






Review

Hybridization of Learning Techniques and Quantum Mechanism for IIoT Security: Applications, Challenges, and Prospects

Ismaeel Abiodun Sikiru ^{1,2}, Ahmed Dooguy Kora ³, Eugène C. Ezin ¹, Agbotiname Lucky Imoize ⁴
and Chun-Ta Li ^{5,*}

¹ Institute of Mathematics and Physical Sciences, Université d'Abomey-Calavi, Cotonou 04 BP 1525, Benin; ismaeel.as@unilorin.edu.ng (I.A.S.); eugene.ezin@uac.bj (E.C.E.)

² Department of Information Technology, University of Ilorin, Ilorin 240103, Nigeria

³ Ecole Supérieure Multinationale des Telecommunications (ESMT), Dakar 13500, Senegal; ahmed.kora@esmt.sn

⁴ Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria; aimoize@unilag.edu.ng

⁵ Bachelor's Program of Artificial Intelligence and Information Security, Fu Jen Catholic University, 510 Zhongzheng Road, New Taipei City 242062, Taiwan

* Correspondence: 157278@mail.fju.edu.tw

Abstract: This article describes our point of view regarding the security capabilities of classical learning algorithms (CLAs) and quantum mechanisms (QM) in the industrial Internet of Things (IIoT) ecosystem. The heterogeneity of the IIoT ecosystem and the inevitability of the security paradigm necessitate a systematic review of the contributions of the research community toward IIoT security (IIoTsec). Thus, we obtained relevant contributions from five digital repositories between the period of 2015 and 2024 inclusively, in line with the established systematic literature review procedure. In the main part, we analyze a variety of security loopholes in the IIoT and categorize them into two categories—architectural design and multifaceted connectivity. Then, we discuss security-deploying technologies, CLAs, blockchain, and QM, owing to their contributions to IIoTsec and the security challenges of the main loopholes. We also describe how quantum-inclined attacks are computationally challenging to CLAs, for which QM is very promising. In addition, we present available IIoT-centric datasets and encourage researchers in the IIoT niche to validate the models using the industrial-featured datasets for better accuracy, prediction, and decision-making. In addition, we show how hybrid quantum-classical learning could leverage optimal IIoTsec when deployed. We conclude with the possible limitations, challenges, and prospects of the deployment.

Keywords: classical learning algorithm; quantum mechanism; industrial Internet of Things; IIoTsec; quantum classical learning; multifaceted connectivity; architectural design



Citation: Sikiru, I.A.; Kora, A.D.; Ezin, E.C.; Imoize, A.L.; Li, C.-T.

Hybridization of Learning Techniques and Quantum Mechanism for IIoT Security: Applications, Challenges, and Prospects. *Electronics* **2024**, *13*, 4153. <https://doi.org/10.3390/electronics13214153>

Academic Editor: Costas Psychalinos

Received: 12 September 2024

Revised: 17 October 2024

Accepted: 18 October 2024

Published: 23 October 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things (IoT) can be defined as a system that incorporates intelligent devices for Internet-based intra- and intercommunication [1]. The IoT environment comprises interdependent tools that are capable of collecting, processing, storing, transmitting, receiving, and making decisions based on the available data. These features enhance smart monitoring and controlling of the environment and devices. With the penetration of IoT, it is predicted that the technology will make a subtle economic impact to the tune of USD 11.1 trillion by 2025 [2]. Interestingly, the needs of consumers have always been the target of developed IoT systems, which have, therefore, enhanced the adoption of IoT in many industrial applications [3].

The integration of IoT into industrial settings has witnessed both gradual and multi-layered approaches in the auto industry, manufacturing, smart city, and smart healthcare, among others [4–8]. The two-factor approaches are borne out of the heterogeneity and

interdependence properties of the industrial setting. Thus, as the gradual process trends from industrial generation 1.0 to 4.0, the inherent layer evolves more. The era of Industry 1.0 was toward the end of the 18th century, precisely the 1780s. The era featured the use of primitive resources such as water, steam, and fossil fuel to generate mechanical power. In the 1870s, a metamorphosis to Industry 2.0 was executed as a result of the generation of electrical energy with the use of assembly lines for mass production. The first DC motor was, in the era, assembled by Zenobe Gramme. In Industry 3.0, use of electronics and information technology (IT) caused a huge evolution as automation became integrated into production industries, thus setting the pace for smart industry. It was in the 1970s that the first programmable logic circuit (PLC) was invented. Industry 4.0 features a set of emerging technologies such as IoT, cloud computing, and artificial intelligence (AI). These technologies integrate smart technology in Industry 3.0 into cyber-physical systems (CPS) to actualize smart CPS (SCPS). The concept of SCPS is the real-time interface between the virtual and physical worlds. The current industrial revolution, i.e., Industry 4.0, has recorded, and is still recording, subtle technological, industrial, societal, and human advancement. However, the potential shift toward better consideration of parallel machine intelligent machines (PMIM) in the industrial framework, workers' ergonomics, and societal transformation endears the preparation for Industry 5.0. [9,10]. The dynamism of the Industrial Revolution and its effects on gross domestic product is presented in Figure 1.

Interestingly, the integration of emerging technologies, such as IoT, in Industry 4.0 gives rise to industrial IoT (IIoT). IIoT can then be defined as the deployment of IoT technology, including sensors, actuators, controllers, and smart systems in an industrial setting to produce hi-tech services with little or no human intervention [11,12]. In addition, IIoT is a conglomerate of intelligent connections, instantaneous information processing, and synergic monitoring for reliable and optimized qualitative industrial products [13]. Based on its transformative features, IIoT is described as the only organ for the survival of 21st-century industrial operations [14]. Hence, the IIoT ecosystem, as depicted in Figure 1, accounts for spontaneous growth in the world economy and instantaneous control of the production process [15].

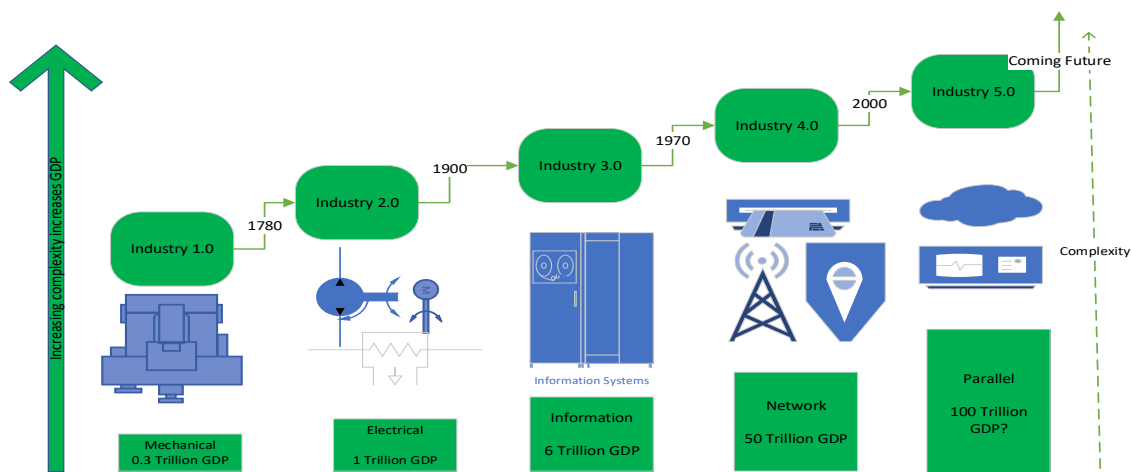


Figure 1. Progressive Trends from Industry 1.0 to Industry 5.0 with Corresponding Effects on GDP [15].

Despite the recorded exponential development in the supply chain, monitoring system, management, and manufacturing process, the technology-aided industrial ecosystem, IIoT, is still being challenged by cyberattacks [3,16–18].

The cyberattack effect on the IIoT ecosystem is found, in the literature, to be aided by the primary architectural focus of industrial machines and devices. In the study of [19], the authors discovered that industrial machines are designed for functionality rather than

security. The architectural design's effect has depicted several assaults in the industrial machines and consequently opens disruptive vulnerabilities in IIoT communication protocol, operational mismanagement, device compromise, denial of service (DoS), and even buffer overflow [11]. It is, therefore, noteworthy to state that the cyber-challenges in the IIoT ecosystem could be broadly divided into two categories—information technology (IT) and operational technology (OT) challenges. While IT challenges have a drastic effect on the data-centric computing part of IIoT, OT challenges make the monitoring of events, processes, and devices dormant [20]. Hence, in recognition of the sensitivity of OT systems, many research studies in smart logistical processes, industrial techniques, and cities advance their security defenses toward OT challenges more than its counterparts [8]. The objectives and peculiar vulnerabilities of each layer of IT/OT convergence architecture [21,22] are depicted in Table 1.

Table 1. IT/OT layers with their peculiar attacks.

IIoT Architecture	Layers	Objectives	Peculiar Vulnerabilities
Operational Technology (OT)	Layer 1	It houses sensors, actuators, transmitters, and embedded devices. It is the lowest (physical) layer of OT and deals with physical industrial processing.	Reverse engineering, eavesdropping, brute force, and malware
	Layer 2	This layer communicates with the physical layer. The communication devices in this layer include a distributed control system, PLC, and gateways.	Replay attacks, MITM attacks, brute force, and sniffing
	Layer 3	It is the topmost layer of OT that collects and shares the incoming data from the preceding OT layers. The devices for this task include SCADA, HMI, control rooms, and operation stations	IP spoofing, malware, data sniffing, and data manipulation
Information Technology (IT)	Layer 4	It is the bottom IT layer that collects incoming data from the topmost OT layer for storage at the remote data centers. Layer 4, thus, supports office applications, intranet, mail, and web services.	Phishing, SQL injection, malware, DNS poisoning, and brute force
	Layer 5	It is the top IT layer for strategic business planning using cloud computing, data analytics, the Internet, mobile devices, and smart devices.	DoS attack, malware, password, side channel attack, and MITM

Eventually, the complex architectural-driven features of IIoT make it practically unrealistic to have a prediction of 100 percent triads of security. Thus, the industry and people encounter open challenges such as loss of data, privacy and integrity, data theft, insecure communication lines, DoS, and industrial non-sovereignty, among others [23]. In the same vein, Otoum et al. [24] identified the attackers' focus on privacy and security of the industrial ecosystem as an intelligent devices-centered vulnerability. For instance, a case of intruders' sovereignty was recorded in a 2018 investigation of the Winter Olympics via the vulnerability in the reciprocal endorsement and key-exchange mechanism. Though an IIoT environment was developed to manage the illumination and ventilation at the Sochi arena, unfortunately, about 17,823 smart building network gadgets and 78,000 supervisory control and data acquisition (SCADA) devices had illegitimate access to the network without any security safeguards [14].

In recognition of the assaults in the IIoT ecosystem, the research community has given more attention to the security of the IIoT (IIoTsec) ecosystem through various approaches. Senapati and Rawal [7] highlighted emerging smart technologies that have been adopted in different capacities against assaults in the IIoT ecosystem. The technologies include AI [25–27], machine learning (ML) [9,26,28–32], quantum computing (QC) [4,33–37], multi-factor authentication (MFA) [38–40], and edge technologies [41] for sustainable industrial manufacturing and smart factories in the digital age. Hence, our contributions to the knowledge in this paper are summarized as follows:

1. We surveyed the security challenges of IIoT and discovered that they could be broadly divided into two categories: architectural design and multifaceted connectivity.
2. We reviewed how learning techniques have been deployed in the IIoT ecosystem to predict, identify, and mitigate the launch of attacks against a secure IIoT environment.
3. Also, as we are in a post-quantum era, we conducted an in-depth analysis of how quantum mechanisms have advanced IIoTsec and examined the limitations of quantum deployment in the IIoT ecosystem.
4. Based on the inherent features of learning algorithms and quantum principles, we highlighted a few prospects for hybridizing the two techniques to realize a secure IIoT ecosystem.
5. In conclusion, we advocated that IIoT-centric datasets should be used for validation as long as the model is tailored toward IIoTsec and presented IIoT-centric datasets with their distinguished features.

The remaining part of the work is structured as follows: Section 2 elaborates on the review approach of the study, where the research questions are explicitly spelled out. Our key findings are presented in Section 3. In Section 4, we highlight the challenges, limitations, and prospects of the study. Finally, the concluding remark is made in Section 5.

2. Review Approach

In this review study, we adopt the approach of [42], which is accepted as a structured form for conducting a systematic literature review (SLR). Although we are not oblivious to other literature review techniques [43,44]. However, to the best of our knowledge, the former is widely used, systematic, easy to adopt, and more informative to the readers. Hence, Kitchenham and Charters [42] operate on the principle of planning, conducting, and reporting the review. These phases promise comprehensiveness in carrying out SLR. Each of the three phases encompasses several activities. In a simplified outlook, we present the methodological process flow of this study in Figure 2.

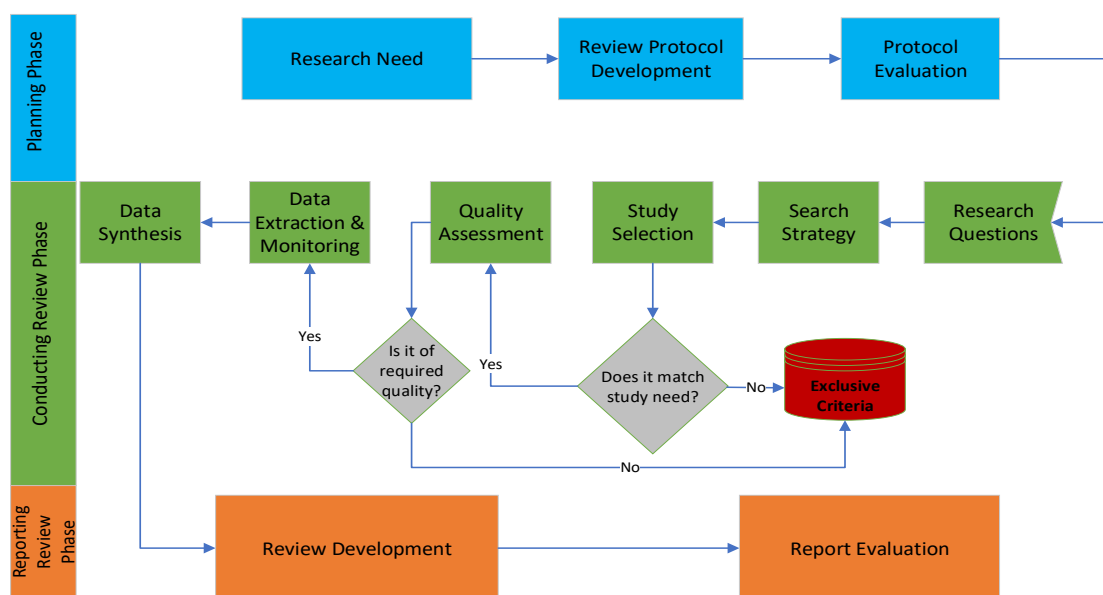


Figure 2. The methodological flow of the study.

2.1. Planning the Review Phase

This phase serves as the bedrock for the subsequent two phases because a poorly planned research study is research in futility. Moreover, this phase has three different activities to achieve the study's aim. The activities are the identification of study needs, development of a review protocol, and evaluation of the protocol.

2.2. Conducting the Review Phase

This phase is the second stage of the adopted SLR methodology. It serves as the nucleus of the process flow. The major activities of SLR are carried out in the “conducting the review phase”. Hence, this middle phase consists of six important activities to actualize the objectives of SLR. The activities are presented below.

2.2.1. Research Questions (RQs)

The choice of objective-driven RQs is paramount to achieving the research’s objectives. Hence, we identified, examined, and presented a set of research questions related to our review study. The following are our developed RQs:

- RQ1: What are the security challenges of IIoT?

The objective of RQ1 is to identify and broadly classify the security challenges in an IIoT ecosystem, as well as the corresponding diverse security approaches by the research community.

- RQ2: What kinds of learning algorithms are being deployed toward the security of IIoT?

The objective of RQ2 is to determine the extent to which ML, deep learning (DL), and blockchain techniques have changed the narratives of security challenges in the IIoT ecosystem. This includes a set of evaluating datasets used by the researchers and the bottlenecks in the deployment of the algorithms.

- RQ3: What security enhancement could the quantum mechanism offer the IIoT ecosystem?

The objective of RQ3 is to advocate for an alternative security measure, such as quantum mechanisms, in the IIoT ecosystem through the state-of-the-art (SOTA).

- RQ4: Is hybrid quantum-classical more efficient against IIoT security challenges than a single technique deployment?

The objective of RQ4 is to determine a better deployable technique to combat the increasing security menace in the IIoT environment.

2.2.2. Search Strategy

To actualize as many research works as possible in this niche, after the development of RQs, we followed acceptable laid-down principles in the search strategy. We were able to identify suitable search terms from the RQs. Then, we formulated query strategy as (Machine learn* OR ML) AND (Quantum Machine learn* OR QML OR Quantum mechanics*) AND (Industrial Internet of Thing* OR Industrial IoT OR IIoT) OR (IIoTsec OR Industrial IoT sec). This is followed by querying different digital repositories using the formulated search terms. Below are the selected digital libraries queried for our research work hunt:

- Google Scholar
- IEEE Xplore digital library
- ScienceDirect
- SpringerLink
- ACM Digital Library

2.2.3. Study Selection

While fetching related studies in the five selected digital repositories, we filtered the collections using inclusion/exclusion criteria to reckon with only relevant works in peer-reviewed journals and conference papers. The process of selecting final works for this study is thus explained:

- Step 1: All the non-English written studies were removed from the collection at the collation stage.

- Step 2: A preliminary study that focused on the title and abstract of the retrieved documents in Step 1 was conducted. At this stage, the non-consistent works to the defined RQs were excluded. Also excluded at this stage are the non-accessible full texts.
- Step 3: Here, the filtered documents were fully read. Then, three sets of works were removed based on the following:
 1. works that do not discuss any security-deployed techniques
 2. works that focused on other techniques different from the scope of this study and
 3. duplicate works that were found either in different digital libraries or appeared in conferences and journals

Conference papers were discarded to deduplicate dual appearances. This is because we discovered that such conference papers became extended in quality and comprehensiveness in their journal outlet [45]. Figure 3 shows the flow of study selection.

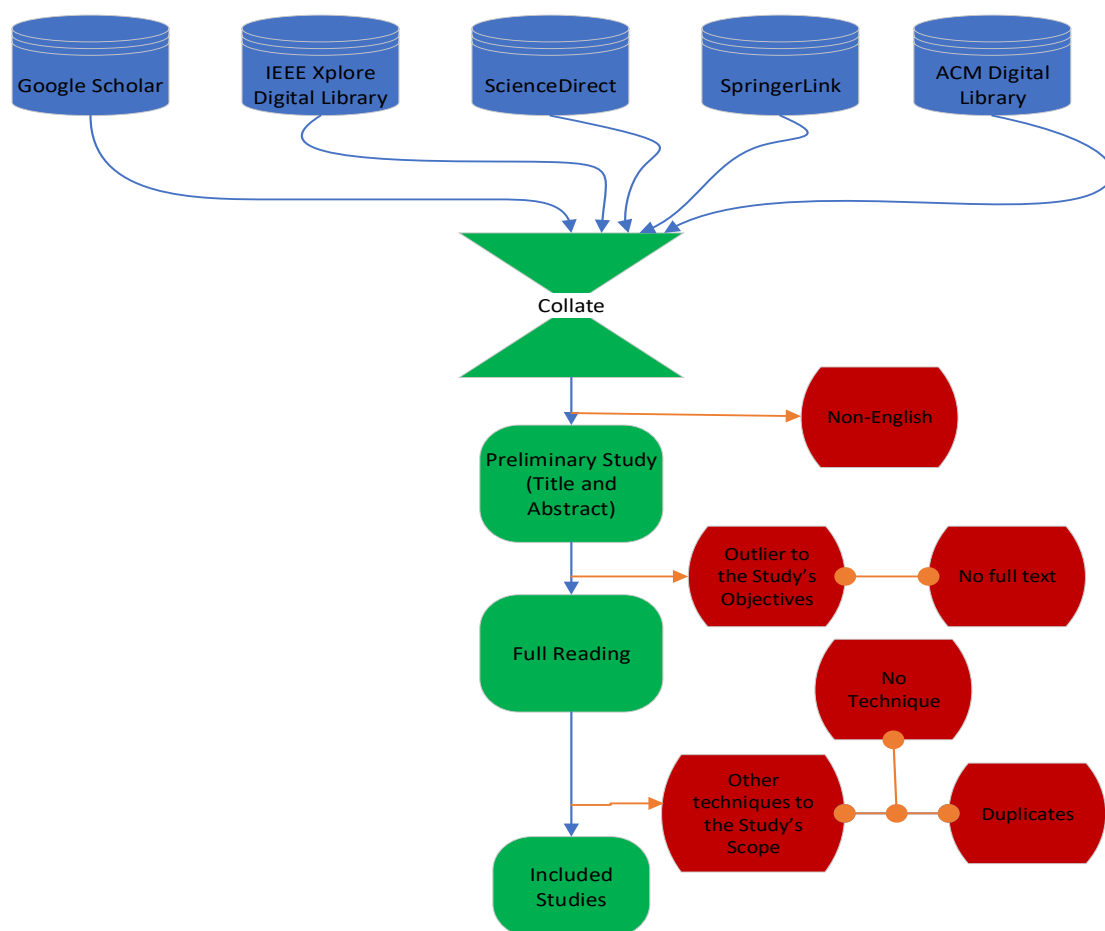


Figure 3. Process flow showing the study selection.

2.2.4. Quality Assessment Activity (QAA)

The quality of the included articles for review was thoroughly assessed here. This is to avoid bias in our study. As a result, the criteria set by [46] were refined. Then, we defined our five quality assessment criteria to ensure the integrity of the selected articles as follows:

- QAA1: Recognition of the study's objectives
- QAA2: Well-defined learning techniques and/or quantum approach for IIoTsec
- QAA3: Justifiable designed or deployed techniques for IIoTsec
- QAA4: Admissible evaluation report
- QAA5: Finally, contribution to knowledge

2.2.5. Data Extraction and Monitoring Activity (DEMA)

At this level, the final documents were analyzed to acquire answers to the raised RQs. This activity was aided by the thorough query of five digital repositories. Hence, using DEMA, we extracted from each document ten pieces of information: authors, authors' information, titles of the papers, journal sources, years of publication, publication types, available datasets for IIoTsec, analysis features, adopted methodologies, and performance metrics.

2.2.6. Data Synthesis

In a bid to synthesize the information extracted from the filtered papers, we aggregated RQs-answering evidence using different approaches. After collating the data, we analyzed it and presented the results using a narrative synthesis technique of tabulation. The tabular form makes the result informative for suitable decision-making.

3. Key Findings

In this section, we present the findings of this review study. The results relating to each research question are concisely discussed here in detail. We finally obtained a total of 100 studies revolving around the deployment of learning techniques and quantum mechanisms toward the security of industrial IoT. In addition, the presentation of the key findings in this section is guided by our highlighted quality assessment activity in Section 2.2.4. Therefore, we have four major subsections presented here, and each subsection addresses a typical RQ accordingly.

3.1. RQ1: What Are the Security Challenges of IIoT?

As briefly introduced in Section 1 and highlighted in Table 1, industrial IoT is grossly challenged with several attacks despite its promising dominance in the 21st century and beyond [14]. The security challenges in the IIoT ecosystem have been traced in the literature to various loopholes. However, in this work, we classify the main loopholes threatening the secure operation of IIoT into two—architectural design and multifaceted connectivity. The objective of this RQ is to determine the dual challenges and the diverse security approaches the challenges have attracted from the research community.

3.1.1. RQ1-1: Architectural Design Loopholes of IIoTsec

According to Aguru et al. [47] and Perwej et al. [19], IIoT would remain insecure for operation until the architectural structure of the system is re-engineered. This is because the system is built with the main intention of functionality rather than the secure dynamicity of the system. Thus, the loophole remains persistent and becomes a backdoor access to the intended attacks. For instance, IIoT uses the SCADA system as a monitoring tool for all data collected from network-dependent multiple devices [47]. Meanwhile, Modbus technology, one of SCADA's most commonly used protocols, operates using serial communication on a master–slave-based configuration. However, it lacks the triads of security—confidentiality, integrity, and availability—plus authentication [48]. As a result of the identification deficiency of an unauthorized slave-master IP address within the SCADA network [11].

Furthermore, the pioneer cyberattacks on SCADA systems can be traced back to 1982, with a massive explosion occasioned by the trojan effect on the Trans-Siberian pipeline [49]. Since then, the weakness of SCADA has been continuously exploited by intruders. In 2010, Stuxnet targeted PLCs of Iran's gas pipeline (GP) and power plants, which eventually destroyed 984 centrifuges in a uranium enrichment plant. In 2014, a BlackEnergy trojan was created for the SCADA system. This worm traversed in a Microsoft Word document, which devastated several media and energy firms, mining industries, railways, and airports in Ukraine. In 2015, several hours of blackout were experienced when the Kyiv power distribution company was disconnected from its 30 substations for three hours through BlackEnergy 3. Also, in 2017, another malware, TRITON, intrusively recoded some unique

PLCs of the SCADA system into a failed state. This failure caused a sudden shutdown of a Saudi Arabian petrochemical processing plant. In addition, Kaspersky's products experienced a SCADA assault in 2016—an attack that relegated almost 39.2% of Kaspersky-secured industrial machines [50].

Eventually, the “success” record of vulnerable SCADA devices becomes accountable to the threats on the entirety of industrial processes [51]. As a result, the authors in [52] proposed an ensemble of deep belief networks (DBNs) algorithms and support vector machines (SVM) to checkmate architectural intrusions in SCADA networks to safeguard industrial control systems (ICSs). Considering the adverse consequences of architectural design loopholes, Huang et al. [52] designed an automatic architecture of convolutional neural networks (CNNs) based on differential evolution for intrusion detection systems (IDS) in ICSs. The proposed DL-IDS was evaluated using two intrusion detection datasets for ICS. The findings depicted acceptable performance results for threat detection in the ICSs. Moreover, Rao et al. [53] identified access control leakage of SCADA, therefore making supervisory control management, role engineering, and assignment propagation deficient. To, therefore, ensure privacy and users' access to resources in a SCADA-enabled IIoT ecosystem, a mapping framework of multilayer feedforward artificial neural network (ANN) and extreme learning machine (ELM) was proposed in [53]. The finding showed that MLP has better accuracy compared to the ELM mode, though the latter is more time-efficient in its deployment.

Similarly, soft strict operational guidelines for the emerging “smart” deployments into the IIoT ecosystem are another factor for the security shortcomings in IIoT devices. IIoT devices become open to several assaults due to uncensored cyber data and devices [23,54]. In addition, sensors' positioning in a perception layer is also identified as an architectural design loophole in an IIoT environment. In the work of Ghorpade et al. [36], the authors discovered a high level of signal attenuation in an IIoT environment due to the topological positioning of sensors and the resource-constraint of IIoT devices. Thus, the recommendation proposed in the study is to design an appropriate topology to ensure network coverage and instantaneous connectivity. Moreover, Sikiru et al. [55] showed how security challenges the architectural design in emerging wireless communication systems like IIoT. To combat the effect, the authors proposed a boundary technique. They implemented its efficiency at the physical layer to decry delay and signal attenuation occasioned by the off-zone positioning of sensors.

3.1.2. RQ1-2: Multifaceted Connectivity Loopholes of IIoTsec

It is noteworthy to state that the reality of IIoT dominance over traditional industrialization is based on the evolution of IoT and increasing emerging technologies. As a result, IIoT contains abstraction properties of IoT such as open connectivity, heterogeneity, resource constraint, big data generation, real-time processing, and scalability [56–58]. These properties open the IIoT ecosystem to greater connectivity challenges. On that discovery, Valeske et al. [59] showed the rate at which the IIoT ecosystem is more susceptible to vulnerability as a result of its openness to message queue telemetry transport (MQTT), Modbus TCP, cellular networks, Long-Range Radio Wide Area Network (LoRaWAN), and other TCP/IP-based communication protocols. Additionally, all components in an IIoT ecosystem are Internet operational for seamless intercommunication between various nodes, devices, and systems, which eventually subject storage and sharing to centralized servers. However, the operating costs, delays, and possible exposure to security risks are the fundamental challenges of the centralized architecture [60,61].

Such exposure to security risks in an IIoT ecosystem is owed to the multifaceted connectivity (MFC) of IIoT devices [62]. Hence, the security and reliability of the systems become an integral concern. By such consideration, the authors [63] identified the scenario as a CPS-based security challenge that must be urgently identified for prevention. Also, in [6], the scenario is termed industrial CPS-inclined assault, and the authors proposed distributed data storage and management-enabled technology to curtail the effect of MFC

challenges of IIoT. Meanwhile, the study presented by Chawla and Mehra in [64] is observed applicable to this security challenge. The authors designed a detection model with CNNs, recurrent neural networks (RNNs), and their variants to defend against cyberattacks occasioned by MFC. In the model, CNN was used to extract local attributes, which eventually became inputs to the gated recurrent units (GRU) layer.

In addition, MFC-tailored assault is also detectable in IIoT smart devices. This portrays more risks to the IIoTsec ecosystem due to the physical layer at which most of these devices are, coupled with the state of device communication [55]. This understanding, therefore, inspired [3] to design a smart contract token-based architecture comprising a token issue contract (TIC), user register contract (URC), and manage contract (MC), for synergetic supervision and management of IIoT ecosystem's events against MFC-like challenges. In the study [65], diverse connectivity of the smart machine operation cycle, better referred to as MFC, accounts for time-lag errors in productivity. A proposal of Operation-Constrained Process Control (OCPC) was instead introduced into the IIoT ecosystem to identify time lags and errors in production under the guise of repeated training-informed-multi-sensor knowledge updates. The experimental analysis showed the efficiency of OCPC.

3.2. RQ2: What Kinds of Learning Algorithms Are Being Deployed Towards the Security of IIoT?

In recourse to the identification of the main loopholes of IIoTsec in Section 3.1, techniques such as ML and DL have become an important approach to tame the security risks, in recognition of their successful efficiency in similar studies. And for the fact that the security challenges are in two modes—active and asleep, the corresponding approach should be detective and preventive, accordingly [49]. Thus, IDSs are, in general, helpful to signal alert at the potential attempt of an intruder into network data flow [45], though an intrusion prevention system (IPS) proves better as it preempts the attacks and subsequently prevents their occurrence [1]. Thus, both are essentially cybersecurity approaches, especially for the guard of the IIoT ecosystem. For instance, ML-based IDSs were formerly challenged by the passive mode of intrusion, in which the discovery of assault awareness is likely to remain obscure. Then, the accuracy and precision rate at which ML algorithms detect such anomalies distinguish it from other IDSs. Such a feat has thus made ML algorithms deployable in many fields of cybersecurity [30,66–69]. Interestingly, ML algorithms have attracted the attention of the research community in IIoT for their sensitivity and sustenance to the living economy [30–32,48]. Based on this background, we present three techniques mostly deployed toward IIoTsec in the literature as RQ2-1.

3.2.1. Machine Learning-Based Technique

In the study of Guezzaz et al. [9], the authors present an ML-IDS-based framework for detecting misuse and anomaly detection for Edge-Based IIoTsec. K-nearest neighbor (KNN) and Principal Component Analysis (PCA) techniques were evaluated on NSL-KDD and Bot-IoT datasets. While KNN was adopted to improve accuracy for admirable decisions, PCA was used for an enhanced feature engineering and fitting process. The model had a better performance result on the NSL-KDD dataset, that is, 99.10% accuracy, 98.4% detection rate, and a 2.7% false alarm rate (FAR). In addition, the authors in [70] also proposed a KNN algorithm for intrusion detection in the IIoT ecosystem. To reduce computation complexity and speed up processing time, PCA, univariate statistics, and genetic algorithms (GA) were selected for feature engineering. The model was validated with a Bot-IoT dataset with an accuracy rate of 99.99%. Another study by Ruiz-Villafranca et al. [62] identified a increasing number of emerging technologies and their hybridization in the IIoT ecosystem as a direct proportionate to threats and vulnerabilities. The authors therefore proposed an ML-boosted tree algorithms-based smart vulnerability detector. The experimental result revealed the efficiency of the detector as it recorded a mean efficiency of 95%–99% in the F1 score metric.

Gaber et al. [31] implemented two bioinspired-based feature selection algorithms—particle swarm optimization (PSO) and bat algorithm (BA)—toward the reduction in

computational time and FAR while also advancing the detection rate of attacks in an IIoT ecosystem. Three weak learners were validated with the WUSTL-IIOT-2021 dataset. Consequently, Random Forest (RF) had the best values in performance metrics, which therefore makes hybridization with BA the best model for the study. From another perspective, Abosata et al. [1] argued that in a heterogeneous environment of IoT, like industrial IoT, security of routing protocol for low-power and lossy networks (RPL) remains paramount. Unfortunately, most of the present IDS approaches are deficient in identifying novel RPL assaults. Hence, the authors proposed a federated-transfer-learning-assisted customized distributed IDS (FT-CID) model to identify RPL in such an environment. The model has an accuracy of 85.2% in detecting RPL intrusions. The model also proved better when compared with logistic regression (LR), multilayer perceptron (MLP), and CNN-based RPL-IIoT IDS with accuracies of 56.12%, 58.04%, and 74.89%, respectively. However, the authors did not consider the intrusion behaviors of the intruders, as expected to enhance the study, based on the features of FT-CID.

3.2.2. Deep Learning-Based Technique

Likewise, Diro and Chilamkurti [71] implemented a long short-term memory (LSTM) algorithm to checkmate the discovered DoS attacks in a distributed fog environment of an IIoT firm. Before the deployment, the firm had been challenged with an attenuated network performance and inefficiency of the network entities. The proposed technique was validated with two datasets—ISCX and AWID. When its performance was compared with the LR algorithm, the proposed technique had better accuracies of 99.91% and 98.22% on ISCX and AWID datasets, respectively, as well as acceptable precision of attacks' detection. However, LR has a record of shorter training times than the LSTM technique. Additionally, Guizani and Ghafoor [72] combined two DL algorithms, RNN and LSTM, as IDS to address brute force attacks. DL algorithms were used for malware detection, while network functions virtualization (NFV) technology was adopted as malware diffusion resistant in a heterogeneous IoT ecosystem. The authors validated the proposed technique using the UNSW-NB15 dataset.

Similarly, Khan et al. [73] implemented an LSTM autoencoder to uniquely distinguish several malicious actions and reduce false alarms in IIoT-driven IICS networks. GP dataset was collected for anomaly detection in IICS networks, while the UNSW-NB15 dataset was for anomaly detection from exterior networks. The malicious actions discovered in the ecosystem include DoS, reconnaissance, exploits, fuzzers, and NMRI. Accuracy values of 97.95% and 97.62% were achieved for GP data and the UNSW-NB15 dataset, respectively. The recurrence of DoS, DDoS, and botnet attacks in an IIoT ecosystem became more of a concern in the work of Mudassir et al. [74], which, therefore, inspired the authors to proffer security remedies using hybrid DL algorithms consisting of RNN-LSTM, RNN-GRU, and ANN. Meanwhile, the three models have a low-performance percentage of recall and precision in classifying the assaults with a smaller number of instances until an under-sampling of the majority class was carried out. Of the models, ANN achieved the highest accuracy performance of 99%, while RNN-GRU was able to excellently detect DoS and DDoS attacks targeting HTTP protocol, even with minimal samples. All three models were validated with the Bot-IoT dataset.

Moreover, the hybrid approach of ML and DL techniques has been explored several times to identify and mitigate cyberattacks in IIoT networks. Soliman et al. [75] conceived the idea and implemented it. The authors henceforth considered ML-based IDSs such as ensemble bagging, decision tree (DT), and KNN for attack prediction and classification. For the precise identification of the attacks in the IIoT environment, DL-based approaches such as LSTM, bidirectional LSTM, and GRU were trained to identify the cyber-attacks. SVD was employed for feature engineering while SMOTE was used to address imbalanced data challenges. The study was evaluated on the ToN-IoT dataset for binary and multiclass classification. In addition, Jayalaxmi et al. [76] also proposed a PIGNUS model—a hybrid AE and Cascade Forward Back Propagation Neural Network (CFBPNN) algorithms—against

zero-day vulnerabilities in an IIoT ecosystem. The proposed technique was validated with five publicly available datasets. The obtained result revealed an accuracy of above 95% and a zero percent false rate in detecting multi-class attacks. Meanwhile, in 2022, the work [77] implemented an IDS using three techniques CFBPNN, CFS, and NARX against botnet attacks. Unlike the autoencoder (AE) used for feature selection and improved detection rate performance in 2023, CFS was used. While NARX was utilized as a time-series technique to identify high-impactful elements in the target class. The proposed technique was also tested on different five datasets—NF-UNSW-NB15, NF-CSE-CIC-IDS2018, NF-ToN-IIoT, and NF-BoT-IIoT for validation. When the performance outcome was compared with various existing NN models, the proposed technique was better in accuracy, F1 score, and precision.

Also, as discussed in Section 3.1.2, safe data transmission is an issue in an IIoT ecosystem due to its multi-nodal architecture. Therefore, to ensure safety and strict coordination, and to deter key leakages, Qi et al. [78] proposed a ciphertext policy attribute-based encryption mechanism scheme for secure access control. The authors utilized a hybrid cloud infrastructure for encryption and decryption to minimize the computational overhead effect. Likewise, Sankaran and Kim [79] also proposed a DL-based energy-efficient optimal RMC-CNN model to secure data transmission and anomaly detection in IIoT. In the authors' approach, RMC-CNN was used to distinguish types of attack—sybil and DoS—in the network while a multi-scale grasshopper optimization scheme was implemented to optimize the network model. Data encryption was performed using a dynamic honeypot encryption algorithm, which was thereafter securely transmitted into the cloud for storage. The validation of the scheme was conducted using the power, loop sensor, and land sensor dataset. When its throughput, delay, and detection rate analysis were compared with existing techniques, the scheme had a better outcome of accuracy, precision, recall, and F1 score. Another defense approach against DDoS attacks in an IIoT ecosystem was presented in [52]. The authors deployed multi-point synergic capability at the edge to protect IIoT devices from attackers. The authors adopt two DL mechanisms, LSTM-Attention network and 1D CNN architecture. While the former differentiated benign traffic from attack, the latter categorized and detected the attacks. The proposal was validated using the DoS2019 dataset. Both the DL methods achieved high-performance metrics in precision, recall, and F1 score. However, the 1D CNN-based method had a better result.

Moreover, in a continuous effort of the research community to achieve safe data transmission in the IIoT environment, a chaotic map and resource-efficient AE scheme (ASCON)-based authentication framework for IIoT (CMAF-IIoT) was proposed in [39]. The proposed framework [39] was to ensure seamless communication between the users and smart devices via local authentication on the devices and the establishment of secure session keys with the devices. The evaluation of the scheme revealed its low-cost communication, computation, and storage with resource friendly and improved security measures against privileged insiders, passive attacks, and MITM attacks. Similarly, an approach toward secure intranodal device communication in the IIoT ecosystem was also conceived by the authors in [14]. The authors, therefore, proposed a memristive hyperchaotic system-based complex-valued artificial neural network (ANN) synchronization to ensure secure coordination and synchronization of session key switch-over in a hyperchaotic environment like IIoT. The authors generated secure input for ANN synchronization using the proposed scheme alongside complex-valued parameters for ANN. Such hard weight values of ANN were to make the attacker's guess difficult. However, the absence of an optimization technique for the weight value would likely cause a long synchronization time. Having provided answers to the first segment of RQ2, we concisely present learning approaches toward IIoTsec, the models used, limitations, and the datasets for validation in Table 2.

Table 2. Learning models approach for IIoTsec. (NA: Not applicable).

Citations	Learning Techniques	Attack Types	Security Model/Types/Architecture	Contributions	Limitations	Dataset
[31]	RF and Bat Algorithm	Command injection, backdoors, and SQL injection	Classification	Two bioinspired-based feature selection algorithms were trained to reduce computational time and false alarm rate in IIoT	The ranking of attack traffic from the normal traffic was not by DL	WUSTL-IIOT-2021
[14]	Hyperchaotic-guided PRNG	MITM, impersonation, etc.	Memristive hyperchaotic system-based complex-valued Artificial Neural Network	Use of hyperchaotic environment to swiftly assess the ANN's coordination and synchronization of session-key switch over	Longer time of sync of ANN's parameters, and no optimization technique to optimize weight values for sync's time effects	NA
[39]	Hash algorithm, chaotic map, and ASCON	Password guessing, impersonation, replay attacks, and MITM	Chaotic map-based authentication framework (CMAF-IIoT)	Reliable communication between smart devices and users. Efficient resource and enhanced security with low storage, communication and computational costs. Validated by Real-or-Random (ROR) model + Scyther	Only 3 participants and 3 messages were considered	Custom
[75]	MLs and DLs	Backdoor, DDoS, DoS, Injection, MITM, XSS, Password, Ransomware, Scanning	Classification	Achieved an accuracy rate of 99.99%, and a reduced error rate of 0.001% for binary classification. And an accuracy rate of 99.98% and a reduced error rate of 0.016% for multi-class classification	The model has a longer training time for its high computation	ToN-IoT
[52]	LSTM and 1D CNN	DDoS	Availability	Both approaches achieved significant precision, recall, and F1 score making it protect devices from DDoS attacks	Complexity for IoT devices	DoS2019
[79]	Robust Multi-cascaded CNN (RMC-CNN)	Sybil and DDoS.	Dynamic honey pot encryption algorithm for data (key) encryption	Secure data transmission scheme in power, loop, and land IIoT	Computational complexity in comparison with others	Loop, power, and land sensors
[76]	Auto Encoders AE and CFBPNN	Zero-day vulnerabilities	deePlearnIG model intrusion detection in indUStrial Internet-of-Things (PIGNUS).	Offers better classification of normal and abnormal behavior patterns. 95% accuracy. Compared to existing models, 20% improved FPR, 10% better recall, 10% better in precision	Adopts a signature-based attack pattern	NSLKDD+, UNSW-NB15, X-IIoTID, Gas pipeline, and Water storage tank
[3]	3 smart contracts—TIC, URC, and MC. Blockchain	Malicious attack	Access control. Lightweight PQE algorithm- NTRU preserves user privacy during the registration	Offer a smart contract token-based secure and dynamic access control solution for decentralized access control in IIoT systems	Limited storage space. Response time still needs to be upgraded	NA
[9]	KNN and PCA	Intrusions	Lightweight PK-IDS framework	It offers an enhanced accuracy, precision, and detection rate for Edge-Based IIoT intrusions	Computational complexity	Bot-IoT dataset and NSL-KDD
[73]	LSTM	DoS, Reconnaissance, Exploits, Fuzzers, NMRI,	Deep-autoencoder based IDS	Distinguish malicious actions from IIoT-driven IICS networks in real time. 97.95% and 97.62% accuracy for the dataset respectively	Not suitable for multiclass identification	Gas pipeline and UNSWNB-15

Table 2. Cont.

Citations	Learning Techniques	Attack Types	Security Model/Types/Architecture	Contributions	Limitations	Dataset
[74]	ANN, RNN-LSTM, and RNN-GRU	Botnet	Availability	The models have a better result of accuracy, unlike precision and recall, particularly with smaller samples	High computation and memory usage for IIoT networks	BotIoT
[77]	CFBPNN, CFS, NARX	Botnet	Availability	The results indicated perfect accuracy, an outstanding F1 score, and good precision of the proposed model	Datasets evaluated are not fully IIoT-centric	NF-BoT-IoT, NF-ToN-IoT, NF-CSE-CIC-IDS 201, NF-UNSWNB15
[78]	Ciphertext policy attribute-based encryption mechanism	Malicious data transmission	Confidentiality, authentication	Proposed IDP scheme on access control for data transmission in the IIoT paradigm	Proposal	NA
[72]	DL-based IDS (RNN and LSTM)	Malware	Integrity	It addressed the security vulnerability that enables the attacker to break into the system	Malware-resistant NFV software-based framework	UNSW-NB15
[80]	Hashed Needham Schroeder (HNS) Cost Optimized Deep ML	NA	Integrity	Secure transmission of IIoT data through the cloud environment. It enhanced execution time	HNS public key generation estimates the flag value and a public key using a public key	NA
[71]	LSTM algorithm	DoS	Availability. Distributed fog environments	Improving the security of fog environment with high accuracy and precision of attacks detection	Longer training time compared to LR	ISCX and AWID

3.2.3. Blockchain Technique

The research community has considered distinct properties of emerging technologies to ameliorate security challenges in Industry 4.0. In this case, the blockchain technique also passes the integrity test, based on its decentralization and tamper-proof features, to be deployed against the assaults in IIoT [81]. In addition, Bouachir et al. [6] carried out a study on the security challenges across CPSs with a focus on the smart industry. The authors considered security challenges in RQ1 and, therefore, identified six attributes of blockchain, such as cryptographic-based security design, immutable data structure; distributable system (SPOF-free), aggregated transactions ordering (blocks), P2P interaction, fault-tolerance, and gossip-based communication protocol, making it a better-deployed technique for IIoTsec. Likewise, refs. [6,81] considered scalability and data security leakage as an inference of the MFC loophole, which could be mitigated by the blockchain technique. Thus, the authors designed a highly scalable data storage mechanism and cryptographic accumulator-based data storage scheme to improve fault tolerance and block data storage leakage respectively using local repairable code (LRC) sharding technology combined with a bilinear accumulator. The proposed performance scheme proved better toward IIoTsec when compared with existing polynomial coding sharding in the literature.

In the same vein, ref. [17] discovered that data insecurity is caused by the distrust between the devices of IIoT. The authors affirmed other research works toward the identified security loopholes but argued that they are unsuitable in distributed networks. Consequently, a hybrid framework of blockchain-based cloud-edge-end and trust mechanism were designed by the authors. The researchers inclusively used a consensus mechanism of BLS-based proof of replication (PoRep) to ensure device mutual trust and to proactively

prevent dynamic calculation of data replicas by the cloud server. However, verifiable delay functions (VDF) were executed in resistance to parallelization. The experimental result revealed that the scheme is low-cost-computing, communication, and storage. Despite the wider storage space provided by the cloud server, cloud computing is still being challenged with security. This security challenge is still open for research. As a result, Rahman et al. [82] argued for the safety of confidential information being exchanged with cloud infrastructure and instead merged blockchain and software-defined networking (SDN) techniques for enhanced cloud security within the IIoT paradigm. In the proposed model, DistB-SDCloud, blockchain ensures privacy, integrity, flexibility, and scalability, while SDN improves the durability, stability, and load balancing of cloud infrastructure toward IIoTsec. In recognition of the emerging technologies that necessitate recency in research outlets, we present in Table 3 only the recent publications that execute blockchain technology toward IIoTsec.

Table 3. Blockchain technique for IIoTsec.

Citation	Technique	Point-of-Deployment	Key Contributions	Limitation
[81]	LRC sharding technology	Data storage	It addresses data leakage and scalability in IIoT	No consideration of possible data replica
[17]	BLS-based proof of replication and VDF	Device's trust management	Mutual trust of the device was performed. Data replicas in cloud servers was mitigated	Scalability was not prioritized
[13]	Digital twin, Blockchain	Multi-party collaboration	Provides a heuristic digital twin data scheduling framework that guarantees data privacy, efficiency, and security in an IIoT	Centralization of the model caused possible malicious behavior within
[82]	Blockchain, SDN, and Cloud computing	IIoT devices and information-safe storage	It maximizes efficiency and security in cloud computing without any challenge to response time and CPU utilization	The proposed model is yet to be reliant on IIoT
[16]	A Survey	Critical infrastructure—IIoT devices	It presented various adopted authentications toward IIoTsec	Only considered is the authentication of devices
[6]	Blockchain and Fog computing	Critical Infrastructure—CPS	It advances CPSs in terms of QoS, data storage, computing, and security	Deployment's incompatibility with IIoT's heterogeneity

3.2.4. RQ2-2: Set of Available Datasets Used by Learning Models for IIoTsec

In RQ2-1, we discussed how learning algorithms are deployed in various approaches against numerous attacks in the IIoT ecosystem. We also highlighted different datasets that were used to validate the models in Table 2. However, our critical observation of the datasets reveals that the majority of the datasets are not IIoT-centric, coupled with the fact that a significant gap is witnessed in some security development solutions toward smart environments, like IIoT, without dataset [49,83]. And when the dataset is even available, training and validating the fidelity of IIoTsec using a non-IIoT-centric dataset is also a vulnerability [39]. Therefore, in this subsection, the aim is to present IIoT-centric datasets. Henceforth, the research community in this niche would find it appropriate for validation.

The dataset is the major component for learning algorithm prediction. However, datasets are attributes-oriented, identical, and highly sensitive. Whether the datasets are generated via experimental testbed or synthetically produced, they are all subjected to various noises and, most times, imbalance [49]. Also, the datasets are non-universal; a particular dataset does not fit all disciplines nor all scenarios in a single discipline. Therefore, a technical approach, such as feature engineering, is needed to determine an appropriate dataset that is usable and useful to the concept at hand. In this work, we found out that many available datasets are IoT based, such as CIC IoT 2022, MQTT-IOT-IDS2020, UNSW-

NB15, Bot-IoT, and WUSTL-IIOT-2021. The research community has therefore extensively evaluated the proposal and deployment using the IoT-based dataset in different dimensions, as shown in Table 2. The findings are heart soothing, but a significant research gap is that if IoT-based datasets are more appropriate for IoT-based scenarios, it looks damning when it is extended to IIoT-based problems. The unique part of IIoT, the industrial concept, attracts a huge feature that should not be underestimated for reliable performance accuracy, especially for a security-tailored remedy. Consequently, we filtered the IIoT-based datasets, and their concepts are highlighted as follows.

- WUSTL-IIoT-2018

In 2018, Teixeira and his team created an IIoT-centric dataset named WUSTL-IIOT-2018 using a SCADA system testbed [84]. The research team used the system testbed in the water treatment and distribution system's water storage tank (WST) to have a real-life replica. The network traffic was under the surveillance of the audit record generation and utilization system (ARGUS) tool. A total data size of 627 MB was captured for 25 h, while 7,049,989 observations were made. The observations showed 93.93% and 6.07% of benign and malicious traffic, respectively. When cleaned of missing values, corrupted values, and outliers, the data were reduced to 7,037,983 samples. The 25 features of WUSTL-IIOT-2018 include source port, total packets, total bytes, source packets, destination packets, and source bytes, thereby making their observed features vary during benign and malicious traffic. Likewise, some of the attacks made on the testbed include port scanners, address scanners, device identifiers, and exploits.

- WUSTL-IIoT-2021

WUSTL-IIoT-2021 is a network-driven IIoT-based data. It has no traffic, data, or assaults from any IoT-based devices. Thus, it is more suitable for exclusively IIoT-based scenarios. Benign and malicious data through various IIoT and industrial devices are the main sources of these dataset [48]. The dataset aims to mimic real-life industrial systems alongside likely real-life cyberattacks. WUSTL-IIoT-2021 has a total data size of 2.7 GB when captured for about 53 h. Then, a preprocessing was performed to clean the data of missing values, extreme outliers, and invalid entries. The preprocessing activity reduced the total size by one-seventh to ease the intrusion detection model. The total observations then become 1,194,164, containing 1,107,448 and 87,016 samples as benign and malicious observations, respectively. The testbed was executed on an average data rate of 419 kbit/s and an average packet size of 76.75 bytes. The dataset has approximately 90% of the attacks focusing on DoS attacks, on the assumption that DoS attacks are traffic resourceful compared to other attacks, that even convey a small amount of traffic.

- X-IIoTID

X-IIoTID dataset is another example of real-life IIoT data captured by Al-Hawawreh et al. [85] at the University of New South Wales (UNSW) in Canberra, to reveal both the host and network processes in safe and unsafe environments. For this dataset, statistical, ML, and DL techniques were utilized to identify and detect assault strategies. The X-IIoTID dataset has 421,417 benign and 399,417 assault observations, totaling a total instance of 820,834 with 59 features. The features were extracted from log files and network traffic using device resources and public IDS logs in an Industrial Internet Reference Architecture (IIRA) model-based laboratory architecture. Three class label levels were implemented to represent the attack scenario of the dataset. Class 1 depicted a binary category. Class 2 revealed a benign and 18 sub-categories of attack, while Class 3 also had a benign but 10 sub-sub attack categories.

- Edge-IIoTset

Edge-IIoTset is a new comprehensive cyber security dataset for IoT and IIoT applications [86]. The dataset was prepared mainly for cyber security researchers to evaluate ML-based IDS. The dataset is organized into seven layers, namely the cloud computing layer, the NFV Layer, the blockchain network layer, the fog computing layer, the SDN layer,

the edge computing layer, and the IoT and IIoT perception layer. The dataset was generated from different 10 device sensors. In total, 14 attacks were identified and categorized under five threats, while 61 features are proposed for use. The dataset was validated using a primary exploratory data analysis with the performance of ML and DL approaches in both centralized and federated learning modes.

Other IIoT-based datasets specifically used for AI-centric cyber security applications are the ICS generated WST dataset [87], and the GP dataset. Both datasets possess seven attack categories each, and they were taken from normal and abnormal observations in the ICSs laboratories [49]. The WST dataset had a preprocessed network transaction data of 236,180 samples when it was collected from the testbed at Mississippi State University's critical infrastructure protection center for 25 h [88]. Of these, 172,415 are normal, and 63,764 are malicious values. The researchers used a bump-in-the-wire approach to gather data logs and inject attacks into Modbus communication. The dataset is also identified with 24 features. On the other hand, the GP dataset contains a collection of labeled Modbus/RTU telemetry systems in a total of 10,619 observations via the critical infrastructure protection center at Mississippi State University. Of the total observations, 6672 are normal and 3947 are malicious values. GP dataset possesses 27 features. Table 4 shows other information on IIoT-centric datasets, such as evaluated attacks.

Table 4. IIoT-centric datasets in the literature.

IIoT-Based Datasets	Year	Number of Features	Testbed Layers	Types of Attacks
WUSTL-IIoT-2018	2018	25	4 layers	Port scanners, address scan attacks, device identification attacks, and exploit attacks
WUSTL-IIoT-2021	2019	41	4 layers	SYN, HTTP
X-IIoTID	2021	59	3 layers	Modbus, WebSocket, CoAP, MQTT, TCP, ARP, HTTP, SSH, DNS, ICMP, SMTP, and UDP
Edge-IIoTset	2022	61	7 layers	MITM, backdoor, DDoS, password guessing, ransomware, XSS, port scanning, SQL injection, OS fingerprinting
Water Storage Tank dataset	2014	24	2 layers	Malicious Response Injection, Malicious State Command Injection, Malicious Parameter Command Injection
Gas pipeline	2015	27	2 layers	Malicious Function Code Injection, DoS, and reconnaissance

3.3. What Security Enhancement Could the Quantum Mechanism Offer the IIoT Ecosystem?

In Section 3.2, we discussed the extent to which learning and blockchain techniques have advanced the security frontiers of IIoT. The limitations informing future works were also highlighted. We also discovered the state of importance of evaluating the techniques using IIoT-generated datasets, and we presented available IIoT-based datasets. In this section, a novel mechanism defined as more robust security-wise is discussed here. As a review study, the presentation is executed in three subsections. The first subsection reveals the concept of quantum mechanism. In the second subsection, we summarize and present the methodologies of quantum mechanisms toward IIoTsec that have been adopted by the research community under SOTA. The last subsection shows the extent of researchers' application of the mechanism and its shortcomings.

3.3.1. Concept of Quantum Mechanism

Quantum mechanism is a recent emerging approach aimed at rebranding the state of advancement in the security concept. The high demand for fast computations, guaranteed reliability and security, and energy efficiency by IoT devices in particular has created a need for quantum computing [89]. Based on its quantum principles, it supports the seamless processing of multidimensional voluminous data [90]. Additionally, its properties

of photons—the tiniest individual particles on Earth’s surface—assure overwhelming capability of processing speed. As a result, the research community has recently discovered that the classical cryptographic structures-based security is less effective against quantum computing (QC) attacks [64], for the fact that its mathematically strengthened property has been challenged by the Shor’s algorithm of quantum since 1994 [91]. For instance, a 30-qubit quantum computer has the equivalent computing capability of 10 teraflops per second-computing by a traditional silicon-based computer [92]. Therefore, IoT-enabled communication requires quantum-based security to resist both the present sophisticated attacks and futuristic quantum attacks [64].

Accordingly, the research community in this niche has equally developed quantum-based cryptographically secured architectures for IoT-related communication, quantum-resistant remedies against various attacks both within the capability of classical cryptography and beyond, quantum authentication methods, as well as challenges in the implementation of quantum deployment. Thus, the sustainability of IIoTsec has necessitated the dependence on quantum principles for its pervasive security strength, scalability, immediacy, and miniaturized, less power-consuming devices, which are essential for heterogeneous resource-constrained networks. In recognition of these features, Singamaneni et al. [93] described quantum devices, compared to classical computers, as the new revolution of IIoT as a result of its vast computational properties and efficacy. These novel research opportunities have been well amplified by the research community in the niche of optimization with applications in operational planning [94], molecular design [95], process scheduling and operations [33], logistics optimization [96], and energy systems [95]. In addition, Nawaz et al. [90] identified multi-user detection, indoor localization, routing and load balancing optimization, and channel estimation as the traditional requirements of security need in industrial settings, which are easily obtainable through the qubits of quantum mechanisms.

The result achieved through the proof-of-concept of quantum mechanisms, compared to conventional computing-based approaches, facilitated huge funding by both the nationally based research institutes and private investors. An example includes quantum technologies funding from the United Kingdom [97], the United States [98,99], and China. Also, the potential capability of the quantum for promising uncompromising-digital-sovereignty, national security, and sustainable industrial competitiveness [100] received the attention of the United States National Quantum Initiative Act of 2018, for the approval of a sum of \$1.275 billion for a 5-year initiative to expedite quantum research and development. As a result of its amazing return on investment and promising future, funding earmarked in 2019 and 2020 exceeded the budget set by Congress [101,102]. Similarly, according to the Quantum Business Report, private investors, such as venture capital financiers, are reported to have expended a total of US\$2.2 billion in research and development assistance since 2017. And only in January 2019, QC startups attracted an investment of US\$147 million [7]. Table 5 further illustrates the effects of the quantum principle approach in security compared to the conventional computing approach.

Table 5 shows the state of conventional cryptographic algorithms in the pre- and post-quantum deployment eras. Though cryptologists dared take an advanced approach against quantum-based attacks—post-quantum cryptography—all public-key cryptography types were broken in the wake of QC technology. Another instance is the requirement of larger key sizes by the majority of symmetric key types to cope with the capability of quantum deployment.

Table 5. State of conventional cryptographic algorithms in the era of quantum computing.

Cryptographic Algorithm	Cryptographic Type	Main Function	Security Level Metrics		Towards QC Requirements
			Pre-Quantum	Post-Quantum	
Advanced Encryption Standard (AES-128)	Symmetric	Block cipher	128	64	Larger key sizes
Advanced Encryption Standard (AES-256)	Symmetric	Block cipher	128	64	Larger key sizes
Poly1205	Symmetric	MAC	128	128	Larger key sizes
Galois Message Authentication Code (GMAC)	Symmetric	MAC	128	128	Larger key sizes
Ron Rivest, Adi Shamir, and Len Adleman (RSA 3072)	Asymmetric	Encryption	128	Broken	Insecure
Ron Rivest, Adi Shamir, and Len Adleman (RSA 3072)	Asymmetric	Signature	128	Broken	Insecure
Diffie–Hellman (DH 3072)	Asymmetric	Key Exchange	128	Broken	Insecure
Digital Signature Algorithm (DSA 3072)	Asymmetric	Signature	128	Broken	Insecure
Elliptic-curve Diffie–Hellman 256-bit	Asymmetric	Key Exchange	128	Broken	Insecure
Elliptic-curve Diffie–Hellman 256-bit	Asymmetric	Signature	128	Broken	Insecure
Salsa20	Symmetric	Stream Cipher	256	12	Insecure
Secure Hash Algorithm SHA-256	Symmetric	Hash function	256	128	Enlarged output
Secure Hash Algorithm 3 (SHA3)	Symmetric	Hash function	256	128	Enlarged output

3.3.2. SOTA of Quantum Mechanism as an Alternative Security Measure

In line with our search strategy and QAA in Sections 2.2.2 and 2.2.4, respectively, the vast majority of research works in quantum deployment toward IIoTsec are categorizable into three—survey proposal, review, and deployment. The survey proposal is highly statistical and opinion-gathering research. In this concept, researchers seek to be acquainted with the opinions of end users on their knowledge of quantum mechanisms in the IIoT domain. The review category is classically to garner scholastic and systematic synthesis of previous findings in quantum deployments, aiming to give current knowledge and identify research gaps opened for future works. The deployment category is the proposal and/or execution of quantum principles in the domain of IIoT by researchers to detect or prevent security loopholes. The three categories are aimed to advance the frontiers of IIoTsec.

In the work of [103], the authors elucidate two varieties of threats from the review of the literature. One is a traditional threat, and the other is a quantum-aided threat. The traditional threats are the assaults that are recognized as pre-quantum vulnerabilities. Some of these threats are recorded to have been detected, prevented, and mitigated using conventional cryptographic approaches. Contrarily, quantum-aided threats are classified as post-quantum attacks, which are not likely to be tamed by a conventional approach but a sophisticated means of quantum approach [92]. The authors emphasized that this category of threats is launched with a quantum element. They also emphasized that a quantum-based security approach would be top-notch as soon as QC is fully commercialized. Hence, more research studies on security are encouraged to be tailored toward quantum deployment.

Rivero-Angeles [104] carried out a review of the integration of quantum principles into wireless sensor networks (WSN). The researcher found out that WSN has become

a convergent point for the research community in a cybersecurity ecosystem. Any compromise to the security of WSN is a red flag for IIoT security in particular. Hence, in this adaptation, the proposal was made to explore mathematical modeling and analytics approaches to adopt quantum mechanisms for the security of WSNs. The author henceforth encouraged the research community to intensify the integration, as the literature depicts the fast metamorphosis from quantum computing to a proposed new era of quantum Internet. Relatively, EL Azzaoui et al. [105] proposed a quantum cloud for the security of healthcare management systems based on its sensitivity and necessity to all. The study revealed that quantum features such as entanglement and no-cloning theory are most appropriate to safeguard the sensitivity of medical data, while the deployable quantum cloud system (QCS) would be appropriate to take care of the data's processing complexity, molecular simulation, drug discovery, diagnostic exercise, among others.

Another industrial realm was considered in the work of [106]. In the study, several security approaches for the automotive industry were considered and compared based on KPIs. Of the approaches, some forms of quantum algorithms take precedence in securing the industry. In recognition of the studies in a quantum ecosystem, a bibliometric study of a decade's research output was conducted by [107]. The authors queried and analyzed 15,911 publications on QC-based security for the IoT environment using VOSViewer's algorithm, ranging from the notable contributing nations, organizations, researchers, citation networks, and collaboration networks to publishing sources. The result showed the researchers' interest in exploring quantum mechanisms for IoT security to the fullest, as it has significant capability over conventional cryptography. Based on this, developed countries such as India and the US have a concentrated leading record in the proposal and deployment of quantum approaches to both quantum attacks and non-quantum attacks, while other countries such as China, Egypt, the UK, South Korea, Saudi Arabia are also in the top following layer in terms of contribution frequency to the creation of, and improvement on, theories and protocols underlying QC-based IoT security. Also, in the same year, [108] decried a lot of optimization problems in an IIoT ecosystem. While considering a variety of available quantum algorithms expressed by [106], the authors conceded to the adoption of a quantum annealing (QA) processor for the optimization problems. The outcome was satisfactory, and the authors suggested the efficacy of the quantum approach as a preventive measure for present and future quantum attacks in an IIoT ecosystem. In a tabular presentation, Table 6 reveals the SOTA on quantum techniques deployment toward diverse industrial settings.

3.3.3. Quantum Deployment in IIoT

Despite the infant stage of QC deployment, the IIoT sector has inclusively gained tremendously from the capability features of quantum security. Its merits have been felt in most strategic units of the IIoT ecosystem. In this section, the core contributions of quantum security deployment, as well as its limitations, are discussed. As discussed in RQ1-1, signal attenuation is very challenging for IIoTsec. For this fact, Ghorpade et al. [36] proposed a novel enhanced quantum PSO (EQPSO) algorithm based on quantum and bio-inspired techniques to regain energy efficiency and achieve optimal routing, reliability, and scalability in an already signally attenuated IIoT ecosystem. When a quantum-based approach was compared with the conventional approach, the former had a record of improved searching precision and convergence swiftness, additional diverse paths generation, and 29.87% throughput improvement beyond the latter. However, the authors only considered optimizing sensors and fog nodes in the IIoT ecosystem. Moreover, Singamaneni et al. [93] discovered another set of vulnerabilities against IIoTsec, such as MITM, photon number splitting (PNS), and faked state attacks. The authors admitted that only MITM had been addressed by a conventional approach. To fill the research gap, a novel chaotic dynamic QKD, multi-state qubit QKD, was implemented to ensure secure communication and distribution of sensitive information in a large-scale industrial network. Also, with the progressive launch and discovery of sophisticated attacks against IIoTsec, in particular, [37] discovered

that secure, confidential, and accessible industrial operations could only be guaranteed with the supremacy power of quantum cryptography and QKD applications. The authors even depicted how the quantum technique is far better security-wise than the conventional asymmetric approach, with a reduced dynamic key generation computational overhead. Unfortunately, as good as the secure deployment approach of [93] between the IIoT devices, it does not consider the possible presence of intruders in its evaluation.

Table 6. State of the art on Quantum Techniques Deployment.

Authors	Findings	Methodology	Future Direction
[103]	Quantum computers reveal the classical cryptographic weakness to the threats from the classical and quantum mechanisms. Breakthroughs in the field of quantum-resistant cryptosystems	Review	IoT devices are to be engineered toward the integration of quantum attack-resistant capability
[106]	Each of the following quantum algorithms is identical in solving industrial problems. QAOA, quantum adiabatic algorithm, Grover's search algorithm, differential quantum circuits, variational quantum classifiers, and networks	Survey	Quantum algorithms are to be more widely deployed, especially in the automotive industry to curtail the current challenges in the system
[105]	Quantum cloud system is observed to safeguard sensitive medical data due to its distinct features of entanglement and no-cloning	Review	Deployment of a QCS to solve processing complexity of medical data: molecule simulation and drug discovery processes
[108]	Implementation of QA processor for optimization challenges in an industry setting	Deployment	Industries are to adopt the quantum approach as a safeguard against present and future quantum attacks
[104]	Trends in QC from quantum computers to quantum algorithms and even to the development of quantum Internet	Review	Researchers are to integrate QC into WSN using mathematical modeling
[107]	Analyzed QC-based security of IoT environment. QC, unlike classical computing, has high processing power to rapidly tame current encryption techniques. Developed countries are leading in this research niche	Review	The authors opted for more research work in this area to ameliorate the security risk in the computing era with the help of QC-based IoTsec
[109]	ML approaches in data training and processing are incapacitated for 6G networks due to their dynamic applications and services. QML algorithms enhance processing efficiency for effective quantum data representation, storage, secure communications, and superposition framework	Survey	Adoption of Quantum-inspired ML applications by the next generation's quantum developers and researchers for 6G networks and beyond
[110]	Need of quantum technology, for 6G communication, due to its efficient ultra-reliable, faster, economic power, and reliable communication in revolutionizing wireless resource optimization challenges in 6G communication systems	Survey	Intensification of more research work on emerging QC for its potential capability in solving computing complexity efficiently

Moreover, in recognition of the QKD technique as a vital security mechanism of quantum, Senapati and Rawal [7] proposed and deployed time-sensitive QKD against DDoS, backdoor, injection, ransomware, XSS, and scanning vulnerabilities to ensure a QKD security model across smart industrial operations. QKD has also been proposed for a large-scale networks (LSN) protocol against a common eavesdropping vulnerability in Internet ICSs [35,73]. In another study of [35], a performance comparison between QLSN and DH key exchange was carried out to minimize risk and maximize reliable communication against a possible showdown occasioned by the eavesdropping effect in an LSN. The result satisfied a QKD-approach effectiveness in a vigorous safety and speedy attack discovery. To validate its viability, the researchers proposed the integration of the QLSN protocol into the IBM Qiskit simulator.

Likewise, Liu et al. [111] stepped further to adopt multi-party collaborative signatures from the lattice hard technique against additional attacks, such as impersonation, reply, side channels, and quantum algorithm attacks. The researchers were able to use multi-party signatures and public auditing to ensure the triads of security of the new protocol in the random oracle model. The authors developed a prototype under the hardness of MLWE as a demonstration of the protocol's feasibility and efficiency evaluation. Similarly, a Lightweight PQE algorithm-Nth-degree Truncated Polynomial Ring Units (NTRU) approach was proposed in [3] to ensure the privacy preservation of the authorized party during registration in an IIoT ecosystem. This approach does not only offer reliability and dynamism of access control management system for IIoT devices in a decentralized setting but also utilizes TIC, URC, and MC to manage all events in an IIoT environment. The traditional identity scheme was advanced to a flexible identity token, which eventually undermined the malicious attack.

In reality, all the vulnerabilities are virtually data-dependent and intensified in this era of big data. Thus, the cause of such vulnerable data is assumed to a compromised data or ill-processed data for decision-making. Meanwhile, smart industries rely on data analysis to optimize production, make predictions, preempt risk, and manage threats if they eventually occur. With this discovery, an attempt was made by the authors in [4] to identify hidden vulnerabilities in the smart industry settings via data classification with the aid of QNN to have secure and reliable big data decision-making in the IIoT ecosystems. The researchers, thus, implemented a quantum approximate optimization algorithm (QAOA) for the production optimization in logistics and product shipping across the four divisional layers of the IIoT system, namely the device, edge, fog, and cloud layers. However, the study did not provide a practical scenario to visualize the results of hands-on on quantum computers, though the simulation was run using IBM Quantum Lab's Qiskit software v.0.19.0. Conclusively, the trend at which quantum techniques have been deployed for IIoTsec in recent years is presented in Table 7.

3.4. Is Hybrid Quantum-Classical More Efficient Against IIoT Security Challenges than a Single Technique Deployment?

In Section 3.2, we discussed how learning techniques and blockchain have leveraged security enhancement to IIoT. At the same time, we discovered that DL algorithms have subtle records of deployment to IIoTsec, as presented in Table 7. Likewise, Section 3.3 revealed the esteemed value of quantum deployment to IIoTsec in the literature. Meanwhile, in both sections, we highlighted the limitations of each technique in their deployment accordingly. In this subsection, we aim to address the remnant security deficit in the IIoT should a hybrid of quantum principles and learning techniques be deployed. Our aim is inspired by the findings of [89,109]. Duong et al. [109] emphasized the security strength of hybridization of techniques in terms of being exponentially faster and computationally efficient for complex multidimensional functions than a classical algorithm for the same function. In addition, Rajawat et al. [89] pointed out the advantages of hybrid quantum-classical, in particular, as it offers immediate detection and resolution of any security issue through its features of tight protections, comprehensive testing, and regular monitoring. Unfortunately, we discovered through our QAA that the quantum-classical approach is still at the infant stage owing to the state of access, technical know-how, and cost of quantum hardware. And even when quantum access is available, mostly via simulation, many works on quantum-classical approaches are still at the theoretical stage.

Quantum-classical learning (QCL) is a novel and emerging subfield of quantum computing that uses quantum algorithms to solve problems in classical learning—ML and DL while speeding up the process exponentially [112]. A heterogeneous environment, like IIoT, has been characterized by several security breaches by adversaries; hence, it necessitates a blink-of-eye security approach. QCL has been identified for such an approach as it combines the inherent security properties of quantum with classical algorithms [36,113]. In QCL, a classical dataset is often encrypted for use in quantum information processing,

and the quantum result is only obtained when the state of such a quantum system is measured. A quantum state, unlike classical, are quantum bits (qubits) that communicate with each other at a faster speed than the speed of light, regardless of the distance apart. This feature also enhances qubit storage capability. For instance, a classical computer, using classical bits, could only store one of four possible binary configurations (00, 01, 10, or 11) at any given time, unlike a 2-qubit registry that is capable of simultaneously storing all four qubits because a qubit carries two integers. Thus, the increased capacity of qubits is proportional to the square number of qubits [114].

Table 7. Applications of Quantum Mechanisms in IIoT. (NA: Not available.).

Citations	Architecture	Attack Types	Security Types/Tools	Contributions	Limitations
[35]	Proposed QKD for large-scale networks (QLSN) protocol	Eavesdropping	QLSN was validated in the IBM Qiskit simulator	Risk minimization and reliability maximization in an LSN. It outperformed the DH key exchange.	No data was reported used
[4]	Logistic system optimization	NA	QAOA and quantum neural network (QNN)	Securely classify industrial data with QNN. And instant predictive decision-making with QAOA	Non-in-depth practical approach
[7]	Rawal Liang and Peter's (RLP) sequence for QKD	DDoS, Backdoor, Injection, Ransomware, XSS, Scanning	Time-sensitive QKD	Digital twins, and quantum cryptography were jointly applied for IIoTsec, alongside QKD	No Sum Sequence approach
[111]	Multi-party collaborative signature from lattice hard	Quantum algorithm attacks, Reply attacks, Impersonation attacks, MITM attacks, side-channel attacks, and so on	Data integrity and authentication	Supports multiparty signatures and public auditing. Proved the unforgeability, conditional privacy preservation, and deterrability of the new protocol in the random oracle model	Formal proofs of security given in the random oracle assume that AMLWE and AMSIS problems are hard
[93]	Multi-state qubit QKD model	MIMD, photon number splitting (PNS) attacks, and faked state attacks	Confidentiality and Integrity. Java snippet	Virtualize the generation and transmission of qubits, thus reducing the key generation's computational complexity. While with QKD's security enhancement, attacks are discarded	Secure key exchanges between IIoT devices were only executed in a non-present intruder environment
[36]	Enhanced Quantum Particle Swarm Optimization Algorithm	NA	Quantum and bio-inspired techniques for IIoT networks	Proposed EQPSO to actualize reliability, improved processing time, buffer's healthiness in the IIoT ecosystem, while focusing on improving energy efficiency	Only optimized deployments of sensor and fog nodes in IIoT environments

In a general term, QCL could be categorized into three: classical learning with quantum data [34,90], quantum speed-ups for classical learning [34,89,115], and quantum algorithms used on quantum data [113]. In the first category, quantum data are fed into a classical learning algorithm. An instance is the construction of many-body systems using AI [116] or the estimation of physical parameters in quantum metrology [117]. The second category is the potential capability of quantum information processors to produce unclonable patterns and also recognize patterns that are classically undistinguishable [118]. For example, classical data could be encoded as quantum states to quantize subroutines of classical

algorithms. The last category of QCL is when both the algorithms and training data are based on quantum mechanisms. QNNs are mostly deployable for this task [119]. Though this category promises better efficiency and scalability, the hunt for the optimal quantum versions of neurons, network structures, and training algorithms remains open research for the research community [113].

Unfortunately, to the best of our knowledge, and as of the time of writing this paper, no study has comprehensively considered the deployment of QCL in the IIoT ecosystem. However, very few works discuss a narrow part of QCL in an industrial sector, which is insufficient to generalize. Meanwhile, the authors [120] pointed out the potential of QCL, such as QNN, to improve performance, reduce processing time, and identify adversaries in material science, financial predictive analytics, medical precision, and pharmaceutical structure. As a result, related works of QCL are henceforth discussed. Rajawat et al. [89], in recognition of the sensitivity and heterogeneity of large voluminous health-related data, implemented quantum machine learning (QML) to detect and assess security loopholes in the Internet of Medical Things (IoMT) for accurate predictions. The authors proposed an innovative fused semi-supervised learning model, compared QML-based results with the other five ML algorithms, and highlighted the merits of QML for a veritable security assessment in IoMT. In addition, EL Azzaoui et al. [4] discovered operational flaws in the finance sector, and therefore implemented a QNN to actualize an optimized scalable and smart transparent financial sector. Furthermore, the quantum capability to remedy the longer training time [35], computational complexity in CLAs using different approaches [7,93,111] and inelasticity of classical bits promises to allay the fear of processing times, computational complexity, and classical bits challenges when QML is deployed for IIoTsec. However, possible limitations and challenges surrounding the deployment of QML are presented in Section 4.

4. Limitations, Challenges, and Prospects

In this study, our scope of study is the capabilities of learning techniques and quantum mechanisms in the deployment of security approaches toward industrial IoT. Meanwhile, the security paradigm in blockchain was briefly discussed because some studies hybridize it into learning techniques. Thus, the review of the learning techniques shows that the volume and velocity of data featured with IIoT are the causes of a larger percentage of the DL approach by the research community than ML. While the data are fundamental to modeling, it is, however, discovered in this study as a challenge. Hence, we categorize the challenges emanating from this SLR into modeling building blocks and quantum in infancy, as discussed in Sections 4.1 and 4.2. In furtherance, identification of the challenges and the contribution of the security-deploying techniques foster new development in the realm of IIoTsec. Such new development extends the research innovation and, therefore, opens research direction for the exploration of the research community, which is discussed under the prospects of the study.

4.1. Modelling Building Block

In this concept, the fundamental feature that needs to be well-finetuned for the process and success of the building model, classical or quantum, is the dataset. Our findings show that many researchers do not validate their modeling using the IIoT-centric dataset. Hopefully, the reason could be a generalization that IIoT sprouts from IoT [12]. However, such thought is likely to be inimical to the accuracy of prediction as a result of the possible lack of industrial features in such a dataset. We, therefore, have presented the available IIoT-centric datasets for the researchers in the niche to validate. In addition, as much as the IIoT dataset is prioritized, preprocessing would be required by the domain expert. While in a QCL environment, preprocessing could be executed using any of the three categories of QCL discussed in Section 3.

4.2. Quantum at Infancy

As much as quantum mechanisms promise an optimized effectiveness and efficiency toward IIoTsec against present and future quantum attacks, it is still at the infant stage as most of the studies on it are at the theoretical stage. As a result, both the quantum resources and quantum hardware are currently limited, and even the limited available resources and hardware are financially expensive, making their use exclusive. When a simulator is freely accessible, like Qiskit, obtainable qubits are limited. In addition, the expertise in quantum use, skills, and knowledge are still below the expected threshold, especially in Africa. Thus, the research community keeps advancing the concept by rolling several media, so that interested researchers might become skilled in leveraging quantum security advancement. Moreover, owing to the sensitivity of security-tailored techniques, standardization of the technique must be prioritized. Surprisingly, the standardization of QCL algorithms is yet to be concluded [4].

4.3. Prospects of the Study

Our research findings pointed out that the challenges in the literature and the deployed approaches foster the prospects of this SLR. As such, the prospects of this SLR are presented here. IIoT bridges the gap between intelligent machines, advanced analytics, and people at work, as it stems from endogenous requirements of industrial development and technology-driven features of Internet evolution to the delivery of an optimal smart, productive ecosystem [10,121]. Our study, therefore, depicts how the IIoT ecosystem promises large-scale customization, dynamic optimized and real-time production flexibility, and maximized resource utilization and minimized energy consumption. However, the vulnerabilities embedded in IT/OT convergence as presented in Table 1 are yet to receive adequate attention from the researchers for their persistence, whereas the convergence is fundamental to the IIoT ecosystem [21,22].

According to Tange et al. [8], the IT paradigm, unlike OT, of convergence has been marginalized in the research cycle of IIoTsec. Unfortunately, it is at the upper layer of IT/OT convergence. It, therefore, serves as the loophole for data-centric security, which is a threat to the IIoT ecosystem. Likewise, our broad classification unveils how architectural design loopholes require more research attention than MFC. As a result of the research gap in these two concepts, it is pertinent for the research community to fill the gap to realize the required IIoTsec. In addition to the CLAs for IIoTsec, the DL approach receives significant attention from the researchers toward IIoTsec, as depicted in Table 2. This is not unconnected to the heterogeneity concerns of the IIoT ecosystem and the unique velocity and massive features of the industrial data. Meanwhile, the evaluation of IIoT-tailored models with non-IIoT-centric data are assumed to be unreliable for decision-making and generalization. Thus, instances of IIoT-centric datasets are presented, and subsequent researchers are encouraged to evaluate using IIoT-based datasets in this niche.

Furthermore, execution time, computational complexity, and energy consumption remain the major drawbacks across CLAs. These bottlenecks have drastic effects on a heterogeneous network, like IIoT, and even make the network more susceptible to classical and quantum attacks. Thus, QM recently gained the attention of the researchers to mitigate such attacks in LSNs of the IIoT ecosystem [35]. Our findings show promising efficiency in deploying QM, although this emerging technology has some challenges as earlier highlighted owing to its infant stage of deployment [122]. In addition, the research direction shows that hybrid QCL would reinforce IIoTsec, and henceforth advance the optimization of technological operation, enterprise management, and the IIoT ecosystem [123–125]. The security capability demonstrated by QSVM, QPSO, and QNN in the related concepts of IoMT, finance analytics, material sciences, and medicine therapies over a single deployment technique is a testimony to the veritability of QCL in IIoTsec [33,36,96,101,126,127]. Hence, the deployment of hybrid QCL is very promising for IIoTsec. Thus, continuous research in this field is promising to proffer practicable remedies to the outstanding challenges, such as awaiting wearing-out of classical bits according to Moore's law [4], decoherence and gate

infidelity, infeasibility of non-IIoT working environment, quantum attacks, exponential rate of IoT penetration, and proposed quantum Internet [37]. Thus, the primary takeaway from the findings depicts that hybridizing quantum with DL promises better reliability for IIoTsec.

5. Conclusions

In this SLR paper, our assessment of the variety of security assaults against IIoT shows that they are categorizable into two main loopholes, architectural design and MFC. Based on this, we discussed how emerging technologies, blockchain, CLAs, and quantum mechanisms have offered security fidelity in detecting, preventing, predicting, and mitigating the loopholes in the IIoT ecosystem. We showed the strengths and weaknesses of security technologies. Consequently, our research-based answers to the RQs show that a larger percentage of the approaches in the literature are tailored toward the MFC of IIoT ecosystem challenges in RQ1-2. Such a discovery revealed that the architectural design challenges of IIoTsec are still open research, as the vulnerabilities of IT layers. Our work also revealed that hybrid QCL shows a promising fidelity for IIoTsec. Hence, it is also open for exploration by the research community. Meanwhile, for a reliable prediction and accuracy of IIoTsec's models, we propose that the research community should prioritize the IIoT-centric dataset. Finally, it is hoped that this study will serve as a reference for future advancement in IIoTsec, employing QCL for IIoTsec against architectural design threats, MFC challenges, and IT/OT convergence vulnerabilities.

Author Contributions: Conceptualization, I.A.S.; methodology, I.A.S.; validation, A.D.K., E.C.E. and A.L.I.; formal analysis, I.A.S.; investigation, A.L.I.; resources, E.C.E.; writing—original draft preparation, I.A.S. and C.-T.L.; writing—review and editing, I.A.S., E.C.E., A.D.K., C.-T.L. and A.L.I.; visualization, I.A.S.; supervision, E.C.E. and A.D.K.; project administration, E.C.E. and A.D.K.; funding acquisition, I.A.S. and C.-T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Partnership for Skills in Applied Sciences, Engineering and Technology—Regional Scholarship and Innovation Fund (PASET-RSIF). This work was supported in part by the National Science and Technology Council in Taiwan under contract no: NSTC 113-2410-H-030-077-MY2.

Data Availability Statement: Data sharing is not applicable to this review paper.

Acknowledgments: The authors acknowledge the anonymous reviewers for their valuable comments which helped to improve the quality of the paper.

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

Abbreviations

AE	Autoencoder
AI	Artificial Intelligence
ANN	Artificial Neural Network
ARGUS	Audit Record Generation and Utilization System
BA	Bat Algorithm
CFBPNN	Cascade Forward Back Propagation Neural Network
CLA	Classical Learning Algorithm
CMAF-IIoT	Chaotic Map and resource-efficient AE scheme-based Authentication Framework for IIoT
CNN	Convolutional Neural Network
CPS	Cyber-Physical Systems
DBN	Deep Belief Network
DEMA	Data Extraction and Monitoring Activity
DH	Diffie–Hellman
DL	Deep Learning
DNS	Domain Name System

DoS	Denial of Service
DT	Decision Tree
ELM	Extreme Learning Machine
EQPSO	Enhanced Quantum Particle Swarm Optimization
FT-CID	Federated-Transfer-learning-assisted Customized distributed IDS
GA	Genetic Algorithm
GDP	Gross Domestic Product
GRU	Gated Recurrent Unit
GP	Gas Pipeline
HMI	Human Machine Interface
HNS	Hashed Needham Schroeder
ICS	Industrial Control System
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
Industry 1.0	First industrial revolution
Industry 2.0	Second industrial revolution
Industry 3.0	Third industrial revolution
Industry 4.0	Fourth industrial revolution
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
KNN	K-Nearest Neighbor
LoRaWAN	Long-Range Radio Wide Area Network
LRC	Local Repairable Code
LSTM	Long Short-Term Memory
LR	Logistic Regression
LSN	Large-Scale Network
MC	Manage Contract
MFA	Multifactor Authentication
MFC	Multifaceted Connectivity
MITM	Man-in-the-Middle
ML	Machine Learning
MLP	Multilayer Perceptron
MQTT	Message Queue Telemetry Transport
NFV	Network Functions Virtualization
NTRU	Nth-degree Truncated Polynomial Ring Unit
OCPC	Operation-Constrained Process Control
OT	Operational Technology
PCA	Principal Component Analysis
PLC	Programmable Logic Circuit
PMIM	Parallel Machine Intelligent Machines
PNS	Photon Number Splitting
PoRep	Proof of Replication
PQE	Post Quantum Era
PSO	Particle Swarm Optimization
QA	Quantum Annealing
QAA	Quality Assessment Activity
QAOA	Quantum Approximate Optimization Algorithm
QC	Quantum Computing
QCS	Quantum Cloud System
QCL	Quantum-Classical Learning
QKD	Quantum Key Distribution
QLSN	Quantum Large Scale Network
QM	Quantum Mechanisms

QML	Quantum Machine Learning
QNN	Quantum Neural Network
QPSO	Quantum Particle Swarm Optimization
QSVM	Quantum Support Vector Machine
RF	Random Forest
RLP	Rawal Liang and Peter
RMC-CNN	Robust Multi-cascaded CNN
RNN	Recurrent Neural network
RPL	Routing Protocol for low-power and Lossy networks
RQ	Research Question
SCADA	Supervisory Control and Data Acquisition
SCPS	Smart Cyber-Physical System
SDN	Software-Defined Networking
SLR	Systematic Literature Review
SOTA	state-of-the-art
SQL	Structure Query Language
TIC	Token Issue Contract
UNSW	University of New South Wales
URC	User Register Contract
VDF	Verifiable Delay Functions
WSN	Wireless Sensor Network
WST	Water Storage Tank

References

- Abosata, N.; Al-Rubaye, S.; Inalhan, G. Customised Intrusion Detection for an Industrial IoT Heterogeneous Network Based on Machine Learning Algorithms Called FTL-CID. *Sensors* **2023**, *23*, 321. [\[CrossRef\]](#) [\[PubMed\]](#)
- Tufail, A.; Namoun, A.; Sen, A.A.A.; Kim, K.H.; Alrehaili, A.; Ali, A. Moisture Computing-Based Internet of Vehicles (Iov) Architecture for Smart Cities. *Sensors* **2021**, *21*, 3785. [\[CrossRef\]](#) [\[PubMed\]](#)
- Wang, W.; Huang, H.; Yin, Z.; Gadekallu, T.R.; Alazab, M.; Su, C. Smart Contract Token-Based Privacy-Preserving Access Control System for Industrial Internet of Things. *Digit. Commun. Netw.* **2023**, *9*, 337–346. [\[CrossRef\]](#)
- EL Azzaoui, A.; Salim, M.M.; Park, J.H. Secure and Reliable Big-Data-Based Decision Making Using Quantum Approach in IIoT Systems. *Sensors* **2023**, *23*, 4852. [\[CrossRef\]](#) [\[PubMed\]](#)
- Tang, L.L.; Chan, Y.W.; Shen, S.L. Investigating Radio-Frequency Identification Usage Behaviours and Organisational Performance According to Factors of User Perception. *Int. J. Serv. Technol. Manag.* **2019**, *25*, 199–214. [\[CrossRef\]](#)
- Bouachir, O.; Aloqaily, M.; Tseng, L.; Boukerche, A. Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry. *Computer* **2020**, *53*, 36–45. [\[CrossRef\]](#)
- Senapati, B.; Rawal, B.S. Quantum Communication with RLP Quantum Resistant Cryptography in Industrial Manufacturing. *Cyber Secur. Appl.* **2023**, *1*, 100019. [\[CrossRef\]](#)
- Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [\[CrossRef\]](#)
- Guezaz, A.; Azrou, M.; Benkirane, S.; Mohy-Eddine, M.; Attou, H.; Douiba, M. A Lightweight Hybrid Intrusion Detection Framework Using Machine Learning for Edge-Based IIoT Security. *Int. Arab J. Inf. Technol.* **2022**, *19*, 822–830. [\[CrossRef\]](#)
- Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. A Literature Review of the Challenges and Opportunities of the Transition from Industry 4.0 to Society 5.0. *Energies* **2022**, *15*, 6276. [\[CrossRef\]](#)
- Alnajim, A.M.; Habib, S.; Islam, M.; Thwin, S.M.; Alotaibi, F. A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. *Technologies* **2023**, *11*, 161. [\[CrossRef\]](#)
- Alotaibi, B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. *Sensors* **2023**, *23*, 7470. [\[CrossRef\]](#) [\[PubMed\]](#)
- Chen, H.; Jeremiah, S.R.; Lee, C.; Park, J.H. A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment. *Appl. Sci.* **2023**, *13*, 1440. [\[CrossRef\]](#)
- Khan, M.Z.; Sarkar, A.; Noorwali, A. Memristive Hyperchaotic System-Based Complex-Valued Artificial Neural Synchronization for Secured Communication in Industrial Internet of Things. *Eng. Appl. Artif. Intell.* **2023**, *123*, 106357. [\[CrossRef\]](#)
- Lu, J.; Wang, X.; Cheng, X.; Yang, J.; Kwan, O.; Wang, X. Parallel Factories for Smart Industrial Operations: From Big AI Models to Field Foundational Models and Scenarios Engineering. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 2079–2086. [\[CrossRef\]](#)
- Aldossary, N.S.; Zagrouba, R. Authentication Solutions in Industrial Internet of Things: A Survey. *Appl. Math. Inf. Sci.* **2023**, *17*, 953–965. [\[CrossRef\]](#)
- Zhang, F.; Wang, H.; Zhou, L.; Xu, D.; Liu, L. A Blockchain-Based Security and Trust Mechanism for AI-Enabled IIoT Systems. *Future Gener. Comput. Syst.* **2023**, *146*, 78–85. [\[CrossRef\]](#)

18. Wang, J.; Liu, J. Deep Learning for Securing Software-Defined Industrial Internet of Things: Attacks and Countermeasures. *IEEE Internet Things J.* **2022**, *9*, 11179–11189. [\[CrossRef\]](#)
19. Perwej, Y.; Abbas, S.Q.; Dixit, J.P.; Akhtar, N.; Jaiswal, A.K. A Systematic Literature Review on the Cyber Security. *Int. J. Sci. Res. Manag.* **2021**, *9*, 669–710. [\[CrossRef\]](#)
20. Paes, R.; Mazur, D.C.; Venne, B.K.; Ostrzenski, J. A Guide to Securing Industrial Control Networks: Integrating IT and OT Systems. *IEEE Ind. Appl. Mag.* **2020**, *26*, 47–53. [\[CrossRef\]](#)
21. Maleh, Y. IT/OT Convergence and Cyber Security. *Comput. Fraud Secur.* **2021**, *2021*, 13–16. [\[CrossRef\]](#)
22. George, A.S. The impact of IT/OT Convergence on digital transformation in manufacturing. *Partn. Univers. Int. Innov. J.* **2024**, *2*, 18–38.
23. Gebremichael, T.; Ledwaba, L.P.I.; Eldefrawy, M.H.; Hancke, G.P.; Pereira, N.; Gidlund, M.; Akerberg, J. Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access* **2020**, *8*, 152351–152366. [\[CrossRef\]](#)
24. Otoum, Y.; Liu, D.; Nayak, A. DL-IDS: A Deep Learning-Based Intrusion Detection Framework for Securing IoT. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3803. [\[CrossRef\]](#)
25. Saleem, I.; Abdeljawad, I.; Nour, A.I. Artificial Intelligence and the Future of Accounting Profession: Implications and Challenges. In *Artificial Intelligence, Internet of Things, and Society 5.0; Studies in Computational Intelligence*; Springer: Cham, Switzerland, 2023; Volume 1113.
26. Muruganandam, S.; Salameh, A.A.; Pozin, M.A.A.; Manikanthan, S.V.; Padmapriya, T. Sensors and Machine Learning and AI Operation-Constrained Process Control Method for Sensor-Aided Industrial Internet of Things and Smart Factories. *Meas. Sens.* **2023**, *25*, 100668. [\[CrossRef\]](#)
27. Rezwaniul Mahmood, M.; Matin, M.A.; Sarigiannidis, P.; Goudos, S.K. A Comprehensive Review on Artificial Intelligence/Machine Learning Algorithms for Empowering the Future IoT Toward 6G Era. *IEEE Access* **2022**, *10*, 87535–87562. [\[CrossRef\]](#)
28. Dhini, A.; Surjandari, I.; Kusumoputro, B.; Kusiak, A. Extreme Learning Machine–Radial Basis Function (ELM-RBF) Networks for Diagnosing Faults in a Steam Turbine. *J. Ind. Prod. Eng.* **2022**, *39*, 572–580. [\[CrossRef\]](#)
29. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of Machine Learning and Deep Learning in Securing 5G-Driven Industrial IoT Applications. *Ad Hoc Netw.* **2021**, *123*, 102685. [\[CrossRef\]](#)
30. Usman, M.; Sarfraz, M.S.; Habib, U.; Aftab, M.U.; Javed, S. Automatic Hybrid Access Control in SCADA-Enabled IIoT Networks Using Machine Learning. *Sensors* **2023**, *23*, 3931. [\[CrossRef\]](#)
31. Gaber, T.; Awotunde, J.B.; Folorunso, S.O.; Ajagbe, S.A.; Eldesouky, E. Industrial Internet of Things Intrusion Detection Method Using Machine Learning and Optimization Techniques. *Wirel. Commun. Mob. Comput.* **2023**, *2023*, 3939895. [\[CrossRef\]](#)
32. Ji, C.; Niu, Y. A Hybrid Evolutionary and Machine Learning Approach for Smart City Planning: Digital Twin Approach. *Sustain. Energy Technol. Assess.* **2024**, *64*, 103650. [\[CrossRef\]](#)
33. Sharma, V.; Gupta, S.; Mehta, G.; Lad, B.K. A Quantum-Based Diagnostics Approach for Additive Manufacturing Machine. *IET Collab. Intell. Manuf.* **2021**, *3*, 184–192. [\[CrossRef\]](#)
34. Rani, K.S.K.; Priyadarsheni, J.M.; Karthikeyan, B.; Pugalendhi, G.S. Applications of Quantum AI for Healthcare. In *Quantum Computing and Artificial Intelligence: Training Machine and Deep Learning Algorithms on Quantum Computers*; De Gruyter: Berlin, Germany, 2023.
35. Mangla, C.; Rani, S.; Abdelsalam, A. QLSN: Quantum Key Distribution for Large Scale Networks. *Inf. Softw. Technol.* **2024**, *165*, 107349. [\[CrossRef\]](#)
36. Ghorpade, S.N.; Zennaro, M.; Chaudhari, B.S.; Saeed, R.A.; Alhumyani, H.; Abdel-Khalek, S. A Novel Enhanced Quantum PSO for Optimal Network Configuration in Heterogeneous Industrial IoT. *IEEE Access* **2021**, *9*, 134022–134036. [\[CrossRef\]](#)
37. Shamshad, S.; Riaz, F.; Riaz, R.; Rizvi, S.S.; Abdulla, S. An Enhanced Architecture to Resolve Public-Key Cryptographic Issues in the Internet of Things (IoT), Employing Quantum Computing Supremacy. *Sensors* **2022**, *22*, 8151. [\[CrossRef\]](#) [\[PubMed\]](#)
38. Ali, W.; Ahmed, A.A. An Authenticated Group Shared Key Mechanism Based on a Combiner for Hash Functions over the Industrial Internet of Things. *Processes* **2023**, *11*, 1558. [\[CrossRef\]](#)
39. Tanveer, M.; Badshah, A.; Khan, A.U.; Alasmay, H.; Chaudhry, S.A. CMAF-IIoT: Chaotic Map-Based Authentication Framework for Industrial Internet of Things. *Internet Things* **2023**, *23*, 100902. [\[CrossRef\]](#)
40. Izza, S.; Benssalah, M.; Drouiche, K. An Enhanced Scalable and Secure RFID Authentication Protocol for WBAN within an IoT Environment. *J. Inf. Secur. Appl.* **2021**, *58*, 102705. [\[CrossRef\]](#)
41. Prakash, V.; Savaglio, C.; Garg, L.; Bawa, S.; Spezzano, G. Cloud- and Edge-Based ERP Systems for Industrial Internet of Things and Smart Factory. *Procedia Comput. Sci.* **2022**, *200*, 537–545. [\[CrossRef\]](#)
42. Kitchenham, B.; Charters, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering Version 2.3. *Engineering* **2007**, *45*.
43. Schreiber, F.; Cramer, C. Towards a conceptual systematic review: Proposing a methodological framework. *Educ. Rev.* **2024**, *76*, 1458–1479. [\[CrossRef\]](#)
44. Azevedo, B.F.; Rocha, A.M.; Pereira, A.I. Hybrid approaches to optimization and machine learning methods: A systematic literature review. *Mach. Learn.* **2024**, *113*, 4055–4097. [\[CrossRef\]](#)

45. Sikiru, I.A.; Dossou, M. A Bibliometric Analysis of Research on Techniques for Network Communications Security. In Proceedings of the 2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2023, Purwokerto, Indonesia, 29–30 November 2023.
46. Do, H.; Elbaum, S.; Rothermel, G. Supporting Controlled Experimentation with Testing Techniques: An Infrastructure and Its Potential Impact. *Empir. Softw. Eng.* **2005**, *10*, 405–435. [\[CrossRef\]](#)
47. Kumar, A.; Bhushan, B.; Malik, A.; Kumar, R. Protocols, Solutions, and Testbeds for Cyber-Attack Prevention in Industrial SCADA Systems. In *Internet of Things and Analytics for Agriculture; Studies in Big Data*; Springer: Singapore, 2021; Volume 99. [\[CrossRef\]](#)
48. Zolanvari, M.; Teixeira, M.A.; Gupta, L.; Khan, K.M.; Jain, R. Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 6822–6834. [\[CrossRef\]](#)
49. Conti, M.; Donadel, D.; Turrin, F. A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2248–2294. [\[CrossRef\]](#)
50. Threat Landscape for Industrial Automation Systems in the Second Half of 2016. Kaspersky Lab ICS CERT. Available online: <https://ics-cert.kaspersky.com/publications/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/> (accessed on 11 September 2024).
51. Huda, S.; Yearwood, J.; Hassan, M.M.; Almogren, A. Securing the Operations in SCADA-IoT Platform Based Industrial Control System Using Ensemble of Deep Belief Networks. *Appl. Soft Comput. J.* **2018**, *71*, 66–77. [\[CrossRef\]](#)
52. Huang, H.; Ye, P.; Hu, M.; Wu, J. A Multi-Point Collaborative DDoS Defense Mechanism for IIoT Environment. *Digit. Commun. Netw.* **2023**, *9*, 590–601. [\[CrossRef\]](#)
53. Rao, E.; Kushwaha, A.P.; Sahukaru, J.; Ramkishore, P.; Burle, T. An Intelligent Security Framework for Industrial IoT Using Swarm Based Optimized Ensemble Machine Learning Model. *Int. J. Comput. Digi-Tal Syst.* **2024**, *16*, 1–10.
54. Gollmann, D.; Krotofil, M. Cyber-Physical Systems Security. In *The New Codebreakers; Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2016; Volume 9100, pp. 195–204. [\[CrossRef\]](#)
55. Sikiru, I.A.; Olawoyin, L.A.; Faruk, N.; Oloyede, A.A.; Abdulkarim, A.; Olayinka, I.Y.; Sowande, O.A.; Garba, S.; Imoize, A.L. Physical Layer Security Using Boundary Technique for Emerging Wireless Communication Systems. *Secur. Priv.* **2023**, *6*, e288. [\[CrossRef\]](#)
56. Ahmed, S.F.; Alam, M.S.B.; Hoque, M.; Lameesa, A.; Afrin, S.; Farah, T.; Kabir, M.; Shafiullah, G.M.; Muyeen, S.M. Industrial Internet of Things Enabled Technologies, Challenges, and Future Directions. *Comput. Electr. Eng.* **2023**, *110*, 108847. [\[CrossRef\]](#)
57. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4724–4734. [\[CrossRef\]](#)
58. Ottolini, D.; Zyrianoff, I.; Kamienski, C. Interoperability and Scalability Trade-Offs in Open IoT Platforms. In Proceedings of the 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022.
59. Valeske, B.; Osman, A.; Römer, F.; Tschuncky, R. Next Generation NDE Sensor Systems as IIoT Elements of Industry 4.0. *Res. Nondestruct. Eval.* **2020**, *31*, 340–369. [\[CrossRef\]](#)
60. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [\[CrossRef\]](#)
61. Miller, S.W.; Brugan, J.M. Technological Trends: A Focus on Citizen Security. *Ing. Solidar.* **2021**, *17*, 1–28. [\[CrossRef\]](#)
62. Ruiz-Villafranca, S.; Roldán-Gómez, J.; Carrillo-Mondéjar, J.; Gómez, J.M.C.; Villalón, J.M. A MEC-IIoT Intelligent Threat Detector Based on Machine Learning Boosted Tree Algorithms. *Comput. Netw.* **2023**, *233*, 109868. [\[CrossRef\]](#)
63. Arat, F.; Akleylek, S. Attack Path Detection for IIoT Enabled Cyber Physical Systems: Revisited. *Comput Secur* **2023**, *128*, 103174. [\[CrossRef\]](#)
64. Chawla, D.; Mehra, P.S. A Survey on Quantum Computing for Internet of Things Security. *Procedia Comput. Sci.* **2023**, *218*, 2191–2200. [\[CrossRef\]](#)
65. Shafik, W. Artificial Intelligence and Internet of Things Roles in Sustainable Next-Generation Manufacturing: An Overview of Emerging Trends in Industry 6.0. *Sustain. Innov. Ind. 6.0* **2024**, 207–239.
66. Nassif, A.B.; Talib, M.A.; Nasir, Q.; Dakalbab, F.M. Machine Learning for Anomaly Detection: A Systematic Review. *IEEE Access* **2021**, *9*, 78658–78700. [\[CrossRef\]](#)
67. Pokhrel, S.; Abbas, R.; Aryal, B. IoT Security: Botnet Detection in IoT Using Machine Learning. *arXiv* **2021**, arXiv:2104.02231.
68. Santos, R.; Souza, D.; Santo, W.; Ribeiro, A.; Moreno, E. Machine Learning Algorithms to Detect DDoS Attacks in SDN. *Concurr. Comput.* **2020**, *32*, e5402. [\[CrossRef\]](#)
69. Tuan, N.N.; Hung, P.H.; Nghia, N.D.; Van Tho, N.; Van Phan, T.; Thanh, N.H. A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. *Electronics* **2020**, *9*, 413. [\[CrossRef\]](#)
70. Mohy-eddine, M.; Guezaz, A.; Benkirane, S.; Azrou, M. An Efficient Network Intrusion Detection Model for IoT Security Using K-NN Classifier and Feature Selection. *Multimed. Tools Appl.* **2023**, *82*, 23615–23633. [\[CrossRef\]](#)
71. Diro, A.A.; Chilamkurti, N. Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [\[CrossRef\]](#)
72. Guizani, N.; Ghafoor, A. A Network Function Virtualization System for Detecting Malware in Large IoT Based Networks. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1218–1228. [\[CrossRef\]](#)

73. Khan, I.A.; Keshk, M.; Pi, D.; Khan, N.; Hussain, Y.; Soliman, H. Enhancing IIoT Networks Protection: A Robust Security Model for Attack Detection in Internet Industrial Control Systems. *Ad Hoc Netw.* **2022**, *134*, 102930. [\[CrossRef\]](#)
74. Mudassir, M.; Unal, D.; Hammoudeh, M.; Azzedin, F. Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 2845446. [\[CrossRef\]](#)
75. Soliman, S.; Oudah, W.; Aljuhani, A. Deep Learning-Based Intrusion Detection Approach for Securing Industrial Internet of Things. *Alex. Eng. J.* **2023**, *81*, 371–383. [\[CrossRef\]](#)
76. Jayalaxmi, P.L.S.; Saha, R.; Kumar, G.; Alazab, M.; Conti, M.; Cheng, X. PIGNUS: A Deep Learning Model for IDS in Industrial Internet-of-Things. *Comput. Secur.* **2023**, *132*, 103315. [\[CrossRef\]](#)
77. Jayalaxmi, P.L.S.; Kumar, G.; Saha, R.; Conti, M.; Kim, T.H.; Thomas, R. DeBot: A Deep Learning-Based Model for Bot Detection in Industrial Internet-of-Things. *Comput. Electr. Eng.* **2022**, *102*, 108214. [\[CrossRef\]](#)
78. Qi, S.; Lu, Y.; Wei, W.; Chen, X. Efficient Data Access Control With Fine-Grained Data Protection in Cloud-Assisted IIoT. *IEEE Internet Things J.* **2021**, *8*, 2886–2899. [\[CrossRef\]](#)
79. Sakthidasan Sankaran, K.; Kim, B.H. Deep Learning Based Energy Efficient Optimal RMC-CNN Model for Secured Data Transmission and Anomaly Detection in Industrial IOT. *Sustain. Energy Technol. Assess.* **2023**, *56*, 102983. [\[CrossRef\]](#)
80. Alzubi, J.A.; Manikandan, R.; Alzubi, O.A.; Qiqieh, I.; Rahim, R.; Gupta, D.; Khanna, A. Hashed Needham Schroeder Industrial IoT Based Cost Optimized Deep Secured Data Transmission in Cloud. *Measurement* **2020**, *150*, 107077. [\[CrossRef\]](#)
81. Ren, Y.; Liu, X.; Sharma, P.K.; Alfarraj, O.; Tolba, A.; Wang, S.; Wang, J. Data Storage Mechanism of Industrial IoT Based on LRC Sharding Blockchain. *Sci. Rep.* **2023**, *13*, 2746. [\[CrossRef\]](#)
82. Rahman, A.; Islam, M.J.; Band, S.S.; Muhammad, G.; Hasan, K.; Tiwari, P. Towards a Blockchain-SDN-Based Secure Architecture for Cloud Computing in Smart Industrial IoT. *Digit. Commun. Netw.* **2023**, *9*, 411–421. [\[CrossRef\]](#)
83. Getman, A.I.; Goryunov, M.N.; Matskevich, A.G.; Rybolovlev, D.A. Methodology for Collecting a Training Dataset for an Intrusion Detection Model. *Proc. Inst. Syst. Program. RAS* **2021**, *33*, 83–104. [\[CrossRef\]](#) [\[PubMed\]](#)
84. Teixeira, M.A.; Salman, T.; Zolanvari, M.; Jain, R.; Meskin, N.; Samaka, M. SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach. *Future Internet* **2018**, *10*, 76. [\[CrossRef\]](#)
85. Al-Hawawreh, M.; Moustafa, N. Explainable Deep Learning for Attack Intelligence and Combating Cyber-Physical Attacks. *Ad Hoc Netw.* **2024**, *153*, 103329. [\[CrossRef\]](#)
86. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* **2022**, *10*, 40281–40306. [\[CrossRef\]](#)
87. Morris, T.; Gao, W. Industrial Control System Traffic Data Sets for Intrusion Detection Research. In *Critical Infrastructure Protection VIII*; IFIP Advances in Information and Communication Technology; Springer: Berlin/Heidelberg, Germany, 2014; Volume 441. [\[CrossRef\]](#)
88. Morris, T.; Vaughn, R.; Dandass, Y.S. A Testbed for SCADA Control System Cybersecurity Research and Pedagogy. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, TN, USA, 12–14 October 2011.
89. Rajawat, A.S.; Goyal, S.B.; Bedi, P.; Jan, T.; Whaiduzzaman, M.; Prasad, M. Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). *Future Internet* **2023**, *15*, 271. [\[CrossRef\]](#)
90. Nawaz, S.J.; Sharma, S.K.; Wyne, S.; Patwary, M.N.; Asaduzzaman, M. Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future. *IEEE Access* **2019**, *7*, 46317–46350. [\[CrossRef\]](#)
91. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* **1999**, *41*, 303–332. [\[CrossRef\]](#)
92. Kumari, S.; Singh, M.; Singh, R.; Tewari, H. Signature Based Merkle Hash Multiplication Algorithm to Secure the Communication in IoT Devices. *Knowl. Based Syst.* **2022**, *253*, 109543. [\[CrossRef\]](#)
93. Singamaneni, K.K.; Dhiman, G.; Juneja, S.; Muhammad, G.; AlQahtani, S.A.; Zaki, J. A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks. *Sensors* **2022**, *22*, 6741. [\[CrossRef\]](#)
94. Irie, H.; Wongpaisarnsin, G.; Terabe, M.; Miki, A.; Taguchi, S. Quantum Annealing of Vehicle Routing Problem with Time, State and Capacity. In *Quantum Technology and Optimization Problems*; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Cham, Switzerland, 2019; Volume 11413, pp. 145–156. [\[CrossRef\]](#)
95. Ajagekar, A.; You, F. Quantum Computing for Energy Systems Optimization: Challenges and Opportunities. *Energy* **2019**, *179*, 76–89. [\[CrossRef\]](#)
96. Mehta, A.; Muradi, M.; Woldetsadick, S. Quantum Annealing Based Optimization of Robotic Movement in Manufacturing. In *Quantum Technology and Optimization Problems*; Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Cham, Switzerland, 2019; Volume 11413, pp. 136–144. [\[CrossRef\]](#)
97. Knight, P.; Walmsley, I. UK National Quantum Technology Programme. *Quantum Sci. Technol.* **2019**, *4*, 040502. [\[CrossRef\]](#)
98. Nekuda Malik, J.A. Science Advocacy Drives Passage of US National Quantum Initiative Act. *MRS Bull.* **2019**, *44*, 158–159. [\[CrossRef\]](#)
99. Raymer, M.G.; Monroe, C. The US National Quantum Initiative. *Quantum Sci. Technol.* **2019**, *4*, 020504. [\[CrossRef\]](#)
100. Peral-García, D.; Cruz-Benito, J.; García-Peñalvo, F.J. Systematic literature review: Quantum machine learning and its applications. *Comput. Sci. Rev.* **2024**, *51*, 100619. [\[CrossRef\]](#)

101. Awschalom, D.; Berggren, K.K.; Bernien, H.; Bhawe, S.; Carr, L.D.; Davids, P.; Economou, S.E.; Englund, D.; Faraon, A.; Fejer, M.; et al. Development of Quantum Interconnects (QulCs) for Next-Generation Information Technologies. *PRX Quantum* **2021**, *2*, 017002. [\[CrossRef\]](#)
102. Schulz, W.G. US Government Shows Favor for National Quantum Initiative. *MRS Bull.* **2018**, *43*, 817–818. [\[CrossRef\]](#)
103. Marghny, M.H.; Abd El-Aziz, R.M.; Taloba, A.I. Differential Search Algorithm-Based Parametric Optimization of Fuzzy Generalized Eigenvalue Proximal Support Vector Machine. *Int. J. Comput. Appl.* **2014**, *108*, 38–46. [\[CrossRef\]](#)
104. Rivero-Angeles, M.E. Quantum-Based Wireless Sensor Networks: A Review and Open Questions. *Int. J. Distrib. Sens. Netw.* **2021**, *17*, 15501477211052210. [\[CrossRef\]](#)
105. EL Azzaoui, A.; Sharma, P.K.; Park, J.H. Blockchain-Based Delegated Quantum Cloud Architecture for Medical Big Data Security. *J. Netw. Comput. Appl.* **2022**, *198*, 103304. [\[CrossRef\]](#)
106. Luckow, A.; Klepsch, J.; Pichlmeier, J. Quantum Computing: Towards Industry Reference Problems. *Digit. Welt* **2021**, *5*, 38–45. [\[CrossRef\]](#)
107. Arya, V.; Almomani, A.; Han, C. Analysis of Quantum Computing-Based Security of Internet of Things(IoT) Environment. *Cyber Secur. Insights Mag.* **2022**, *4*, 7–14.
108. Yarkoni, S.; Raponi, E.; Bäck, T.; Schmitt, S. Quantum Annealing for Industry Applications: Introduction and Review. *Rep. Prog. Phys.* **2022**, *85*, 104001. [\[CrossRef\]](#)
109. Duong, T.Q.; Ansere, J.A.; Narottama, B.; Sharma, V.; Dobre, O.A.; Shin, H. Quantum-Inspired Machine Learning for 6G: Fundamentals, Security, Resource Allocations, Challenges, and Future Research Directions. *IEEE Open J. Veh. Technol.* **2022**, *3*, 375–387. [\[CrossRef\]](#)
110. Ali, M.Z.; Abohmra, A.; Usman, M.; Zahid, A.; Heidari, H.; Imran, M.A.; Abbasi, Q.H. Quantum for 6G Communication: A Perspective. *IET Quantum Commun.* **2023**, *4*, 112–124. [\[CrossRef\]](#)
111. Liu, J.; Wen, J.; Zhang, B.; Dong, S.; Tang, B.; Yu, Y. A Post Quantum Secure Multi-Party Collaborative Signature with Deterability in the Industrial Internet of Things. *Future Gener. Comput. Syst.* **2023**, *141*, 663–676. [\[CrossRef\]](#)
112. Chen, S.Y.C.; Yoo, S. Introduction to quantum federated machine learning. In *Federated Learning*; Academic Press: Cambridge, MA, USA, 2024; pp. 311–328.
113. Nguyen, Q.T.; Schatzki, L.; Braccia, P.; Ragone, M.; Coles, P.J.; Sauvage, F.; Larocca, M.; Cerezo, M. Theory for equivariant quantum neural networks. *PRX Quantum* **2024**, *5*, 020328. [\[CrossRef\]](#)
114. Gyongyosi, L.; Imre, S. A Survey on Quantum Computing Technology. *Comput. Sci. Rev.* **2019**, *31*, 51–71. [\[CrossRef\]](#)
115. Dunjko, V.; Briegel, H.J. Machine Learning & Artificial Intelligence in the Quantum Domain: A Review of Recent Progress. *Rep. Prog. Phys.* **2018**, *81*, 074001. [\[CrossRef\]](#) [\[PubMed\]](#)
116. Carleo, G.; Troyer, M. Solving the Quantum Many-Body Problem with Artificial Neural Networks. *Science* **2017**, *355*, 602–606. [\[CrossRef\]](#)
117. Lovett, N.B.; Crosnier, C.; Perarnau-Llobet, M.; Sanders, B.C. Differential Evolution for Many-Particle Adaptive Quantum Metrology. *Phys. Rev. Lett.* **2013**, *110*, 220501. [\[CrossRef\]](#)
118. Fingerhuth, M.; Babej, T.; Wittek, P. Open Source Software in Quantum Computing. *PLoS ONE* **2018**, *13*, e0208561. [\[CrossRef\]](#)
119. Sentís, G.; Monràs, A.; Muñoz-Tapia, R.; Calsamiglia, J.; Bagan, E. Unsupervised Classification of Quantum Data. *Phys. Rev. X* **2019**, *9*, 041029. [\[CrossRef\]](#)
120. Li, L.; Fan, M.; Coram, M.; Riley, P.; Leichenauer, S. Quantum Optimization with a Novel Gibbs Objective Function and Ansatz Architecture Search. *Phys. Rev. Res.* **2020**, *2*, 023074. [\[CrossRef\]](#)
121. Silva, V.L.; Kovaleski, J.L.; Pagani, R.N.; Corsi, A.; Gomes, M.A.S. Human Factor in Smart Industry: A Literature Review. *Future Stud. Res. J. Trends Strateg.* **2020**, *12*, 87–111. [\[CrossRef\]](#)
122. Hasanovic, M.; Panayiotou, C.; Silberman, D.; Stimers, P.; Merzbacher, C. Quantum Technician Skills and Competencies for the Emerging Quantum 2.0 Industry. *Opt. Eng.* **2022**, *61*, 081803. [\[CrossRef\]](#)
123. Lu, Y.; Sigov, A.; Ratkin, L.; Ivanov, L.A.; Zuo, M. Quantum Computing and Industrial Information Integration: A Review. *J. Ind. Inf. Integr.* **2023**, *35*, 100511. [\[CrossRef\]](#)
124. Sood, V.; Chauhan, R.P. Archives of Quantum Computing: Research Progress and Challenges. *Arch. Comput. Methods Eng.* **2023**, *31*, 73–91. [\[CrossRef\]](#)
125. van Erp, T.; Gladysz, B. Quantum Technologies in Manufacturing Systems: Perspectives for Application and Sustainable Development. *Procedia CIRP* **2022**, *107*, 1120–1125. [\[CrossRef\]](#)
126. Wang, D.; Wang, N. Quantum Computation Based Bundling Optimization for Combinatorial Auction in Freight Service Procurements. *Comput. Ind. Eng.* **2015**, *89*, 186–193. [\[CrossRef\]](#)
127. Antons, O.; Arlinghaus, J.C. Designing distributed decision-making authorities for smart factories—understanding the role of manufacturing network architecture. *Int. J. Prod. Res.* **2024**, *62*, 204–222. [\[CrossRef\]](#)

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.