that the data has not been modified (intentionally or unintentionally) during transmission (i.e., using checksums) or in storage (i.e., using referential integrity checks). Availability means that the data is accessible when needed and is resilient against environmental issues such as computer hardware or network failure, power interruption, cyberattack, etc.

In contrast, OT networks have priorities that are the exact reverse of IT networks and follow an A-I-C (Availability, Integrity, and Confidentiality) approach [19,60]. Availability takes precedence, followed by integrity, with confidentiality considered the least significant pillar of system security. This distinction arises from CPS evolving from earlier ICS networks used in industrial control processes, where ensuring availability was paramount and integrity and confidentiality were rarely prioritized due to trusted and air-gapped isolated network environments. The emphasis on availability stems from the potential consequences of its loss, including economic impact and life safety concerns.

As OT networks merged with IT networks to form modern CPS, the divergent priorities have posed ongoing challenges that remain unresolved. IT networks place significant emphasis on authentication and authorization, which correspond to the confidentiality and integrity facets of the CIA triad. In contrast, OT networks traditionally focused so heavily on availability that authentication and authorization were assumed based on physical access to the trusted and isolated OT network.

However, this historical assumption of a fully trusted and isolated environment no longer holds true with the interconnection of IT and OT networks, making CPS vulnerable to network-based attacks such as DDoS, Man-in-the-Middle (MitM), replay attacks, impersonation, spoofing, and false data injection. Compounding the issue, OT networks often lack integration with anti-malware programs and detailed logging capabilities, hampering the detection of potentially hostile activity [81].

Efforts are underway to extend the Intrusion Detection System/Intrusion Prevention System (IDS/IPS) capabilities of IT networks into OT networks, but the absence of standardized protocols and interfaces for the physical components of CPS poses significant challenges for threat detection. IDS/IPS systems that have been extended into CPS environments struggle with high levels of false positives and false negatives due to the inherent complexity of CPS.

The most prominent challenge in secure CPS design and operation stems from the lack of standardized communication protocols and the proprietary nature of these systems [50]. Without a clear industry consensus on the system development life cycle of CPS, each system designer essentially builds a new CPS from scratch, often neglecting considerations for multivendor interoperability, secure patching mechanisms, or consistent system telemetry for health and security monitoring. While progress is being made through industry consortiums like O-PAS (Open Process Automation Standard) [296], achieving broad industry consensus remains elusive.

The high levels of heterogeneity found in CPS offer a plethora of research possibilities. However, the absence of a shared design framework [20] or standardized communication protocols poses challenges in effectively utilizing prior research and industry knowledge to advance the current state of the art. In simpler terms, the pervasive heterogeneity often necessitates “reinventing the wheel,” leading to duplicated efforts across academia and industry. This redundancy in work hampers progress within the field and slows down advancements.

The unique and bespoke characteristics of CPS products stem from their historical development based on ICS, which were originally designed to function within closed networks without the need for interoperability or communication with external networks. As the realms of OT and IT converged to form CPS, the open standards and communication protocols prevalent in IT networks have been swiftly embraced by OT networks [19]. However, considerable room for enhancement remains, particularly for OT networks that have unexpectedly found themselves interconnected with public and untrusted networks, including the Internet.

Recognizing that proprietary and heterogenous communication protocols are a barrier to effective anomaly detection as well as the effective development of industry best practices for CPS security postures, the O-PAS (Open Process Automation Standard) [260] is an industry consortium that is attempting to standardize the wide range of proprietary CPS into a set of open and collaborative standards around communication protocols and security postures, with the goal of increasing efficiency through multivendor interoperability. By achieving broad consensus within the open industry consortium, a particular CPS can be designed to meet the O-PAS standard, which allows for standardized methods of threat detection, health monitoring, and the use of standardized security methods. By designing a CPS to support open standards, significant benefits can be gained through the accelerated product development lifecycle thanks to the reliance on pre-existing standards, as well as ongoing efficiencies throughout the lifecycle of the CPS.

The use of IDS/IPS for anomaly detection is well established in IT networks but still suffers from excessive false positives in OT networks, which hinders their adoption in CPS. The use of machine learning models for anomaly detection shows promise but also suffers from excessive false positives due to the challenges of precisely defining abnormal behavior. Additionally, challenges in obtaining sufficiently representative data for the learning model can make the detection algorithm opaque and unpredictable to the human operators of the CPS, resulting in low confidence in the IDS alerts. Mahbooba et al. [145] propose a method of using Explainable Artificial Intelligence (XAI) to improve the accuracy of anomaly detection in IDS by bringing the human operator of the CPS into the loop by providing a human-readable explanation of why an IDS alert was generated, allowing the human operator to accept or reject the anomaly detection. The human-in-the-loop decisions are fed back into the learning model, leading to improved accuracy over time as well as increased confidence levels from the human operators of the CPS.

6. Conclusions and Future Works

The automated detection of anomalies and/or threats to CPS is still a field in a rapid state of development due to multiple confounding factors, the most significant of which are outlined below.

Many CPSs grew out of legacy SCADA and ICS networks, which assumed operation in an isolated and fully trusted network. The current reality of ubiquitous connectivity to increasingly hostile networks is only grudgingly accepted by many CPS network operators, who still see additional security requirements as an impediment to system availability.

Due to their extreme diversity, there is no one-size-fits-all anomaly detection model that can be generalized. Many researchers have proposed a generic or universal framework for anomaly detection in CPS, but as detection methods increase in generality to aid rapid test case development, they necessarily reduce in real-world fidelity, making them less representative of the live CPS. The reverse is also true: as anomaly detection accuracy for a real-world CPS increases, its generic applicability to other CPS environments decreases. The optimal solution seems to be a low-level generic framework with a modular architecture that allows plugins to be developed for the unique characteristics of a particular CPS.

CPS are typically not built with observability as a design feature. Gathering telemetry data is frequently an afterthought, if it is considered at all. This lack of observability makes it challenging to detect anomalies since a good baseline dataset is often unavailable. This is particularly challenging for AI researchers, as the quality of training data for ML is frequently lacking.

Signature-based detection (i.e., traditional antivirus) is less effective in CPS than in traditional enterprise networks due to the lack of standardization, i.e., heterogeneous sensors, different actuators, and various communication protocols.

Behavior-based detection methods (i.e., heuristic analysis, AI/ML) are less effective because CPS have highly variable (i.e., unpredictable) behavior (i.e., power grid fluctuations vary widely due to randomized events such as scheduled/unscheduled maintenance, weather events, etc.).

Threshold-based detection (i.e., power grid usage outside of “acceptable” thresholds). This is effectively a subset of behavior-based analysis, with the system operator deciding what the acceptable range of inputs/outputs should be. Unfortunately, accurately determining what those thresholds should be has proven elusive, especially because CPS tend to be dynamic, with regular changes throughout the system life cycle.

Future directions and opportunities for further research include embedding telemetry functionality at the design stage of CPS, which will provide higher quality baseline data, which is vital for AI-based models to accurately detect anomalous activity.

For low-power sensor devices with constrained CPU/battery/bandwidth resources, embedding resource-intensive intrusion detection functionality may be impractical. Consider moving IDS/IPS functionality up one level to the network layer (i.e., throttle access at the network perimeter to prevent DDoS attacks, use behavior-based traffic analysis on the upstream firewall, etc.).

There are recent enhancements in IDS/IPS (i.e., Cisco Talos cloud-based threat intelligence) designed for use in enterprise networks that can be adapted to CPS. These IDS/IPS leverage the use of network flow data gathered from the network edge, with resource-intensive data mining and intrusion detection performed outside of the resource-constrained CPS.

A particularly promising area of research is the development of a hybrid model for anomaly detection that includes threshold-based anomaly detection for simple threats such as brute force password attacks or temperature extremes, signature-based detection for known threats, and behavior-based detection for unknown threats. Behavior-based detection is the most difficult to perform with high accuracy, but there are promising options for using AI/ML to increase accuracy over time.

Author Contributions: Conceptualization, N.J., Q.T. and J.R.V.; methodology, N.J., Q.T. and J.R.V.; software, N.J., Q.T. and J.R.V.; validation, N.J., Q.T. and J.R.V.; formal analysis, N.J., Q.T. and J.R.V.; investigation, N.J., Q.T. and J.R.V.; resources, N.J., Q.T. and J.R.V.; data curation, N.J., Q.T. and J.R.V.; writing—original draft preparation, N.J.; writing—review and editing, N.J.; visualization, N.J.; supervision, Q.T. and J.R.V.; project administration, Q.T. and J.R.V.; funding acquisition, Q.T. and J.R.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by Principado de Asturias (grant SV-PA-21-AYUD/2021/50994), Missions Science and Innovation project (MIG-20211008 INMERBOT), SUDOE Interreg Program (grant INUNDATIO), the Spanish Research Agency (RED2018-102312-T IA-Biomed), the Ministry of Science and Innovation under (CERVERA Excellence Network project CER-20211003), and the Spanish Ministry of Economics and Industry (grant PID2020-112726RB-I00).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

Abbreviations and Acronyms

AI	Artificial Intelligence
APT	Advanced Persistent Threat
AR	Augmented Reality
BP-NN	Back Propagation Neural Networks
CIA	Confidentiality, Integrity, Availability
CNN	Convolutional Neural Network
CPS	Cyber-Physical System
CPU	Central Processing Unit
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DoS	Denial of Service
DNN	Deep Neural Network
FCI	False Command Injection
FDI	False Data Injection
GAN	Generative Adversarial Network
ICS	Industrial Control System
IDS	Intrusion Detection System
IF	Isolation Forest
IPS	Intrusion Prevention System
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
LOF	Local Outlier Factor
LR	Logistic Regression
LSTM	Long Short Term Memory

MitM	Man in the Middle
ML	Machine Learning
MQTT	Message Queue Telemetry Transport
NN	Neural Network
OCSVM	One Class Support Vector Machine
O-PAS	Open Process Automation Standard
OT	Operational Technology
PLC	Programmable Logic Controller
RBAC	Role Based Access Control
RF	Random Forest
RNN	Recurrent Neural Network
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information Event Management
SVM	Support Vector Machine
VR	Virtual Reality
XAI	eXplainable Artificial Intelligence
ZT	Zero Trust

References

1. Bansal, S.; Kumar, D. IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 340–364. [CrossRef]
2. Serpanos, D. The Cyber-Physical Systems Revolution. *Computer* **2018**, *51*, 70–73. [CrossRef]
3. Langner, R. To kill a centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. 2013. Available online: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf (accessed on 15 October 2022).
4. Alhaidari, F.A.; Al-Dahasi, E.M. New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–6. [CrossRef]
5. Hewage, C. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. *Eng. Technol. Open Access J.* **2021**, *3*, 555622. [CrossRef]
6. Pivoto, D.G.S.; de Almeida, L.F.F.; Da Rosa Righi, R.; Rodrigues, J.J.P.C.; 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. [CrossRef]
7. Agrawal, N.; Kumar, R. Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-wide Survey. *ISA Trans.* **2022**, *130*, 10–24. [CrossRef]
8. Qassim, Q.S.; Jamil, N.; Mahdi, M.N.; Rahim, A.A.A. Towards SCADA Threat Intelligence based on Intrusion Detection Systems—A Short Review. In Proceedings of the 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Selangor, Malaysia, 24–26 August 2020; pp. 144–149. [CrossRef]
9. Amin, M.; El-Sousy, F.F.M.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. *IEEE Access* **2021**, *9*, 38571–38601. [CrossRef]
10. Wolf, M.; Serpanos, D. *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*; Springer International Publishing: Cham, Switzerland, 2020. [CrossRef]
11. Tian, J.; Tan, R.; Guan, X.; Xu, Z.; Liu, T. Moving Target Defense Approach to Detecting Stuxnet-Like Attacks. *IEEE Trans. Smart Grid* **2019**, *11*, 291–300. [CrossRef]
12. Murray, G.; Peacock, M.; Rabadia, P.; Kerai, P. Detection techniques in operational technology infrastructure. In Proceedings of the Australian Information Security Management Conference, Perth, Australia, 29–31 May 2018. [CrossRef]
13. National Science Foundation. "Cyber-Physical Systems", National Science Foundation. 2020. Available online: https://www.nsf.gov/pubs/2021/nsf21551/nsf21551.htm (accessed on 15 October 2022).
14. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *J. Intell. Manuf.* **2017**, *30*, 1111–1123. [CrossRef]
15. Kabiri, P.; Chavoshi, M. Destructive Attacks Detection and Response System for Physical Devices in Cyber-Physical Systems. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; pp. 1–6. [CrossRef]
16. Etalle, S. Network Monitoring of Industrial Control Systems. In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy—CPS-SPC'19, London, UK, 11 November 2019; p. 1. [CrossRef]
17. Altunay, H.C.; Albayrak, Z.; Ozalp, A.N.; Cakmak, M. Analysis of Anomaly Detection Approaches Performed Through Deep Learning Methods in SCADA Systems. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021; pp. 1–6. [CrossRef]

18. Rubio, J.E.; Alcaraz, C.; Roman, R.; Lopez, J. Current cyber-defense trends in industrial control systems. *Comput. Secur.* **2019**, *87*, 101561. [CrossRef]
19. Yugha, R.; Chithra, S. A survey on technologies and security protocols: Reference for future generation IoT. *J. Netw. Comput. Appl.* **2020**, *169*, 102763. [CrossRef]
20. Kabore, R.; Kouassi, A.; N'goran, R.; Asseu, O.; Kermarrec, Y.; Lenca, P. Review of Anomaly Detection Systems in Industrial Control Systems Using Deep Feature Learning Approach. *Engineering* **2021**, *13*, 30–44. [CrossRef]
21. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
22. Ahanger, T.A.; Aljumah, A.; Atiquzzaman, M. State-of-the-art survey of artificial intelligent techniques for IoT security. *Comput. Netw.* **2022**, *206*, 108771. [CrossRef]
23. Al-Turjman, F.; Abujubbeh, M.; Malekloo, A.; Mostarda, L. UAVs assessment in software-defined IoT networks: An overview. *Comput. Commun.* **2019**, *150*, 519–536. [CrossRef]
24. Alrefaei, F. The Importance Of Security In Cyber-Physical System. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–3. [CrossRef]
25. Alrefaei, F.; Alzahrani, A.; Song, H.; Zohdy, M. Security of Cyber Physical Systems: Vulnerabilities, Attacks and Countermeasure. In Proceedings of the 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Vancouver, BC, Canada, 9–12 September 2020; pp. 1–6. [CrossRef]
26. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
27. Cherdantseva, Y.; Burnap, P.; Nadjm-Tehrani, S.; Jones, K. A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment. *Appl. Sci.* **2022**, *12*, 4880. [CrossRef]
28. Dafflon, B.; Moalla, N.; Ouzrout, Y. The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review. *Int. J. Adv. Manuf. Technol.* **2021**, *113*, 2395–2412. [CrossRef]
29. Dupont, G.; Hartog, J.D.; Etalle, S.; Lekidis, A. A survey of network intrusion detection systems for controller area network. In Proceedings of the 2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Cairo, Egypt, 4–6 September 2019; pp. 1–6. [CrossRef]
30. Elbez, G.; Keller, H.B.; Hagenmeyer, V. A New Classification of Attacks against the Cyber-Physical Security of Smart Grids. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018. [CrossRef]
31. Gressl, L.; Krisper, M.; Steger, C.; Neffe, U. Towards Security Attack and Risk Assessment during Early System Design. In Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 15–19 June 2020; pp. 1–8. [CrossRef]
32. Hartsell, C.; Mahadevan, N.; Nine, H.; Bapty, T.; Dubey, A.; Karsai, G. Workflow Automation for Cyber Physical System Development Processes. In Proceedings of the 2020 IEEE Workshop on Design Automation for CPS and IoT (DESTION), Sydney, Australia, 21 April 2020; pp. 1–9. [CrossRef]
33. Jeffrey, N.; Tan, Q.; Villar, J.R. Anomaly Detection of Security Threats to Cyber-Physical Systems: A Study. In Proceedings of the 17th International Conference on Soft Computing Models in Industrial and Environmental Applications, Salamanca, Spain, 12 October 2022; pp. 3–12. [CrossRef]
34. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wirel. Netw.* **2021**, *27*, 2595–2613. [CrossRef]
35. Sicato, J.C.S.; Singh, S.K.; Rathore, S.; Park, J.H. A Comprehensive Analyses of Intrusion Detection System for IoT Environment. *J. Inf. Process. Syst.* **2020**, *16*, 975–990. [CrossRef]
36. Jurcut, A.; Niculcea, T.; Ranaweera, P.; Le-Khac, N.-A. Security Considerations for Internet of Things: A Survey. *SN Comput. Sci.* **2020**, *1*, 193. [CrossRef]
37. Kelli, V.; Radoglou-Grammatikis, P.; Lagkas, T.; Markakis, E.K.; Sarigiannidis, P. Risk Analysis of DNP3 Attacks. In Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 27–29 July 2022; pp. 351–356. [CrossRef]
38. Ketu, S.; Mishra, P.K. Internet of Healthcare Things: A contemporary survey. *J. Netw. Comput. Appl.* **2021**, *192*, 103179. [CrossRef]
39. Kumar, V.; Jha, R.K.; Jain, S. NB-IoT Security: A Survey. *Wirel. Pers. Commun.* **2020**, *113*, 2661–2708. [CrossRef]
40. Luo, B.; Beuran, R.; Tan, Y. Smart Grid Security: Attack Modeling from a CPS Perspective. In Proceedings of the 2020 IEEE Computing, Communications and IoT Applications (ComComAp), Beijing, China, 20-22 December 2020; pp. 1–6. [CrossRef]
41. Lv, Z.; Han, Y.; Singh, A.K.; Manogaran, G.; Lv, H. Trustworthiness in Industrial IoT Systems Based on Artificial Intelligence. *IEEE Trans. Ind. Inform.* **2020**, *17*, 1496–1504. [CrossRef]
42. Mahboub, S.A.; Ahmed, E.S.A.; Saeed, R.A. Smart IDS and IPS for Cyber-Physical Systems. In *Advances in Systems Analysis, Software Engineering, and High Performance Computing*; Luhach, A.K., Elçi, A., Eds.; IGI Global: Hershey, PA, USA, 2021; pp. 109–136. [CrossRef]
43. Mahbub, M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *J. Netw. Comput. Appl.* **2020**, *168*, 102761. [CrossRef]

44. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
45. Mousavi, S.K.; Ghaffari, A.; Besharat, S.; Afshari, H. Security of internet of things based on cryptographic algorithms: A survey. *Wirel. Netw.* **2021**, *27*, 1515–1555. [CrossRef]
46. Oztemel, E.; Gursev, S. Literature review of Industry 4.0 and related technologies. *J. Intell. Manuf.* **2018**, *31*, 127–182. [CrossRef]
47. Panoff, M.; Dutta, R.G.; Hu, Y.; Yang, K.; Jin, Y. On Sensor Security in the Era of IoT and CPS. *SN Comput. Sci.* **2021**, *2*, 51. [CrossRef]
48. Peng, H.; Liu, C.; Zhao, D.; Ye, H.; Fang, Z.; Wang, W. Security Analysis of CPS Systems Under Different Swapping Strategies in IoT Environments. *IEEE Access* **2020**, *8*, 63567–63576. [CrossRef]
49. Radanliev, P.; De Roure, D.C.; Nurse, J.R.C.; Montalvo, R.M.; Cannady, S.; Santos, O.; Maddox, L.; Burnap, P.; Maple, C. Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Appl. Sci.* **2020**, *2*, 169. [CrossRef]
50. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
51. Raj, A.; Shetty, S.D. IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey. *Wirel. Pers. Commun.* **2021**, *122*, 1481–1517. [CrossRef]
52. Rao, P.M.; Deebak, B.D. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *J. Ambient. Intell. Humaniz. Comput.* **2022**, *14*, 10517–10553. [CrossRef]
53. Rasool, R.U.; Ahmad, H.F.; Rafique, W.; Qayyum, A.; Qadir, J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *J. Netw. Comput. Appl.* **2022**, *201*, 103332. [CrossRef]
54. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [CrossRef]
55. Sicato, J.C.S.; Sharma, P.K.; Loia, V.; Park, J.H. VPNFilter Malware Analysis on Cyber Threat in Smart Home Network. *Appl. Sci.* **2019**, *9*, 2763. [CrossRef]
56. Estay, D.A.S.; Sahay, R.; Barfod, M.B.; Jensen, C.D. A systematic review of cyber-resilience assessment frameworks. *Comput. Secur.* **2020**, *97*, 101996. [CrossRef]
57. Sgueglia, A.; Di Sorbo, A.; Visaggio, C.A.; Canfora, G. A systematic literature review of IoT time series anomaly detection solutions. *Futur. Gener. Comput. Syst.* **2022**, *134*, 170–186. [CrossRef]
58. Singh, V.K.; Ebrahem, H.; Govindarasu, M. Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment. In Proceedings of the 2018 North American Power Symposium (NAPS), Fargo, ND, USA, 9–11 September 2018; pp. 1–6. [CrossRef]
59. Snehi, M.; Bhandari, A. Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. *Comput. Sci. Rev.* **2021**, *40*, 100371. [CrossRef]
60. Stojanović, B.; Hofer-Schmitz, K.; Kleb, U. APT datasets and attack modeling for automated detection methods: A review. *Comput. Secur.* **2020**, *92*, 101734. [CrossRef]
61. Sudarsan, S.V.; Schelen, O.; Bodin, U. Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT. *IEEE Access* **2021**, *9*, 98169–98184. [CrossRef]
62. Syed, N.F.; Shah, S.W.; Trujillo-Rasua, R.; Doss, R. Traceability in supply chains: A Cyber security analysis. *Comput. Secur.* **2021**, *112*, 102536. [CrossRef]
63. Trcek, D. Mollitia: Toward Standardization of Resilience Provisioning in IoT/CPS Structures. *IEEE Internet Things Mag.* **2021**, *4*, 109–113. [CrossRef]
64. Tripathi, D.; Biswas, A.; Tripathi, A.K.; Singh, L.K.; Chaturvedi, A. An integrated approach of designing functionality with security for distributed cyber-physical systems. *J. Supercomput.* **2022**, *78*, 14813–14845. [CrossRef]
65. Werth, A.; Morris, T.H. A Specification-Based Intrusion Prevention System for Malicious Payloads. In *National Cyber Summit (NCS) Research Track*; Choo, K.-K.R., Morris, T.H., Peterson, G.L., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 1055, pp. 153–168. [CrossRef]
66. Wu, M.; Moon, Y.B. Intrusion Detection of Cyber-Physical Attacks in Manufacturing Systems: A Review. In Proceedings of the Volume 2B: Advanced Manufacturing, Salt Lake City, UT, USA, 11–14 November 2019; p. V02BT02A001. [CrossRef]
67. Yaacoub, J.-P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef]
68. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433. [CrossRef]
69. Yaici, W.; Krishnamurthy, K.; Entchev, E.; Longo, M. Internet of Things for Power and Energy Systems Applications in Buildings: An Overview. In Proceedings of the 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Madrid, Spain, 9–12 June 2020; pp. 1–6. [CrossRef]
70. Yousefnezhad, N.; Malhi, A.; Främling, K. Security in product lifecycle of IoT devices: A survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102779. [CrossRef]
71. Zhang, Y. A Systematic Security Design Approach for Heterogeneous Embedded Systems. In Proceedings of the 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE), Kyoto, Japan, 12–15 October 2021; pp. 500–502. [CrossRef]

72. Zhou, L.; Guo, H. Anomaly Detection Methods for IIoT Networks. In Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 31 July–2 August 2018; pp. 214–219. [CrossRef]
73. Huang, L.; Zhu, Q. A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. *Comput. Secur.* **2019**, *89*, 101660. [CrossRef]
74. Seng, S.; Garcia-Alfaro, J.; Laarouchi, Y. Why Anomaly-Based Intrusion Detection Systems Have Not Yet Conquered the Industrial Market? In *Foundations and Practice of Security*; Aïmeur, E., Laurent, M., Yaich, R., Dupont, B., Garcia-Alfaro, J., Eds.; Springer International Publishing: Cham, Switzerland, 2022; Volume 13291, pp. 341–354. [CrossRef]
75. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 18. [CrossRef]
76. Vasan, D.; Alazab, M.; Venkatraman, S.; Akram, J.; Qin, Z. MTHAEL: Cross-Architecture IoT Malware Detection Based on Neural Network Advanced Ensemble Learning. *IEEE Trans. Comput.* **2020**, *69*, 1654–1667. [CrossRef]
77. Abid, A.; Jemili, F.; Korbaa, O. Distributed Architecture of an Intrusion Detection System in Industrial Control Systems. In *Advances in Computational Collective Intelligence*; Bădică, C., Treur, J., Benslimane, D., Hnatkowska, B., Krótkiewicz, M., Eds.; Springer International Publishing: Cham, Switzerland, 2022; Volume 1653, pp. 472–484. [CrossRef]
78. Bai, Y.; Park, J.; Tehranipoor, M.; Forte, D. Real-time instruction-level verification of remote IoT/CPS devices via side channels. *Discov. Internet Things* **2022**, *2*, 1. [CrossRef]
79. Chavez, A.; Lai, C.; Jacobs, N.; Hossain-McKenzie, S.; Jones, C.B.; Johnson, J.; Summers, A. Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 29 April–1 May 2019; pp. 1–6. [CrossRef]
80. Gu, H.; Lai, Y.; Wang, Y.; Liu, J.; Sun, M.; Mao, B. DEIDS: A novel intrusion detection system for industrial control systems. *Neural Comput. Appl.* **2022**, *34*, 9793–9811. [CrossRef]
81. Rakas, S.V.B.; Stojanovic, M.D.; Markovic-Petrovic, J.D. A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 93083–93108. [CrossRef]
82. Ravikumar, G.; Singh, A.; Babu, J.R.; A, A.M.; Govindarasu, M. D-IDS for Cyber-Physical DER Modbus System—Architecture, Modeling, Testbed-based Evaluation. In Proceedings of the 2020 Resilience Week (RWS), Salt Lake City, ID, USA, 19–23 October 2020; pp. 153–159. [CrossRef]
83. Sheng, C.; Yao, Y.; Fu, Q.; Yang, W. A cyber-physical model for SCADA system and its intrusion detection. *Comput. Netw.* **2020**, *185*, 107677. [CrossRef]
84. Hwang, C.; Lee, T. E-SFD: Explainable Sensor Fault Detection in the ICS Anomaly Detection System. *IEEE Access* **2021**, *9*, 140470–140486. [CrossRef]
85. Chromik, J.J.; Remke, A.; Haverkort, B.R. Bro in SCADA: Dynamic intrusion detection policies based on a system model. In Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018, Hambug, Germany, 29–30 August 2018. [CrossRef]
86. Adil, M.; Jan, M.A.; Mastorakis, S.; Song, H.; Jadoon, M.M.; Abbas, S.; Farouk, A. Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber–Physical Systems. *IEEE Internet Things J.* **2021**, *9*, 22173–22183. [CrossRef]
87. Al-Ghamdi, M.I. WITHDRAWN: Effects of knowledge of cyber security on prevention of attacks. *Mater. Today Proc.* **2021**, *2021*, S2214785321029941. [CrossRef]
88. Alam Majumder, A.J.; Veilleux, C.B.; Miller, J.D. A Cyber-Physical System to Detect IoT Security Threats of a Smart Home Heterogeneous Wireless Sensor Node. *IEEE Access* **2020**, *8*, 205989–206002. [CrossRef]
89. Alipour-Fanid, A.; Dabaghchian, M.; Wang, N.; Jiao, L.; Zeng, K. Online-Learning-Based Defense Against Jamming Attacks in Multichannel Wireless CPS. *IEEE Internet Things J.* **2021**, *8*, 13278–13290. [CrossRef]
90. Alrefaei, F.; Alzahrani, A.; Song, H.; Zohdy, M.; Alrefaei, S. Cyber Physical Systems, a New Challenge and Security Issue for the Aviation. In Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021; pp. 1–5. [CrossRef]
91. Barrere, M.; Hankin, C.; Barboni, A.; Zizzo, G.; Boem, F.; Maffeis, S.; Parisini, T. CPS-MT: A Real-Time Cyber-Physical System Monitoring Tool for Security Research. In Proceedings of the 2018 IEEE 24th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), Hakodate, Japan, 28–31 August 2018; pp. 240–241. [CrossRef]
92. Bogosyan, S.; Akgul, T.; Gokasan, M. MTD Based Novel Scheme for BMS Security against CAN Bus Attacks during BEV Charging. In Proceedings of the 2020 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 8–11 June 2020; pp. 1–7. [CrossRef]
93. Cheng, L.; Tian, K.; Yao, D.D.; Sha, L.; Beyah, R.A. Checking is Believing: Event-Aware Program Anomaly Detection in Cyber-Physical Systems. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 825–842. [CrossRef]
94. Chhetri, S.R.; Faezi, S.; Rashid, N.; Al Faruque, M.A. Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0. *J. Hardw. Syst. Secur.* **2017**, *2*, 51–68. [CrossRef]
95. Colom, J.F.; Gil, D.; Mora, H.; Volckaert, B.; Jimeno, A.M. Scheduling framework for distributed intrusion detection systems over heterogeneous network architectures. *J. Netw. Comput. Appl.* **2018**, *108*, 76–86. [CrossRef]
96. Das, T.K.; Adepu, S.; Zhou, J. Anomaly detection in Industrial Control Systems using Logical Analysis of Data. *Comput. Secur.* **2020**, *96*, 101935. [CrossRef]

97. Bhavani, A.D.; Mangla, N. A Review on Intrusion Detection Approaches in Resource-Constrained IoT Environment. In *Mobile Computing and Sustainable Informatics*; Shakya, S., Bestak, R., Palanisamy, R., Kamel, K.A., Eds.; Springer: Singapore, 2021; Volume 68, pp. 171–183. [CrossRef]
98. Eke, H.; Petrovski, A.; Ahriz, H. Detection of False Command and Response Injection Attacks for Cyber Physical Systems Security and Resilience. In Proceedings of the 13th International Conference on Security of Information and Networks, Merkez, Turkey, 4–7 November 2020. [CrossRef]
99. Fujdiak, R.; Blazek, P.; Mlynek, P.; Misurec, J. Developing Battery of Vulnerability Tests for Industrial Control Systems. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–5. [CrossRef]
100. Girdhar, M.; Hong, J.; Lee, H.; Song, T.-J. Hidden Markov Models-Based Anomaly Correlations for the Cyber-Physical Security of EV Charging Stations. *IEEE Trans. Smart Grid* **2021**, *13*, 3903–3914. [CrossRef]
101. Hakim, M.A.; Aksu, H.; Uluagac, A.S.; Akkaya, K. U-PoT: A Honeypot Framework for UPnP-Based IoT Devices. In Proceedings of the 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC), Orlando, FL, USA, 17–19 November 2018; pp. 1–8. [CrossRef]
102. Hong, S. Secure and light IoT protocol (SLIP) for anti-hacking. *J. Comput. Virol. Hacking Tech.* **2017**, *13*, 241–247. [CrossRef]
103. Hopkins, S.; Kalaimannan, E.; John, C.S. Foundations for Research in Cyber-Physical System Cyber Resilience using State Estimation. In Proceedings of the 2020 SoutheastCon, Raleigh, NC, USA, 28–29 March 2020; pp. 1–2. [CrossRef]
104. Hu, Y.; Zhu, P.; Xun, P.; Liu, B.; Kang, W.; Xiong, Y.; Shi, W. CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack. *Comput. Secur.* **2021**, *111*, 102465. [CrossRef]
105. Huang, X.; Liu, J.; Lai, Y.; Mao, B.; Lyu, H. EEFED: Personalized Federated Learning of Execution&Evaluation Dual Network for CPS Intrusion Detection. *IEEE Trans. Inf. Forensics Secur.* **2022**, *18*, 41–56. [CrossRef]
106. Jagtap, S.S.; S., S.S.V.; V., S. A hypergraph based Kohonen map for detecting intrusions over cyber–physical systems traffic. *Futur. Gener. Comput. Syst.* **2021**, *119*, 84–109. [CrossRef]
107. Jahromi, A.N.; Karimipour, H.; Dehghantanha, A.; Choo, K.-K.R. Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems. *IEEE Internet Things J.* **2021**, *8*, 13712–13722. [CrossRef]
108. Kalhara, D.; De Alwis, U.; Jinadasa, A.; Randunu, D.; Nuwanthika, W.S.; Abeygunawardhana, P.K.W. Comprehensive Security Solution for an Industry 4.0 Garment Manufacturing System. In Proceedings of the 2021 3rd International Conference on Advancements in Computing (ICAC), Colombo, Sri Lanka, 9–11 December 2021; pp. 67–72. [CrossRef]
109. Kelli, V.; Radoglou-Grammatikis, P.; Sesis, A.; Lagkas, T.; Fountoukidis, E.; Kafetzakis, E.; Giannoulakis, I.; Sarigiannidis, P. Attacking and Defending DNP3 ICS/SCADA Systems. In Proceedings of the 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), Marina del Rey, Los Angeles, CA, USA, 30 May–1 June 2022; pp. 183–190. [CrossRef]
110. Keshk, M.; Sitnikova, E.; Moustafa, N.; Hu, J.; Khalil, I. An Integrated Framework for Privacy-Preserving Based Anomaly Detection for Cyber-Physical Systems. *IEEE Trans. Sustain. Comput.* **2021**, *6*, 66–79. [CrossRef]
111. Khan, I.A.; Pi, D.; Khan, N.; Khan, Z.U.; Hussain, Y.; Nawaz, A.; Ali, F. A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks. *Appl. Intell.* **2021**, *51*, 7306–7321. [CrossRef]
112. Khan, R.; McLaughlin, K.; Laverty, J.H.D.; David, H.; Sezer, S. Demonstrating Cyber-Physical Attacks and Defense for Synchrophasor Technology in Smart Grid. In Proceedings of the 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 28–30 August 2018; pp. 1–10. [CrossRef]
113. Kholidy, H.A. Autonomous mitigation of cyber risks in the Cyber–Physical Systems. *Futur. Gener. Comput. Syst.* **2020**, *115*, 171–187. [CrossRef]
114. Li, B.; Lu, R.; Xiao, G. *Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems*; Springer International Publishing: Cham, Switzerland, 2020. [CrossRef]
115. Li, F.; Xie, R.; Wang, Z.; Guo, L.; Ye, J.; Ma, P.; Song, W. Online Distributed IoT Security Monitoring With Multidimensional Streaming Big Data. *IEEE Internet Things J.* **2019**, *7*, 4387–4394. [CrossRef]
116. Majumder, A.J.; Miller, J.D.; Veilleux, C.B.; Asif, A.A. Smart-Power: A Smart Cyber-Physical System to Detect IoT Security Threat through Behavioral Power Profiling. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 1041–1049. [CrossRef]
117. Malchow, J.-O.; Marzin, D.; Klick, J.; Kovacs, R.; Roth, V. PLC Guard: A practical defense against attacks on cyber-physical systems. In Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015; pp. 326–334. [CrossRef]
118. Muralidhar, N.; Wang, C.; Self, N.; Momtazpour, M.; Nakayama, K.; Sharma, R.; Ramakrishnan, N. illiad: InteLLigent Invariant and Anomaly Detection in Cyber-Physical Systems. *ACM Trans. Intell. Syst. Technol.* **2018**, *9*, 1–20. [CrossRef]
119. Negi, R.; Dutta, A.; Handa, A.; Ayyangar, U.; Shukla, S.K. Intrusion Detection & Prevention in Programmable Logic Controllers: A Model-driven Approach. In Proceedings of the 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), Tampere, Finland, 10–12 June 2020; Volume 1, pp. 215–222. [CrossRef]
120. Pasikhani, A.M.; Clark, J.A.; Gope, P. Adaptive Hybrid Heterogeneous IDS for 6LoWPAN. *arXiv* **2022**. [CrossRef]
121. Rahmatulloh, A.; Ramadhan, G.M.; Darmawan, I.; Widiyasono, N.; Pramesti, D. Identification of Mirai Botnet in IoT Environment through Denial-of-Service Attacks for Early Warning System. *JOIV Int. J. Inform. Vis.* **2022**, *6*, 623–628. [CrossRef]

122. Schneider, P.; Böttinger, K. High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, Toronto, ON, Canada, 19 October 2018; pp. 1–12. [CrossRef]
123. Settanni, G.; Skopik, F.; Karaj, A.; Wurzenberger, M.; Fiedler, R. Protecting cyber physical production systems using anomaly detection to enable self-adaptation. In Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 15–18 May 2018; pp. 173–180. [CrossRef]
124. Settanni, G.; Skopik, F.; Wurzenberger, M.; Fiedler, R. Countering targeted cyber-physical attacks using anomaly detection in self-adaptive Industry 4.0 Systems. *e i Elektrotechnik Und Inf.* **2018**, *135*, 278–285. [CrossRef]
125. Singh, V.K.; Govindarasu, M. Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid. In *Wide Area Power Systems Stability, Protection, and Security*; Alhelou, H.H., Abdelaziz, A.Y., Siano, P., Eds.; Springer In-ternational Publishing: Cham, Switzerland, 2020; pp. 571–599. [CrossRef]
126. Sun, M.; Lai, Y.; Wang, Y.; Liu, J.; Mao, B.; Gu, H. Intrusion Detection System Based on In-Depth Understandings of Industrial Control Logic. *IEEE Trans. Ind. Inform.* **2022**, *19*, 2295–2306. [CrossRef]
127. Thakur, S.; Chakraborty, A.; De, R.; Kumar, N.; Sarkar, R. Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model. *Comput. Electr. Eng.* **2021**, *91*, 107044. [CrossRef]
128. Vaigandla, K.; Azmi, N.; Karne, R. Investigation on Intrusion Detection Systems (IDSs) in IoT. *Int. J. Emerg. Trends Eng. Res.* **2022**, *10*, 158–166. [CrossRef]
129. Weissman, D.; Jayasumana, A. Integrating IoT Monitoring for Security Operation Center. In Proceedings of the 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, 3 June 2020; pp. 1–6. [CrossRef]
130. Xu, L.; Wang, B.; Wu, X.; Zhao, D.; Zhang, L.; Wang, Z. Detecting Semantic Attack in SCADA System: A Behavioral Model Based on Secondary Labeling of States-Duration Evolution Graph. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 703–715. [CrossRef]
131. Yin, X.C.; Liu, Z.G.; Nkenyereye, L.; Ndibanje, B. Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach. *Sensors* **2019**, *19*, 4952. [CrossRef] [PubMed]
132. You, I.; Yim, K.; Sharma, V.; Choudhary, G.; Chen, I.-R.; Cho, J.-H. On IoT Misbehavior Detection in Cyber Physical Systems. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; pp. 189–190. [CrossRef]
133. Zhang, F.; Kodituwakku, H.A.D.E.; Hines, J.W.; Coble, J.B. Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4362–4369. [CrossRef]
134. Zizzo, G.; Hankin, C.; Maffeis, S.; Jones, K. Adversarial Attacks on Time-Series Intrusion Detection for Industrial Control Systems. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2021; pp. 899–910. [CrossRef]
135. Zohrevand, Z.; Glasser, U. Dynamic Attack Scoring Using Distributed Local Detectors. In Proceedings of the ICASSP 2020—2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020; pp. 2892–2896. [CrossRef]
136. Bogdan, P.; Pedram, M. Toward Enabling Automated Cognition and Decision-Making in Complex Cyber-Physical Systems. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 27–30 May 2018; pp. 1–4. [CrossRef]
137. Lesi, V.; Jovanov, I.; Pajic, M. Integrating Security in Resource-Constrained Cyber-Physical Systems. *ACM Trans. Cyber-Phys. Syst.* **2020**, *4*, 1–27. [CrossRef]
138. Tsochev, G.; Sharabov, M. Artificial intelligence methods used in industry 4.0 in particular industrial control systems. *AIP Conf. Proc.* **2021**, *2333*, 070017. [CrossRef]
139. Fatani, A.; Elaziz, M.A.; Dahou, A.; Al-Qaness, M.A.A.; Lu, S. IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization. *IEEE Access* **2021**, *9*, 123448–123464. [CrossRef]
140. Hindy, H.; Brosset, D.; Bayne, E.; Seeam, A.; Bellekens, X. Improving SIEM for Critical SCADA Water Infrastructures Using Machine Learning. In *Computer Security*; Katsikas, S.K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., Kalloniatis, C., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 11387, pp. 3–19. [CrossRef]
141. Shahriar, H.; Haque, N.I.; Rahman, M.A.; Alonso, M. G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 376–385. [CrossRef]
142. Srikanth Yadav, M.; Kalpana, R. A Survey on Network Intrusion Detection Using Deep Generative Networks for Cyber-Physical Systems. In *Advances in Systems Analysis, Software Engineering, and High Performance Computing*; Luhach, A.K., Elçi, A., Eds.; IGI Global: Hershey, PA, USA, 2021; pp. 137–159. [CrossRef]
143. Chen, J.; Gao, X.; Deng, R.; He, Y.; Fang, C.; Cheng, P. Generating Adversarial Examples Against Machine Learning-Based Intrusion Detector in Industrial Control Systems. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1810–1825. [CrossRef]
144. Alsaedi, A.; Tari, Z.; Mahmud, R.; Moustafa, N.; Mahmood, A.N.; Anwar, A. USMD: UnSupervised Misbehaviour Detection for Multi-Sensor Data. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 724–739. [CrossRef]
145. Al-Shabi, M.; Abuhamdah, A. Using deep learning to detecting abnormal behavior in internet of things. *Int. J. Electr. Comput. Eng. (IJECE)* **2022**, *12*, 2108–2120. [CrossRef]

146. Borcherding, A.; Feldmann, L.; Karch, M.; Meshram, A.; Beyerer, J. Towards a Better Understanding of Machine Learning based Network Intrusion Detection Systems in Industrial Networks. In Proceedings of the 8th International Conference on Information Systems Security and Privacy, Online, 9–11 February 2022; pp. 314–325. [CrossRef]
147. Ha, D.T.; Hoang, N.X.; Du, N.H.; Huong, T.T.; Tran, K.P. Explainable Anomaly Detection for Industrial Control System Cybersecurity. *IFAC-PapersOnLine* **2022**, *55*, 1183–1188. [CrossRef]
148. Huong, T.T.; Bac, T.P.; Ha, K.N.; Hoang, N.V.; Hung, N.T.; Tran, K.P. Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems. *IEEE Access* **2022**, *10*, 53854–53872. [CrossRef]
149. Tahir, M.; Ali, M.I. On the Performance of Federated Learning Algorithms for IoT. *IoT* **2022**, *3*, 273–284. [CrossRef]
150. Perez, R.L.; Adamsky, F.; Soua, R.; Engel, T. Forget the Myth of the Air Gap: Machine Learning for Reliable Intrusion Detection in SCADA Systems. *ICST Trans. Secur. Saf.* **2019**, *6*, 159348. [CrossRef]
151. Mahbooba, B.; Timilsina, M.; Sahal, R.; Serrano, M. Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model. *Complexity* **2021**, *2021*, 6634811. [CrossRef]
152. Boateng, E.A.; Bruce, J.W. Unsupervised Machine Learning Techniques for Detecting PLC Process Control Anomalies. *J. Cybersecur. Priv.* **2022**, *2*, 220–244. [CrossRef]
153. Jamal, A.A.; Majid, A.-A.M.; Konev, A.; Kosachenko, T.; Shelupanov, A. A review on security analysis of cyber physical systems using Machine learning. *Mater. Today Proc.* **2021**, *80*, 2302–2306. [CrossRef]
154. Akamadu, J.C.; Eke, J.; Kalu, E.C. Improving Data Protection in Industrial Control System Networks Using Machine Learning Technique. *IRE J.* **2022**, *5*. [CrossRef]
155. Alabadi, M.; Albayrak, Z. Q-Learning for Securing Cyber-Physical Systems: A survey. In Proceedings of the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 26–28 June 2020; pp. 1–13. [CrossRef]
156. Aljumah, A. IoT-based intrusion detection system using convolution neural networks. *PeerJ Comput. Sci.* **2021**, *7*, e721. [CrossRef]
157. Alrashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.; Ming, H. AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning. In Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 0305–0310. [CrossRef]
158. Altaha, M.; Hong, S. Anomaly Detection for SCADA System Security Based on Unsupervised Learning and Function Codes Analysis in the DNP3 Protocol. *Electronics* **2022**, *11*, 2184. [CrossRef]
159. Althobaiti, M.M.; Kumar, K.P.M.; Gupta, D.; Kumar, S.; Mansour, R.F. An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems. *Measurement* **2021**, *186*, 110145. [CrossRef]
160. Bajpai, S.; Sharma, K. A Framework for Intrusion Detection Models for IoT Networks using Deep Learning. *Res. Sq.* **2022**. [CrossRef]
161. Balla, A.; Habaebi, M.H.; Islam, R.; Mubarak, S. Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system. *Clean. Eng. Technol.* **2022**, *9*, 100532. [CrossRef]
162. Bhatia, R.; Benno, S.; Esteban, J.; Lakshman, T.V.; 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. [CrossRef]
163. Boateng, E.A.; Bruce, J.W.; Talbert, D.A. Anomaly Detection for a Water Treatment System Based on One-Class Neural Network. *IEEE Access* **2022**, *10*, 115179–115191. [CrossRef]
164. Brown, J.; Saha, T.; Jha, N.K. GRAVITAS: Graphical Reticulated Attack Vectors for Internet-of-Things Aggregate Security. *IEEE Trans. Emerg. Top. Comput.* **2021**, *10*, 1331–1348. [CrossRef]
165. Colelli, R.; Magri, F.; Panzieri, S.; Pascucci, F. Anomaly-Based Intrusion Detection System for Cyber-Physical System Security. In Proceedings of the 2021 29th Mediterranean Conference on Control and Automation (MED), Puglia, Italy, 22–25 June 2021; pp. 428–434. [CrossRef]
166. Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35. [CrossRef]
167. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 2716–2725. [CrossRef]
168. Osman, N.F.M.; Elamin, A.A.A.; Ahmed, E.S.A.; Saeed, R.A. Cyber-Physical System for Smart Grid. In *Research Anthology on Smart Grid and Microgrid Development*; Management Association, I.R., Ed.; IGI Global: Hershey, PA, USA, 2022; pp. 325–347. [CrossRef]
169. Funchal, G.; Pedrosa, T.; Vallim, M.; Leitao, P. Security for a Multi-Agent Cyber-Physical Conveyor System using Machine Learning. In Proceedings of the 2020 IEEE 18th International Conference on Industrial Informatics (INDIN), Warwick, UK, 20–23 July 2020; Volume 1, pp. 47–52. [CrossRef]
170. Raman, M.R.G.; Somu, N.; Mathur, A.P. Anomaly Detection in Critical Infrastructure Using Probabilistic Neural Network. In *Applications and Techniques in Information Security*; Sriram, V.S.S., Subramaniyaswamy, V., Sasikaladevi, N., Zhang, L., Batten, L., Li, G., Eds.; Springer: Singapore, 2019; Volume 1116, pp. 129–141. [CrossRef]
171. Ghimire, B.; Rawat, D.B. Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 8229–8249. [CrossRef]
172. Gumaei, A.; Hassan, M.M.; Huda, S.; Hassan, R.; Camacho, D.; Del Ser, J.; Fortino, G. A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Appl. Soft Comput.* **2020**, *96*, 106658. [CrossRef]

173. Haji, S.H.; Ameen, S.Y. Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review. *Asian J. Res. Comput. Sci.* **2021**, *2021*, 30–46. [CrossRef]
174. Hao, W.; Yang, T.; Yang, Q. Hybrid Statistical-Machine Learning for Real-Time Anomaly Detection in Industrial Cyber–Physical Systems. *IEEE Trans. Autom. Sci. Eng.* **2021**, *20*, 32–46. [CrossRef]
175. Hasan, M.; Islam, M.M.; Zarif, M.I.I.; Hashem, M.M.A. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet Things* **2019**, *7*, 100059. [CrossRef]
176. 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]
177. Huc, A.; Trcek, D. Anomaly Detection in IoT Networks: From Architectures to Machine Learning Transparency. *IEEE Access* **2021**, *9*, 60607–60616. [CrossRef]
178. Idrissi, I.; Azizi, M.; Moussaoui, O. An unsupervised generative adversarial network based-host intrusion detection system for internet of things devices. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *25*, 1140–1150. [CrossRef]
179. Idrissi, I.; Azizi, M.; Moussaoui, O. A Stratified IoT Deep Learning based Intrusion Detection System. In Proceedings of the 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 3–4 March 2022; pp. 1–8. [CrossRef]
180. Johnson, A.P.; Al-Aqrabi, H.; Hill, R. Bio-Inspired Approaches to Safety and Security in IoT-Enabled Cyber-Physical Systems. *Sensors* **2020**, *20*, 844. [CrossRef]
181. Jung, W.; Zhao, H.; Sun, M.; Zhou, G. IoT botnet detection via power consumption modeling. *Smart Health* **2019**, *15*, 100103. [CrossRef]
182. Kim, H.; Shon, T. Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing. *J. Supercomput.* **2022**, *78*, 13554–13563. [CrossRef]
183. Koay, A.M.Y.; Ko, R.K.L.; Hettema, H.; Radke, K. Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. *J. Intell. Inf. Syst.* **2022**, *60*, 377–405. [CrossRef]
184. Kumaran, S.S.; Balakannan, S.P.; Li, J. A deep analysis of object capabilities for intelligence considering wireless IoT devices with the DNN approach. *J. Supercomput.* **2021**, *78*, 4745–4758. [CrossRef]
185. Li, B.; Wu, Y.; Song, J.; Lu, R.; Li, T.; Zhao, L. DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5615–5624. [CrossRef]
186. Liang, W.; Xie, S.; Cai, J.; Xu, J.; Hu, Y.; Xu, Y.; Qiu, M. Deep Neural Network Security Collaborative Filtering Scheme for Service Recommendation in Intelligent Cyber–Physical Systems. *IEEE Internet Things J.* **2021**, *9*, 22123–22132. [CrossRef]
187. Liang, Y.; Samtani, S.; Guo, B.; Yu, Z. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet Things J.* **2020**, *7*, 9128–9143. [CrossRef]
188. Luo, Y.; Xiao, Y.; Cheng, L.; Peng, G.; Yao, D. Deep Learning-based Anomaly Detection in Cyber-physical Systems. *ACM Comput. Surv.* **2021**, *54*, 1–36. [CrossRef]
189. Lv, Z.; Chen, D.; Lou, R.; Alazab, A. Artificial intelligence for securing industrial-based cyber–physical systems. *Future Gener. Comput. Syst.* **2021**, *117*, 291–298. [CrossRef]
190. Ma, H.; Tian, J.; Qiu, K.; Lo, D.; Gao, D.; Wu, D.; Jia, C.; Baker, T. Deep-Learning–Based App Sensitive Behavior Surveillance for Android Powered Cyber–Physical Systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5840–5850. [CrossRef]
191. Maleh, Y. Machine Learning Techniques for IoT Intrusions Detection in Aerospace Cyber-Physical Systems. In *Machine Learning and Data Mining in Aerospace Technology*; Hassanien, A.E., Darwish, A., El-Askary, H., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 836, pp. 205–232. [CrossRef]
192. Malik, Z.A.; Siddique, M.; Paracha, Z.J.; Imran, A.; Yasin, A.; Butt, A.H. Performance Evaluation of Classification Algorithms for Intrusion Detection on NSL-KDD Using Rapid Miner. *Int. J. Innov. Sci. Technol.* **2022**, *4*, 135–146. [CrossRef]
193. Mendonça, R.V.; Silva, J.C.; Rosa, R.L.; Saadi, M.; Rodriguez, D.Z.; Farouk, A. A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Syst.* **2021**, *39*, e12917. [CrossRef]
194. Mokbal, F.; Dan, W.; Osman, M.; Ping, Y.; Alsamhi, S. An Efficient Intrusion Detection Framework Based on Embedding Feature Selection and Ensemble Learning Technique. *Int. Arab. J. Inf. Technol.* **2022**, *19*, 237–248. [CrossRef]
195. Mothukuri, V.; Khare, P.; Parizi, R.M.; Pouriyeh, S.; Dehghantanha, A.; Srivastava, G. Federated-Learning-Based Anomaly Detection for IoT Security Attacks. *IEEE Internet Things J.* **2021**, *9*, 2545–2554. [CrossRef]
196. Mozaffari, F.S.; Karimipour, H.; Parizi, R.M. Learning Based Anomaly Detection in Critical Cyber-Physical Systems. In *Security of Cyber-Physical Systems*; Karimipour, H., Srikantha, P., Farag, H., Wei-Kocsis, J., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 107–130. [CrossRef]
197. Mubarak, S.; Habaebi, M.H.; Islam, R.; Rahman, F.D.A.; Tahir, M. Anomaly Detection in ICS Datasets with Machine Learning Algorithms. *Comput. Syst. Sci. Eng.* **2021**, *37*, 33–46. [CrossRef]
198. Narayanan, V.; Bobba, R.B. Learning Based Anomaly Detection for Industrial Arm Applications. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, Toronto, ON, Canada, 15–19October 2018; pp. 13–23. [CrossRef]
199. Nazir, S.; Patel, S.; Patel, D. Autoencoder Based Anomaly Detection for SCADA Networks. *Int. J. Artif. Intell. Mach. Learn.* **2021**, *11*, 83–99. [CrossRef]

200. Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.-R. DÏoT: A Federated Self-learning Anomaly Detection System for IoT. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 756–767. [CrossRef]
201. Nirmala, P.; Manimegalai, T.; Arunkumar, J.R.; Vimala, S.; Rajkumar, G.V.; Raju, R. A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1955009. [CrossRef]
202. Pahl, M.-O.; Aubet, F.-X. All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection. In Proceedings of the 2018 14th International Conference on Network and Service Management (CNSM), Rome, Italy, 5–9 November 2018; Available online: https://ieeexplore.ieee.org/document/8584985 (accessed on 16 June 2023).
203. Park, S.-T.; Li, G.; Hong, J.-C. A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. *J. Ambient. Intell. Humaniz. Comput.* **2018**, *11*, 1405–1412. [CrossRef]
204. Pinto, R.; Goncalves, G.; Tovar, E.; Delsing, J. Attack Detection in Cyber-Physical Production Systems using the Deterministic Dendritic Cell Algorithm. In Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020; Volume 1, pp. 1552–1559. [CrossRef]
205. Plakhotnikov, D.P.; Kotova, E.E. The Use of Artificial Intelligence in Cyber-Physical Systems. In Proceedings of the 2020 XXIII International Conference on Soft Computing and Measurements (SCM), St. Petersburg, Russia, 27–29 May 2020; pp. 238–241. [CrossRef]
206. Pranto, B.; Alam Ratul, H.; Rahman, M.; Diya, I.J.; Zahir, Z.-B. Performance of Machine Learning Techniques in Anomaly Detection with Basic Feature Selection Strategy—A Network Intrusion Detection System. *J. Adv. Inf. Technol.* **2022**, *13*, 1. [CrossRef]
207. 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.* **2021**, *6*, 171–185. [CrossRef]
208. Radanliev, P.; De Roure, D.; Van Kleek, M.; Santos, O.; Ani, U. Artificial intelligence in cyber physical systems. *AI Soc.* **2020**, *36*, 783–796. [CrossRef]
209. Hadi, M.R.; Mohammed, A.S. A Novel Approach to Network Intrusion Detection System using Deep Learning for SDN: Futuristic Approach. *Mach. Learn. Appl.* **2022**, *2022*, 69–82. [CrossRef]
210. Ramotsoela, D.; Abu-Mahfouz, A.; Hancke, G. A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study. *Sensors* **2018**, *18*, 2491. [CrossRef] [PubMed]
211. Rawat, S.; Srinivasan, A.; Ravi, V.; Ghosh, U. Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. *Internet Technol. Lett.* **2020**, *5*, e232. [CrossRef]
212. Rodríguez, E.; Valls, P.; Otero, B.; Costa, J.J.; Verdú, J.; Pajuelo, M.A.; Canal, R. Transfer-Learning-Based Intrusion Detection Framework in IoT Networks. *Sensors* **2022**, *22*, 5621. [CrossRef]
213. Haghighi, M.S.; Farivar, F.; Jolfaei, A. A Machine Learning-based Approach to Build Zero False-Positive IPSs for Industrial IoT and CPS with a Case Study on Power Grids Security. *IEEE Trans. Ind. Appl.* **2020**, *2020*, 1. [CrossRef]
214. Sharma, V.; You, I.; Yim, K.; Chen, I.-R.; Cho, J.-H. BRIoT: Behavior Rule Specification-Based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems. *IEEE Access* **2019**, *7*, 118556–118580. [CrossRef]
215. Shishvan, O.R.; Zois, D.-S.; Soyata, T. Incorporating Artificial Intelligence into Medical Cyber Physical Systems: A Survey. In *Connected Health in Smart Cities*; El Saddik, A., Hossain, M.S., Kantarci, B., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 153–178. [CrossRef]
216. Srivastava, G.; Lin, J.C.-W.; Zhang, X.; Tseng, V.S. Guest Editorial: Artificial Intelligence for Securing Industrial-Based Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5738–5741. [CrossRef]
217. Thakkar, A.; Lohiya, R. A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. *Arch. Comput. Methods Eng.* **2020**, *28*, 3211–3243. [CrossRef]
218. Ullah, I.; Mahmoud, Q.H. Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks. *IEEE Access* **2021**, *9*, 103906–103926. [CrossRef]
219. Umer, M.A.; Junejo, K.N.; Jilani, M.T.; Mathur, A.P. Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100516. [CrossRef]
220. Uprety, A.; Rawat, D.B. Reinforcement Learning for IoT Security: A Comprehensive Survey. *IEEE Internet Things J.* **2020**, *8*, 8693–8706. [CrossRef]
221. Veith, E.M.; Fischer, L.; Tröschel, M.; Nieße, A. Analyzing Cyber-Physical Systems from the Perspective of Artificial Intelligence. In Proceedings of the 2019 International Conference on Artificial Intelligence, Robotics and Control, Cairo, Egypt, 14–16 December 2019. [CrossRef]
222. Wang, C.; Wang, B.; Liu, H.; Qu, H. Anomaly Detection for Industrial Control System Based on Autoencoder Neural Network. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8897926. [CrossRef]
223. Yang, H.; Cheng, L.; Chuah, M.C. Deep-Learning-Based Network Intrusion Detection for SCADA Systems. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–7. [CrossRef]
224. Yeboah-Ofori, A.; Islam, S.; Brimicombe, A. Detecting Cyber Supply Chain Attacks on Cyber Physical Systems Using Bayesian Belief Network. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019; pp. 37–42. [CrossRef]

225. Zhang, J.; Pan, L.; Han, Q.-L.; Chen, C.; Wen, S.; Xiang, Y. Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey. *IEEE/CAA J. Autom. Sin.* **2021**, *9*, 377–391. [CrossRef]
226. Zhao, S.; Li, S.; Qi, L.; Da Xu, L. Computational Intelligence Enabled Cybersecurity for the Internet of Things. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 666–674. [CrossRef]
227. Zhu, N.; Zhu, C.; Zhou, L.; Zhu, Y.; Zhang, X. Optimization of the Random Forest Hyperparameters for Power Industrial Control Systems Intrusion Detection Using an Improved Grid Search Algorithm. *Appl. Sci.* **2022**, *12*, 10456. [CrossRef]
228. Gardiner, J.; Craggs, B.; Green, B.; Rashid, A. Oops I Did it Again: Further Adventures in the Land of ICS Security Testbeds. In Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy—CPS-SPC'19, London, UK, 11 November 2019; pp. 75–86. [CrossRef]
229. Robles-Durazno, A.; Moradpoor, N.; McWhinnie, J.; Russell, G.; Porcel-Bustamante, J. Implementation and Evaluation of Physical, Hybrid, and Virtual Testbeds for Cybersecurity Analysis of Industrial Control Systems. *Symmetry* **2021**, *13*, 519. [CrossRef]
230. Al-Hawawreh, M.; Sitnikova, E. Developing a Security Testbed for Industrial Internet of Things. *IEEE Internet Things J.* **2020**, *8*, 5558–5573. [CrossRef]
231. Hankin, C.; Chana, D.; Green, B.; Khan, R.; M3, P.; Popov, P.; Rashid, A.; Sezer, S. Open Testbeds for CNI. 2018. Available online: https://eprints.lancs.ac.uk/id/eprint/139028/1/Open_Testbeds_deliverable_final.pdf (accessed on 16 June 2023).
232. Craggs, B.; Rashid, A.; Hankin, C.; Antrobus, R.; Serban, O.; Thapen, N. A Reference Architecture for IIoT and Industrial Control Systems Testbeds. In Proceedings of the Living in the Internet of Things (IoT 2019), London, UK, 1–2 May 2019; p. 44. [CrossRef]
233. Williams, T.J. The Purdue enterprise reference architecture. *Comput. Ind.* **1994**, *24*, 141–158. [CrossRef]
234. Abu Waraga, O.; Bettayeb, M.; Nasir, Q.; Abu Talib, M. Design and implementation of automated IoT security testbed. *Comput. Secur.* **2019**, *88*, 101648. [CrossRef]
235. Ani, U.D.; Watson, J.M.; Green, B.; Craggs, B.; Nurse, J. Design Considerations for Building Credible Security Testbeds: A Systematic Study of Industrial Control System Use Cases. *arXiv* **2019**. [CrossRef]
236. Adepu, S.; Palleti, V.R.; Mishra, G.; Mathur, A. Investigation of Cyber Attacks on a Water Distribution System. In *Applied Cryptography and Network Security Workshops*; Zhou, J., Conti, M., Ahmed, C.M., Au, M.H., Batina, L., Li, Z., Lin, J., Losiouk, E., Luo, B., Majumdar, S., et al., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 12418, pp. 274–291. [CrossRef]
237. Ahmed, C.M.; Palleti, V.R.; Mathur, A.P. WADI: A water distribution testbed for research in the design of secure cyber physical systems. In Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, Pittsburgh, PA, USA, 21 April 2017; pp. 25–28. [CrossRef]
238. Ahmed, C.M.; Palleti, V.R.; Mishra, V.K. A practical physical watermarking approach to detect replay attacks in a CPS. *J. Process. Control.* **2022**, *116*, 136–146. [CrossRef]
239. Babun, L.; Aksu, H.; Ryan, L.; Akkaya, K.; Bentley, E.S.; Uluagac, A.S. Z-IoT: Passive Device-class Fingerprinting of ZigBee and Z-Wave IoT Devices. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–7. [CrossRef]
240. Battisti, F.; Bernieri, G.; Carli, M.; Lopardo, M.; Pascucci, F. Detecting Integrity Attacks in IoT-based Cyber Physical Systems: A Case Study on Hydra Testbed. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp. 1–6. [CrossRef]
241. 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. [CrossRef]
242. Grigoriou, E.; Liatifis, A.; Grammatikis, P.R.; Lagkas, T.; Moscholios, I.; Markakis, E.; Sarigiannidis, P. Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots. In Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 27–29 July 2022; pp. 345–350. [CrossRef]
243. Jeffrey, N.; Tan, Q.; Villar, J.R. Simulators and Testbeds for IIoT Development and Validation. In Proceedings of the 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 1–4 June 2022; pp. 1–5. [CrossRef]
244. 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]
245. Maiti, R.R.; Yoong, C.H.; Palleti, V.R.; Silva, A.; Poskitt, C.M. Mitigating Adversarial Attacks on Data-Driven Invariant Checkers for Cyber-Physical Systems. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 3378–3391. [CrossRef]
246. Nock, O.; Starkey, J.; Angelopoulos, C.M. Addressing the Security Gap in IoT: Towards an IoT Cyber Range. *Sensors* **2020**, *20*, 5439. [CrossRef]
247. Oliveira, L.M.C.; Dias, R.; Rebello, C.M.; Martins, M.A.F.; Rodrigues, A.E.; Ribeiro, A.M.; Nogueira, I.B.R. Artificial Intelligence and Cyber-Physical Systems: A Review and Perspectives for the Future in the Chemical Industry. *AI* **2021**, *2*, 429–443. [CrossRef]
248. Osman, F.A.; Hashem, M.Y.M.; Eltokhy, M.A.R. Secured cloud SCADA system implementation for industrial applications. *Multimed. Tools Appl.* **2022**, *81*, 9989–10005. [CrossRef]
249. Pospisil, O.; Blazek, P.; Kuchar, K.; Fujdiak, R.; Misurec, J. Application Perspective on Cybersecurity Testbed for Industrial Control Systems. *Sensors* **2021**, *21*, 8119. [CrossRef] [PubMed]
250. Qamsane, Y.; Phillips, J.R.; Savaglio, C.; Warner, D.; James, S.C.; Barton, K. Open Process Automation- and Digital Twin-Based Performance Monitoring of a Process Manufacturing System. *IEEE Access* **2022**, *10*, 60823–60835. [CrossRef]

251. Schranz, C.; Strohmeier, F.; Damjanovic-Behrendt, V. A Digital Twin Prototype for Product Lifecycle Data Management. In Proceedings of the 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA), Antalya, Turkey, 2–5 November 2020; pp. 1–6. [CrossRef]
252. Siboni, S.; Sachidananda, V.; Meidan, Y.; Bohadana, M.; Mathov, Y.; Bhairav, S.; Shabtai, A.; Elovici, Y. Security Testbed for Internet-of-Things Devices. *IEEE Trans. Reliab.* **2018**, *68*, 23–44. [CrossRef]
253. Tekeoglu, A.; Bekiroglu, K.; Chiang, C.-F.; Sengupta, S. Unsupervised Time-Series based Anomaly Detection in ICS/SCADA Networks. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October –2 November 2021; pp. 1–6. [CrossRef]
254. Zhu, S.; Yang, S.; Gou, X.; Xu, Y.; Zhang, T.; Wan, Y. Survey of Testing Methods and Testbed Development Concerning Internet of Things. *Wirel. Pers. Commun.* **2021**, *123*, 165–194. [CrossRef]
255. Gunnarsson, M. Security Solutions for Constrained Devices in Cyber-Physical Systems. Lund University. 2020. Available online: https://lucris.lub.lu.se/ws/portalfiles/portal/76905617/lic_avhandling_2020_03_05.pdf (accessed on 16 June 2023).
256. An, Y.; Yu, F.R.; Li, J.; Chen, J.; Leung, V.C.M. Edge Intelligence (EI)-Enabled HTTP Anomaly Detection Framework for the Internet of Things (IoT). *IEEE Internet Things J.* **2020**, *8*, 3554–3566. [CrossRef]
257. Huong, T.T.; Bac, T.P.; Long, D.M.; Luong, T.D.; Dan, N.M.; Quang, L.A.; Cong, L.T.; Thang, B.D.; Tran, K.P. Detecting cyberattacks using anomaly detection in industrial control systems: A Federated Learning approach. *Comput. Ind.* **2021**, *132*, 103509. [CrossRef]
258. Wang, T.; Liang, Y.; Yang, Y.; Xu, G.; Peng, H.; Liu, A.; Jia, W. An Intelligent Edge-Computing-Based Method to Counter Coupling Problems in Cyber-Physical Systems. *IEEE Netw.* **2020**, *34*, 16–22. [CrossRef]
259. Javed, A.; Robert, J.; Heljanko, K.; Främling, K. IoTEF: A Federated Edge-Cloud Architecture for Fault-Tolerant IoT Applications. *J. Grid Comput.* **2020**, *18*, 57–80. [CrossRef]
260. Das, R.; Menon, V.; Morris, T.H. On the Edge Realtime Intrusion Prevention System for DoS Attack. In Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018 (ICS-CSR 2018), Hamburg, Germany, 29–30 August 2018. [CrossRef]
261. Eskandari, M.; Janjua, Z.H.; Vecchio, M.; Antonelli, F. Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices. *IEEE Internet Things J.* **2020**, *7*, 6882–6897. [CrossRef]
262. Tsukada, M.; Kondo, M.; Matsutani, H. A Neural Network-Based On-device Learning Anomaly Detector for Edge Devices. *IEEE Trans. Comput.* **2020**, *69*, 1027–1044. [CrossRef]
263. Xu, S.; Qian, Y.; Hu, R.Q. Data-Driven Edge Intelligence for Robust Network Anomaly Detection. *IEEE Trans. Netw. Sci. Eng.* **2019**, *7*, 1481–1492. [CrossRef]
264. Darabseh, A.; Freris, N.M. A software-defined architecture for control of IoT cyberphysical systems. *Clust. Comput.* **2019**, *22*, 1107–1122. [CrossRef]
265. Amangele, P.; Reed, M.J.; Al-Naday, M.; Thomos, N.; Nowak, M. Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In Proceedings of the 2019 International Conference on Information Technologies (InfoTech), St. St. Constantine and Elena resort (near the city of Varna), Varna, Bulgaria, 19–20 September 2019; pp. 1–4. [CrossRef]
266. Correa, J.D.A.; Pinto, A.S.R.; Montez, C. Lossy Data Compression for IoT Sensors: A Review. *Internet Things* **2022**, *19*, 100516. [CrossRef]
267. Ferrari, P.; Rinaldi, S.; Sisinni, E.; Colombo, F.; Ghelfi, F.; Maffei, D.; Malara, M. Performance evaluation of full-cloud and edge-cloud architectures for Industrial IoT anomaly detection based on deep learning. In Proceedings of the 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT), Naples, Italy, 4–6 June 2019. [CrossRef]
268. Garagad, V.G.; Iyer, N.C.; Wali, H.G. Data Integrity: A security threat for Internet of Things and Cyber-Physical Systems. In Proceedings of the 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2–4 July 2020; pp. 244–249. [CrossRef]
269. Huang, H.; Yang, L.; Wang, Y.; Xu, X.; Lu, Y. Digital Twin-driven online anomaly detection for an automation system based on edge intelligence. *J. Manuf. Syst.* **2021**, *59*, 138–150. [CrossRef]
270. Hussain, B.; Du, Q.; Imran, A.; Imran, M.A. Artificial Intelligence-Powered Mobile Edge Computing-Based Anomaly Detection in Cellular Networks. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4986–4996. [CrossRef]
271. Hussain, B.; Du, Q.; Zhang, S.; Imran, A.; Imran, M.A. Mobile Edge Computing-Based Data-Driven Deep Learning Framework for Anomaly Detection. *IEEE Access* **2019**, *7*, 137656–137667. [CrossRef]
272. Kurdi, H.; Thayananthan, V. A Multi-Tier MQTT Architecture with Multiple Brokers Based on Fog Computing for Securing Industrial IoT. *Appl. Sci.* **2022**, *12*, 7173. [CrossRef]
273. Rathore, S.; Park, J.H. A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5522–5532. [CrossRef]
274. Ray, P.P.; Kumar, N. SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. *Comput. Commun.* **2021**, *169*, 129–153. [CrossRef]
275. Adamsky, F.; Aubigny, M.; Battisti, F.; Carli, M.; Cimorelli, F.; Cruz, T.; Di Giorgio, A.; Foglietta, C.; Galli, A.; Giuseppi, A.; et al. Integrated protection of industrial control systems from cyber-attacks: The ATENA approach. *Int. J. Crit. Infrastruct. Prot.* **2018**, *21*, 72–82. [CrossRef]
276. Szymanski, T.H. The "Cyber Security via Determinism" Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access* **2022**, *10*, 45893–45930. [CrossRef]

277. Ameer, S.; Gupta, M.; Bhatt, S.; Sandhu, R. BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, New York, NY, USA, 8 June 2022. [CrossRef]
278. Federici, F.; Martintoni, D.; Senni, V. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics* **2023**, *12*, 566. [CrossRef]
279. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
280. Alshomrani, S.; Li, S. PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6367579. [CrossRef]
281. Eckhart, M.; Ekelhart, A.; Luder, A.; Biffl, S.; Weippl, E. Security Development Lifecycle for Cyber-Physical Production Systems. In Proceedings of the IECON 2019—45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 14–17 October 2019; Volume 1, pp. 3004–3011. [CrossRef]
282. Rehman, S.U.; Gruhn, V. An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. *Technologies* **2018**, *6*, 65. [CrossRef]
283. Alipour, M.A.; Ghasemshirazi, S.; Shirvani, G. Enabling a Zero Trust Architecture in a 5G-enabled Smart Grid. *arXiv* **2022**. [CrossRef]
284. Alshehri, M.D.; Hussain, F.K. A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing* **2018**, *101*, 791–818. [CrossRef]
285. Huang, W.; Xie, X.; Wang, Z.; Feng, J. A Zero Trust and Attribute-Based Encryption Scheme for Dynamic Access Control in Power IoT Environments. In *Advances in Natural Computation, Fuzzy Systems and Knowledge Discovery*; Xiong, N., Li, M., Li, K., Xiao, Z., Liao, L., Wang, L., Eds.; Springer International Publishing: Cham, Switzerland, 2023; Volume 153, pp. 1338–1345. [CrossRef]
286. Li, S.; Iqbal, M.; Saxena, N. Future Industry Internet of Things with Zero-trust Security. *Inf. Syst. Front.* **2022**, *2022*, 1–14. [CrossRef]
287. Liu, Y.; Hao, X.; Ren, W.; Xiong, R.; Zhu, T.; Choo, K.-K.R.; Min, G. A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things. *IEEE Trans. Comput.* **2022**, *72*, 501–512. [CrossRef]
288. Mahmud, M.; Kaiser, M.S.; Rahman, M.M.; Shabut, A.; Al-Mamun, S.; Hussain, A. A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications. *Cogn. Comput.* **2018**, *10*, 864–873. [CrossRef]
289. Meng, L.; Huang, D.; An, J.; Zhou, X.; Lin, F. A continuous authentication protocol without trust authority for zero trust architecture. *China Commun.* **2022**, *19*, 198–213. [CrossRef]
290. Sarkar, S.; Choudhary, G.; Shandilya, S.K.; Hussain, A.; Kim, H. Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability* **2022**, *14*, 11213. [CrossRef]
291. Shen, Y.; Tang, X.; Zhang, X.; Zhou, Y.; Zou, H. A flexible continuous-wave quantum cryptography scheme with zero-trust security for Internet of Things. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 155013292211369. [CrossRef]
292. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, *10*, 57143–57179. [CrossRef]
293. Trček, D.; Abie, H.; Skomedal, Å. Adaptive Safety for Internet of Things in e-Health. *arXiv* **2022**. [CrossRef]
294. Wang, J.; Chen, J.; Xiong, N.; Alfarraj, O.; Tolba, A.; Ren, Y. S-BDS: An Effective Blockchain-based Data Storage Scheme in Zero-Trust IoT. *ACM Trans. Internet Technol.* **2022**, *2022*, 3511902. [CrossRef]
295. Xiao, S.; Ye, Y.; Kanwal, N.; Newe, T.; Lee, B. SoK: Context and Risk Aware Access Control for Zero Trust Systems. *Secur. Commun. Netw.* **2022**, *2022*, 7026779. [CrossRef]
296. Bartusiak, R.D.; Bitar, S.; DeBari, D.L.; Houk, B.G.; Stevens, D.; Fitzpatrick, B.; Sloan, P. Open Process Automation: A standards-based, open, secure, interoperable process control architecture. *Control Eng. Pract.* **2022**, *121*, 105034. [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.