EXPLORING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY WITHIN THE INDUSTRY 4.0 FRAMEWORK: A COMPREHENSIVE SURVEY

Mounika Nakrekanti[1], Ramesh Polisetti[2]

1. Working as a Assistant Professor in the Department of Information Technology at TKR College of Engineering & Technology, Medbowli, Meerpet, Saroor Nagar, Hyderabad. Pin – 500097
2. Working as a Assistant Professor in the Department of Artificial Intelligence & Machine Learning at TEEGALA KRISHNA REDDY Engineering College, Medbowli, Meerpet, Saroor Nagar, Hyderabad. Pin – 500097

Abstract:

The surge in cyber-attacks is significantly impacting the operational resilience of organizations within the industrial sector, exploiting vulnerabilities inherent in networked machinery. The pervasive digitization and technological advancements emblematic of Industry 4.0 have prompted substantial investments in innovation and automation. Nevertheless, this digital transformation introduces a suite of risks, prominently among them being cyber security vulnerabilities.

Cyber adversaries continuously evolve their tactics, leveraging artificial intelligence (AI) to enhance the sophistication of their attacks. AI-powered cyber threats, when coupled with conventional methods, pose exponential risks to organizations operating within the Industry 4.0 paradigm. The expanding reliance on networked information technology further amplifies the attack surface, underscoring the urgent need for robust cyber security measures.

In response, this paper conducts a systematic literature review to identify and analyze publications detailing AI-based cyber-attacks. The objective is twofold: firstly, to gain a deeper understanding of the tactics employed by cybercriminals, and secondly, to derive insights for the development of effective cyber security measures. By synthesizing existing research, this study aims to provide the research community with valuable insights to fortify defenses against emergent cyber threats.

The findings of this research can serve as a foundation for enhancing the detection and mitigation of AI-driven cyber-attacks. Ultimately, this study endeavors to empower organizations and cybersecurity practitioners with the knowledge needed to navigate the evolving threat landscape of Industry 4.0 securely.

Keywords: artificial intelligence; cyber security; industry 4.0; machine learning; deep learning inclusions are presented in Section 6.

1. Introduction

The fourth industrial revolution, commonly referred to as Industry 4.0, is aimed at establishing real-time manufacturing ecosystems, smart factories, and autonomous systems within industrial environments. Projects associated with Industry 4.0 leverage a spectrum of information technologies, including cyber-physical systems (CPS), the Internet of Things (IoT), cloud computing, automation, big data, and artificial intelligence (AI). These initiatives are driven by the imperative to enhance competitiveness and address the imperatives of digital transformation [1].

The technological advancements ushered in by Industry 4.0 enable the widespread application of digitization, connectivity, and automation technologies. This digital transformation yields a substantial increase in the volume of data within cyberspace [2]. While the potential of Industry 4.0 is promising, its realization necessitates the development of methodological frameworks to navigate the complexities of digitization and machine interconnectivity, thereby bolstering competitiveness. However, the intricate network of CPS introduces risks, particularly in terms of cybersecurity [3].

The digitization of operational processes and business models, reliant on information technologies, heightens exposure to potential cyber-attacks [4]. Consequently, cybersecurity has ascended to a prominent position on the agendas of both public and private sector leadership [5], catalyzed by notable cyber incidents such as Black Energy in Ukraine (2007), Stuxnet (2010), Havex (2014), SolarWinds (2020), Colonial Pipeline (2021), and Pilz (2021). Cyber adversaries continuously refine their methodologies and attack strategies, leveraging AI technologies to augment their capabilities. This malicious use of AI has reshaped the cybersecurity landscape [6].

The proliferation of network-connected manufacturing devices, facilitated by the Internet, expands the attack surface for cyber adversaries. Exploiting their intelligence, attackers transcend geographical boundaries to perpetrate nefarious activities while minimizing detection [7]. Consequently, staying abreast of cybercrime trends is imperative to mount effective defense strategies. Given the evolving technological landscape, comprehensive studies are warranted to counter the potential weaponization of AI by cybercriminals. This research endeavors to address this gap.

This paper aims to conduct systematic literature research to identify publications on AI-based cyber-attacks and assess their relevance to cybersecurity within the Industry 4.0 context. The analysis seeks to furnish the research community with insights to fortify defenses against potential AI-driven threats. The paper comprises six sections: Section 2 elucidates the theoretical underpinnings of the research concepts, Section 3 delineates the methodological approach, Section 4 reviews related literature and examines the state-of-the-art research on AI-based cyber-attacks, Section 5 analyzes and discusses the impacts of AI-based cyber-attacks on the Industry 4.0 ecosystem, and Section 6 presents conclusions.

2. Theoretical Background

In the following, the reader can have a vision of the theoretical background of Artificial Intelligence, Cyber Security, Industry 4.0, and Cyber-Physical Systems.

2.1. Artificial Intelligence

AI dates to the 1950s and recent AI technological advances have impacted growth in innovation and automation in manufacturing. Despite the inherent benefits of AI technologies, the use of these echniques has sparked debates about their use in malicious ways [8]. AI is a field of computer science that develops theories, methods, techniques, and systems to simulate and expand human intellect into machines [9]. The goal of AI is to endow machines with human intelligence. Machine learning is a method to implement AI using algorithms to analyze and learn from data. Deep learning is a technology used in the process of machine learning, enabling the expansion of the scope of AI [10]. The essence of AI is based on the context that human intelligence can be accurately described, enabling its replication by machines and/or software [11].

AI addresses topics such as reasoning, knowledge, planning, automation, machine learning, natural language processing, robotics, human intelligence, and cyber security [11]. AI applications form a multidisciplinary intersection with cyber security issues. However, as AI technologies become more advanced and ubiquitous, cyber-attacks on CPS are on the rise, exploiting the interface between the connection of physical and cyber elements [12,13]. The threat landscape involves multiple players, attackers seek different types of vulnerabilities to launch their attacks. These attacks include the complexity and sophistication of advanced persistent threats, malicious actions in cyberspace, and monetization of cybercrime [6]. The cyber security community needs to understand how AI can be used for cyber-attacks and identify its weaknesses in order to implement defense actions [14].

2.1.1. Machine Learning

Machine learning (ML) is a method used to implement AI algorithms to analyze data, learn from the data, and make decisions about real-world events [10]. ML systems can be divided into (i) systems for initial training on the dataset; (ii) systems already trained for later decision-making [15]. Given the large amount of data available, there is a strong demand for the application of ML techniques.

Researchers apply various approaches to deal with this large amount of data. Industry applies these techniques to extract relevant data. ML relies on different algorithms to solve data problems. The type of algorithm depends on the problem to be solved, considering the variables involved in the learning process [16]. In the age of digital transformation, ML is a relevant discipline in the research field of AI-based cyber security. Importantly, AI, particularly ML, has been used in both attack and defense of cyberspace. From the attacker’s point of view, ML is employed to compromise cyber protection strategies. On the defense side, ML is applied to provide robust resilience against threats, in order to adaptively minimize the damaging impacts of cyber-attacks [17].

ML algorithms can be categorized into supervised learning, unsupervised learning, and reinforcement learning [18]. The following is a contextualization of these algorithms. Supervised learning is when the model learns from predefined results by using past values for the target variable to learn what its output results should be [15]. Unsupervised learning, unlike supervised learning, does not have predefined results for the model to use as a reference for learning. The model works with a set of data and tries to find patterns and differences in this data [15]. Supervised and unsupervised learning applications are widely used for intrusion, malware detection, cyber-physical attacks, and data privacy protection [19–21]. Reinforcement learning, a branch of ML, demands sequential actions in an omitted way with or without knowledge of the environment, thus allowing a closer approximation to human learning [17].

There are several ML algorithms used in industry. For example: (i) Supervised Learning: Additive Models, Artificial Neural Networks, Bayesian Networks, Decision Tree, Random Forest, K-Nearest Neighbors, Logistic Regression, Naïve Bayesian Networks, and Regression Tree; (ii) Unsupervised Learning: K-means, and Self Organizing Map; (iii) Reinforcement Learning: Smart, and Pilco [8,22,23].

2.1.2. Deep Learning

Deep learning (DL) is a powerful ML technique that seeks to establish an artificial neural network that simulates the human brain for analytical learning in the interpretation of data [24]. An artificial neural network is a series of algorithms that seek to recognize implicit relationships in a dataset, through a process that mimics the way the human brain works. Neural networks refer to a system of neurons, either organic or artificial in nature [16].

DL uses multiple layers to build artificial neural networks with the ability to make intelligent decisions by processing large amounts of data with a high level of complexity without human intervention [25]. DL techniques can process a large amount of cyber security-related data made available in cyberspace. Researchers use ML and DL methods to detect malicious behavior in information systems arising from cyber-attacks [26]. The applications of DL techniques provide proactive monitoring in the industrial environment, producing essential data about the manufacturing process [23].

The combination of deep learning and reinforcement learning indicates excellent effectiveness and efficiency for cyber security applications dealing with increasingly dynamic and complex cyber-attacks [17]. There are several deep learning models used in industry. For example, (i) Supervised Learning: Convolutional Neural Network, Multiple Linear Perceptron, Recurrent Neural Network, Restricted Boltzmann Machine, Multiple Linear Perceptron, and YOLO v5; (ii) Unsupervised Learning: Auto Encoders, CAMP-BD, and Restricted Boltzmann Machine [8,17,22,23].

2.2. Cyber Security

Cyber security is constantly changing as the research environment changes rapidly. The cyber security community recognizes that cyber threats cannot be totally eliminated [27]. Therefore, research and technology development is essential to reduce the harmful impacts of cyber-attacks [28]. Research has sought a more proactive approach to preventing or mitigating security incidents before they cause damage in cyberspace. Cyber security threats are growing exponentially, becoming one of the main challenges for companies, due to the disruptive concepts of digital transformation present in the Industry 4.0 ecosystem [29]. Cyber security makes use of various measures, methods, and means to ensure that systems are protected against threats and vulnerabilities. Cyberattacks aim to gain access to connected services, resources, or systems in an attempt to compromise their confidentiality, integrity, and availability [30,31]. To increase the level of cyber security, intelligent methods for cyber defense must be developed to cope with the diversity and dynamics of attacks [9]. Cyber security has evolved over the years from a technical domain focused on network security to an issue of global concern. It is a topic that is becoming increasingly important on the agenda of business leaders [32]. Proactively addressing AI-based security issues is a key factor for an industrial environment with smart factories, autonomous systems, CPS, IoT, cloud computing, and big data [33]. In this sense, AI has the potential to automatically provide significant cyber security insights without human interaction. AI and ML are potentially transformative tools for cyber security and information sharing in cyberspace [34].

2.3. Industry 4.0

Industry 4.0, a term that originated in Germany in 2011, is a product of the information technology age. Technological development paves the way for intelligent factories with machines based on automated and digitized manufacturing systems [35]. These systems comprise computer network technologies and physical processes that enable the interconnection of the physical and technological environment and enable data processing through technologies such as the Internet [36]. The incorporation of digitization into industrial activity, integrating physical and virtual components, is a characteristic of Industry 4.0. This integration allows greater data capture, transport, storage, and analysis. Connected products, machines, and equipment became sources of data and information to support decision-making. The main industrialized countries have focused on the development of Industry 4.0, as a strategic instrument of industrial policy to increase their competitiveness [37]. Intelligent manufacturing processes use AI in automation systems for machine interaction. Intelligent automation platforms play a key role in obtaining, processing, and interpreting data generated in industrial production [38]. AI provides information to track all activities in the manufacturing process. It makes it possible to improve management to increase or decrease production, considering demand, aiming to reduce downtime to ensure constant efficiency of the production line [39]. While technological advancement is a competitive differentiator, factors such as smart production, smart maintenance, smart logistics, CPS connectivity, machine-to-machine variations, and production data quality demand actions with greater cyber security control in the Industry 4.0 ecosystem [35,40,41].

2.4. Cyber-Physical Systems

Cyber-Physical Systems are one of the most significant advances in the development of computer science [42]. In CPS there is a combination of networked physical processes integrated with cybernetic components, sensors, and actuators, which interact in a process monitoring cycle, providing information for decision-making in the production line [43]. Industry 4.0 seeks to create smart factories where CPS operations are monitored, controlled, coordinated, and integrated by a computing and communication core. The human-machine and machine-to-machine interactions are essential concepts in the context of smart manufacturing. Such production makes use of technologies for flexible, intelligent, and econfigurable manufacturing according to market dynamics [1]. CPS, considering aiming at individual process analysis and monitoring [44]. With the exponential growth of CPS, new cyber security challenges have emerged. The exploitation of vulnerabilities in integrated and connected cyber-physical systems, due to technological evolution, demands technical detection measures of the application, transmission, and perception layers of CPS [45]. The focus of CPS security has shifted from computer risk assessment to risk in the computational network, in which there is the presence of embedded systems with sensors, actuators, and information system processing, in conjunction with a communication layer [37]. The increasing use of connected technologies makes the manufacturing system vulnerable to cyber risks [41]. Cyber security for CPS is attracting interest from academia and industry, though it is problematic because it benefits both defensive and offensive sides [46]. Even though companies are investing resources to develop cyber defense applications, the number of cyber-attacks has increased in quantity and complexity with the application of AI.

3. Methodology

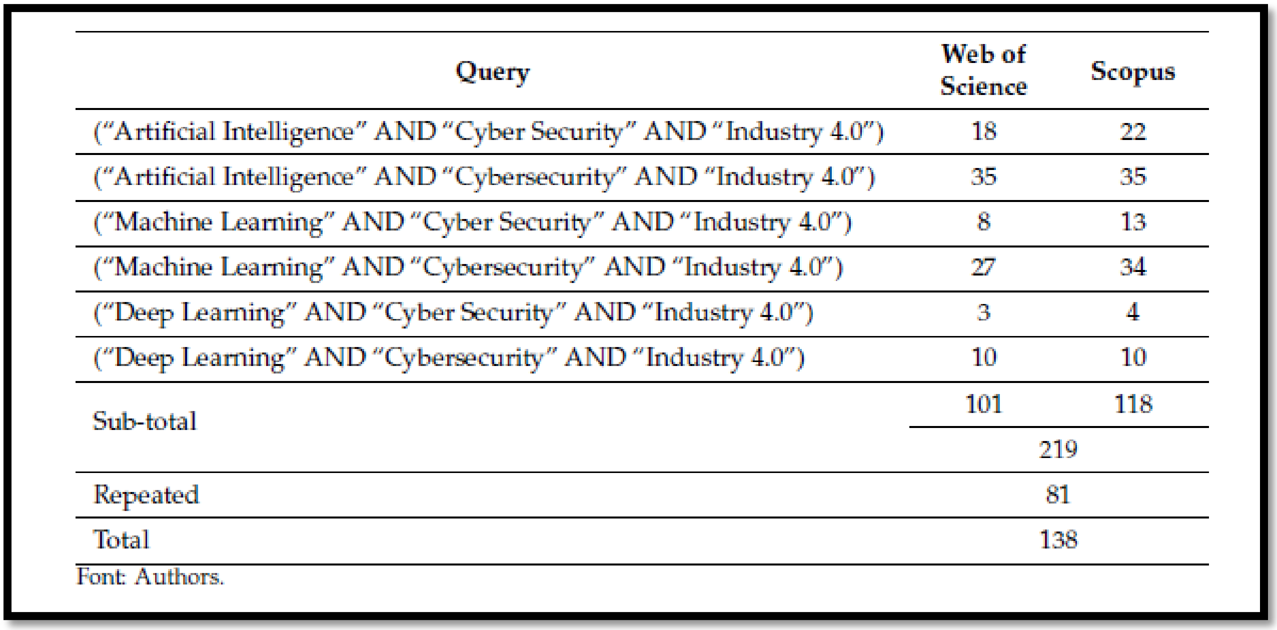
In this paper, a four-step methodology was developed to identify existing studies in the literature that address Artificial Intelligence-based cyber-attacks. In addition, relevant information on the impact of attacks using AI is extracted to provide insights for structuring defense measures. The collection source was the Web of Science and Scopus database, covering the period between 2015 and 2022. The database allows for retrieving a greater diversification of relevant metadata to the research. According to a systematic approach, the process of reviewing the literature was based on searching the following keywords: Artificial Intelligence,Machine Learning, Deep Learning, Cyber Security, Cybersecurity, and Industry 4.0. Although the literature review is not exhaustive, the method provides a comprehensive overview of the research topic in the literature.

Steps of the Search Process

These databases, Web of Science and Scopus, allow retrieving a greater diversification of relevant metadata to the research. In theWeb of Science database with the field “TS = Topic” and the Scopus database with the field “TITLE-ABS”. These tags combine fields that search document titles, abstracts, and keywords. The steps are described in the following:

Step 1—Identification: The keywords “Artificial Intelligence”, “Machine Learning” and “Deep Learning” were combined with “Cyber Security”, Cyber security”, and “Industry 4.0” in the advanced searches of the databases. The results of the searches are presented in Table 1.

Table 1. Search results by Queries



Query	Web of Science	Scopus
("Artificial Intelligence" AND "Cyber Security" AND "Industry 4.0")	18	22
("Artificial Intelligence" AND "Cybersecurity" AND "Industry 4.0")	35	35
("Machine Learning" AND "Cyber Security" AND "Industry 4.0")	8	13
("Machine Learning" AND "Cybersecurity" AND "Industry 4.0")	27	34
("Deep Learning" AND "Cyber Security" AND "Industry 4.0")	3	4
("Deep Learning" AND "Cybersecurity" AND "Industry 4.0")	10	10
Sub-total	101	118
	219	
Repeated	81	
Total	138	

Font: Authors.

Step 2—Screening: A filter excludes repeated publications. From a total of 219 publications, 81 repeated publications are identified, leaving a residual of 138 publications.

Step 3—Eligibility: A critical analysis evaluates the 138 selected publications. The goal is to filter out the studies that address the use of AI for both defense and cyber-attacks in the Industry 4.0 environment. In this step, 45 articles are identified after a filter is applied to exclude some selected document types: conference papers, proceeding papers, review articles, books and chapters, early access, editorial material, show surveys, and not published in English. Altogether 93 documents are excluded from the search.

Step 4—Included: A critical reading of the material identified in step 3 is performed, considering the challenges and issues related to AI applied for cyber security in the context of Industry 4.0. After that, more than 18 studies were excluded, because they did not meet this criterion. An overview of the individual steps and the associated number of studies is given in Figure 1 with the Prisma Flow diagram describing the literature search and the selection of eligible studies [47]. The keywords used in the articles are shown in Figure 2, while Figure 3 presents quantitative data on citations and publications per year. The list of the 27 selected articles is presented in Table 2. The next section presents an analysis of the selected studies.

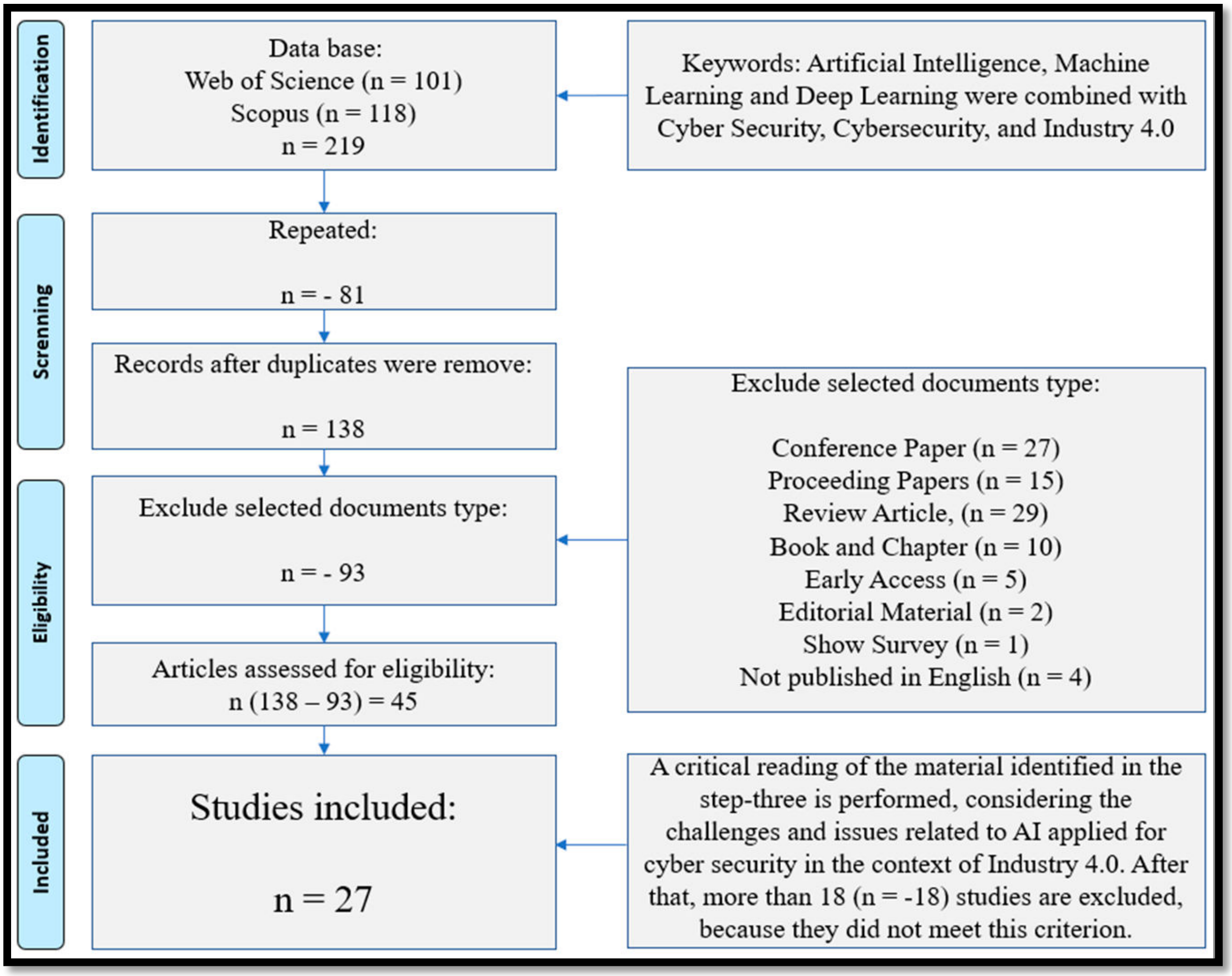

Identification
Data base:
Web of Science (n = 101)
Scopus (n = 118)
n = 219
Keywords: Artificial Intelligence, Machine Learning and Deep Learning were combined with Cyber Security, Cybersecurity, and Industry 4.0
Screnning
Repeated:
n = - 81
Records after duplicates were remove:
n = 138
Eligibility
Exclude selected documents type:
n = - 93
Exclude selected documents type:
Conference Paper (n = 27)
Proceeding Papers (n = 15)
Review Article, (n = 29)
Book and Chapter (n = 10)
Early Access (n = 5)
Editorial Material (n = 2)
Show Survey (n = 1)
Not published in English (n = 4)
Articles assessed for eligibility:
n (138 – 93) = 45
Included
Studies included:
n = 27
A critical reading of the material identified in the step-three is performed, considering the challenges and issues related to AI applied for cyber security in the context of Industry 4.0. After that, more than 18 (n = -18) studies are excluded, because they did not meet this criterion.

Figure 1. Prisma Flow

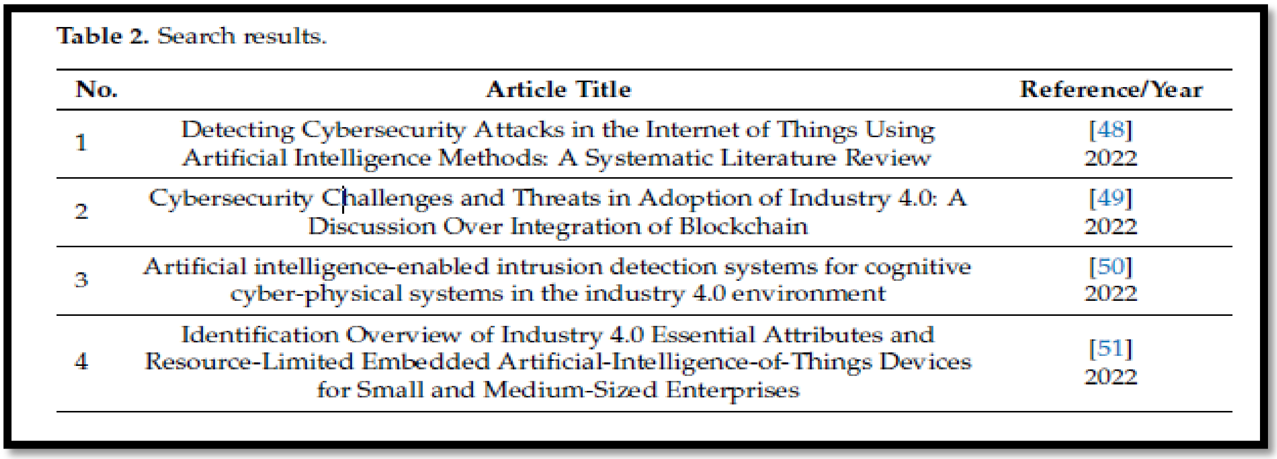


Table 2. Search results.

No.	Article Title	Reference/Year
1	Detecting Cybersecurity Attacks in the Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review	[48] 2022
2	Cybersecurity Challenges and Threats in Adoption of Industry 4.0: A Discussion Over Integration of Blockchain	[49] 2022
3	Artificial intelligence-enabled intrusion detection systems for cognitive cyber-physical systems in the industry 4.0 environment	[50] 2022
4	Identification Overview of Industry 4.0 Essential Attributes and Resource-Limited Embedded Artificial-Intelligence-of-Things Devices for Small and Medium-Sized Enterprises	[51] 2022

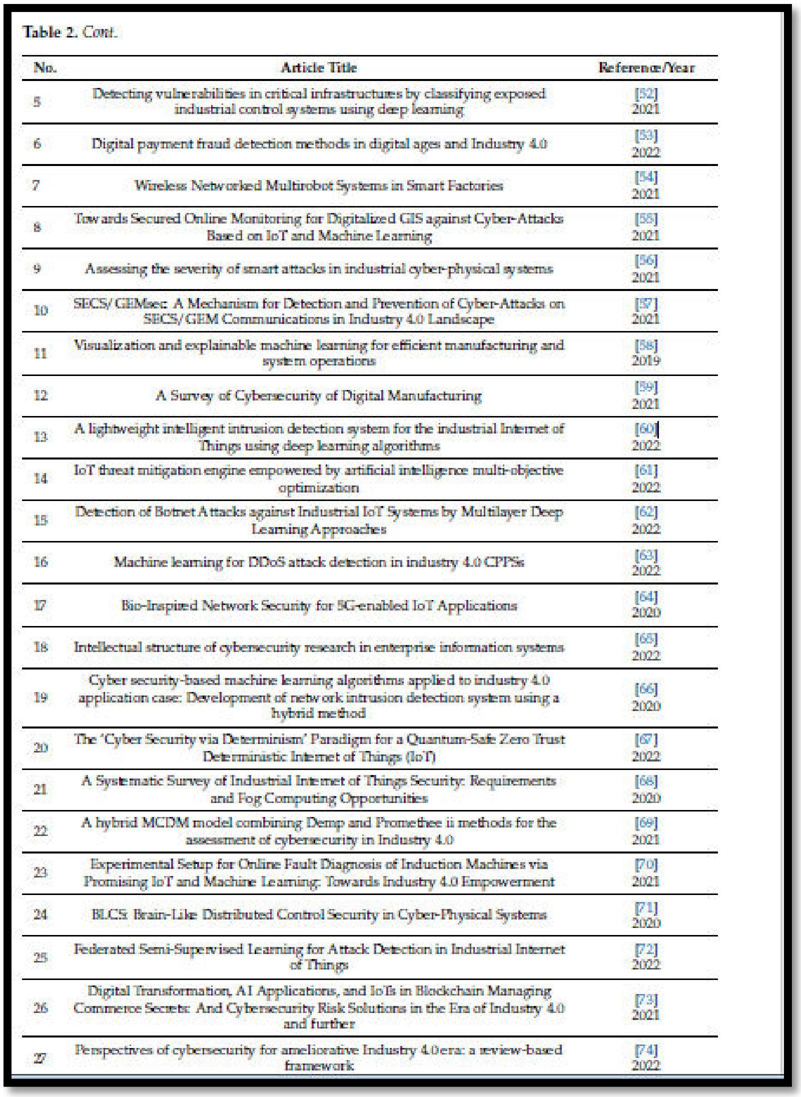


Table 2. *Cont.*

No.	Article Title	Reference/Year
5	Detecting vulnerabilities in critical infrastructures by classifying exposed industrial control systems using deep learning	[52] 2021
6	Digital payment fraud detection methods in digital ages and Industry 4.0	[53] 2022
7	Wireless Networked Multirobot Systems in Smart Factories	[54] 2021
8	Towards Secured Online Monitoring for Digitalized GIS against Cyber-Attacks Based on IoT and Machine Learning	[55] 2021
9	Assessing the severity of smart attacks in industrial cyber-physical systems	[56] 2021
10	SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape	[57] 2021
11	Visualization and explainable machine learning for efficient manufacturing and system operations	[58] 2019
12	A Survey of Cybersecurity of Digital Manufacturing	[59] 2021
13	A lightweight intelligent intrusion detection system for the industrial Internet of Things using deep learning algorithms	[60] 2022
14	IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization	[61] 2022
15	Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches	[62] 2022
16	Machine learning for DDoS attack detection in industry 4.0 CPPSs	[63] 2022
17	Bio-Inspired Network Security for 5G-enabled IoT Applications	[64] 2020
18	Intellectual structure of cybersecurity research in enterprise information systems	[65] 2022
19	Cyber security-based machine learning algorithms applied to industry 4.0 application case: Development of network intrusion detection system using a hybrid method	[66] 2020
20	The 'Cyber Security via Determinism' Paradigm for a Quantum-Safe Zero Trust Deterministic Internet of Things (IoT)	[67] 2022
21	A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities	[68] 2020
22	A hybrid MCDM model combining Demp and Promethee ii methods for the assessment of cybersecurity in Industry 4.0	[69] 2021
23	Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment	[70] 2021
24	BLCS: Brain-Like Distributed Control Security in Cyber-Physical Systems	[71] 2020
25	Federated Semi-Supervised Learning for Attack Detection in Industrial Internet of Things	[72] 2022
26	Digital Transformation, AI Applications, and IoTs in Blockchain Managing Commerce Secrets: And Cybersecurity Risk Solutions in the Era of Industry 4.0 and further	[73] 2021
27	Perspectives of cybersecurity for ameliorative Industry 4.0 era: a review-based framework	[74] 2022

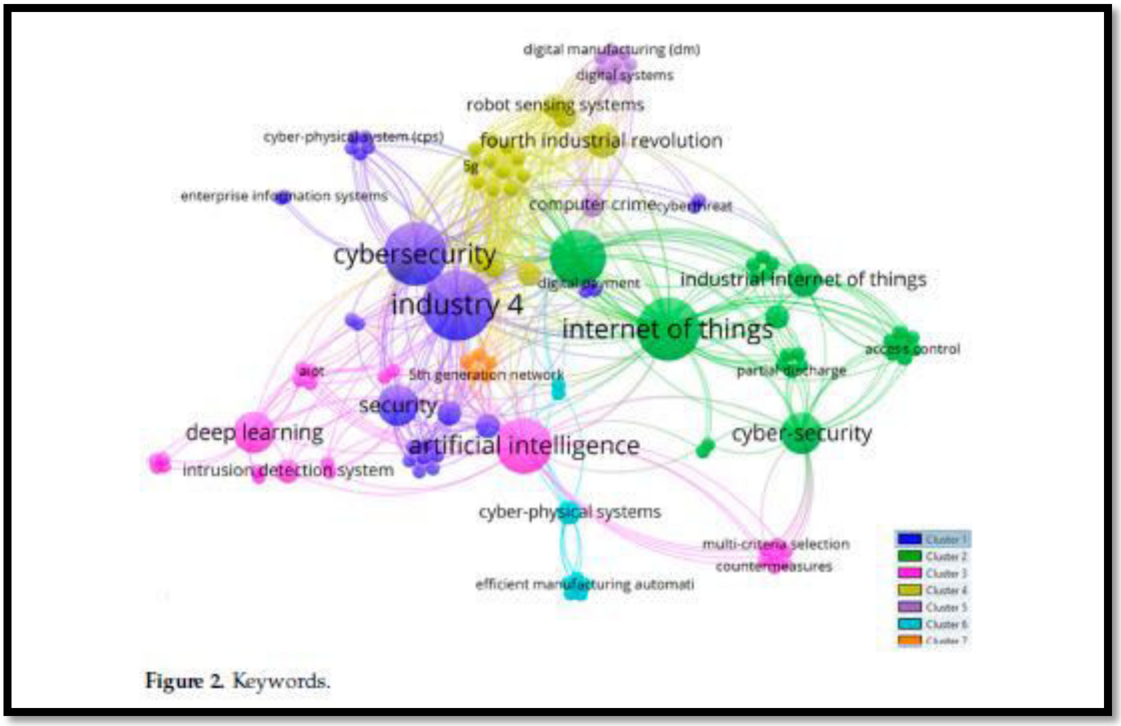


Figure 2. Keywords.

Table 2. Search results.

Figure 2 shows the representativeness of the identified keywords separated into seven clusters. An analysis of the representativeness of the keywords used in the publications was performed. Keywords are defined by authors to attract readers, with general, intermediate, or specific terms about the research. The larger circle reflects the representativeness of the keywords in a cluster. Cluster 1 (blue) has the highest representativeness. Followed by cluster 2 (green) and cluster 3 (purple).

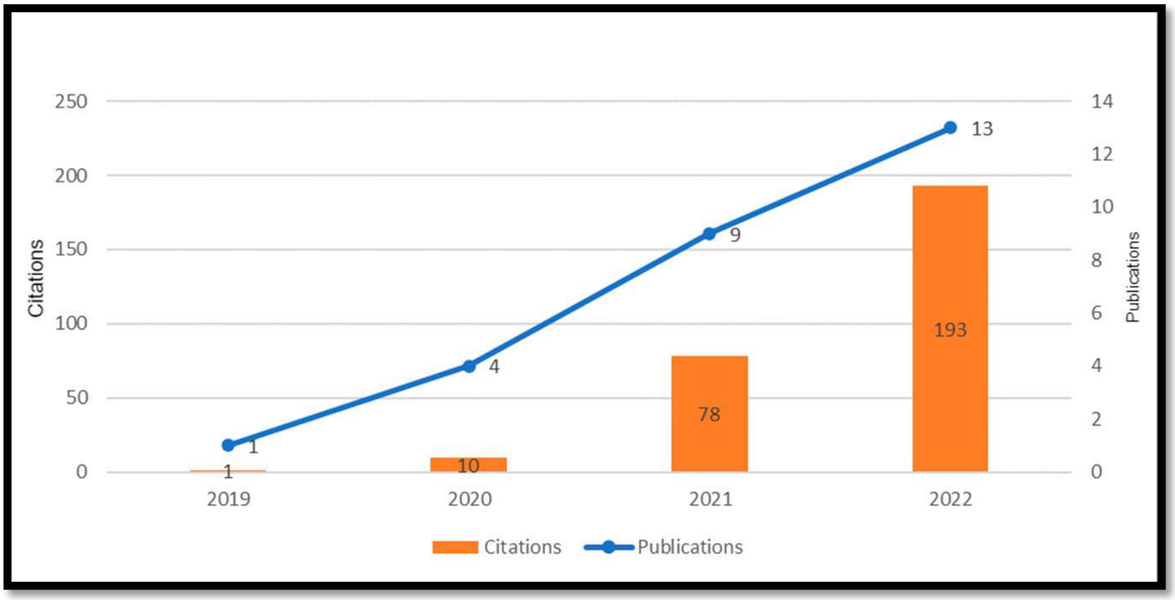


Figure 3. Times Cited and Publications Over Time

4. RelatedWorks

This section discusses the applications of AI in the cyber security domain adopted by the authors of the selected studies, shown in Table 2, considering their applicability in Industry 4.0. Abdullahi et al. [48] present a systematic literature review about using AI methods to detect cyber security attacks in IoT devices and networks. A systematic review identified 80 studies published between 2016 and 2021, with a focus on exploring ML and DL techniques used in IoT security. The research presents an AI roadmap view to establish strategies, categories, and types of detection, attacks, and threats in the IoT environment.

Ahmar et al. [49] show the importance of cyber security in the fourth industrial revolution with a focus on vulnerabilities found in IoT appliances under Industry 4.0. The authors address the use of blockchain technology to offer solutions to cyber security issues related to vulnerabilities, and threats to IoT in Industry 4.0 ecosystem and discuss and highlight potential impacts correlated with security, and data privacy. Alohali et al. [50] propose a new AI-enabled multimodel fusion-based intrusion for the detection of systems for cognitive CPS in the Industry 4.0 environment. This model uses Recurrent Neural Network, bi-directional long short-term memory, and Deep Belief Network. The model simulation analysis erformed better than the latest state-of-the-art techniques published in the academic literature. Barton et al. [51] address in their research attributes for small and medium enterprises (SMEs) to develop strategic plans for the digitization requirements, with a focus on the development of AI as part of the implementation of the IoT pillar. AI is likely to have a huge impact to improve manufacturing. According to the authors, achieving the best possible results will depend on harnessing the full potential of AI in SMEs. Blanco-Medina et al. [52] present a pipeline based on existing DL models to solve issues related to cyber security. This pipeline proposes to classify screenshots of industrial control panels into the following categories: (i) internet technologies; and (ii) operation technologies. The authors compare the use of transfer learning and fine-tuning in a pretrained dataset to identify the best Convolutional Neural Networks architecture to classify the screenshots related to the categories. Chang et al. [53] show an efficient and stable model for fraud detection platforms to be adapted for Industry 4.0. Fraud detection is a relevant part of cyber security in the Industry 4.0 era. This study proposes and evaluates ML models to detect fraudulent transactions in the Industry 4.0 ecosystem. The analysis included classification and approaches to detect vulnerabilities in digital financial transactions. Chen et al. [54] discuss the challenges presented in smart manufacturing based on AI and communication technology. Smart manufacturing has holistically integrated wireless networks, cloud computing, AI, and automation. This complex system engineering from wireless networks lays down a new perspective for the cyber security of smart factories. The authors present highlights of the technological opportunities related to AI omputing, wireless networks, control, and robotic engineering in the smart factories context. Elsisi et al. [55] present new online monitoring and tracking for gas-insulated switchgear (GIS) defects based on IoT architecture and ML. The IoT architecture is based on the concept of CPS applied in the Industry 4.0 ecosystem. Advanced ML techniques are used to detect cyber-attacks in different test scenarios on the Internet network. These techniques provide decision-makers with reliable data on the status of the GIS. Khaled et al. [56] highlight the importance of cyber security infrastructure and discuss how to evaluate, prevent, and mitigate cyber-attacks in industrial cyber-physical systems (ICPS). This study presents attacks generated by ML based on multiple criteria to show the application of the proposed solution. Therefore, the authors analyze and evaluate ICPS security in two real use cases. Laghari et al. [57] propose a digital signature-based security mechanism that offers authentication, integrity, and protection against cyber-attacks. The results identified in this research show Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) is an efficient communications mechanism to protect industrial equipment against untrusted entities from establishing communication. In addition, SECS/GEM communications demonstrated the capacity to protect industrial equipment against denialof- service attacks, replay attacks, and false data injection attacks. Le et al. [58] present a framework for ML with real-time predictive analytics to protect manufacturing automation networks and complex system operations from cyber-attacks. The research approach is based on multivariate time series characterizations and real-time predictive analytics to project threats and estimate the time to detect cyber-attacks, thereby identifying the time of failure.

Mahesh et al. [59] address the digital manufacturing (DM) paradigm that can increase productivity and improve quality in the context of Industry 4.0. However, DM also poses cyber security risks that need to be mitigated. This study analyzes the risks, assesses the impacts on production, and identifies perspectives to protect DM. Mendonça et al. [60] present a methodology to detect cyber-attacks, through an application of a DL model. The research results demonstrate that the proposed model was more efficient when compared to other ML models in the market in a real cyber security scenario for IoT quipment applied to Industry 4.0. Mpatziakas et al. [61] present an automatic mechanism to identify mitigation actions to implement cyber security countermeasures to protect IoT networks. This mechanism uses AI based on a Deep Neural Architecture called Pointer Networks to improve the value of cyber security KPIs and interact with programmable networks to define strategies to mitigate risks to IoT networks. Mudassir et al. [62] propose DL models for the classification of malicious packets with origin in Internet of Things (IoT) devices. These devices and their networks require cyber security, data privacy, and information integrity to protect CPS. This study presents DL models such as Artificial Neural Networks that can be used to classify IoT malware attacks. Saghezchi et al. [63] approach ML to identify non-standard behavior on the networks aiming to develop data-driven models to detect DDoS attacks on CPS. The authors investigate different supervised, unsupervised, and semi-supervised algorithms to assess their performance through extensive simulations. In this study, supervised algorithms (e.g., Decision Trees) show better performance than unsupervised and semi-supervised algorithms. Saleem et al. [64] analyze the security of 5G-enabled IoT applications to list vulnerabilities and equirements in wireless devices. The 5G will further boost IoT systems; the expansion of the use of this technology increases the surface for cyber-attacks. The complexity of massive scale deployment of IoT makes the challenges of protecting critical applications, a relevant area of research. Singh et al. [65] present core themes of cyber security research in enterprise information systems: (i) AI in cyber security; (ii) grids, networks, and platform security; (iii) algorithms and methods; (iv) optimization and modelling; and (v) cyber security management. This research discusses several studies related to security in enterprise information systems. Tamy et al. [66] discuss the complex process to implement Industry 4.0 related to production, supply chain, engineering, and information systems. This complexity requires a cyber security strategy to protect the industrial environment. The authors present a cyber security strategy based on ML applied in Industry 4.0. For that, they used threat management based on ML algorithms to develop an accurate system to detect network intrusion. Szymanski et al. [67] present the use of a centralized software-defined networking (SDN) control plane to configure deterministic traffic flow that can strengthen cyber security to the next-generation IoT. In this context, deterministic traffic flows receive strict Qualityof-Service (QoS) guarantees. Deterministic cyber security can identify unauthorized packets targeting a deterministic virtual private network. Tange et al. [68] show a systematic review with a focus on the security requirements of the IoT device. An IoT device creates opportunities for industries to connect devices, and these opportunities not only implement but also expand the possibilities for cybercriminals' actions using the interconnectivity of network equipment in combination with cloud computing and AI technologies. IoT security represents one key factor that explains why to adopt the widespread use of IoT devices. Torbacki et al. [69] propose a cyber security structure divided into seven dimensions: (i) trust services; (ii) encryption; (iii) network security; (iv) application security; (v) endpoint security; (vi) access control; and (vii) cyber-attacks, with twenty criteria and three groups: (a) operational; (b) technological; and (c) organizational. These dimensions, criteria, and groups, compose a cyber security framework with a ranking of security criteria with guidelines for the process of implementing cyber security solutions.

Tran et al. [70] propose a new architecture based on ML techniques. The advanced ML echniques used in this research allowed online monitoring on the panel of the proposed IoT platform, in order to visualize failures in the status of the induction motor, as well as cyberattacks on communication networks. The Random Forest, known as an effective method, to identify failure problems, shows excellent accuracy in the results to identify induction motor failures due to equipment vibration, when compared to other ML algorithms. Yang et al. [71] present a brain-like distributed control security (BLCS) in fog radio and optical networks (F–RON) for CPS. Cyber security is a challenge in the CPS scenario because in this context there is a trade-off between security control and privacy environment in F–RON. BLCS adopts a computing mechanism to anonymously distribute control without disclosing private information related to network analysis, creating a cyber security and privacy control. Aouedi et al. [72] propose a federated semi-supervised learning scheme, which uses unlabeled and labeled data in a federated way, to detect intrusion and attacks on the Industry 4.0 ecosystem. The proposed model has been evaluated for capacity to identify the attacks on the network traffic. The use of unlabeled data in the training process can improve the performance of the learned model, according to the research results.Trung et al. [73] analyze findings on the connection between blockchain technology, AI, and IoT. Considering this analysis, the authors propose solutions to mitigate cyber security risks, based on policies to implement security mechanisms in the era of Industry 4.0. Haleem et al. [74] discuss technologies used to improve the cyber security process in Industry 4.0 context. These technologies are AI, cloud computing, IoT, and robots to support the interconnection of CPS, which connects the physical and digital worlds by collecting digital data from physical objects and processes, present in the Industry 4.0 ecosystem. These interconnections demand cyber security actions to protect this environment.

5. Analysis and Results

In this section, different types of cyber-attacks, algorithms, methods, advantages, and disadvantages of AI solutions in the context of the Industry 4.0 ecosystem are analyzed.

5.1. Steps of the Search Process

While Industry 4.0 provides a framework for integrating CPS for smart, flexible, and adaptive manufacturing, it carries with it concerns about cyber security. Indeed, the growth of IoT devices and CPS in networked production increases the surface of attacks on critical systems and infrastructures with damaging impacts on production processes [7,48]. In this research, different types of cyber-attacks presented by the authors of the selected studies are analyzed with their respective references:

5.2. Countermeasures for Cyber Defense

The actions for cyber defense against internal and external threats can be implemented with security controls, known as defense countermeasures. ICS security has three high-level approaches: (i) isolate the plant network from the administrative network using firewalls and demilitarized zone (DMZ); (ii) implement defense in profundity, with multiple layers for perimeter protection across the network; and (iii) structured network access control to isolate internal threats and remote users in a segmented DMZ [48]. However, to keep up with the dynamics and complexity of attacks it is necessary to update security patches throughout the network on a regular basis. Countermeasures play an essential role in cyber defense. Proactive measures for AI-based threat detection by adopting ML mechanisms are essential to ensure greater accuracy in the timely detection of cyber-attacks [63].

5.3. ML and DL Applied in Industry

The following presents an analysis of the ML and DL techniques identified in the studies listed in Table 2, used for cyber security. To this end, concepts and references are provided for each technique. In this paper, the cyber security attack detection based on ML and DL methods is categorized into six classes: Convolutional Neural Network (CNN), Deep Autoencoder (DAE), Deep Belief Network (DBN), Recurrent Neural Network (RNN), Generative Adversarial Network (GAN), and Deep Reinforcement Learning (DRL).

5.4. Advantages and Disadvantages of AI for Cyber Security

When discussing the advantages of intelligence in cyber security, it is necessary to understand the diversity of the different cyber-attacks that exist, as already mentioned in Section 5.1. Cyber security experts work to develop algorithms to analyze and identify new and emerging cyber threats. As AI systems are further developed, actions to deceive AI techniques emerge in cyberspace [67]. By applying AI techniques to protect the industrial ecosystem, systems will continue to learn from attempted attacks. As a result, systems will benefit from predictive analytics to deal with the complexity of cyber-attacks. AI aids in the monitoring to identify patterns of normal and abnormal activity with malicious characteristics. Monitoring makes it possible to mitigate and localize attacks [73]. AI technologies do not guarantee absolute security for industrial environments. These technologies have also several ethical concerns in their implementation, such as the lack of a moral code for machines. Regarding decision-making that may have moral impacts, AI may not have the ability to recognize these impacts, so the inability to sense and make decisions considering moral issues is a challenge [57].

6. Conclusions

Cyber-attacks are constantly growing and changing, improving their malicious performance with the application of AI technologies. The malicious use of AI has transformed the landscape of potential threats in the cyber environment with technological advancement. Technological evolution demands up-to-date studies to defend against AI being used as a malicious tool by cyber criminals. Networked manufacturing devices connected via the Internet provide a greater surface for cyber-attacks. Attackers exploit this interconnectivity to amplify their actions. This literature analysis addresses the types of cyber-attacks, defense countermeasures, application of ML and DL for cyber security in Industry 4.0, advantages, and disadvantages of using AI for security. The studies reviewed in this research also address technologies for cyber-attack detection, however, these approaches have not been included as part of the current strategic planning of organizations in the Industry 4.0 ecosystem. This is a relevant fact that demonstrates a limitation in the selected articles to deal with the strategic issues of cyber security. Future research may use this present work as a reference to address AI-based cyber security issues in the context of Industry 4.0. Our approach in this research allows the improvement of the state of the art of this study, generating insights for the research community to structure defenses against potential cyber threats. As future work in this area, there is a need for constant updating of the requirements to implement cyber security actions, arising from the cybernetic technological evolution applied for both defense and attack in the context of the Industry 4.0 ecosystem.

References

- Zhong, R.Y.; Xu, X.; Klotz, E.; Newman, S.T. Intelligent Manufacturing in the Context of Industry 4.0: A Review. Engineering **2017**, 3, 616–630. [CrossRef]
- Schumacher, A.; Sihn, W.; Erol, S. Automation, digitization and digitalization and their implications for manufacturing processes. In Innovation and Sustainability Conference Bukarest; Elsevier: Amsterdam, The Netherlands, 2016; pp. 1–5.
- Matt, D.T.; Modrák, V.; Zsifkovits, H. Industry 4.0 for SMEs: Challenges, Opportunities and Requirements; Springer: Cham, Switzerland, 2020.
- Wu, D.; Ren, A.; Zhang,W.; Fan, F.; Liu, P.; Fu, X.; Terpenny, J. Cybersecurity for digital manufacturing. J. Manuf. Syst. **2018**, 48, 3–12. [CrossRef]
- 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]
- Kaloudi, N.; Jingyue, L.I. The AI-based cyber threat landscape: A survey. ACM Comput. Surv. **2020**, 53, 20. [CrossRef] Matsuda,W.; Fujimoto, M.; Aoyama, T.; Mitsunaga, T. Cyber Security Risk Assessment on

Industry 4.0 using ICS testbed with AI and Cloud. In Proceedings of the 2019 IEEE Conference on Application, Information and Network Security, AINS, Penang, Malaysia, 19–21 November 2019; pp. 54–59.

- 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]
- Li, J. hua: Cyber security meets artificial intelligence: A survey. Front. Inf. Technol. Electron. Eng. **2018**, 19, 1462–1474. [CrossRef]
- Ji, H.; Alfarraj, O.; Tolba, A. Artificial Intelligence-Empowered Edge of Vehicles: Architecture, Enabling Technologies, and Applications. IEEE Access **2020**, 8, 61020–61034. [CrossRef]
- Trifonov, R.; Nakov, O.; Mladenov, V. Artificial intelligence in cyber threats intelligence. In Proceedings of the 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), Plaine Magnien, Mauritius, 6–7 December 2018; pp. 1–4.
- Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitzoff, T.; Filar, B.; et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. arXiv **2018**, arXiv:1802.07228.
- Monostori, L.; Kádár, B.; Bauernhansl, T.; Kondoh, S.; Kumara, S.; Reinhart, G.; Sauer, O.; Schuh, G.; Sihn, W.; Ueda, K. Cyber-physical systems in manufacturing. CIRP Ann. **2016**, 65, 621–641. [CrossRef]
- Novikov, I. How AI can be applied to cyberattacks. Retrieved Novemb. **2018**, 25, 2019.
- Mubarakova, S.R.; Amanzholova, S.T.; Uskenbayeva, R.K. Using Machine Learning Methods in Cybersecurity. Eurasian J. Math. Comput. Appl. **2022**, 10, 69–78. [CrossRef]
- Batta, M. Machine Learning Algorithms—A Review. Int. J. Sci. Res. **2020**, 9, 381. [CrossRef]
- Nguyen, T.T.; Reddi, V.J. Deep Reinforcement Learning for Cyber Security. IEEE Trans. Neural Netw. Learn. Syst. **2021**, 1–17. [CrossRef] [PubMed]
- Wuest, T.;Weimer, D.; Irgens, C.; Thoben, K.D. Machine learning in manufacturing: Advantages, challenges, and applications. Prod. Manuf. Res. **2016**, 4, 23–45. [CrossRef]
- Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access **2018**, 6, 35365–35381. [CrossRef]
- Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A survey of deep learning methods for cyber security. Information **2019**, 10, 122. [CrossRef]
- 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]
- Alkahtani, H.; Aldhyani, T.H.H. Artificial Intelligence Algorithms for Malware Detection in Android-Operated Mobile Devices. Sensors **2022**, 22, 2268. [CrossRef]
- Kotsiopoulos, T.; Sarigiannidis, P.; Ioannidis, D.; Tzovaras, D. Machine Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm. Comput. Sci. Rev. **2021**, 40, 100341. [CrossRef]
- Avdoshin, S.M.; Lazarenko, A.B.; Chichileva, N.I.; Naumov, P.A.; Klyucharev, P.G. Machine Learning Use Cases in Cybersecurity. Proc. Inst. Syst. Program. RAS **2019**, 31, 191–202. [CrossRef]
- Wang, J.; Ma, Y.; Zhang, L.; Gao, R.X.; Wu, D. Deep learning for smart manufacturing: Methods and applications. J. Manuf. Syst. **2018**, 48, 144–156. [CrossRef]
- Huang, T.H.; De Kao, H.Y. R2-D2: ColoR-inspired Convolutional NeuRal Network (CNN)-based AndroiD Malware Detections.

- In Proceedings of the 2018 IEEE International Conference on Big Data, Seattle,WA, USA, 10–13 December 2018; pp. 2633–2642. [CrossRef]
- Husák, M.; Bartoš, V.; Sokol, P.; Gajdoš, A. Predictive methods in cyber defense: Current experience and research challenges.
- Future Gener. Comput. Syst. **2021**, 115, 517–530. [CrossRef] Guan, Y.; Ge, X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Trans. Signal Inf. Process. Netw. **2017**, 4, 48–59. [CrossRef]
- Schumacher, A.; Erol, S.; Sihn, W. A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises. Procedia CIRP **2016**, 52, 161–166. [CrossRef]