energies

MDPI

Article

Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems

Namhla Mtukushe [1,2], Adeniyi K. Onaolapo [3], Anuoluwapo Aluko [4] and David G. Dorrell [1,*]

[1] School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg 2000, South Africa; namhlam@dut.ac.za
[2] Department of Electrical Power Engineering, Durban University of Technology, Durban 4000, South Africa
[3] Department of Electrical and Electronics Engineering Technology, University of Johannesburg, Johannesburg 2092, South Africa; adeniyi.onaolapo@gmail.com
[4] Power Research Laboratory, Department of Electrical and Software Engineering, University of Calgary, Calgary, AB T2N 1N4, Canada; alukoanuoluwapotobi@gmail.com
* Correspondence: david.dorrell@wits.ac.za

Abstract: With the rapid proliferation of cyber-physical systems (CPSs) in various sectors, including critical infrastructure, transportation, healthcare, and the energy industry, there is a pressing need for robust cybersecurity mechanisms to protect these systems from cyberattacks. A cyber-physical system is a combination of physical and cyber components, and a security breach in either component can lead to catastrophic consequences. Cyberattack detection and mitigation methods in CPSs involve the use of various techniques such as intrusion detection systems (IDSs), firewalls, access control mechanisms, and encryption. Overall, effective cyberattack detection and mitigation methods in CPSs require a comprehensive security strategy that considers the unique characteristics of a CPS, such as the interconnectedness of physical and cyber components, the need for real-time response, and the potential consequences of a security breach. By implementing these methods, CPSs can be better protected against cyberattacks, thus ensuring the safety and reliability of critical infrastructure and other vital systems. This paper reviews the various kinds of cyber-attacks that have been launched or implemented in CPSs. It reports on the state-of-the-art detection and mitigation methods that have been used or proposed to secure the safe operation of various CPSs. A summary of the requirements that CPSs need to satisfy their operation is highlighted, and an analysis of the benefits and drawbacks of model-based and data-driven techniques is carried out. The roles of machine learning in cyber assault are reviewed. In order to direct future study and motivate additional investigation of this increasingly important subject, some challenges that have been unaddressed, such as the prerequisites for CPSs, an in-depth analysis of CPS characteristics and requirements, and the creation of a holistic review of the different kinds of attacks on different CPSs, together with detection and mitigation algorithms, are discussed in this review.

Keywords: cyber-attack; cybersecurity; cyber-physical systems; detection

check for updates

Citation: Mtukushe, N.; Onaolapo, A.K.; Aluko, A.; Dorrell, D.G. Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems. *Energies* **2023**, *16*, 5206. https://doi.org/10.3390/en16135206

Academic Editor: Edmund Widl

Received: 11 May 2023
Revised: 11 June 2023
Accepted: 30 June 2023
Published: 6 July 2023

1. Introduction

Since the beginning of the millennium, there has been an exponential increase in the use of the modern computer for different forms of computation at any given time and place. Currently, many different fields of computation are focusing on cyber-physical systems (CPSs) to increase reliability, resilience, and the safety of physical processes [1–3]. A CPS involves the combination of several areas of science and engineering to achieve a unified task [4]. One of the widely used definitions of a CPS is the "integration of calculation and physical process, which involves embedded computers, network monitoring and controlling the physical process". The physical processes are usually engineering processes in systems such as bio-medical systems, defense systems, electrical power systems, process control in chemical and mechanical engineering systems, and transportation systems [5–9].

A cyber system often involves 3C technology (communication, computation, and control) with a feedback loop to the physical system. With a feedback loop, real-time communication, usually two-way, is achieved to monitor and control the physical system in a safe and reliable way. Generally, a CPS has actuators, sensors, and other communication links/protocols that interface with the physical system. They are mostly supervised by a supervisory control and data acquisition (SCADA) system or other dedicated control centers [10,11]. A SCADA system oversees the high-level management and control of the CPS. In early SCADA systems, communication was usually between a few devices via telemetry, which allowed for regulated access to information between linked devices in a CPS [12]. These SCADA systems were known as "monolithic" SCADA systems because of the closed communication network that was usually adopted [13,14]. As the use of the internet has increased in recent years, "networked" SCADA systems were developed. A networked SCADA system can be hosted on local area networks (LANs) or wide area networks (WANs) to exploit information technology (IT) for dedicated communication [15]. For example, in smart grids, for a typical CPS, measurements such as voltage, current, and frequency are collected from physical plants by the sensors and transmitted via remote terminal units (RTUs) to the SCADA system that hosts various control architectures; signals are sent back to different actuators in the physical plant for efficient and safe operation [16]. A CPS involves a heterogeneous integration of subsystems with physical and network characteristics. The open communication structure of a CPS allows for tampering, falsification, delay, invasion, and other kinds of attack on the data transmission that may affect the physical operation of the system [17–19]. These cyber-attacks are a major concern in terms of the safety, reliability, resilience, and security of a CPS. The impacts of an attack on a CPS can range from service disruption and theft, to equipment damage and information theft, as well as, in more severe cases, the loss of lives.

Over the years, several kinds of attacks have been successfully launched on various CPSs. The passport control system at the Istanbul Ataturk airport was attacked by hackers, which led to the delay and cancellation of flights [20]. The David–Besse nuclear plant in Ohio was attacked by the Slammer worm from a contractor's system. The worm initiated a denial of service attack on the control system. The impact of the worm led to the deactivation of the safety and protection devices for about 6 h [21]. In 2007, the code-named "Aurora" attack was launched on a generator control system. This led to the continuous tripping of the protection devices, which caused a loss of synchronization between the generator and grid. It was reported the Aurora attack caused an explosion at the generator that was valued at $1 million [22]. Another successful cyber-attack with significant impact is the Ukraine attack that caused a major blackout affecting over 220,000 customers for several hours [23]. In 2009, two industrial control systems—Pacific Energy Resources, California, and Energy Future Holdings, Texas—were attacked by two ex-staff members. They attacked the leak detection system of the marine oil plant and energy forecast system of the nuclear plant, respectively [24]. In 2012, Aramco, Saudi Arabia, and RasGas, Qatar, were attacked by malware that caused significant disruptions in the generation of energy and affected business processes. An attack on a SCADA-based water CPS that caused usual behaviour in the system is reported in [25]. The attack affected the pump and caused a denial of service of the central control system. Even after the control software was reinstalled, the pumps continued to change their configurations erratically until an engineer discovered that it was a cyber-attack carried out about three months after the initial attack was launched by the attacker [24]. For health-based CPSs, attacks can be programmed on devices such as pacemakers, neurostimulators, and other embedded computers that can be programmed wirelessly [26]. It was demonstrated that implantable defibrillators can be reconfigured without permission. In 2009, an employee of the Carrell Clinic, Texas installed malware that granted remote access to the control of the heating, ventilation, and air conditioning (HVAC) system of the clinic [26]. Several other attacks have been reported in the transportation and defense sectors [27].

These cyber-attack incidents have alerted governments to the severe impacts of these attacks. Thus, various ways to ensure the security of CPSs have been enacted. For example, the National Institute of Standards and Technology (NIST) provides regulation for the security of cyber systems [28,29]. Additionally, the International Society of Automation (ISA) provides the regulation for cyber-based industrial process control systems [30]. Researchers continue to investigate the various loopholes in modern CPSs that make them vulnerable to cyber-attacks. This begins with the identification of attacks, then moves forward to impact assessments of the identified attacks, and concludes with mitigation strategies for these attacks. While several reviews have been conducted in the areas of cyber-attacks and CPSs, they do not provide a holistic review of the different kinds of attacks on different CPSs, together with detection and mitigation algorithms. To fill this gap, this review article presents a survey of cyber-attacks on various CPSs, the implementation of these attacks from a hacker's perspective, and defense (detection and mitigation) strategies from the defender's perspective.

A comprehensive literature search method was adopted in this review. The keywords "Cyberattack" and " Cyber-physical systems" were used to carry out the initial search on Google Scholar to obtain articles that were not necessarily reviewed, which including journal and conference papers. Other journal and conference databases, such as IEEE-Xplore, Science Direct, Web of science and Researchgate, were searched for peer-reviewed journal and conference papers and other specialized publications. The initial search returned 3200 articles; the articles that were returned were screened using titles not related to the subject and articles not written in English, thereby excluding 258 articles. Some web pages and duplicates were further eliminated, thereby excluding 278 articles. Further elimination based on dates was carried out; the year range of choice was 2013–2023, and the total number of relevant articles for review was 169.

The remainder of this paper is organized as follows: Section 2 discusses the basic features and requirements of a typical CPS; in Section 3, cyberattack detection, mitigation, and strategies are presented; Section 4 provides attack implementation and mitigation from an industrial perspective; Section 5 discusses the current challenges and future directions in CPS security; and Section 6 provides the conclusion.

2. Cyber-Physical Systems: Characteristics and Requirements

As previously mentioned, CPSs are an integration of physical systems with a cyber system to create a heterogeneous system. The cyber components of the CPS guarantee the intelligent, secure, resilient, and safe operation of the physical system. Nowadays, most CPSs are internet enabled and use an open-access communication network [31]. This open communication network characteristic make them highly vulnerable to cyberattacks and other malicious activities. The actuators and sensors in the physical system receive and send signals or measurement data from the SCADA system, control centers, and distributed controllers for real-time monitoring and control [32]. In this section, the essential characteristics or requirements of CPSs are discussed, because they are the targets for attackers.

2.1. Safety

Safety is essential, and it is one of the most important features of a CPS. The safe failure fraction (SFF) is defined by IEC 61508 as a confirmation of safety-related system fail-safes. This decides the safety integrity level (SIL) for safe operating functions using a risk-based approach [33]. IEC 61508 is regarded as a basic safety standard for the industry. Other standards were developed using risk acceptance, risk analysis, and hazard criteria (such as ISA 84/IEC 61511) and are in operation [34]. The intra-relationships within the CPS, the inter-relationships between the CPS and the environment, and the inter-relationships between the CPS and the users, are the root causes of safety issues [35]. Safety in a CPS is assessed by identifying assets, analyzing vulnerabilities, and measuring and evaluating probable damage [33].

2.2. Availability

The availability requirements ensure that only authorized users and systems have access to certain CPS features at all times. For a CPS, the availability of measurement data and signals from the control systems, the actuators in the physical plant, and the operator's room, including the communication devices, is important. Availability may be controlled more strictly compared to IT systems, where delays may have minor consequences. In CPSs, a delay in the availability of data may be as a result of a successful attack on the system [30].

2.3. Integrity

Integrity refers to the authenticity of the data and information that are being routed to the CPS. The transmitted data or message should be trustworthy and without compromise from unauthorized or malicious systems or users. The violation of data integrity in a CPS poses a threat to the safety of the the physical system or its environment [36,37]. The risk of data manipulation in a CPS is high; thus, some CPSs, such as those using smart grids, use a bad data detection scheme to ascertain the integrity of measurements, such as voltage and frequency, received from the power system.

2.4. Security

The security requirement of CPSs is very important, because the cyber system in a CPS structure represents the vulnerability of the entire system to malicious activities. CPS cybersecurity has been identified as a critical issue that must be continually addressed to ensure a secure and safe system. The NIST [38], ISA [39], National Infrastructure Protection Plan (NIPP), and IEEE 1402 [40,41], are amongst the several organizations working on the continuous development of the security requirements of CPSs.

2.5. Timeliness

Based on the real-time operation of CPSs, it is important that the data and information are generated and transmitted in real-time for the system to function properly [42]. Delay in the transmission and processing of data in a CPS can have varying degrees of consequence in a CPS.

2.6. Confidentiality

The confidentiality requirement in a CPS refers to the protected access of information only to authorized systems or users [36]. In IT systems, confidentiality in achieved by encrypting or protecting the information with passwords or security keys by the sender, and only authorized or dedicated systems can successfully decrypt the information. However, in a CPS, since the timeliness of data is a crucial requirement, the encryption and decryption processes do not take precedence over data availability. Therefore, methods to protect the transmitted data from external parties without compromising timeliness in the CPS are active areas of research.

2.7. Authentication and Authorization

The authorization requirement refers to prohibiting access to intruders or unauthorized persons to the system. In a CPS, authorization differentiates legal and illegal access to other CPS requirements such as data integrity, confidentiality, and availability. However, authentication refers to the process to ascertain the legitimate identity of the different communication agents within the CPS [43].

3. Cyber-Attack Detection and Mitigation Methods

Various techniques for detecting and mitigating cyber-attacks have been reported. Existing detection techniques may be categorized broadly as model-based detection or data-driven detection schemes, as illustrated in Figure 1. On the basis where state estimation is used in the detection process, model-based detection techniques may be divided into estimation-based and estimation-free approaches. In this section, the various model-based detection approaches are reviewed.

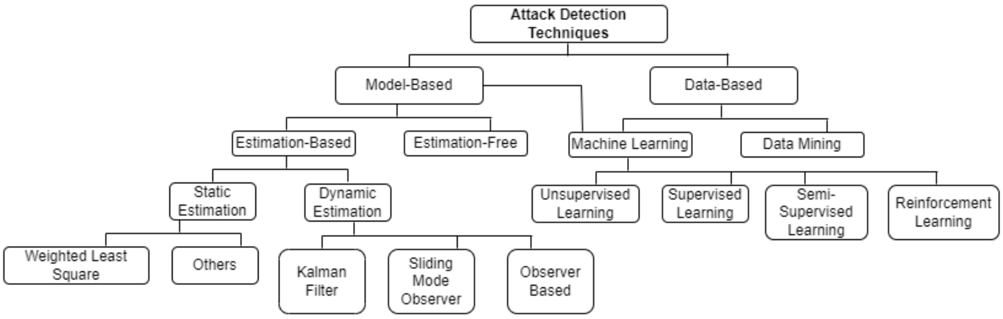

Figure 1. Classification of attack detection techniques.

3.1. Model-Based Methods

A system is often described using a state–space form when using model-based methodologies. Methods that are based on estimation are used in order to monitor the status of the system and provide analytical redundancy for the purpose of attack detection [44]. The most recent advancements in the following methods are surveyed and include the following: (1) the Kalman Filter (KF) [45,46]; (2) the Sliding Mode Observer (SMO) [47,48]; and (3) the Unknown Input Observer (UIO) [49,50].

3.1.1. Kalman Filter (KF)-Based Methods

The Kalman filter (KF) is an iterative mathematical process that executes an optimal predictor–corrector-type estimator by minimizing the estimated error covariance when certain presumptive requirements are satisfied. There are numerous attack detection algorithms that are derived from the standard KF; these include, but are not limited to, the following: an extended Kalman filter (EKF); an unscented Kalman filter (UKF); an adaptive Kalman filter (AKF); and a constrained Kalman filter (CKF). The literature indicates that hybrid implementations of these methods have been successful. To detect a false data injection attack (FDIA) in a power system CPS, a novel attack detection approach was reported in [51]. This used integrated model-based and data-driven methods. The proposed model implemented the AKF and convolutional neural networks (CNN). As a consequence of the capability of attackers to execute an FDI attack at any location in the system, a study [52] analysed the performance of a system under the risk of potential FDIAs on sensors, actuators, and physical systems, both individually and in their combined locations. The study considered the following seven attacks:

1. Compromised actuator;
2. Compromised physical system;
3. Compromised sensor;
4. Compromised actuator and physical system;
5. Compromised actuator and sensor;
6. Compromised physical system and sensor;
7. Compromised actuator, physical system, and sensor.

The impact on the security of the system under the above-mentioned attacks was analyzed. The system was modelled as a discrete linear time-invariant system with white Gaussian noise. The system incorporated both an attack detector in the form of a chi-square detector and a KF as a state estimator. A chi-square detector can reliably identify DoS attacks and other random attacks. The process measurements are sent to the system estimator equipped with a chi-square ($x^2 - detector$), and the output of the estimator provides input to the physical system. Simulation results have indicated the attacker's ability to generate errors that are bounded in certain scenarios, while in other cases, the errors can be unbounded. The effectiveness of the model was demonstrated by comparing the results with those of previous studies [53–56].

The process state and measurement of the KF-based system can be described as follows:

$$\begin{cases} x_{k+1} = A_k x_k + B_k u_k + w_k \\ y_k = C_k x_k + v_k. \end{cases} \tag{1}$$

The process state vector is x_k, where $k \in \mathbb{N}$ is the time step. $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^p$, and $y_k \in \mathbb{R}^m$ are the state, control variable, and measurement vectors, respectively. w_k is the process noise, and v_k is the measurement noise, which is white Gaussian noise with covariances Q and R that satisfy the requirements $E[w_k w_j^T] = \delta_{kj} Q_k$, $E[v_k w_j^T] = \delta_{kj} R_k$, $E[w_k v_j^T] = 0$ and $\forall_k, j \in \mathbb{N}$. The time update using the KF is given by the following:

$$\begin{cases} \hat{x}'_{k\;|k-1} = A_k \hat{x}'_{k\;|k-1} + B_k \hat{u}'_{k\;|k-1} \\ P_{k\;|k-1} = A_k P_{k-1} A_k^T + Q_k. \end{cases} \tag{2}$$

The state estimation is updated using the following:

$$\begin{cases} K_k = P_{k\;|k-1} C_k^T \left(C_k P_{k\;|k-1} C_k^T + R_k \right)^{-1} \\ \hat{x}'_k = \hat{x}'_{k\;|k-1} + K_k \left(y_k - C_k \hat{x}'_{k\;|k-1} \right) P_k = (I - K_k) P_{k\;|k-1}, \end{cases} \tag{3}$$

where $\hat{x}'_{k\;|k-1}$ is the prior estimate of the system at the time step k with the error covariance $P_{k\;|k-1}$. K_k is the KF gain, $\hat{x}'_k$ is the posterior estimate, and P_k is the error covariance. The residue signal $\hat{z}'_k$ and the state estimation error e'_k are defined by the following:

$$\hat{z}'_k \triangleq y'_k - C_k \hat{x}'_{k\;|k-1} \tag{4}$$

$$e'_k \triangleq x'_k - \hat{x}'_k. \tag{5}$$

Considering a steady-state KF where $P_{k\;|k-1}$ and K_k are constants, the error covariance matrix and KF gain are computed as follows:

$$P_k \triangleq \lim_{k \to \infty} P_{k\;|k-1} \tag{6}$$

$$K_k \triangleq P_k C_k^T \left(C_k P_k C_k^T + R_k \right)^{-1}. \tag{7}$$

In the steady state, the value of P_k is obtained by solving the discrete-time Riccati equation [52,57]. Consequently, the estimated state equation can be rearranged to yield the following:

$$\hat{x}'_{k+1} = A_k \hat{x}'_k + B_k \hat{u}'_k + K_k \left(y'_{k+1} - C_k \left(A_k \hat{x}'_k + B \hat{u}'_k \right) \right) \tag{8}$$

$$\hat{x}'_{k+1} = A_k \hat{x}'_k + B_k \hat{u}'_k + K_k z'_{k+1}. \tag{9}$$

The estimated state is sent to the controller to optimize the cost function, which is determined by the following equation:

$$J = \min \lim_{T \to \infty} \frac{1}{T} E\left[\sum_{k=0}^{T-1} \left(x_k'^T G \right) x'_k + u_k'^T H u'_k \right], \tag{10}$$

where G and H are positive weight matrices [58], and $u_k^{'}$ is the controller output. The controller gain can be calculated from the following:

$$L = -\left(B_k^T F B_k^T + H\right)^{-1} B_k^T F A_k^T, \tag{11}$$

where F is the solution of the Riccati equation, which is defined as follows:

$$F = G + A_k^T F A_k - A_k^T F B_k \left(H + B_k^T F A_k^T\right). \tag{12}$$

Finally, the x^2 detector is used for FDIA detection. In the absence of an attack, the system residue has a zero-mean and covariance defined as $(C_k P_k C_k^T + R)$. A threshold value of $n > m$ is given as input to the detector, where its computation yields the degree of freedom, and $E[z_k^{'T} \sum_z^{-1} z_k^{'} = m]$. In the absence of an attack, the value of x^2 is greater than n; otherwise, the value of x^2 is less than n. With the proposed model, seven different FDIA were detected, which demonstrated the effectiveness of the proposed model. The KF and the x^2 detector were used in [59] to investigate the performance deterioration of CPSs confronted by stealthy FDIAs.

There is no doubt that the hybrid detection method of the KF and detector is an effective technique of attack detection; however, in [60], the KF was adopted for state estimation, and the Euclidean detector was emploted for the FDIA of a smart grid. A Euclidean detector was proposed to overcome the limitations of the detector outline [61]. From the results, it was evident that the Euclidean detector could effectively detect sophisticated injection attacks.

3.1.2. Sliding Mode Observer Methods

A conventional state estimate controller has the capability to confine the system to a bounded domain; however, the system cannot converge to its original state. The variable structure control system, such as a sliding mode control, can be implemented in a CPS to mitigate the discrepancy between the actual plant and the mathematical model, which may result from disturbances. The sliding mode strategy forces the state of a system towards a manifold, from which state dynamics and estimation errors slide toward the origin of the state space [62,63]. This regulates the system's state when controlling the system and forces the state estimates toward their actual value, all within a finite amount of time and in the presence of uncertainties and disturbances. In the presence of a fault or disturbance, the SMO-based observer generates a sliding motion on the error to provide state estimates that approximate the actual output [64]. Therefore, the system dynamic behavior may be modified by the selection of the switching function. Subsequently, the closed-loop response becomes entirely insensitive to uncertainties in the system; hence, we have the robustness of the SMO [65,66].

The authors of [67] conducted a study that examined the reliability of an ASMO on a smart grid under an FDIA. The cyberattacks targeted the CPS through the actuators. The SMO error detection model was established, followed by the model for estimating the actual attack signal, which formed part of the attack reconstruction model. The reconstructed signal and the state signal were implemented in the proposed ASMO to eliminate the adverse effects of the FDIA. The proposed control strategy was evaluated in a power system with three generator buses and six load buses. The simulation results demonstrated that the proposed control technique was superior to existing results in securing the system against malicious attacks. Subsequently, in [68], the sliding mode observer was implemented in an improved approach to detect cyber attacks on power systems. The study explored the challenge of automatically detecting cyber attacks in CPSs, especially when an attacker has corrupted some state variables. Timeliness and accuracy are two characteristics that the proposed adaptive sliding mode observer ASMO-based detector must satisfy in order to perform detection and response operations that are both efficient and effective. The ASMO-based detector was equipped with parameter adjustment using a differential evolutionary algorithm. In contrast to existing techniques, the proposed methodology detected unknown attack vectors and modified the parameters to detect attacks quickly and accurately. On an IEEE-39 bus system under state attack, a conventional SMO-based detector and the ASMO-based detector were implemented for a comparative study. Based on the simulation results, the SMO-based detector did not yield accurate detection for the random attack vector. However, the ASMO-based detector showed 100% accuracy. Based on the vulnerability of conventional distributed secondary control, a DC microgrid in [47] incorporated a distributed sliding mode observer (DSMO) in its secondary control scheme. Several cyber-attacks on a communication-based hierarchical control system were presented in [69]. The simulations of the proposed model were carried out on a 48 V DC microgrid with four distributed energy resources (DERs) controlled by the DSMO-based secondary control system. The DSMO detected and compensated for the false signals with the control variables of the secondary control to eliminate the adverse impact under various types of attacks. The effectiveness of the controller was demonstrated by the experiments carried out on a 48 V DC microgrid with two DERs.

Based on a second-order SMO and a hybrid logic dynamic model, a technique for detecting open-circuit faults of a sensorless inverter was presented in [70]. However, the chattering issue of the SMO was quite severe. This encouraged a study, as reported in [71], which proposed a method of diagnosing inverter anomalies under DoS attack. The proposed control strategy incorporated the internal estimation and SMO to improve the convergence speed of the SMO and reduce chattering, thus increasing the robustness of the fault diagnosis system. The linear system is similar to (1) but can be written as follows:

$$\begin{cases} \hat{x}(t) = Ax(t) + \theta Bu(t) + Dv(t) \\ y(t) = Cx(t), \end{cases} \tag{13}$$

where $A \in \mu_{n\times n}$, $B \in \mu_{n\times 1}$, $C \in \mu_{1\times n}$, and $D \in \mu_{n\times q}$ are matrix constants. $x \in \mathbb{R}^n(x(t_0) = x_0)$, $x \in \mathbb{R}$, and $y \in \mathbb{R}$ are the state variable, input variable, and output variable, respectively. $v \in \mathbb{R}^q$ is the upper and lower bounds of both known and unknown disturbances, and θ is an uncertain parameter, and its upper and lower bounds are known as $\theta \in [\theta_-, \theta_+]$. The state output of the initial system can be estimated more accurately through the convex weighted sum upper and lower bound SMO estimator. The sliding mode gain K_s is given by the following:

$$K_s > \frac{||D||_{v_{min}} + ||D||_{v_{max}}}{||C||}. \tag{14}$$

Considering the upper and lower bound SMO expressed in

$$\begin{cases} \hat{x}'^{+}(t) = A\hat{x}^{+}(t) + \theta^{+}Bu(t) + E(y - C\hat{x}^{+}(t)) + K_s(\text{sgn}(y - C\hat{x}^{+}(t)) + Dv_{max} \\ \hat{x}'^{-}(t) = A\hat{x}^{-}(t) + \theta^{-}Bu(t) + E(y - C\hat{x}^{-}(t)) + K_s(\text{sgn}(y - C\hat{x}^{-}(t)) + Dv_{min}, \end{cases} \tag{15}$$

the weighted estimator of the state $x(t)$ is defined as follows:

$$\hat{x}(t) = \alpha\hat{x}^{-}(t) + (1-\alpha)\hat{x}^{+}(t), \tag{16}$$

where α is the weighting factor:

$$\alpha = \frac{y - C\hat{x}^{+}}{C(\hat{x}^{-} - \hat{x}^{+})}. \tag{17}$$

When α = 0, the estimated value of the interval SMO is equivalent to the estimated value of the upper bound SMO. Subsequently, when α=1, the estimated value of the interval

SMO is equal to the estimated value of the lower bound SMO. Thus, the hybrid logic model of the inverter developed in [71] can be given as follows:

$$\begin{cases} i = Ai + \theta Bu + Dv \\ y(t) = Ci. \end{cases} \tag{18}$$

The upper and lower bound SMO of (18) can be described by the following:

$$\begin{cases} \hat{i}'^{+} = A\hat{i}^{+} + \theta^{+}Bu + E(y - C\hat{i}^{+}) + K_s(\text{sgn}(y - C\hat{i}^{+}) + Dv_{max} \\ \hat{i}'^{-} = A\hat{i}^{-} + \theta^{-}Bu + E(y - C\hat{i}^{-}) + K_s(\text{sgn}(y - C\hat{i}^{-}) + Dv_{min}. \end{cases} \tag{19}$$

Hence, the real-time estimate of the system can be obtained from the following equation:

$$\hat{i} = \alpha\hat{i}^{-} + (1 - \alpha)\hat{i}^{+}. \tag{20}$$

The observations from the simulation demonstrate that the technique is highly effective for the detection of inverter DoS attacks.

3.1.3. Unknown Input Observer Methods

A variety of factors necessitate many plants to be modeled with disturbances. Conventional observers have a Luenberger structure that requires the utilization of all input signals to get an estimate of the state vector. This makes the implementation of such observers more challenging. Hence, this constraint makes them inefficient for a wide variety of applications. In contrast, unknown input observers (UIOs) treat uncertainty and disturbance as unknown inputs, thereby allowing them to be approximated and exploited in closed-loop control and to operate in real-time [18,72]. Thus, their use in attack detection applications becomes more feasible.

A fault detection problem was addressed in [73] for non-linear continuous-time multi-agent systems with external disturbances and random time-varying delay. External perturbations and errors caused by other agents were designated as unknown inputs and separated into two components to overcome the UIO's rigorous rank requirements. Based on the established numerical model and simulation results, system faults were efficiently detected, and the residual signal was resilient against disturbances.

An innovative UIO-based sensor detection technique for an MG with various types of energy sources was presented in [72]. The load fluctuations and output power variations were modeled as unknown inputs. The simulation results provided a measure of the model's degree of accuracy. The results illustrated the sensor's ability to detect various types of sensor faults and the robustness of the isolation scheme.

Three novel methods for estimating unknown inputs were developed in [74]; the success of each technique was contingent on the configuration of the system's unknown inputs. A UIO was developed in [75] as a mechanism for state estimates of the load frequency control (LFC) loop of a power system that considered renewable energy sources as unknown inputs. A new UIO that is able to yield the asymptotic system state estimate and unknown input reconstruction concurrently through an interval observer was developed in [76].

In [19], the authors presented a secondary frequency control, which is a hybrid-based control strategy. The UIO was implemented in a standalone MG for state estimation, cyberattack detection, and reconstruction. In order to reduce the degree of frequency variation that the cyberattack may have driven, a type-2 fuzzy logic system was implemented. The stand-alone MG model can be represented in a state–space form and is similar to (1) and (13):

$$\begin{cases} X'(t) = AX(t) + BU(t) + Ed(t) \\ Y(t) = CX(t), \end{cases} \tag{21}$$

where A, B, C, and E are the state, input, output, and disturbance matrices, respectively. X, U, and d are the state, known input, and unknown input or disturbance vectors, respectively. The proposed UI model was defined with the following variables: $Z(t)$ is the state vector of the UIO, and $\hat{X}(t)$ is the estimated state of the MG. The parameters N, G, Q, and H are matrices that describe the estimation characteristics of the UIO. The state estimation error must satisfy the following condition in the presence of unknown inputs:

$$\lim_{t \to \infty} e(t) = X(t) - \hat{X}(t) = 0. \tag{22}$$

Consider the first derivative of (22), which is given by the following:

$$\dot{e}(t) = \dot{X}(t) - \dot{\hat{X}}(t) = 0. \tag{23}$$

Expanding $\dot{e}(t)$ yields the following:

$$\begin{aligned} \dot{e}(t) =& (A - HCA - QC)e(t) + (N - (A - HC_1A_1 - QC))Z(t) \\ & + (Q_2 - (A - HCA - Q_1C))Y(t) + (T - (I - HC))BU(t) \\ & + (HC - I)Ed(t), \end{aligned} \tag{24}$$

which must satisfy the following:

$$\begin{aligned} & H = (CE)^{-1}E, \quad T = I - HC, N = A - HCA - Q_1C, \\ & Q_2 = NH, \quad Q = Q_1 + Q_2. \end{aligned} \tag{25}$$

If all the eigenvalues of N are stable, then $e(t)$ will approach zero asymptotically. Thus, (24) can be reduced and expressed as the following:

$$\dot{e}(t) = Ne(t). \tag{26}$$

The necessary and sufficient conditions to be satisfied for the UIO are the following:

- $\text{rank}(CE) = \text{rank}(E)$;
- $(C,\ P)$ is a detectable pair, where $P = A - E\big((CE)^T CE\big)^{-1}(CE)^T CA$.

3.1.4. Model-Based Machine Learning Methods

The basic principle of model-based machine learning methods is to develop a typical custom model that is specifically designed for particular applications. Examples of model-based machine learning methods are given in [77–79]. Machine learning methods are discussed further in Section 3.2.2.

3.1.5. Advantages and Disadvantages of Model-Based Methods

Memory is an essential resource for data-driven detection algorithms, since the process of monitoring a large number of training samples demands the use of extensive amounts of the resource. The key advantage that model-based detection algorithms provide over data-driven detection algorithms is their independence from the historical dataset, which is a necessary requirement for data-driven detection algorithms. The substantial amount of computing complexity required for each measurement sample obtained is a major hindrance. When an iterative process that has potential divergence concerns is involved, the severity of this issue is amplified significantly. As a direct consequence, the algorithm scalability is adversely affected. The most significant disadvantage of using model-based algorithms is the requirement for both the system parameters and a model. The performance of this detection method might be compromised by any slight inaccuracies in these parameters. Table 1 briefly summarizes the different model-based techniques discussed in the reviewed literature. The next section will review data-driven methods, which have the advantage of being model-free.

Table 1. A summary of model-based methods and their detection accuracies.

Reference	Method	System	Attack Type/Mode	Attacked Element	Detection Accuracy/Rate	Measures
[80]	EKF	Automotive Systems	DoS FDIA	Path Tracking: control of autonomous vehicles	High	Detection and isolation
[81]	KF	Industrial Control Systems (ICS)	Zero-Alarm	Sensor	90 %	Detection
[82]	Sliding Mode Observer	Power Systems	FDIA	Load Frequency Control System	High	Detection and isolation
[83]	Optimal Sliding mode observer	Magneti-Tape-Drive Servo System	FDIA	Actuators	High	Detection
[84]	UI Interval Observer-Based	Smart Grid	FDIA	Smart Sensor	-	Detection and isolation
[49]	UI Observer-Based	DC Micro-Grid	FDIA	Phasor Measurement Unit (PMU)	-	Detection and isolation
[85]	Distribution System State Estimation (DSSE)	Power System	Generic	-	High $\approx$ 100%	Detection
[86]	Sliding Mode Observer	Generic Sub-System	FDIA	Sensor	-	Detection and mitigation
[87]	Weighted Least Square (WLS)	Smart Grid	FDIA	-	High	Detection
[88]	Watermarking	Control System	DoS	Sensor Attack	High	Detection

3.2. Data-Driven Methods

Data-driven methods are model-free, i.e., the detection process of an FDIA involves neither models nor system parameters, unlike the model-based methods. Data-driven methods can be divided into three main groups based on the data used to detect the FDIA in a smart grid. These are the following [87]:

1. Data mining methods.
2. Machine learning methods.
3. Other methods outside of 1 and 2.

3.2.1. Data Mining Methods

These methods are applied to large datasets to discover patterns. Data measurement variables received from a particular system can be processed to draw inferences about data patterns or hidden features using data mining methods. The data mining method is an interdisciplinary field, because it is interconnected with machine learning methods and statistics. The authors of [89] explored the data mining methods in Twitter's Smart Living Environments to address security issues using nearly one million tweets collected under the user-generated data (UGD) framework. These were subjected to a random forest classifier, logistic regression, a multinomial naïve Bayes classifier, and a support vector classifier under the sentiment analysis.

Tomasevic et al. [90] explored data mining methods to investigate the performance of students during exams. This was done to discover high-risk students who were on the verge of dropping out from a particular course to forecast their final exam scores. It was discovered that demographic data did not give sufficient forecasting accuracy, but past performance data and student engagement data gave high precision when fed into artificial neural networks.

Salo et al. [91] conducted a review to detect intrusion systems using data mining methods. The research gap that established the efficiency of the classifiers in identifying network traffic intrusions when aging datasets are used for training was observed. Mughal [92] reviewed the tools and algorithms used in web data mining techniques. Different web data mining types, which help to find informative data from increasingly large and difficult web domains, were described.

Data mining techniques were used in educational environments as described in [93]. These techniques help better understand student results, interests, and behavior. The work reviewed more than 100 documents, analyzed 7 domains, and discussed 12 data mining techniques used to solve, understand, and analyze problems in an educational environment.

Data mining techniques were applied in the study reported in [94] to identify significant features in forecasting heart disease. The study developed prediction models for heart disease using a combination of seven classification techniques: logistic regression, naive Bayes, support vector machine, vote (a hybrid method involving logistic regression and naive Bayes), neural network, decision tree, and k-NN. The forecasting of the survival of heart failure patients was improved when using data mining methods and synthetic minority oversampling techniques [95]. For effective prediction, the study used nine classification models: support vector machine, extra tree classifier, random forest, logistic regression, decision tree, gaussian naive Bayes classifier, gradient boosting classifier, stochastic gradient classifier, and adaptive boosting classifier.

The study reported in [96] integrated data mining algorithms into the PostgreSQL management system. The induction rule and decision tree data mining algorithms were analyzed in the process. This resulted in higher results and response time. Decision making for predicting student performance in the university admission systems was investigated using data mining methods in [97]. The applicants' early academic performance outcomes were predicted with high precision based on some pre-admission criteria such as general aptitude test scores, scholastic achievement admission test scores, and high school grade averages.

3.2.2. Data-Based Machine Learning Methods

In data-based machine learning (ML) methods, machines can be trained to do complex tasks; ML algorithms are data-driven and, therefore, depend largely on the data input from the system to enhance the learning of the machine. Based on the learning procedures of the machine, ML can further be classified as unsupervised learning, supervised learning, and reinforcement learning methods. These methods are reviewed below.

Unsupervised Learning Method

This machine learning method clusters and analyzes unlabeled data to find hidden patterns and classifications without the necessity of human intervention. The machine classifies the data points according to their hidden structures, thereby discovering false data injection algorithms (FDIA), because their data classes should be different from that of normal data in smart grids. Examples of unsupervised learning methods are the hidden Markov model (HMM), probabilistic neural network (PNN), deep belief network (DBN), isolation forest (IF), hierarchical clustering (HC), principal component analysis (PCA), fuzzy clustering (FC), and k-means clustering (KMC). The KMC methods is popular in classification problems, where it works by separating into k clusters and the s observed variables. The cluster prototype, which is the nearest mean, dictates which observation s

belongs to a particular cluster k. For n samples s of mean φ_i in k sets y, the minimization problem, is defined as follows [87]:

$$\arg\min_{y} \sum_{i=1}^{k} \sum_{s \in y_i} ||s - \varphi_i||^2, \tag{27}$$

where y_i is the set with mean φ_i. Although this method is very sensitive to sample noise, its advantage is embedded in its simplicity. In FC, a sample could be a subset of many clusters with diverse grades, thereby leading to a more elaborate clustering process and giving rise to overlapped clusters with well-defined boundaries. HMM is a unique time series model used in FDIA detection for predicting sample models [98]. PNN is a form of feedforward neural network (FNN), which is much faster than multilayer perceptron networks. It is mostly used in classification problems and pattern recognition [99]. In DBN, the time for training the network can be reduced by setting the initial weights as the learned weights and later turning it into a generatively pre-trained deep neural network (DNN) by backpropagation [100]. IF, which is a collection of different isolation trees, is acknowledged as an outlier detection method. With more dimensional datasets, there is a higher possibility of more isolation trees in IF. Because anomalies, such as false data, are usually different from other data, the IF method can isolate them, since there are few of them [101]. In summary, each of these methods is unique despite giving similar results.

Supervised Learning Methods

This machine learning method clusters and analyzes labeled data to find hidden patterns and classifications. This is done with human aid. Thus, each output has a link to a particular input. Examples of supervised learning methods are linear regression (LR), random forests (RF), decision tree (DT), extended nearest neighbor (ENN), k-nearest neighbor (KNN), the extreme learning machine (ELM), autoencoder (AE), artificial neural networks (ANN), and the support vector machine (SVM). LR models, which are known to be simple and straightforward to implement, highlight a connection between independent variable x and dependent scalar variable $f(x)$ so that the following is obtained [102]:

$$f(x) = wx + b, \tag{28}$$

and minimizing, using the least square method, gives the following:

$$\min_{w,b} \sum_{i} (f(x_i) - (wx_i + b))^2, \tag{29}$$

where b and w represent the bias and weight vectors, respectively.

DT models predict their outputs by mapping samples to their targets. The DT learns by creating subsets from input variables. The DT is easy to construct but has the problem of overfitting [103]. RF models have been developed to overcome the problems of overfitting in neural networks by using ensemble learning. Several DTs can be combined to form an RF. The mean and mode values of individual tree classifications lead to the classification of the RF [104].

In the KNN method, a sample is assigned to the class of the nearest possible k-neighbor by the classifier. The assigned class is determined by the Euclidean distance between the prelabeled sample s_j and the unlabeled sample s_i:

$$d_{i,j} = ||s_i - s_j||_2. \tag{30}$$

The classification of the new sample is determined by the lowest distance between the prelabeled samples and the unlabeled sample. The disadvantages of this technique are the prelabeled sample density and distribution [105]. The ENN method was designed to overcome these disadvantages by considering local neighbors of the class and the global distribution to predict the class of the new sample [106].

An AE is a neural network providing nonlinear solutions by decoding and encoding sample variables. When the error between the network input and the decoded sample exceeds a threshold level, an alarm is triggered, which results in the detection scheme. The limitation of this technique is the extensive training time required [107]. Meanwhile, the ELM method was designed to overcome this disadvantage such that the biases of the hidden layers and input weights of ELM are randomly chosen [108].

The ANN was inspired by the working principles of the biological brain [109]. It is used to approximate, estimate, and classify functions [110]. An ANN can have one or multiple hidden layers [111,112]. The output produced by an ANN depends on the activation function, bias, and input weighted sum to the neuron [113].

A convolutional neural network (CNN) does not adopt the matrix multiplication that is generally used, but instead uses the convolution at the layers. It has found wide application in image processing and pattern recognition because of its ability to obtain different characteristics from samples [114].

The deep neural network (DNN) is another neural network method with a high level of precision due to its multiple hidden layers [115].

An SVM is a binary-based non-probabilistic linear method that is based on two parallel hyper-plane boundaries that yield the following:

$$w^T(\phi)s_i + b = +1, \quad \text{if } y_i = +1 \tag{31}$$

$$w^T(\phi)s_i + b = -1, \quad \text{if } y_i = -1, \tag{32}$$

where samples s_i are mapped by function $\phi(.)$ to a linearly separable space, b is the offset constant, and w is the hyperplane orthogonal normal vector. The limitations of an SVM are the requirement for extensive training time and the choice of the kernel function, while its simplicity of implementation is its major advantage [66].

Semi-Supervised Learning Method

Semi-Supervised learning predicts the output using labelled data; it also learns the larger data distribution shape using unlabelled data. Semi-Supervised learning also has applications in cybersecurity, as shown in [116–118].

Reinforcement Learning Methods

In this method, the previous experiences of the machine help it to chart a new course that leads to optimal action. This is achieved through the trial-and-error method, which leads to a series of fruitful choices in the reinforced process by solving the problem in an appropriate manner [119].

3.2.3. Advantages and Disadvantages of Data-Driven Methods

Advantages

The advantages of data-driven methods as compared to their model-based counterparts include the following [120–123]:

1. It has a more powerful ability to select informative samples.
2. Although its training is slower, its prediction is faster.
3. Its dependence on prior assumptions and human experiences is low.
4. It is more efficient to run computationally and simple to implement.
5. It depends on the I/O data and does not depend on the prior knowledge of the system in question.
6. Updating the model with changing conditions over time is straightforward.

Disadvantages

Its comparative disadvantages include the following [120,121]:

1. Designing a good data-driven network architecture is a huge task.

2. Its statistical and physical meaning may not be very clear.
3. It usually requires considerable amounts of sample data for training.
4. The availability of sufficiently large empirical and historical data determines the confidence level of its predictions.
5. In some instances, such as the case of a new component or system, obtaining historical data may be difficult. Some cases may require a long time and expensive tests to generate the required data.

Table 2 briefly summarizes the different model-based techniques discussed in the reviewed literature.

Table 2. A summary of data-based methods and their detection accuracies.

Reference	Method	System	Attack Type/Mode	Attack Parameter	Detection Accuracy/Rate	Measures
[124]	Dynamic-Estimator-Based Cyber-Attack Tolerant Control (CTC)	Power Systems	Generic (malware attacks, password attacks, phishing attacks, and SQL injection attacks)	-	Estimation error $\approx 10^{-17}$; norm order $\approx 10^{-34}$, which is ≈ 0.	Detection and isolation
[125]	Federated Learning, (Gated Recurrent Units and Random Forest)	Vehicular Sensor Networks (VSN)	Intrusion	Car Hacking: Attack and Defense Challenge 2020 dataset.	99.52% and 99.77%	Detection
[126]	Short Circuit Analysis	Industrial Power Plants	Short-Circuiting	Equipment (transformer, breaker, generator, etc.) security breach	High	Detection
[127]	Parallelized Database Approach	Healthcare Systems	Malicious transactions, damage	Damage assessment	High	Detection and isolation.
[128]	Retrospective Impact Analysis	National Health Service (NHS)	WannaCry attack, ransomware attack.	Missed appointments, deaths, and fiscal costs attributable to the ransomware	High	Detection
[129]	A Hybrid Deep Random Neural Network	Industrial Internet of Things (IIoT)	Generic	Two IIoT security-related datasets	98% and 99%	Detection
[130]	Survey	Unmanned Aerial Vehicles (UAV)	Channel jamming, message interception, deletion, injection, spoofing, etc.	Cyberattack countermeasures	-	Prevention, detection, and mitigation
[131]	Unified Architectural Approach	Industrial Control Systems (ICSs)	Generic	Cyberattack resilience	High	-
[132]	Controller Switching	Process Control System (PCS)	Multiplying the data communicated over the link by a factor	Control system and attack-sensitive parameters	High	Detection
[133]	AI Engine, Two-Fold Feature Selection, and Hyper-Parameter Optimization	Network Traffic System	Intrusion	Binary attack, synthesized atypical attack flows	90%	Detection

3.3. The Role of Machine Learning Methods in Cyber Assaults

ML methods are now widely used to salvage many cyber assaults; such roles are categorized into five classes: the analysis of raw data; the management of alerts; the detection of assaults; the assessment of risk exposure; and threat intelligence.

3.3.1. Analysis of Raw Data

The cybersecurity domain deals with heterogenous systems that generate different types of raw data, such as alerts, reports, and logs. ML leverages its ability on such raw data to maximize the opportunities to provide solutions to cybersecurity problems. The more the availability of such data, the more promising the use of ML in cyber security. The benefits of such data came to the fore after several high-profile cyber-assaults. In [134], large-scale log analysis was carried out using ML, in which, out of the 800 incidents detected, 65% were discovered to be true cybersecurity incidents, whereas the non-ML methods used were only able to detect 8 incidents correctly. Likewise, in [135], DeepLog was trained on only 1% of the available data, but achieved a cybersecurity detection rate of almost 100%.

3.3.2. Management of Alerts

It is known that, with or without ML, a perfect detection system cannot be developed. Hence, ML has been used to prevent the automatic execution of actions due to incorrect predictions. Detection system outputs come in the form of alerts, and thousands of such alerts are generated in modern environments every hour [136,137]. To overcome this challenge, ML could be deployed to filter, prioritize, and aggregate the alerts into a more generalized event [138]. Significant quantities of alerts are not malicious but amount to false alarms. Such alerts could be filtered using ML; for instance, in [139], ML was able to reduce false alarms by about 75% as against about a 30% reduction of false alarms using a non-ML method. In situations where many alerts are encountered by security administrators, ML has been used to identify and prioritize the most critical alerts, as ML ranks alerts in order of sensitivity [140]. Also, large amounts of data are well managed by aggregating similar alerts, finding correlations between them, and identifying causal relationships responsible for security problems [141].

3.3.3. Detection of Assaults

Before ML methods were developed, existing cybersecurity detection methods were error-prone, time-consuming, and unable to cope with modern environments that are characterized by increasing growth. But with ML, there are fewer manual efforts, and greater accuracy is achieved [142]. This improved performance is due to ML's intrinsic capability to learn weak signals or make up for missing data and outliers. ML analyzes large data by learning patterns, thereby identifying abnormal or irregular activities from normal or regular ones [143].

3.3.4. Assessment of Risk Exposure

ML strengthens a system by concentrating on its weak point and predicting its most likely threat. In [144], ML crafted attacks using reinforcement learning against a network intrusion detection system (NIDS), which achieved a 90% speedup as against a random attack process. In [145], the weaknesses of databases were assessed against SQL injection attacks using ML were investigated. In the study reported in [146], fake user accounts on social media were identified by correlating different sources using ML, thereby reducing such accounts by 30%.

3.3.5. Threat Intelligence

Threat intelligence acts by collecting and analyzing data for anticipated novel attacks. This is a proactive method for keeping defenses up-to-date, as reported in [147], where threat intelligence using the ML method was configured in such a way that the protection of the business with the most-critical infrastructure was prioritized. Examples where ML was used in threat intelligence can be found in [148–151].

4. Industrial Review

There have been several published studies on industrial cyber-attacks, but there is a need for publication of more up-to-date and relevant research. Ref. [152] presented the results of attack simulations published between 1999 and 2019 and highlighted the steps taken that resulted in successful attacks. The results garnered eleven key contributions and different implementation methods for attack simulations. However, the methodology for constructing a fully unified view of attack simulation remains unclear.

In [153], the IoT-based cyber-attack paths to critical industrial services and infrastructure were assessed in a risk-like manner to determine their current threat and to explore mitigation methods for different application domains.

An exploration of machine learning techniques regarding the stability and security of power systems was carried out in [154]. A comprehensive review of the studies using machine learning methods for the stability and security of the power systems was carried out. In particular, dynamic security assessment, power quality disturbance, and cyber-attack detections were focused on. The limitations, contributions, and methodologies of the test systems, datasets, and classifier designs were highlighted.

Setola itet al [155] presented the behavior of process-engineering-based cyber-attacks. Some relevant approaches, which are useful for protection against industrial control systems, were considered.

In [156], a cyber-attack detection model for industrial control systems was developed using an ensemble deep learning method. This constructed a balanced representation for the problem of the imbalanced nature of industrial control system datasets. The model helps improve the security of the network in preventing critical failures in the industrial control system against cyber-attacks.

The authors in [157] reviewed and defined industrial cyber-physical systems from a cyber-security viewpoint. Real-life industrial cyber-physical system incidents were evaluated using multi-dimensional adaptive attack taxonomy. In [158], the manufacturing sector was the focus of the review of cyber-security problems in critical infrastructures in the industries. The study helped in developing strategies for modeling cyber-security objectives for the mitigation of the effects of cyber-attacks on industrial control system infrastructures.

In [159], the authors proposed a key component kit in an industrial control system as a robust cyber-attack detection method using false data injection techniques in nuclear power plant settings. In the study reported in [160], cyber-security standards were reviewed, and roadmaps were provided to implement, converge, map, align, and identify the right strategies and standards for securing Industrial Internet of Things machine-to-machine communications.

Currently, in most governmental and non-governmental institutions, social, cultural, commercial, and industrial operations are executed in cyber-space. Many of these establishments are currently facing cyber-attacks. Without electronic technology, it is a big challenge to protect this data from cyber-attacks. Cyber-Attacks target industries and other establishments to cause financial, political, or military havoc [161]. The havoc could take the form of data distribution services (DDSs), knowledge breaks, and PC viruses. As a result, establishments use different solutions to protect their systems against cyber-attacks. This section is reviewed to re-emphasize the need for the awareness of industrial cyber-attacks and to showcase some recent advances in industrial prevention and mitigation methods. Researchers globally have proposed different methods, which are either in the study phase or operation phase.

5. Current Challenges and Future Directions

The integration of a CPS into critical infrastructure systems has greatly improved efficiency, accuracy, and safety. However, the dependence on a CPS has made these systems vulnerable to cyber-attacks. In this section, the current challenges and future directions of cybersecurity for a CPS are discussed.

5.1. Complexity of CPS Models

As previously mentioned, CPSs are complex systems that involve multiple components such as sensors, actuators, controllers, and software. This complexity makes it difficult to identify vulnerabilities and potential attack vectors. Additionally, the inter-connectivity of a CPS with other systems and networks further complicates the security landscape. The complexity also makes it difficult to accurately model a modern CPS for cyber-security studies. Thus, advanced modeling methods that can accurately capture the behaviour of emerging CPSs are required to guarantee the security of all components of the CPS.

5.2. Advanced Measurement and Data Collection Techniques

Typically, in prior research, the outcomes regarding detecting attacks, secure estimation, and secure control, particularly when faced with different kinds of attacks, were developed utilizing data from a single measurement device. However, this approach can lead to significant system degradation. In reality, physical systems such as robots and vehicles have redundant measurement devices that may remain available for feedback, even if some of them are compromised. For instance, mobile robots often have numerous measurement devices that provide information about the robot such as local and relative positions, angular velocity, and speed. These devices have different methods of implementation and function on multiple time scales. Consequently, it is hard for an adversary to attack all of these devices and jam all of the communication channels [60,162]. An investigation into applying multiple measurement devices and data collection techniques is worthy of future consideration [163–168]. Nevertheless, collecting and fusing data from various sensors is a complicated task, since most measurement devices operate non-simultaneously, which introduces new challenges due to the presence of different time scales.

5.3. Detection of Advanced and Stealthy Attacks

With the development of new technologies, cyber-attacks are advancing quickly. Advanced attacks have been launched successfully. Stealth FDIAs can be launched randomly and avoid detection by current detection techniques. Thus, preventing sophisticated attacks on a CPS is a difficult but necessary topic that requires further attention. In addition, the area of confidentiality attack detection has not been studied robustly compared to availability and integrity attacks detection. Given the need for privacy protection in a modern CPS, it is important to investigate the impacts on confidentiality attacks.

5.4. Standardization of Security Measures for a CPS

Inadequate security testing is another major challenge in cyber-security for a CPS. Many CPSs are tested for functionality but not for security. As a result, vulnerabilities may go undetected until an actual attack occurs. The standardization of security measures for CPSs will help reduce the complexity of developing security strategies. Standards should be developed for security controls, access controls, and incident response.

5.5. Testing of Detection and Mitigation Methods

In model-based detection and mitigation methods, key parameters such as detection thresholds and other control parameters play a very crucial role. However, the choice of these parameters largely affects the accuracy of the detection and mitigation methods. While some methods attempt to identify a trade-off between these parameters, since they have varying efficiencies, other methods may forgo one efficiency to optimize another. Hence, it is important to investigate the testing of current and future cyber-attack detection methods to analyze the performance and efficiency of the different detection and mitigation parameters. Additionally, CPSs have different characteristics that make the detection and mitigation methods only suitable to a specific CPS and undesirable for other types of CPSs. Thus, providing the appropriate performance analysis of existing and future CPSs is an area that is worthy of consideration.

6. Conclusions

Demands for improved security, operational efficiency, and environmental protection have hastened the adoption of CPSs, which are now standard features of modern businesses.

Given the essential nature of the services provided by CPSs, any disruption to them might have dire effects. This highlights the difficulty inherent in designing a system that can withstand attacks. This paper presents a summary of the requirements that CPSs need to satisfy, in addition to the characteristics that they are expected to exhibit. A concise categorization of the various types of detection and mitigation strategies is provided. Furthermore, recent research on the detection and mitigation techniques of cyber-attacks in CPSs has been discussed, and models have been described. Subsequently, an analysis of the benefits and drawbacks of model-based and data-driven techniques was carried out. This paper presents a survey of the relevant industrial research. In conclusion, the limitations and opportunities for future research focuses were discussed. These are based on recent advancements.

Author Contributions: Conceptualization, N.M., A.K.O., A.A. and D.G.D.; methodology, N.M., A.K.O. and A.A.; formal analysis, N.M., A.K.O. and A.A.; investigation, N.M., A.K.O. and A.A.; writing—original draft preparation, N.M., A.K.O. and A.A.; writing—review and editing, A.A. and D.G.D.; visualization, N.M., A.K.O. and A.A.; supervision, D.G.D.; project administration, A.A. and D.G.D.; funding acquisition, D.G.D. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the NRF BRICS Grant no. 128892.

Data Availability Statement: Not applicable.

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

Abbreviations

AKF	Adaptive Kalman Filter
ANN	Artificial Neural Network
ASMO	Adaptive Sliding Mode Observer
CKF	Contrained Kalman Filter
CNN	Convolutional Neural Networks
CPS	Cyber-Physical System
DER	Distributed Energy Resource
DoS	Denial of Service
DSMO	Distributed Sliding Mode Observer
DT	Decision Tree
EKF	Extended Kalman Filter
ELM	Extreme Learning Machine
FDIA	False Data Injection Attack
IoT	Internet of Things
KF	Kalman Filter
ML	Machine Learning
SCADA	Supervisory Control And Data Acquisition
SMO	Sliding Mode Observer
SVM	Support Vector Machine
UIO	Unknown Input Observer
UKF	Unscented Kalman Filter

References

1. Fan, H.; Ni, M.; Zhao, L.; Li, M. Review of cyber physical system and cyber attack modeling. In Proceedings of the 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Nanjing, China, 20–23 September 2020; pp. 1–5.
2. Liu, Y.; Peng, Y.; Wang, B.; Yao, S.; Liu, Z. Review on cyber-physical systems. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 27–40. [CrossRef]
3. Lozano, C.V.; Vijayan, K.K. Literature review on cyber physical systems design. *Procedia Manuf.* **2020**, *45*, 295–300. [CrossRef]
4. Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man Cybern.-Part A Syst. Hum.* **2010**, *40*, 853–865. [CrossRef]
5. Franze, G.; Fortino, G.; Cao, X.; Sarne, G.M.L.; Song, Z. Resilient control in large-scale networked cyber-physical systems: Guest editorial. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1201–1203. [CrossRef]

6. Zhang, Y.; Qiu, M.; Tsai, C.W.; Hassan, M.M.; Alamri, A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Syst. J.* **2015**, *11*, 88–95. [CrossRef]
7. Muthuppalaniappan, M.; Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *Int. J. Qual. Health Care* **2021**, *33*, mzaa117. [CrossRef]
8. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**, *9*, 5326–5340. [CrossRef]
9. Liagkou, V.; Kavvadas, V.; Chronopoulos, S.K.C.; Tafiadis, D.; Christofilakis, V.; Peppas, K.P. Attack Detection for Healthcare Monitoring Systems Using Mechanical Learning in Virtual Private Networks over Optical Transport Layer Architecture. *Computation* **2019**, *7*, 24. [CrossRef]
10. Duo, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–800. [CrossRef]
11. Hallaji, E.; Razavi-Far, R.; Saif, M. Detection of malicious SCADA communications via multi-subspace feature selection. In Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020; pp. 1–8.
12. Van Long, D.; Fillatre, L.; Nikiforov, I. Sequential monitoring of SCADA systems against cyber/physical attacks. *IFAC-PapersOnLine* **2015**, *48*, 746–753.
13. Bernieri, G.; Miciolino, E.E.; Pascucci, F.; Setola, R. Monitoring system reaction in cyber-physical testbed under cyber-attacks. *Comput. Electr. Eng.* **2017**, *59*, 86–98. [CrossRef]
14. Yang, L.; Cao, X.; Li, J. A new cyber security risk evaluation method for oil and gas SCADA based on factor state space. *Chaos Solitons Fractals* **2016**, *89*, 203–209. [CrossRef]
15. Liu, S.; Wei, G.; Song, Y.; Liu, Y. Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks. *Neurocomputing* **2016**, *207*, 708–716. [CrossRef]
16. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 13–27. [CrossRef]
17. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Comput. Ind.* **2018**, *100*, 212–223. [CrossRef]
18. Aluko, A.O.; Carpanen, R.P.; Dorrell, D.G.; Ojo, E.E. Real-Time Cyber Attack Detection Scheme for Standalone Microgrids. *IEEE Internet Things J.* **2022**, *9*, 21481–21492. [CrossRef]
19. Aluko, A.; Musumpuka, R.; Dorrell, D. Cyberattack-Resilient Secondary Frequency Control Scheme for Stand-Alone Microgrids. *IEEE Trans. Ind. Electron.* **2022**, *70*, 1622–1634. [CrossRef]
20. Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-security incidents: A review cases in cyber-physical systems. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 499–508.
21. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-Physical Systems Security*; Citeseer: San Francisco, CA, USA, 2009; Volume 5.
22. Zeller, M. Common questions and answers addressing the aurora vulnerability. In Proceedings of the DistribuTECH Conference, Tulsa, Okla, 2 February 2011.
23. Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. *Electr. Inf. Shar. Anal. Cent. (E-ISAC)* **2016**, *388*, 1–29.
24. Loukas, G. *Cyber-Physical Attacks: A Growing Invisible Threat*; Butterworth-Heinemann: Oxford, UK, 2015.
25. Cao, X.; Wei, C.; Li, J.; Yang, L.; Zhang, D.; Tang, G. The geological disasters defense expert system of the massive pipeline network SCADA system based on FNN. In Proceedings of the Web Technologies and Applications: APWeb 2012 International Workshops: SenDe, IDP, IEKB, MBC, Kunming, China, 11–13 April 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 19–26.
26. Bradbury, D. The World's Dumbest Hackers. *Infosecurity* **2011**, *8*, 16–19. [CrossRef]
27. Kennedy, D.; Simon, R. Pentesting over Power lines. *Defcon* **2011**, *2011*. [CrossRef]
28. Gopstein, A.; Gopstein, A.; Nguyen, C.; Byrnett, D.S.; Worthington, K.; Villarreal, C. *Framework and Roadmap for Smart Grid Interoperability Standards Regional Roundtables Summary Report*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
29. Stouffer, K.; Falco, J.; Kent, K. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security. *NIST Spec. Publ.* **2006**, *800*, 82.
30. Cardenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 2008 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500.
31. Rezaee, H.; Abdollahi, F. Secure consensus control of multiagent cyber-physical systems with uncertain nonlinear models. *IEEE Syst. J.* **2019**, *14*, 3539–3546. [CrossRef]
32. Gawand, H.L.; Bhattacharjee, A.; Roy, K. Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach. *Nucl. Eng. Technol.* **2017**, *49*, 484–494. [CrossRef]
33. Lyu, X.; Ding, Y.; Yang, S. Safety and security risk assessment in cyberphysical systems. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 221–232. [CrossRef]
34. Catelani, M.; Ciani, L.; Luongo, V. Safety analysis in oil & gas industry in compliance with standards IEC61508 and IEC61511: Methods and applications. In Proceedings of the 2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Minneapolis, MN, USA, 6–9 May 2013; pp. 686–690.

35. Cheminod, M.; Durante, L.; Valenzano, A. Review of security issues in industrial networks. *IEEE Trans. Ind. Inf.* **2013**, *9*, 277–293. [CrossRef]
36. Zhu, B.; Joseph, A.; Sastry, S. A taxonomy of cyber attacks on SCADA systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 19–22 October 2011; pp. 380–388.
37. Aluko, A.O.; Dorrell, D.G.; Ojo, E.E. Observer-Based Detection and Mitigation Scheme for Isolated Microgrid Under False Data Injection Attack. In Proceedings of the 2021 IEEE Southern Power Electronics Conference (SPEC), Kigali, Rwanda, 6–9 December 2021; pp. 1–6. [CrossRef]
38. Widergren, S.; Levinson, A.; Mater, J.; Drummond, R. Smart grid interoperability maturity model. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–6.
39. Guerrero, J.M.; Vasquez, J.C.; Matas, J.; De Vicuña, L.G.; Castilla, M. Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization. *IEEE Trans. Ind. Electron.* **2010**, *58*, 158–172. [CrossRef]
40. Creery, A.; Byres, E. Industrial cybersecurity for power system and SCADA networks. In Proceedings of the Record of Conference Papers Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference, Denver, CO, USA, 12–14 September 2005; pp. 303–309.
41. Dumont, D. Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems. In Proceedings of the 2010 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 8–10 November 2010; pp. 473–475.
42. Silberschatz, A.; Galvin, P.B.; Gagne, G. *Operating System Principles*; John Wiley & Sons: Hoboken, NJ, USA, 2006.
43. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
44. Kordestani, M.; Saif, M. Observer-based attack detection and mitigation for cyberphysical systems: A review. *IEEE Syst. Man Cybern. Mag.* **2021**, *7*, 35–60. [CrossRef]
45. Filter, K.; Dmitry, Z.; Anastasiia, Y. Predicting cyber attacks on industrial systems using the Kalman filter. In Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 30–31 July 2019; pp. 317–321.
46. Ayyarao, S.L.; Tummala, V.; Inapakurthi, R.K. A Two-stage Kalman Filter for Cyber-attack Detection in Automatic Generation Control System. *J. Mod. Power Syst. Clean Energy* **2022**, *10*, 50–59.
47. Jiang, Y.; Yang, Y.; Tan, S.C.; Hui, S.Y. Distributed sliding mode observer-based secondary control for DC microgrids under cyber-attacks. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2020**, *11*, 144–154. [CrossRef]
48. Zhang, N.; Qi, W.; Pang, G.; Cheng, J.; Shi, K. Observer-based sliding mode control for fuzzy stochastic switching systems with deception attacks. *Appl. Math. Comput.* **2022**, *427*, 127153. [CrossRef]
49. Luo, X.; Wang, X.; Pan, X.; Guan, X. Detection and isolation of false data injection attack for smart grids via unknown input observers. *IET Gener. Transm. Distrib.* **2019**, *13*, 1277–1286. [CrossRef]
50. Alhelou, H.H.; Esmail, M.; Golshan, H.; Hatziargyriou, N.D. A Decentralized Functional Observer Based Optimal LFC Considering Unknown Inputs, Uncertainties, and Cyber-Attacks. *IEEE Trans. Power Syst.* **2019**, *34*, 4408–4417. [CrossRef]
51. Qu, Z.; Bo, X.; Yu, T.; Liu, Y.; Dong, Y.; Kan, Z.; Wang, L.; Li, Y. Active and passive hybrid detection method for power CPS false data injection attacks with improved AKF and GRU-CNN. *IET Renew. Power Gener.* **2022**, *16*, 1490–1508. [CrossRef]
52. Padhan, S.; Turuk, A.K. Design of False Data Injection Attacks in Cyber-Physical Systems. *Inf. Sci.* **2022**, *608*, 825–843. [CrossRef]
53. Guan, Y.; Ge, X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Trans. Signal Inf. Process. Netw.* **2017**, *4*, 48–59. [CrossRef]
54. Tu, W.; Dong, J.; Zhai, D. Optimal ϵ-stealthy attack in cyber-physical systems. *J. Frankl. Inst.* **2021**, *358*, 151–171. [CrossRef]
55. Zhang, T.Y.; Ye, D. False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach. *Automatica* **2020**, *120*, 109117. [CrossRef]
56. Ding, D.; Han, Q.L.; Ge, X.; Wang, J. Secure state estimation and control of cyber-physical systems: A survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *51*, 176–190. [CrossRef]
57. Kwon, C.; Liu, W.; Hwang, I. Security analysis for cyber-physical systems against stealthy deception attacks. In Proceedings of the 2013 American control conference, Washington, DC, USA, 17–19 June 2013; pp. 3344–3349.
58. Ye, D.; Zhang, T.Y. Summation detector for false data-injection attack in cyber-physical systems. *IEEE Trans. Cybern.* **2019**, *50*, 2338–2345. [CrossRef]
59. Mo, Y.; Sinopoli, B. On the performance degradation of cyber-physical systems under stealthy integrity attacks. *IEEE Trans. Autom. Control* **2015**, *61*, 2618–2624. [CrossRef]
60. Zhang, D.; Wang, Q.G.; Feng, G.; Shi, Y.; Vasilakos, A.V. A survey on attack detection, estimation and control of industrial cyber–physical systems. *ISA Trans.* **2021**, *116*, 1–16. [CrossRef]
61. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 370–379. [CrossRef]
62. Perruquetti, W.; Barbot, J.P. *Sliding Mode Control in Engineering*; Marcel Dekker: New York, NY, USA, 2002; Volume 11.
63. Singh, K.; Padhy, P.K. Modified PSO based PID Sliding Mode Control using Improved Reaching Law for Nonlinear systems. *arXiv* **2022**, arXiv:2209.09170.
64. Spurgeon, S.K. Sliding mode observers: A survey. *Int. J. Syst. Sci.* **2008**, *39*, 751–764. [CrossRef]

65. Nguyen, M.H.; Dao, H.V.; Ahn, K.K. Extended sliding mode observer-based high-accuracy motion control for uncertain electro-hydraulic systems. *Int. J. Robust Nonlinear Control* **2023**, *33*, 1351–1370. [CrossRef]
66. Wang, H.; Shao, Y.; Zhou, S.; Zhang, C.; Xiu, N. Support Vector Machine Classifier via *L*_{0/1} Soft-Margin Loss. *arXiv* **2019**, arXiv:1912.07418.
67. Li, J.; Yang, D.; Su, Q. Reliable control strategy based on sliding mode observer against FDI attacks in smart grid. *Asian J. Control* **2022**, *25*, 910–920. [CrossRef]
68. Adeli, M.; Hajatipour, M.; Yazdanpanah, M.J.; Hashemi-Dezaki, H.; Shafieirad, M. Optimized cyber-attack detection method of power systems using sliding mode observer. *Electr. Power Syst. Res.* **2022**, *205*, 107745. [CrossRef]
69. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
70. An, Q.; Sun, L.; Sun, L.; Jahns, T. Low-cost diagnostic method for open-switch faults in inverters. *Electron. Lett.* **2010**, *46*, 1021–1022. [CrossRef]
71. Li, J.; Zhang, Y. A Diagnosis Method of Inverter Anomalies under DoS Attack Based on Interval Sliding Mode Observer. In Proceedings of the 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS), Coventry, UK, 24–26 May 2022; pp. 1–6.
72. Alhelou, H.H.; Golshan, M.E.H.; Hatziargyriou, N.D. Deterministic dynamic state estimation-based optimal lfc for interconnected power systems using unknown input observer. *IEEE Trans. Smart Grid* **2019**, *11*, 1582–1592. [CrossRef]
73. Zhao, S.; Yu, J.; Wang, Z.; Gao, D. Unknown input observer based distributed fault detection for nonlinear multi-agent systems with probabilistic time delay. *J. Frankl. Inst.* **2023**, *360*, 1058–1076. [CrossRef]
74. Chaouche, A.; Zemouche, A.; Ramdani, M.; Chaib Draa, K.; Delattre, C. Unknown input estimation algorithms for a class of LPV/nonlinear systems with application to wastewater treatment process. *Proc. Inst. Mech. Eng. Part J. Syst. Control Eng.* **2022**, *236*, 1372–1385. [CrossRef]
75. Aluko, A.O.; Carpanen, R.P.; Dorrell, D.G.; Ojo, E.E. Robust state estimation method for adaptive load frequency control of interconnected power system in a restructured environment. *IEEE Syst. J.* **2020**, *15*, 5046–5056. [CrossRef]
76. Zhu, F.; Fu, Y.; Dinh, T.N. Asymptotic convergence unknown input observer design via interval observer. *Automatica* **2023**, *147*, 110744. [CrossRef]
77. Pan, C.; Peng, Z.; Liu, L.; D, W. Data-driven distributed formation control of under-actuated unmanned surface vehicles with collision avoidance via model-based deep reinforcement learning. *Ocean Eng.* **2023**, *267*, 113166. [CrossRef]
78. Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Mitigating the impacts of covert cyber-attack in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders. *Energies* **2019**, *12*, 3091. [CrossRef]
79. Cohen, M.H.; Serlin, Z.; Leahy, K.; Belta, C. Temporal logic guided safe model-based reinforcement learning: A hybrid systems approach. *Nonlinear Anal. Hybrid Syst.* **2023**, *47*, 101295. [CrossRef]
80. Guo, J.; Li, L.; Wang, J.; Li, K. Cyber-Physical System-Based Path Tracking Control of Autonomous Vehicles under Cyber-Attacks. *IEEE Trans. Ind. Inform.* **2022**, 19, 6624–6635. [CrossRef]
81. Ahmed, C.M.; Ochoa, M.; Zhou, J.; Mathur, A.P.; Qadeer, R.; Murguia, C.; Ruths, J. Noiseprint: Attack detection using sensor and process noise fingerprint in cyber physical systems. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon, Republic of Korea, 4–8 June 2018; pp. 483–497.
82. Syrmakesis, A.D.; Alhelou, H.H.; Hatziargyriou, N.D. Novel SMO-Based Detection and Isolation of False Data Injection Attacks against Frequency Control Systems. *IEEE Trans. Power Syst.* **2023**. [CrossRef]
83. Wu, C.; Dong, B.; Han, S.; Yao, W. An Optimal Sliding Mode Controller Against False Data Injection Attacks. In Proceedings of the 2022 IEEE 11th Data Driven Control and Learning Systems Conference (DDCLS), Chengdu, China, 3–5 August 2022; pp. 102–107.
84. Wang, X.; Luo, X.; Zhang, M.; Jiang, Z.; Guan, X. Detection and isolation of false data injection attacks in smart grid via unknown input interval observer. *IEEE Internet Things J.* **2020**, *7*, 3214–3229. [CrossRef]
85. Long, H.; Wu, Z.; Fang, C.; Gu, W.; Wei, X.; Zhan, H. Cyber-attack detection strategy based on distribution system state estimation. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 669–678. [CrossRef]
86. Ye, L.; Zhu, F.; Zhang, J. Sensor attack detection and isolation based on sliding mode observer for cyber-physical systems. *Int. J. Adapt. Control Signal Process.* **2020**, *34*, 469–483. [CrossRef]
87. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
88. Naha, A.; Teixeira, A.; Ahlen, A.; Dey, S. Quickest detection of deception attacks in networked control systems with physical watermarking. *arXiv* **2021**, arXiv:2101.01466.
89. Saura, J.R.; Palacios-Marqués, D.; Ribeiro-Soriano, D. Using data mining techniques to explore security issues in smart living environments in Twitter. *Comput. Commun.* **2021**, *179*, 285–295. [CrossRef]
90. Tomasevic, N.; Gvozdenovic, N.; Vranes, S. An overview and comparison of supervised data mining techniques for student exam performance prediction. *Comput. Educ.* **2020**, *143*, 103676. [CrossRef]
91. Salo, F.; Injadat, M.; Nassif, A.B.; Shami, A.; Essex, A. Data mining techniques in intrusion detection systems: A systematic literature review. *IEEE Access* **2018**, *6*, 56046–56058. [CrossRef]

92. Mughal, M.J.H. Data mining: Web data mining techniques, tools and algorithms: An overview. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*. [CrossRef]
93. Manjarres, A.V.; Sandoval, L.G.M.; Suárez, M.S. Data mining techniques applied in educational environments: Literature review. *Digit. Educ. Rev.* **2018**, *33*, 235–266. [CrossRef]
94. Amin, M.S.; Chiam, Y.K.; Varathan, K.D. Identification of significant features and data mining techniques in predicting heart disease. *Telemat. Inform.* **2019**, *36*, 82–93. [CrossRef]
95. Ishaq, A.; Sadiq, S.; Umer, M.; Ullah, S.; Mirjalili, S.; Rupapara, V.; Nappi, M. Improving the prediction of heart failure patients' survival using SMOTE and effective data mining techniques. *IEEE Access* **2021**, *9*, 39707–39716. [CrossRef]
96. Viloria, A.; Acuña, G.C.; Franco, D.J.A.; Hernández-Palma, H.; Fuentes, J.P.; Rambal, E.P. Integration of data mining techniques to PostgreSQL database manager system. *Procedia Comput. Sci.* **2019**, *155*, 575–580. [CrossRef]
97. Mengash, H.A. Using data mining techniques to predict student performance to support decision making in university admission systems. *IEEE Access* **2020**, *8*, 55462–55470. [CrossRef]
98. Moudoud, H.; Mlika, Z.; Khoukhi, L.; Cherkaoui, S. Detection and Prediction of FDI Attacks in IoT Systems via Hidden Markov Model. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 2978–2990. [CrossRef]
99. Nguyen, D.; Vadaine, R.; Hajduch, G.; Garello, R.; Fablet, R. GeoTrackNet–A Maritime Anomaly Detector Using Probabilistic Neural Network Representation of AIS Tracks and A Contrario Detection. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 5655–5667. [CrossRef]
100. Zhao, H.; Liu, J.; Chen, H.; Chen, J.; Li, Y.; Xu, J.; Deng, W. Intelligent diagnosis using continuous wavelet transform and gauss convolutional deep belief network. *IEEE Trans. Reliab.* **2022**, *72*, 692–702. [CrossRef]
101. Ahmed, S.; Lee, Y.; Hyun, S.H.; Koo, I. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2765–2777. [CrossRef]
102. Bergh, D.v.d.; Clyde, M.A.; Gupta, A.R.; de Jong, T.; Gronau, Q.F.; Marsman, M.; Ly, A.; Wagenmakers, E.J. A tutorial on Bayesian multi-model linear regression with BAS and JASP. *Behav. Res. Methods* **2021**, 53, 2351–2371. [CrossRef] [PubMed]
103. Amrutha, B.; Meghana, I.; Tejas, R.; Pilare, H.V.; Annapurna, D. An Efficient Automated Intrusion Detection System Using Hybrid Decision Tree. In *Inventive Systems and Control*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 703–716.
104. Chen, Y.; Zheng, W.; Li, W.; Huang, Y. Large group activity security risk assessment and risk early warning based on random forest algorithm. *Pattern Recognit. Lett.* **2021**, *144*, 1–5. [CrossRef]
105. Dong, Y.; Ma, X.; Fu, T. Electrical load forecasting: A deep learning approach based on K-nearest neighbors. *Appl. Soft Comput.* **2021**, *99*, 106900. [CrossRef]
106. Yan, J.; Tang, B.; He, H. Detection of false data attacks in smart grid with supervised learning. In Proceedings of the 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, Canada, 24–29 July 2016; pp. 1395–1402.
107. Pu, W. Shuffle GAN with autoencoder: A deep learning approach to separate moving and stationary targets in SAR imagery. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *33*, 4770–4784. [CrossRef]
108. Manoharan, J.S. Study of variants of Extreme Learning Machine (ELM) brands and its performance measure on classification algorithm. *J. Soft Comput. Paradig. (JSCP)* **2021**, *3*, 83–95.
109. Onaolapo, A.K.; Carpanen, R.P.; Dorrell, D.G.; Ojo, E.E. A Comparative Assessment of Conventional and Artificial Neural Networks Methods for Electricity Outage Forecasting. *Energies* **2022**, *15*, 511. [CrossRef]
110. Onaolapo, A.K.; Carpanen, R.P.; Dorrell, D.G.; Ojo, E.E. Event-Driven Power Outage Prediction using Collaborative Neural Networks. *IEEE Trans. Ind. Inform.* **2022**, *19*, 3079–3087. [CrossRef]
111. Onaolapo, A.; Carpanen, R.P.; Dorrell, D.; Ojo, E. Forecasting Electricity Outage in KwaZulu-Natal, South Africa using Trend Projection and Artificial Neural Networks Techniques. In Proceedings of the 2021 IEEE PES/IAS PowerAfrica, Virtual, 23–27 August 2021; pp. 1–5.
112. Onaolapo, A.K.; Carpanen, R.P.; Dorrell, D.G.; Ojo, E.E. Transmission line fault classification and location using multi-layer perceptron artificial neural network. In Proceedings of the IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 18–21 October 2020; pp. 5182–5187.
113. Onaolapo, A.; Pillay-Carpanen, R.; Dorrell, D.; Ojo, E. A Comparative Evaluation of Conventional and Computational Intelligence Techniques for Forecasting Electricity Outage. In Proceedings of the 2021 Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA), Potchefstroom, South Africa, 27–29 January 2021; pp. 1–6.
114. Sarvamangala, D.; Kulkarni, R.V. Convolutional neural networks in medical image understanding: A survey. *Evol. Intell.* **2022**, *15*, 1–22. [CrossRef]
115. Srinidhi, C.L.; Ciga, O.; Martel, A.L. Deep neural network models for computational histopathology: A survey. *Med Image Anal.* **2021**, *67*, 101813. [CrossRef]
116. Qi, R.; Rasband, C.; Zheng, Z.; Longoria, R. Detecting Cyber Attacks in Smart Grids Using Semi-Supervised Anomaly Detection and Deep Representation Learning. *Information* **2021**, *12*, 328. [CrossRef]
117. Le, D.C.; Zincir-Heywood, N.; Heywood, M. Training regime influences to semi-supervised learning for insider threat detection. In Proceedings of the IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, 27–27 May 2021; pp. 1–14.

118. Parizad, A.; Hatziadoniu, C. A Laboratory Set-Up for Cyber Attacks Simulation Using Protocol Analyzer and RTU Hardware Applying Semi-Supervised Detection Algorithm. In Proceedings of the IEEE Texas Power and Energy Conference, College Station, TX, USA, 2–5 February 2021; pp. 1–6.
119. Gronauer, S.; Diepold, K. Multi-agent deep reinforcement learning: A survey. *Artif. Intell. Rev.* **2022**, *55*, 895–943. [CrossRef]
120. Liu, P.; Wang, L.; Ranjan, R.; He, G.; Zhao, L. A Survey on Active Deep Learning: From Model Driven to Data Driven. *ACM Comput. Surv. (CSUR)* **2022**, *54*, 1–34. [CrossRef]
121. Sutharssan, T.; Stoyanov, S.; Bailey, C.; Yin, C. Prognostic and health management for engineering systems: A review of the data-driven approach and algorithms. *J. Eng.* **2015**, *2015*, 215–222. [CrossRef]
122. Zhang, Y.; Wu, J.; Li, N.; Li, S.; Li, K. Data-driven water supply systems modelling. In Proceedings of the 2013 9th Asian Control Conference (ASCC), Istanbul, Turkey, 23–26 June 2013; pp. 1–6.
123. De Cauwer, C.; Verbeke, W.; Coosemans, T.; Faid, S.; Van Mierlo, J. A data-driven method for energy consumption prediction and energy-efficient routing of electric vehicles in real-world conditions. *Energies* **2017**, *10*, 608. [CrossRef]
124. Alhelou, H.H.; Cuffe, P. A Dynamic-State-Estimator-Based Tolerance Control Method Against Cyberattack and Erroneous Measured Data for Power Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4990–4999. [CrossRef]
125. Driss, M.; Almomani, I.; Ahmad, J. A federated learning framework for cyberattack detection in vehicular sensor networks. *Complex Intell. Syst.* **2022**, *8*, 4221–4235. [CrossRef]
126. Stănculescu, M.; Deleanu, S.; Andrei, P.C.; Andrei, H. A case study of an industrial power plant under cyberattack: Simulation and analysis. *Energies* **2021**, *14*, 2568. [CrossRef]
127. Kaddoura, S.; Haraty, R.A.; Al Kontar, K.; Alfandi, O. A parallelized database damage assessment approach after cyberattack for healthcare systems. *Future Internet* **2021**, *13*, 90. [CrossRef]
128. Ghafur, S.; Kristensen, S.; Honeyford, K.; Martin, G.; Darzi, A.; Aylin, P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digit. Med.* **2019**, *2*, 1–7. [CrossRef]
129. Huma, Z.E.; Latif, S.; Ahmad, J.; Idrees, Z.; Ibrar, A.; Zou, Z.; Alqahtani, F.; Baothman, F. A hybrid deep random neural network for cyberattack detection in the industrial internet of things. *IEEE Access* **2021**, *9*, 55595–55605. [CrossRef]
130. Kong, P.Y. A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 148244–148263. [CrossRef]
131. Zhou, C.; Hu, B.; Shi, Y.; Tian, Y.C.; Li, X.; Zhao, Y. A unified architectural approach for cyberattack-resilient industrial control systems. *Proc. IEEE* **2020**, *109*, 517–541. [CrossRef]
132. Narasimhan, S.; El-Farra, N.H.; Ellis, M.J. Active multiplicative cyberattack detection utilizing controller switching for process systems. *J. Process Control* **2022**, *116*, 64–79. [CrossRef]
133. Sabeel, U.; Heydari, S.S.; Elgazzar, K.; El-Khatib, K. Building an intrusion detection system to detect atypical cyberattack flows. *IEEE Access* **2021**, *9*, 94352–94370. [CrossRef]
134. Yen, T.; Oprea, A.; Onarlioglu, K.; Leetham, T.; Robertson, W.; Juels, A.; Kirda, E. Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks. In Proceedings of the CAnnual Computer Security Applications Conference, New Orleans, LA, USA, 9–13 December 2013; pp. 199–208.
135. Du, M.; Li, F.; Zheng, G.; Srikumar, V. Deeplog: Anomaly detection and diagnosis from system logs through deep learning. In Proceedings of the Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017; pp. 1285–1298.
136. Apruzzese, G.; Marchetti, M.; Colajanni, M.; Zoccoli, G.G.; Guido, A. Identifying Malicious Hosts Involved in Periodic Communications. In Proceedings of the IEEE International Symposium on Network Computing Applications, Cambridge, MA, USA, 30 October–1 November 2017; pp. 1–8.
137. Yagemann, C.; Pruett, M.; Chung, S.P.; Bittick, K.; Saltaformaggio, B.; Lee, W. ARCUS: Symbolic Root Cause Analysis of Exploits in Production Systems. In Proceedings of the Usenix Secur. Symp., virtual, 11–13 August 2021; pp. 1–19. Available online: https://www.usenix.org/conference/usenixsecurity21/presentation/yagemann (accessed on 10 May 2023).
138. Apruzzese, G.; Laskov, P. The Role of Machine Learning in Cybersecurity. pp. 1–38. Available online: https://scholar.google.co.za/scholar?hl=en&as_sdt=0%2C5&q=The+Role+of+Machine+Learning+in+Cybersecurity+&btnG= (accessed on 29 May 2023).
139. Su, Y.; Cheng, M.; Cho, Y.; Huang, H. False Alert Buster: An Adaptive Approach for NIDS False Alert Filtering. In Proceedings of the 2nd International Conference on Computing and Big Data, Taichung, Taiwan, 18–20 October 2019; pp. 58–62.
140. Vidovic, K.; Tomicic, I.; Slovenec, K.; Mikus, M.; Braidic, I. Ranking Network Devices for Alarm Prioritisation: Intrusion Detection Case Study. In Proceedings of the IEEE SoftCOM, Split, Hvar, Croatia, 23–25 September 2021; pp. 1–5.
141. Okutan, A.; Yang, S.J. ASSERT: Attack synthesis and separation with entropy redistribution towards predictive cyber defense. *Cybersecurity* **2021**, *2*, 1–18. [CrossRef]
142. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1153–1176. [CrossRef]
143. Onaolapo, A.K.; Akindeji, K.T. Application of Artificial Neural Network for Fault Location in Distribution Network. In Proceedings of the Southern African Universities Power Engineering Conference, Bloemfontein, South Africa, 28–30 January 2019; pp. 299–304.
144. Ghanem, M.C.; Chen, T.M. Reinforcement learning for intelligent penetration testing. In Proceedings of the IEEE World Conference on Smart Trends in Systems, Security and Sustainability, London, UK, 30–31 October 2018; pp. 185–192.

145. Uwagbole, S.O.; Buchanan, W.J.; Fan, L. Applied machine learning predictive analytics to SQL injection attack detection and prevention. In Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 1087–1090.
146. Xu, T.; Goossen, G.; Cevahir, H.K.; Khodeir, S.; Jin, Y.; Li, F.; Shan, S.; Patel, S.; Freeman, D.; Pearce, P. Deep entity classification: Abusive account detection for online social networks. In Proceedings of the USENIX Security Symposium, Online, 11–13 August 2021; pp. 1–18.
147. Biggio, B.; Roli, F. Wild patterns: Ten years after the rise of adversarial machine learning. *Elsevier Pattern Recognit.* **2018**, *84*, 317–331. [CrossRef]
148. Sweet, C.; Moskal, S.; Yang, S.J. On the Variety and Veracity of Cyber Intrusion Alerts Synthesized by Generative Adversarial Networks. *ACM Trans. Manag. Inf. Syst.* **2020**, *11*, 1–21. [CrossRef]
149. Nadeem, A.; Verwer, S.; Moskal, S.; Yang, S.J. Alert-driven Attack Graph Generation using S-PDFA. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 731–746. [CrossRef]
150. Chua, Z.L.; Shen, S.; Saxena, P.; Liang, Z. Neural nets can learn function type signatures from binaries. In Proceedings of the USENIX Security Symposium, Vancouver, BC, Canada, 16–18 August 2017; pp. 99–116.
151. Kang, C.; Park, N.; Prakash, B.A.; Serra, E.; Subrahmanian, V.S. Ensemble models for data-driven prediction of malware infections. In Proceedings of the ACM International Conference on Web Search and Data Mining, San Francisco, CA, USA, 22–25 February 2016; pp. 583–592.
152. Engströma, V.; Lagerströma, R. Two decades of cyberattack simulations: A systematic literature review. *Comput. Secur.* **2022**, *116*, 102681. [CrossRef]
153. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
154. Alimi, O.A.; Ouahada, K.; Abu-Mahfouz, A.M. A review of machine learning approaches to power system security and stability. *IEEE Access* **2020**, *8*, 113512–113531. [CrossRef]
155. Setola, R.; Faramondi, L.; Salzano, E.; Cozzani, V. An overview of cyber attack to industrial control system. *Chem. Eng. Trans.* **2019**, *77*, 907–912.
156. Al-Abassi, A.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access* **2020**, *8*, 83965–83973. [CrossRef]
157. Kayan, H.; Nunes, M.; Rana, O.; Burnap, P.; Perera, C. Cybersecurity of industrial cyber-physical systems: A review. *ACM Comput. Surv. (CSUR)* **2022**, *54*, 1–35. [CrossRef]
158. Ani, U.P.D.; He, H.; Tiwari, A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *J. Cyber Secur. Technol.* **2017**, *1*, 32–74. [CrossRef]
159. Zhang, F.; Coble, J.B. Robust localized cyber-attack detection for key equipment in nuclear power plants. *Prog. Nucl. Energy* **2020**, *128*, 103446. [CrossRef]
160. Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors* **2021**, *21*, 3901. [CrossRef] [PubMed]
161. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
162. Liu, G.X.; Shi, L.F.; Chen, S.; Wu, Z.G. Focusing matching localization method based on indoor magnetic map. *IEEE Sens. J.* **2020**, *20*, 10012–10020. [CrossRef]
163. Onaolapo, A.K. Reliability Study under the Smart Grid Paradigm Using Computational Intelligent Techniques and Renewable Energy Sources. Ph.D. Thesis, University of KwaZulu-Natal, Durban, South Africa, 2022; pp. 1–181.
164. Adefarati, T.; Sharma, G.; Onaolapo, A.K.; Njepu, A.; Akindeji, K.T.; Oladejo, S.O.; Obikoya, G.D.; Adeyanju, I. Optimal design and techno-economic analysis of a grid-connected photovoltaic and battery hybrid energy system. *Int. J. Eng. Res. Afr.* **2022**, *60*, 125–154. [CrossRef]
165. Adefarati, T.; Obikoya, G.D.; Onaolapo, A.K.; Njepu, A. Design and analysis of a photovoltaic-battery-methanol-diesel power system. *Int. Trans. Electr. Energy Syst. (ITEES)* **2021**, *31*, e12800. [CrossRef]
166. Onaolapo, A.K.; Ojo, E.E. Effects of Upside Risk on Microgrids' Reliability Considering the COVID-19 Pandemic. In Proceedings of the Southern African Universities Power Engineering Conference (SAUPEC), Durban, South Africa, 25–27 January 2022; pp. 1–6.
167. Onaolapo, A.K.; Sharma, G.; Sharma, S.; Adefarati, T. The Economic Feasibility and Cost Reduction of Grid-linked Solar PV Systems in South Africa. In Proceedings of the International Conference on Innovative Sustainable Computational Technologies (CISCT), Dehradun, India, 23–24 December 2022; pp. 1–5.
168. Adefarati, T.; Obikoya, G.D.; Sharma, G.; Onaolapo, A.K.; Akindeji, K.T. Design and Feasibility Analysis of Grid-Connected Hybrid Renewable Energy System: Perspective of Commercial Buildings. *Energy Syst.* **2023**, 1–60. [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.