electronics

MDPI

Review

A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity

Roman Rudenko [1], Ivan Miguel Pires [2,3], Paula Oliveira [2], João Barroso [1] and Arsénio Reis [1,*]

[1] Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), University of Trás-os-Montes e Alto Douro, Quinta de Prados, 5001-801 Vila Real, Portugal; al67552@utad.eu (R.R.); jbarroso@utad.pt (J.B.)
[2] Escola de Ciências e Tecnologia, University of Trás-os-Montes e Alto Douro, Quinta de Prados, 5001-801 Vila Real, Portugal; impires@it.ubi.pt (I.M.P.); pcoliveira@utad.pt (P.O.)
[3] Instituto de Telecomunicações, Universidade da Beira Interior, 6200-001 Covilhã, Portugal
* Correspondence: ars@utad.pt

Abstract: The advance of industrialization regarding the optimization of production to obtain greater productivity and consequently generate more profits has led to the emergence of Industry 4.0, which aims to create an environment called smart manufacturing. On the other hand, the Internet of Things is a global network of interrelated physical devices, such as sensors, actuators, intelligent applications, computers, mechanical machines, objects, and people, becoming an essential part of the Internet. These devices are data sources that provide abundant information on manufacturing processes in an industrial environment. A concern of this type of system is processing large sets of data and generating knowledge. These challenges often raise concerns about security, more specifically cybersecurity. Good cybersecurity practices make it possible to avoid damage to production lines and information. With the growing increase in threats in terms of security, this paper aims to carry out a review of existing technologies about cybersecurity in intelligent manufacturing and an introduction to the architecture of the IoT and smart manufacturing.

Keywords: cybersecurity; industry; Internet of Things; literature review

Citation: Rudenko, R.; Pires, I.M.; Oliveira, P.; Barroso, J.; Reis, A. A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity. *Electronics* **2022**, *11*, 1742. https://doi.org/10.3390/electronics11111742

Academic Editors: Paulo Ferreira and Antonio Pescapè

Received: 14 April 2022
Accepted: 29 May 2022
Published: 30 May 2022

1. Introduction

Industry 4.0 advocates are creating an intelligent manufacturing environment [1], and the IoT can be considered a paradigm in this area with great technological potential. The existence of different objects that communicate with each other intelligently, transmitting large amounts of information, generates security risks, making cybersecurity a very relevant issue of Industry 4.0 [2]. Bearing in mind that IoT solutions are applied in different environments, as is the case of intelligent manufacturing that generates and shares large amounts of information, which, if this is corrupted, can lead to production stoppages that can cause damage. With the growth in the use of IoT, it is estimated that internet traffic by the year 2022 will be around 45% [3,4].

There has been a significant investment by the industry to convert its production lines to create innovative manufacturing, which, according to Rossmann [5], promotes productivity growth by between 17% and 20% and gains in product quality of between 15% and 20%. This evolution is based on the application of IoT, machine learning, and cloud computing. Many of these developments seek to reduce costs and increase profits, leaving aside cybersecurity, one of the most critical aspects that can jeopardize product. This is due to the growing increase in cyber-attacks, poor understanding of vulnerabilities, and action lack of concern about this problem [6].

This study reviews the leading cybersecurity technologies currently used in the IoT paradigm in Industry 4.0 [7]. Aimed at the search for the most used cybersecurity technologies today in the Industry 4.0 and IoT paradigm, this study will show the added value

these can bring to smart manufacturing and demonstrate how they can solve problems of current attacks and the most common and the most common solutions. Two promising strategies in combating cyberattacks will also be demonstrated.

2. Methods

In this scientific review, a systematic methodology was chosen, highlighting the most critical points of the selected articles. In this systematic review, the research topic is based on applying the IoT paradigm in Industry 4.0, specifically cybersecurity. A critical phase is the choice of questions for the investigation since it will be based on the attempt to answer these same questions. For this purpose, the following two questions were formulated:

- Q1: What are the challenges of IoT cybersecurity in smart manufacturing?
- Q2: What types of cybersecurity are used in IoT for smart manufacturing?

Based on the research topic, exploratory research was carried out using the Snowball technique [8], which consists of selecting base articles focused on the research topic and the continuous investigation of the cited articles. When determining a base of three articles, they were read. The keywords were extracted, which were later used to create a query for the research. The following was obtained: ("internet of things" OR "IoT") AND ("smart manufacturing" OR "smart industry" OR "smart factory" OR "industry 4.0") AND ("cybersecurity" OR "cyber security").

Two online libraries were used for this research: IEEE and ScienceDirect. The IEEE library obtained 221 results, and 69 published articles were selected. In the ScienceDirect library, a result of 845 articles was obtained, and 108 papers were selected.

In the third stage of this review, selection, exclusion, and inclusion criteria were created. The inclusion criteria selected articles with the keywords mentioned above, published in journals, written in English, and published since 2016, utilizing more recent publications since we are talking about an innovative topic. As for the exclusion criteria, duplicate articles were removed whose titles followed a different theme from the intended one, and abstract content which was not related. After applying the inclusion criteria, a list of 177 publications was obtained:

1. Removed for not being in English;
2. Six duplicate publications were discarded;
3. One hundred and twenty-four publications were excluded due to their title;
4. Sixteen publications were excluded due to their content (little relevance).

Thus, after applying this methodology, we obtained 30 scientific articles published in journals that met the exclusion and inclusion criteria, which allowed us to answer the previously defined research questions. All papers were analyzed to select the most relevant to the topic in question.

In Figure 1, we can see the flowchart of the methodology used in the literature review, presenting the result in graphical form as recommended by PRISMA (preferred reporting items for systematic reviews and meta-analyses) [9]. Next, Table 1 summarizes the cybersecurity methods and their analysis, where the majority are related to IoT and industrial IoT.

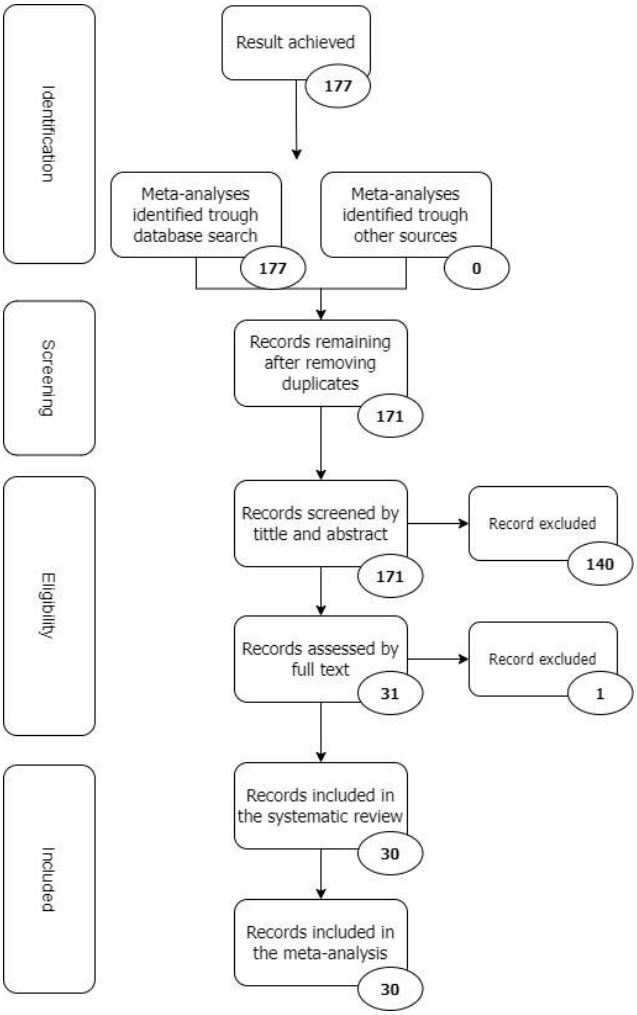

Figure 1. Flowchart of the methodology used in the literature review.

Table 1. Overview of the articles included in the review.

Study	Cybersecurity Method	Application
[10]	Blockchain	Smart manufacturing
[6]	State of the art	Smart manufacturing
[11]	Physical Hash	3D Production by STL
[12]	Blockchain	IoT
[13]	Innovative random hybrid neural network (HDRaNN)	Industrial IoT
[14]	Random neural network (RaNN)	Industrial IoT
[15]	Cybersecurity Guidelines	Smart manufacturing
[16]	Authentication Mechanism	Industrial IoT
[17]	Convolution Neural Network (CNN).	IoT
[18]	Decision tree (DT), random forest (RF), and extreme gradient boosting (XGBoost)	Industry 4.0 and IoT

Table 1. *Cont.*

Study	Cybersecurity Method	Application
[19]	State of the art	IoT
[20]	State of the art	IoT
[21]	State of the art Authentication Mechanism	IoT
[2]	A methodology to assess the impacts of cyber-attacks	Industry 4.0
[22]	Collaborative Learning Model for Cyberattack Detection	Industry 4.0 and IoT
[23]	Cyber security architecture	Industry 4.0 and IoT
[24]	Microsoft Threat Modelling Tool	Smart manufacturing
[25]	State of the art	Industry 4.0 and IoT
[26]	Deep Learning	IIoT
[27]	Logistic regression, decision tree, k-nearest neighbors, random forest, and autoencoder	Industry 4.0
[28]	State of the art, Blockchain	Industry 4.0
[29]	Protect machine-to-machine communication	IIoT
[30]	State of the art	IIoT
[31]	State of the art, Blockchain	Industry 4.0 and IoT
[32]	Basic cybersecurity requirements	Industry 4.0
[33]	Testbed	IoT
[34]	State of the art, cybersecurity threats	Industry 4.0
[35]	Ontology-Based Cybersecurity Framework	IoT
[36]	Hierarchical Network Intrusion Detection	IoT
[37]	Deep Learning	IoT

3. Results

The research in this scientific review resulted in many outcomes within Industry 4.0, IoT, and cybersecurity. Currently, there is no standard technology to ensure cybersecurity, as demonstrated in this study. The reviews focus on different computing areas, ranging from machine learning to blockchain, these being the promising technologies mentioned in several reviews. In Table 1, an overview of the articles included in the study, we can see the list of selected papers and their main characteristics.

Among the 30 articles of the result, 11 are related to state of the art. Their content focuses on presenting the main threats and possible solutions for them. Two of the studies are related to blockchain technology, and eight articles related to machine learning were obtained. Seven papers are related to attack detection models and attack response mechanisms. One article is related to calculating the impact of cyberattacks. One of the articles is focused on authentication technology.

The 28 articles present different technologies related to information on the topic. The articles related to machine learning present actual tests and comparisons with other existing technologies for the same purpose. However, none of the articles can be considered a final product that can be applied in an industrial environment.

The study by Latif et al. [14] aimed to demonstrate the great potential of integrating blockchain technology in an IoT environment aimed at an intelligent industry, focusing on creating a decentralized environment with ease of evolution. The author proposed a blockchain-based architecture for the security and confidentiality of a smart industry composed of two private blockchain modules. The first performs real-time asymmetric cryptography with ARM Cortex-M processors. The second contains a scalable and IoT-compatible system of proof of authentication (PoAh) implemented on the main blockchain network, which makes the transaction process lighter.

For this purpose, a blockchain architecture composed of three layers was proposed:

- Physical layer—consists of several sensors, microcomputers, and actuators. The sensors perform data collection and preprocessing, then send it through blockchain layers to the actuators.
- Blockchain service layer—the most critical layer that contains all the modules and services needed for the blockchain technology, it is subdivided into two parts, one related to real-time asymmetric cryptography with ARM Cortex-M processors and a private blockchain network which, through the proof of authentication (PoAh) consensus algorithm, allows the easy addition of new transactions.
- Application layer—layer with a user interface that allows the control, management, and visualization of systems and data.

In short, the author considers the proposed system as a secure, lightweight, and decentralized blockchain-based IoT network that allows performing various tasks reliably. Saxe et al. [12] studied trends in integrating blockchain technology with the IoT and the challenges. The main security improvements in IoT using blockchain are access control that allows for improving the general security of the network, data integration management, privacy guarantee, and the improvement of IoT availability. Despite the advances in the use of blockchain in the IoT, there are also significant challenges in their implementation, such as the reliability of the information generated by the IoT; IoT restrictions on resources to apply consensus algorithms, such as PoW, storage capacity, and scalability; smart contracts, anonymity, and confidentiality. The main challenges of blockchain are immature systems to compete with the speed of centralized systems, complex technical barriers, mobile networks and their initial state in decentralization, exploitable gaps in contract encryption standards, the need to carry out field tests, energy consumption, and mobile edge computing (MEC).

Tuptuk et al. [6] presented a state of the art exploration of the challenges of implementing smart manufacturing safely, evaluating existing systems, the principal vulnerabilities of intelligent manufacturing, possible future attacks, possible solutions, and the current weaknesses.

According to Brandman et al. [11], some technical equipment cannot withstand current threats and the possibility of updating them. For this purpose, the method proposed by Brandman et al. [11] consists of a physical hash directed to a 3D production through the STL (Standard Language of the Triangle). The hash in this process aims to generate a QR code with the input data, compare the predefined values with the obtained values, and connect intervals to a string. This string is sent through a hash function compared with the original if there is no match, the system is attacked, and the system aborts the production. In conclusion, the author considers separating the monitoring system from the machine itself a critical factor; another point is to ensure data transfer security between these two systems. For this purpose, a physical hash system in a QR code was developed. The proposed method was validated with three case studies, proving a robust mechanism for detecting attacks.

Huma et al. [13] aimed to demonstrate and evaluate a system based on deep learning that consists of an innovative random hybrid neural network (HDRaNN) for attacking IoT and IIoT attacks. HDRaNN combines an arbitrary neural network and a multilayer preceptor with dropout regularization. The technique proposed by the author was evaluated with two datasets related to IIoT security, DS2OS, and UNSW-NB15, and evaluated with several performance metrics and compared with state-of-the-art attack detection systems.

The proposed HDRaNN consists of a deep random neural network (DRaNN) and a multilayer perceptron (MLP). This model contains eight layers, one input, three RNN, three MLP layers, and one output. The system was implemented and adjusted according to the two initially proposed datasets DS2OS and UNSW-NB15. The performance was tested with two different datasets, DS2OS with a set of 86,984 test data with seven different types of attacks in which they obtained an accuracy of 98.56%, and with dataset UNSW-NB15 with a collection of 23,250 test data with nine kinds of attacks achieved an accuracy of 99.19%.

Latif et al. [14] demonstrated a system similar to that of Huma et al. [13], which aimed to create a system based on machine learning that consists of an innovative neural network based on a random neural network (RaNN), whose purpose is the detection of different cyber-attacks. After validating the proposed system, the authors performed tests with a DS2OS dataset that contained 357,952 samples with seven different types of attacks, reporting an accuracy of 99.20%.

Mullet et al. [15] presented a literature review that focuses on the practical aspects of Industry 4.0 relating to cybersecurity, presenting the vulnerabilities and threats to the network and devices, and the possible guidelines and solutions.

Srinivas et al. [16] propose a new user authentication approach with a user-authenticated key in which only authorized users can access the services of IoT devices. In this scheme, they demonstrate the technique for biometric verification with the possibility of applying new devices after implementation. The proposed project includes pre-implementation, user registration, login, authentication with password and biometrics, smart card revocation, and dynamic IoT detection. So, in the pre-implementation phase, a gateway node (GWN) is used, which stores the credentials in the database; in the registration phase, this is carried out offline with the introduction of the name and the keyword, then two random numbers are generated, and these are registered secretly in the GWN, after validation, it secretly creates a smart card for this user, after obtaining the smart card, the user makes their biometric registration in a specific terminal or mobile device and then everything is processed secretly, assigning a new smart card id to complete the registration. Proceeding to the login phase, the user must insert his card, access data, and perform the biometric reading. If validated, access is allowed to a selected IoT device. The login message is transmitted to the GWN, which makes the advance to authentication, reads the transfer order's time and date, and confirms all data. If everything is accepted, the user is authenticated. To validate its section, start system, the user used the ruby-on-rails (ROR) model, which is used for security analysis and based on various attacks, such as a man-in-the-middle attack, and mutual authentication, which demonstrated its ability to deal with these attacks.

Jeon et al. [17] proposed using convolution neural network (CNN) and malware analysis in IoT dynamically in the cloud, with the objective of dynamic research for IoT malware detection (DAIMD). This reduces damage to IoT devices by detecting both well-known and new IoT malware.

Trane et al. [18] proposed a new IoT architecture based on machine learning to detect and remediate cyber-attacks and provide reliable online monitoring. The machine-learning algorithm was random forest and allowed fault detection with an accuracy of 99.03%. Lu et al. [19] carried out a systematic analysis of cybersecurity in IoT, presenting IoT cybersecurity architecture and taxonomy, the primary enabling countermeasures and strategies, the main applications in the industries, and research trends and challenges. Similar to Lu et al., the authors Meneghello et al. [20] conducted a review to provide an insight into IoT security risks. Nandy et al. [21] reviewed IoT security, particularly authentication mechanisms and existing security verification techniques.

Corallo et al. [2] proposed a study that aims at a structured evaluation of critical industrial objects in Industry 4.0 and their impacts on industry performance due to security breaches, offering a 4-step cybersecurity policy to be implemented in a company's decision-making process. Thus, suggesting a methodology in which each step corresponds to an assessment of the level of impact on the business. The first step consists of evaluating the critical assets involved in cybersecurity. The second, which follows in parallel with

the first, consists of characterizing the impacts of each breached security requirement on an industry's data and systems. The third step consists of defining an impact matrix and evaluating assets affected by cyber threats and related commercial impacts. Finally, in the last step, the level of impact on the business is defined, adopting the proposed quantitative and qualitative assessment. In this way, it concludes that implementing this analysis methodology will allow the characterization of critical data, defining and isolating the impacts on the business. Khoa et al. [22] proposed a collaborative learning system to detect intrusions efficiently in the IoT of Industry 4.0. This system creates a filter in the IoT gateway to detect and prevent cyberattacks. The objective is training with deep learning algorithms using data collected on the industry network. After completing the training, this model will be shared with other IoT getaways to improve its accuracy in detecting attacks. The authors conclude that the proposed solution can outperform current machine learning models and allow the control of data and network traffic between IoT getaways.

Vijayakumaran et al. [23] presented a new cybersecurity architecture for the industrial IoT environment that detects cybersecurity threats and vulnerabilities and allows the exchange of information between devices automatically, protecting entities and network traffic involved in a wireless IIoT environment. The proposed system provides authentication for all devices using secure key cryptography to create a defense point between the external internet and the internal IIoT network. After analyzing the system, the author states that it will reduce storage space both on the server and in the cloud and reduce the overhead of transitions in the IIoT environment.

AbuEmera et al. [24] proposed a study that creates a catalog of components and a database of threats based on rules that allow solving possible threats in a smart factory. It uses STRIDE-based threat modeling (spoofing, tampering, repudiation, information disclosure, denial of Service, and elevation of privilege) and threat modeling tools, such as the Microsoft Threat Modeling Tool (TMT), are based on predefined rules to react to different attack scenarios. This solution allows the creation a smart manufactory system prepared for possible threats to identify potential vulnerabilities and a resolution of these in less time.

Abdullahi et al. [25] presented a systematic study of artificial intelligence methods to deal with current cyberattacks in the IoT environment in the Industry 4.0. The study's authors explored both machine learning and deep learning techniques that can be applied to ensure cybersecurity. Of the studies reviewed, the author mentioned that support vector machines (SVM) and random forest (RF) techniques were the most used because they guarantee better accuracy in attack detection. However, better performance techniques, such as extreme gradient boosting, were also mentioned, as were (XGBoost), neural networks (NN) and recurrent neural networks (RNN). After analyzing each of these techniques, the authors consider that the use of artificial intelligence methods is the most promising in the fight against cyber-attacks, allowing the detection and identification of threats.

Abdel-Basset et al. [26] aimed to demonstrate a deep learning model based on forensics with the primary objective of identifying intrusions and cyber-attacks in the IIoT network, giving the name Deep IFS to this system. This model uses LocalGrU to extract the local representation of the traffic and introduces a multi-head attention layer that captures the dependencies of this same traffic. One of the challenges of this project would be to overcome the limitations that come from a large dataset in a Big IIoT. For this purpose, the authors produced a programming environment in fog. This node is responsible for sharing training parameters and aggregating the work node that performs the classification sent to the platform cloud to mitigate the attacks. The authors concluded that the proposed system allows for more straightforward and less burdensome communication, allowing IIoT services to communicate securely and reliably.

Chang et al. [27] looked for an efficient and stable system for platforms to detect fraudulent activities and fraud in digital payments adapted to the Industry 4.0. For this purpose, five learning models were compared: logistic regression, decision tree, k-nearest neighbors, random forest, and autoencoder. According to the authors, all models presented

positive results in solving the proposed problems after carrying out the tests. However, the random forest and logistic regression algorithms managed to overcome the results of the other algorithms. Second, supervised algorithms were automated to improve fraud classification and minimize modeling time and resources.

Leng et al. [28] aimed to demonstrate research to discuss how blockchain systems can guarantee cybersecurity to achieve intelligence in the industry. The authors identified eight cybersecurity issues in the industry and ten metrics for implementing blockchain applications. Finally, the authors consider that based on the research carried out, they can serve to create an intelligent industry protected by blockchain.

Dhirani et al. [29] conducted a study that presents a path to identify, align, map, converge, and implement appropriate cybersecurity standards and tactics to secure machine to machine communications in the IIoT. In addition to the knowledge gained through research, the authors provide insights derived from the project of cybersecurity in Industry 4.0 that they are currently developing. The authors also mention the cybersecurity risks exposed to IIoT regardless of security standards and protocols implemented. Finally, the authors consider that their protection roadmap will provide guidelines that allow identifying, evaluating, and mitigating threats, creating different layers of protection, providing convergence and alignment, and finally helping to secure the heterogeneous production environment.

Shah et al. [30] analyzed different cyberattacks that can be launched against IIoT devices and described methods to mitigate these attacks. The authors divided IIoT into five different layers, presenting the various components of each layer and the possible cyberattacks and describing solutions that can be used as guides to ensure the cybersecurity of IoT and IIoT devices.

ElMammy et al. [31] described the classification of the most critical cyberattacks of the last decade in Industry 4.0 based on four classes, as well as protocols and blockchain implementations are discussed, and finally, a comparative study of blockchain application in Industry 4.0 to ensure secrecy, integrity, availability, privacy, and multi-factor authentication. The authors demonstrated that the use of hash function and cryptography proofs are solutions that have proven to be viable against various types of cyberattacks in the IoT environment. In conclusion, the authors made an application study of different blockchain-based frameworks.

Ilhan et al. [32] described the main components of Industry 4.0 and analyze the cyber threats in these components. In this way, the authors define the basic cybersecurity requirements, which consist of inventory of systems and devices, inventory of software and applications, secure configuration of software, malware protection, protecting network boundaries, and managing user accounts, record keeping and monitoring, backup and developing defense skills. The authors consider that this area is too broad and diversified, making it impossible to provide definitive solutions.

Lee et al. [33] aimed to analyze an energy control system's network configurations and characteristics and present and implement a database to verify security technologies applied to IIoT. For this purpose, several cyberattack scenarios were evaluated on the internal network of a power plant using the proposed database called a testbed, which allows the assessment of whether security technologies guarantee system availability.

Pereira et al. [34] presented reflections on the main cybersecurity challenges in Industry 4.0 to raise awareness of good security practices. The authors introduce the main threats that Industry 4.0 needs to focus on to mitigate its impact. The mentioned threats are enterprise cyber-espionage, confidential information, intellectual property, denial-of-service, supply chain, extended systems and smart security, and the smart factory. The authors consider it essential to make organizations aware of the impacts of attacks and the benefits of implementing security solutions.

Mozzaquatro et al. [35] proposed an ontological-based cybersecurity framework to improve IoT security adapted and appropriate to threats. The authors' proposal separates the framework into three layers: design time, run time, and IoTSec Ontology and a data

integration layer. The author presents adequate security solutions for each of these layers that can adapt and act in different IoT environments. Finally, the authors implemented their proposal and evaluated it based on knowledge of known cybersecurity issues and the corresponding prevention measures.

Bovenzi et. al. [36] proposed a hierarchical network intrusion detection adapted for IoT scenarios that are capable of detecting known and unknown attacks, subdivided into two stages; the H2ID (hierarchical network intrusion detection) performs attack detection through a lightweight solution based on a MultiModal Deep AutoEncoder (M2-DAE) and secondly performs attack classification with smooth output classifiers. The authors consider their innovative system that performs a hybrid task of attack classification detection and open-set attack classification. To evaluate the system, a BotIoT dataset was used with four types of attacks and unknown attacks, based on this evaluation the system showed very high performance for anomaly detection and attack recognition as well as being advantageous due to being suitable for distribution and privacy preservation, high efficiency, and good flexibility that is needed in IoT scenarios.

Nascita et al. [37] presented a work to evaluate attack classifiers in traffic based on state-of-the-art deep learning with multimodal and monomodal architecture and its comparison with traditional machine learning approaches. The authors evaluated the effectiveness of different systems in detecting attacks in an IoT environment with an IoT-23 database with various scenarios corresponding to malware samples or benign traffic. The results obtained showed that the ML mechanisms present a satisfactory result superior to the DL mechanisms; however, the authors used a multimodal traffic classifier called MIMETIC based on Dl which presented a very high precision, about 92%. In this way, the authors managed to shed some light on the main works of DL architecture in attack classification.

4. Discussion

4.1. Analysis of the Analyzed Studies

Based on the articles evaluated and their publication dates, we conclude that cybersecurity has been a growing concern due to increasingly sophisticated threats and greater automation of manufacturing processes. Lately, the security of an industry is a significant factor in its productivity: an undetected cyber-attack can lead to production stoppages, damage to the producer, and theft of confidential information. Today's security technologies are well known to cybersecurity professionals and cybercriminals, making it difficult to protect an industry. In this way, the contents above demonstrate current trends in cybersecurity and the IoT.

These are in line with blockchain technology solutions and the machine learning paradigm, which are innovative and promising technologies that ensure high accuracy in cybersecurity. Based on the review, many current threats and their solutions were obtained. However, little relevant content was obtained regarding future innovative technologies that would allow better detection and resolution of attacks, with most studies mentioning widespread technologies.

4.2. Relation with Industry 4.0 and the IoT

The industry is part of the economy that produces material goods automated. Industry 4.0 introduces grid-related intelligent systems that make self-regulated production sustainable [38]. Industry 4.0 was first initiated and promoted by the German government in 2011, taking this trend to all industrialized countries to enable cybernetic production systems. These changes and solutions need significant investments, sometimes leading to long implementation periods [39,40]. One of the main reasons for the emergence of a new industrial revolution is the need to strengthen the competitiveness of the European economy, which, with its increasing price of labor and progressive globalization, is losing its share in industrial production [41].

The Internet of Things consists of a network of devices, vehicles, physical objects, software, and sensors and is connected to a network that can collect and exchange data [7].

The IoT environment has allowed companies to become more efficient, reducing errors and accelerating processes. This technology represents the future of computing and communications, and its evolution depends on innovation and dynamic techniques [42]. IoT is constantly evolving, being the most promoted concept in the world of technologies; it projects the vision of a global infrastructure of networked physical objects, giving connectivity to anything anywhere [43].

IoT is a technology with a rapid growth rate that contributes to the realization of Industry 4.0. IoT and Industry 4.0 can provide many solutions, quickly generating personal, professional, and economic opportunities and benefits [44].

The traditional architecture of an IoT solution is organized into three layers: perception layer, network layer, and application layer. Each of these layers has vulnerabilities that can be exploited by hackers [45]. In the following section, the architectural reference model and the most common vulnerabilities in each layer are described.

There are several opinions regarding the number of layers used in IoT architecture. Each layer is defined with the devices and functions used in that layer. According to [46–48], an IoT solution comprises three layers: The perception layer, the network layer, and the application layer as observed in Figure 2. According to each one of the layers, the most widespread threats used for each one of them are presented.

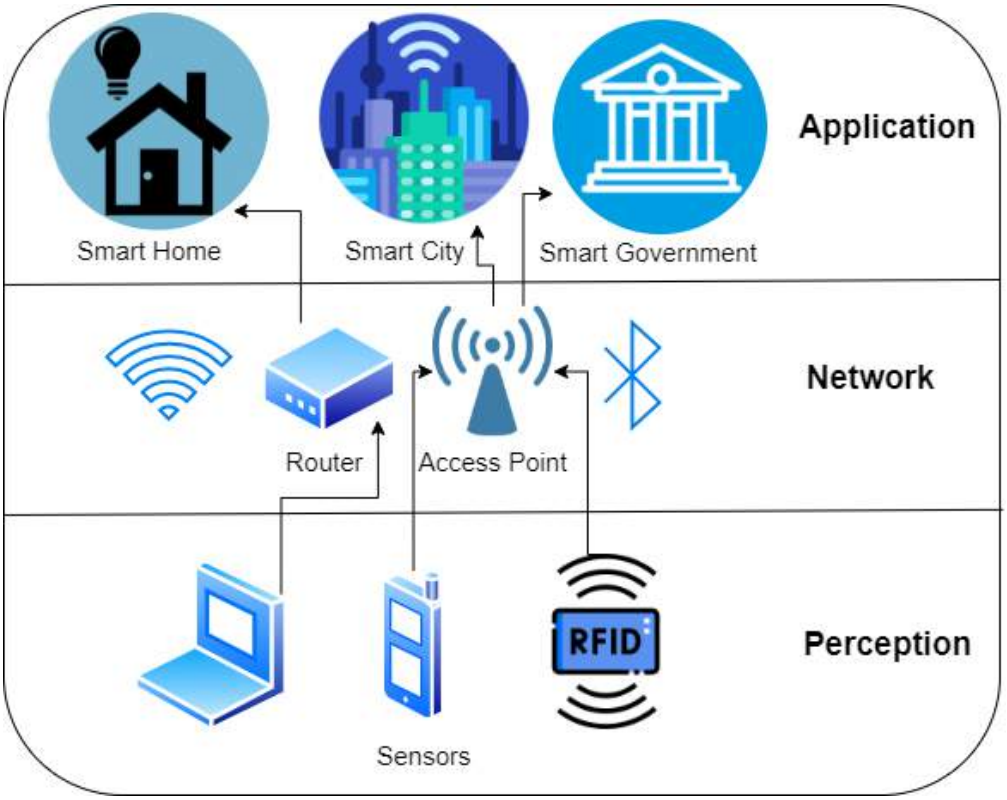

Figure 2. IoT architecture.

4.2.1. Perception Layer

This layer corresponds to the various sensors of the IoT solution, consisting of a large set of sensors linked together in a self-organized network through wireless communications. It is the layer that connects the IoT solution and the real world [49]. Security has become an enormous challenge that hinders the development of the IoT. In the case of the perception layer, the security challenges are even more significant due to the sensors having limited processing and data storage capabilities, making them more vulnerable. The most frequent attacks at this level are: node capture attacks, malicious code injection attacks, false data injection attacks, side-channel attacks [20], eavesdropping and interference, sleep

deprivation attacks, booting vulnerabilities, hardware exploitation, software exploitation, denial of service attack, and distributed denial of service (DDoS) attack [50–52].

4.2.2. Network Layer

This layer corresponds to the communication infrastructure, consisting of several private wired and wireless communication networks (WiFi, Bluetooth, WiMAX, and LoRaWAN, 2G, 3G, 4G, and 5G mobile networks). The network layer's primary function is to transport information from the perception layer to an information processing system [53]. The most frequent attacks at the network layer level are traffic analysis attacks, RFID spoofing, RFID cloning, RFID unauthorized access, sinkhole attacks, man-in-the-middle attacks, denial of service, routing information attacks, and Sybil attacks [50,52,54].

4.2.3. Application Layer

This layer is responsible for interacting with the end-user and providing various services. It has implementations in several areas, e.g., smart homes or smart factories, with CoAP, MQTT, and XMPP [55]. The main application layer security threats are malicious software such as phishing attacks, viruses, worms, trojan horses, spyware and aware, denial of service, malicious scripts, and encryption attacks [50].

4.3. Most Common Security Solutions Applied in the IoT Architecture

Following the previous topic, some possible solutions used in an IoT architecture will be presented. These are subdivided according to each IoT layer and their brief description.

4.3.1. Authentication on the Perception Layer

Authentication is how to identify and verify the authenticity of users' identification, allowing access to confidential data only to authorized personnel. Encryption processes allow sensor data security in the IoT, key and hash generation (maps varied data into fixed data), signature, and hash verification. Below are some of the security solutions used at this level:

- Triple data encryption algorithm (3DES or TDES)—a type of encryption where encryption algorithms are applied three times to each block of data;
- Advanced encryption standard (AES)—uses only a single key to encrypt and decrypt the information and is widely used for secure authentication [56];
- Asymmetric cryptography, or public-key cryptography, uses a pair of keys to encrypt and decrypt information, where one of the keys is public, and the other is private [57];
- Elliptic curve digital signature algorithm (ECDSA) is a digital signature algorithm that uses keys derived from elliptic curve cryptography, widely used on the web [58];
- Transport layer security (TLS) is a protocol whose objective is to guarantee communication security in a computer network. Transport layer security pre-shared key cipher suites (TLS-PSK) are a set of cryptographic protocols that allow secure transmission using pre-shared keys. TLS-DHE-RSA uses Rivest–Shamir–Adleman (RSA) key exchange, which is a public-key encryption system, and the Diffie–Hellman (DHE) protocol, which is a secure public key exchange system, to perform authentication [59,60];
- Multi-factor authentication, which uses biohashing, which that incorporates tax tokens, such as smart cards, and anonymity that allows hiding the identity of third parties, is another method that enables the performance of a secure authentication [59];
- A blockchain is a database that contains a distributed record so that there is not just one computer that includes the entire chain. Instead, users have a copy of the string. Blockchain allows the recording of transactions or any other digital interaction. It was designed to be safe and resistant to interruptions [61].

4.3.2. Secure Communication Solutions/Network Layer

The use of security protocols in an IoT network allows for secure communication and data protection in wireless and wired networks. One of the solutions is the use of

a virtual private network (VPN), which consists of a private communication network that uses the protocols: secure socket layer/transport layer security (SSL/TLS), which validates the transfer of data between servers, systems, applications, and users; media access control security (MACsec), which is a network security standard that provides point-to-point security over ethernet links; or datagram transport layer security (DTLS), which is a security protocol for applications that allows the prevention of eavesdropping, tampering, or the forging of messages [56]. Hash encryption is also a solution to guaranteeing data integrity and end-to-end message secrecy, ensuring data confidentiality and allowing it to be read-only by the person to whom the information is intended [62]. Private pre-shared key (PPSK) is a secure method used to connect to WiFi networks in a business environment [60].

The most common systems should also be mentioned, such as a firewall, which allows the analysis of traffic to guarantee the secure transmission of information and may be based on hardware or software, and an intrusion detection system/intrusion prevention system (IDS/IPS)—IDS responds to attacks using the firewall or other network devices, and IPS protects in real-time [56,60].

4.3.3. Application Security/Application Layer

IoT applications need to ensure their security using various techniques for this purpose, such as:

- Secure coding corresponds to a good software development practice to avoid the accidental introduction of security vulnerabilities;
- The secure boot protects against malicious attacks that can happen before the operating system starts;
- Access control list (ACL), which allows the specification of an object or user with access to a specific part of the system, allows only authorized processes [56];
- Firewall and IDS [63];
- Secure software updates correspond to software updates to ensure security [63].

4.4. Promising Cyber Security Techniques

After a systematic review of existing technologies today, we chose to demonstrate in more depth two technologies that, in our opinion, could be the future of cybersecurity, allowing a stable operation of an intelligent factory. These technologies could be the future of cybersecurity once they can gain greater confidence from industries. In this way, we present the terms of blockchain and machine learning in cybersecurity more in-depth. These two areas allow an innovative way to protect the IoT in intelligent manufacturing and quickly and effectively detect current threats.

4.4.1. Blockchain

Blockchain is a decentralized technology that guarantees the security and confidentiality of an intelligent industry and greater automation. Blockchain has emerged as a promising technology that promises to provide secure, distributed support and IoT ecosystems [64]. This technology was first mentioned in 1991 by Haber et al. It was defined as "a cryptographically protected blockchain" [65]. However, the greatest interest in blockchain emerged after the emergence of Bitcoin, which led to its promising recognition in various areas such as finance, agriculture, security, etc. [66].

Blockchain records information called blocks connected and protected using cryptographic algorithms [67]. This innovative technology promises a high level of responsibility. Several sectors are testing this innovation, which has key features such as transparency, decentralization, immutability, pseudonymization, non-repudiation, and traceability [12].

The increasing number of physical devices connected to the internet network consequently presents an increase in vulnerabilities in IoT systems. Devices are at high risk of being targets of different attacks like spying, DDoS, etc. [68]. One of the ways to improve IoT security is by implementing a blockchain-based IoT framework that will allow the prevention of various types of attacks [69], excluding dependence on third-party secu-

rity. In this way, it can introduce blockchain-based security improvements in IoT, such as providing blockchain access control that allows for improved overall network status [70], data management [71], ensuring privacy [72], and improving IoT availability, all through blockchain [73]. However, integrating IoT with blockchain can present several challenges. In the case of security, the blockchain can guarantee data immutability, but it can present certain threats if the entered data is corrupted: it will remain registered on the blockchain. Thus, it can have consequences in communication, such as in devices and in blockchain IoT communication, due to communication protocols [12].

Based on the articles reviewed in Chapter 3, we were able to identify two of the articles that used blockchain techniques to ensure cybersecurity in an IoT environment; the authors, Latif et al., proposed a blockchain-based architecture for security and confidentiality composed of two private blockchain modules, which, after their development and implementation, proved to be safe, lightweight, and decentralized with the ability to perform various tasks reliably. Saxe et al. presented a study on the integration of IoT with blockchain in which they mentioned that the use of blockchain would improve the security of a network and ensure data integrity as well as improve the privacy and availability of the IoT.

Thus, we can conclude that it is a promising technology that can bring many benefits. However, the IoT still needs to be refined, which can be resolved with studies already being carried out on this subject.

4.4.2. Machine Learning

Machine learning (ML) can be considered a subset of artificial intelligence, aiming to improve computer algorithms based on experience or data, building a model based on training data to make predictions or decisions without being programmed [74]. Machine learning creates behavior models based on mathematical techniques and a large amount of training data, making it possible to predict the future based on the data entered. These techniques are used where humans cannot use their knowledge, such as speech recognition, malicious code detection, pattern recognition for industrial use, and even cybersecurity.

Most of the existing solutions to ensure the security of IoT systems generates a sizeable computational load for IoT devices, such as sensors. A possible technique that could reduce this computational load is machine learning. Lately, it has been widely used in different areas, such as network security, authentication, access control, and malware detection [75]. The generation of large data sets by the IoT allows the broad use of ML (machine learning) technologies to make intelligent decisions. ML techniques can identify malicious code in software and applications and detect DDoS attacks through the behavior analysis, authentication, detection, and mitigation of attacks and intrusions [76]. The existence of several machine learning techniques that can be used to solve different security problems allows a more appropriate choice for our situation based on the accuracy of the chosen design.

The use of ML techniques has been extensively studied and implemented in different environments, which can be confirmed by our review that presents eight studies focused on cybersecurity using ML systems, which proves a growing interest in this type of system. However, its implementation can present specific challenges. The different ways of performing similar tasks can take longer times when discovering the correct method to achieve training or when a sufficient explanation and vision for a model or system does not yet exist.

5. Conclusions

With the new industrial revolution, which led industries to seek greater digitalization and advance towards Industry 4.0, equipment that previously operated in isolation underwent a transformation that allowed their integration and communication to bring greater productivity, integrity, flexibility, and quality of industries. The use of the IoT paradigm by industries permitted the integration of different equipment in a production line that

communicates with each other to create more intelligent production lines and, in this way, increases productivity. This industrial revolution faces a significant challenge: its security, as cyber-attacks can cause great damage to organizations and customers.

Current cyber-attacks are increasingly efficient, with more incredible difficulty in being detected and resolved, which leads to the search for more effective and innovative solutions to guarantee a company's security. Despite several cybersecurity techniques, these can often be unviable in financial terms, leading to significant investments that many organizations do not make in this area. To create new technologies in cybersecurity, given that there has been a growing concern regarding this problem, industries are looking for more innovative and productive ways to detect threats and prevent them, such as the promising blockchain technology and machine learning techniques.

After the analysis of the eleven studies presented in this systematic review, we can find answers to our main questions. Regarding Q1: "What are the challenges of IoT cybersecurity in smart manufacturing?", we verified that in most of the articles analyzed, the biggest challenge is the rapid detection of attacks and their identification to act more effectively, thus reducing severe consequences, as we are talking about an IoT environment that consists of several connected sensors. Usually, low processing capacity makes it difficult to protect them. Researchers seek to create innovative tools that can overcome these obstacles while keeping IoT sensors protected to solve this problem. A significant challenge is linked to the evolution of increasingly innovative and sophisticated attacks, leading industries to seek innovative solutions to combat current and future attacks. As security evolves, cyberattacks evolve too.

Regarding Q2: "What types of cybersecurity are used in IoT for smart manufacturing?", the studies analyzed show several forms of protection against cyberattacks in different industry layers. The cybersecurity of intelligent manufacturing has to be developed in a personalized way. There is no common method of use, although the concept presents variations with similarities. However, the most promising are based on machine learning and blockchain.

This article sought to obtain knowledge in cybersecurity and the latest trends in a smart manufacturing environment to be applied in future work that involves developing a threat detection system in an IoT architecture within smart manufacturing. This work's contribution consists of providing several perspectives for solving cybersecurity problems in an industrial environment linked to IoT. For this purpose, an analysis of 28 articles was made that resulted in a large set of possible threats and solutions for these threats and some technologies that can be applied in the future at different levels of IIoT.

The main message of this work was the discovery of current solutions applied to classify and deter different types of attacks in the Industry 4.0 in an IoT environment, including identifying current works in this area, identifying the existing attacks, and the solutions that can be applied to combat these attacks, as well as a vision for solutions that are growing and with greater interest.

Based on knowledge to be obtained in future work, we would propose a tool based on machine learning that will allow the detection of attacks on IoT sensors in a smart manufacturing environment.

Author Contributions: Conceptualization, R.R; methodology, R.R. and A.R.; validation, A.R.; formal analysis, R.R.; investigation, R.R.; data curation, P.O.; writing—original draft preparation, R.R., I.M.P. and A.R.; writing—review and editing, R.R., I.M.P. and J.B.; supervision, A.R.; project administration, P.O.; funding acquisition, I.M.P. and J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the ID Project "DEoLTA: Digitalisation of end-of-line distributed testers for antennas, operação POCI-01-0247-FEDER-049698", financed by the Fundos Europeus Estruturais e de Investimento (FEEI), through the Program "Programa Operacional Competitividade e Internacionalização (POCI)/PORTUGAL 2020". This work is also funded by FCT/MEC through national funds and, when applicable, cofunded by the FEDER-PT2020 partnership agreement under the project UIDB/50008/2020. This article is based upon work from COST Action IC1303-AAPELE—Architectures, Algorithms, and Protocols for Enhanced Living Environments and COST Action CA16226–SHELD-ON—Indoor living space improvement: Smart Habitat for the Elderly, supported by COST (European Cooperation in Science and Technology). COST is a funding agency for research and innovation networks. Their actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. It boosts their research, career, and innovation. More information in www.cost.eu (accessed on 25 May 2022).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Nwakanma, C.; Islam, F.; Maharani, M.; Lee, J.-M.; Kim, D.-S. Detection and Classification of Human Activity for Emergency Response in Smart Factory Shop Floor. *Appl. Sci.* **2021**, *11*, 3662. [CrossRef]
2. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
3. Balda, J.C.; Mantooth, A.; Blum, R.S.; Tenti, P. Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things. *IEEE Power Electron. Mag.* **2017**, *4*, 37–43. [CrossRef]
4. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
5. Shrouf, F.; Ordieres, J.; Miragliotta, G. Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Selangor Darul Ehsan, Malaysia, 9–12 December 2014.
6. Tuptuk, N.; Hailes, S. Security of smart manufacturing systems. *J. Manuf. Syst.* **2018**, *47*, 93–106. [CrossRef]
7. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. Tackling Faults in the Industry 4.0 Era—A Survey of Machine-Learning Solutions and Key Aspects. *Sensors* **2020**, *20*, 109. [CrossRef]
8. Etikan, I.; Alkassim, R.; Abubakar, S. Comparision of snowball sampling and sequential sampling technique. *Biom. Biostat. Int. J.* **2016**, *3*, 55. [CrossRef]
9. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef]
10. Latif, S.; Idrees, Z.; Ahmad, J.; Zheng, L.; Zou, Z. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *J. Ind. Inf. Integr.* **2021**, *21*, 100190. [CrossRef]
11. Brandman, J.; Sturm, L.; White, J.; Williams, C. A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. *J. Manuf. Syst.* **2020**, *56*, 202–212. [CrossRef]
12. Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [CrossRef]
13. Huma, Z.E.; Latif, S.; Ahmad, J.; Idrees, Z.; Ibrar, A.; Zou, Z.; Alqahtani, F.; Baothman, F. A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. *IEEE Access* **2021**, *9*, 55595–55605. [CrossRef]
14. Latif, S.; Zou, Z.; Idrees, Z.; Ahmad, J. A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network. *IEEE Access* **2020**, *8*, 89337–89350. [CrossRef]
15. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
16. Srinivas, J.; Das, A.K.; Wazid, M.; Kumar, N. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 1133–1146. [CrossRef]
17. Jeon, J.; Park, J.H.; Jeong, Y.-S. Dynamic Analysis for IoT Malware Detection with Convolution Neural Network Model. *IEEE Access* **2020**, *8*, 96899–96911. [CrossRef]
18. Tran, M.-Q.; Elsisi, M.; Mahmoud, K.; Liu, M.-K.; Lehtonen, M.; Darwish, M.M.F. Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment. *IEEE Access* **2021**, *9*, 115429–115441. [CrossRef]

19. Lu, Y.; Da Xu, L. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet Things J.* **2018**, *6*, 2103–2115. [CrossRef]
20. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
21. Nandy, T.; Bin Idris, M.Y.I.; Noor, R.; Kiah, M.L.M.; Lun, L.S.; Juma'At, N.B.A.; Ahmedy, I.; Ghani, N.A.; Bhattacharyya, S. Review on Security of Internet of Things Authentication Mechanism. *IEEE Access* **2019**, *7*, 151054–151089. [CrossRef]
22. Khoa, T.V.; Saputra, Y.M.; Hoang, D.T.; Trung, N.L.; Nguyen, D.; Ha, N.V.; Dutkiewicz, E. Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea, 25–28 May 2020; pp. 1–6. [CrossRef]
23. Vijayakumaran, C.; Muthusenthil, B.; Manickavasagam, B. A reliable next generation cyber security architecture for industrial internet of things environment. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 387–395. [CrossRef]
24. AbuEmera, E.A.; ElZouka, H.A.; Saad, A.A. Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach. In Proceedings of the 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 14–16 January 2022.
25. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics* **2022**, *11*, 198. [CrossRef]
26. Abdel-Basset, M.; Chang, V.; Hawash, H.; Chakrabortty, R.K.; Ryan, M. Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7704–7715. [CrossRef]
27. Chang, V.; Doan, L.M.T.; Di Stefano, A.; Sun, Z.; Fortino, G. Digital payment fraud detection methods in digital ages and Industry 4.0. *Comput. Electr. Eng.* **2022**, *100*, 107734. [CrossRef]
28. Leng, J.; Ye, S.; Zhou, M.; Zhao, J.L.; Liu, Q.; Guo, W.; Cao, W.; Fu, L. Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *51*, 237–252. [CrossRef]
29. Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. *Sensors* **2021**, *21*, 3901. [CrossRef]
30. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020.
31. ElMamy, S.; Mrabet, H.; Gharbi, H.; Jemai, A.; Trentesaux, D. A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0. *Sustainability* **2020**, *12*, 9179. [CrossRef]
32. lhan, İ.; Karaköse, M. Requirement Analysis for Cybersecurity Solutions in Industry 4.0 Platforms. In Proceedings of the 2019 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 21–22 September 2019.
33. Lee, S.; Lee, S.; Yoo, H.; Kwon, S.; Shon, T. Design and implementation of cybersecurity testbed for industrial IoT systems. *J. Supercomput.* **2018**, *74*, 4506–4520. [CrossRef]
34. Pereira, T.; Barreto, L.; Amaral, A. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manuf.* **2017**, *13*, 1253–1260. [CrossRef]
35. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors* **2018**, *18*, 3053. [CrossRef]
36. Bovenzi, G.; Aceto, G.; Ciuonzo, D.; Persico, V.; Pescapé, A. A hierarchical hybrid intrusion detection approach in IoT scenarios. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020.
37. Nascita, A.; Cerasuolo, F.; Di Monda, D.; Garcia, J.T.A.; Montieri, A.; Pescape, A. Machine and Deep Learning Approaches for IoT Attack Classification. In Proceedings of the 2022 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Virtual, 2–5 May 2022.
38. Gubán, M.; Kovács, G. Industry 4.0 conception. *Acta Tech. Corviniensis-Bull. Eng.* **2017**, *10*, 111–114.
39. Hermann, M.; Pentek, T.; Otto, B. Design principles for industrie 4.0 scenarios. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016.
40. Grabowska, S. Smart factories in the age of Industry 4.0. *Manag. Syst. Prod. Eng.* **2020**, *28*, 90–96. [CrossRef]
41. Wheeler, K. How a 'Segment of One' Approach Can Help Businesses Connect with Their Customers. Available online: https://www.fourthsource.com/general/how-a-segmentof-one-approach-can-help-businesses-connect-with-theircustomers-23392 (accessed on 12 November 2019).
42. Ferguson, G.T. Have your objects call my objects. *Harv. Bus. Rev.* **2002**, *80*, 138–144.
43. Madakam, S.; Ramaswamy, R.; Tripathi, S. Internet of Things (IoT): A literature review. *J. Comput. Commun.* **2015**, *3*, 164. [CrossRef]
44. Georgios, L.; Kerstin, S.; Theofylaktos, A. Internet of things in the context of industry 4.0: An overview. *Int. J. Entrep. Knowl.* **2019**, *7*, 4–19.
45. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.
46. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (siot)—When social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]

47. Leo, M.; Battisti, F.; Carli, M.; Neri, A. A federated architecture approach for Internet of Things security. In Proceedings of the 2014 Euro Med Telco Conference (EMTC), Naples, Italy, 12–15 November 2014.
48. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Emeishan, Chinay, 14–15 December 2013.
49. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 983–994. [CrossRef]
50. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017, Analytics and Cloud) (I-SMAC).
51. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef]
52. Kumar, S.; Sahoo, S.; Mahapatra, A.; Swain, A.K.; Mahapatra, K.K. Security enhancements to system on chip devices for IoT perception layer. In Proceedings of the 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Bhopal, India, 18–20 December 2017.
53. Yang, Z.; Yue, Y.; Yang, Y.; Peng, Y.; Wang, X.; Liu, W. Study and application on the architecture and key technologies for IOT. In Proceedings of the 2011 International Conference on Multimedia Technology, Hangzhou, China, 26–28 July 2011.
54. Santos, L.; Rabadao, C.; Gonçalves, R. Intrusion detection systems in Internet of Things: A literature review. In Proceedings of the 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018.
55. Nastase, L. Security in the internet of things: A survey on application layer protocols. In Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017.
56. Islam, M.R.; Aktheruzzaman, K.M. An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. *J. Comput. Commun.* **2020**, *8*, 11–25. [CrossRef]
57. Hodgson, R. Solving the security challenges of IoT with public key cryptography. *Netw. Secur.* **2019**, *2019*, 17–19. [CrossRef]
58. Johnson, D.; Menezes, A.; Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
59. Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
60. Leloglu, E. A Review of Security Concerns in Internet of Things. *J. Comput. Commun.* **2016**, *5*, 121–136. [CrossRef]
61. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *J. Intell. Manuf.* **2019**, *30*, 1111–1123. [CrossRef]
62. Li, P.; Su, J.; Wang, X. iTLS: Lightweight Transport-Layer Security Protocol for IoT with Minimal Latency and Perfect Forward Secrecy. *IEEE Internet Things J.* **2020**, *7*, 6828–6841. [CrossRef]
63. Chen, K.; Zhang, S.; Li, Z.; Zhang, Y.; Deng, Q.; Ray, S.; Jin, Y. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *J. Hardw. Syst. Secur.* **2018**, *2*, 97–110. [CrossRef]
64. Butun, I.; Osterberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
65. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
66. Nakamoto, S.; Bitcoin, A. A Peer-to-Peer Electronic Cash System. Bitcoin. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 14 May 2022).
67. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
68. Rathi, R.; Sharma, N.; Manchanda, C.; Bhushan, B.; Grover, M. Security challenges & controls in cyber physical system. In Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 10–12 April 2020.
69. Halpin, H.; Piekarska, M. Introduction to Security and Privacy on the Blockchain. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017.
70. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017.
71. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017.
72. 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.* **2016**, *15*, 840–852. [CrossRef]
73. Bahga, A.; Madisetti, V.K. Blockchain Platform for Industrial Internet of Things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
74. Zhang, X.-D. *Machine Learning, in a Matrix Algebra Approach to Artificial Intelligence*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 223–440.
75. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1153–1176. [CrossRef]
76. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]