electronics

MDPI

Review

AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes

Grzegorz Czeczot, Izabela Rojek *, Dariusz Mikołajewski and Belco Sangho

Faculty of Computer Science, Kazimierz Wielki University, 85-064 Bydgoszcz, Poland; dariusz.mikolajewski@ukw.edu.pl (D.M.)
* Correspondence: irojek@ukw.edu.pl

Abstract: If we look at the chronology of transitions between successive stages of industrialization, it is impossible not to notice a significant acceleration. There were 100 years between the industrial revolutions from 2.0 to 3.0, and only half a century passed from the conventional 3.0 to 4.0. Assuming that progress will inevitably continue to accelerate, and given that 2011 is the set date for the start of the fourth industrial revolution, we can expect Industry 5.0 by 2035. In recent years, Industrial Internet of Things (IIoT) applications proliferated, which include multiple network elements connected by wired and wireless communication technologies, as well as sensors and actuators placed in strategic locations. The significant pace of development of the industry of advantages in predicting threats to infrastructure will be related to the speed of analyzing the huge amount of data on threats collected not locally, but globally. This article sheds light on the potential role of artificial intelligence (AI) techniques, including machine learning (ML) and deep learning (DL), to significantly impact IIoT cyber threat prediction in Industry 5.0.

Keywords: artificial intelligence; Internet of Things; cybersecurity; Industry 4.0; Industry 5.0; deep learning (DL); Industrial Internet of Things (IIoT); machine learning (ML); edge computing

Citation: Czeczot, G.; Rojek, I.; Mikołajewski, D.; Sangho, B. AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes. *Electronics* **2023**, *12*, 3800. https://doi.org/10.3390/electronics12183800

Academic Editors: Nadia Kanwal, Yuhang Ye, Brian Lee and Mohammad Samar Ansari

Received: 30 July 2023
Revised: 3 September 2023
Accepted: 6 September 2023
Published: 8 September 2023

1. Introduction

Industry 5.0 is likely to surprise us in terms of the level of cybersecurity solutions required. In the next phase of industrialization, it should be necessary to anticipate technological trends and try to assess the adaptation of one's own organization to the inevitable future. It can be assumed that in the case of Industry 4.0, predicting the future was not properly carried out. As a result, Industry 4.0 was not properly consumed by companies. On the one hand, an attempt was made to harness the technological revolution through simple evolutionary activities, on the other hand, the multitude of technologies behind Industry 4.0, whose adaptation to the existing organizational framework consumes huge resources of enterprises, creates an unsatisfactory pace of change. The Industrial Internet of Things, intelligent sensors, industrial robots, and three-dimensional (3D) printers are elements of the current digital transformation. Their technological maturity is undeniable. In the case of non-hardware elements, such as big data, machine learning, or artificial intelligence, it seems that we are still at the beginning of the road and every year we open new doors to new possibilities [1,2].

Properly planned and managed, Industry 4.0 should be able to manage a multitude of systems supporting individual areas: manufacturing execution systems (MES), supervisory control and data acquisition (SCADA), supply chain management (SCM), customer relationship management (CRM), supplier relationship management (SRM), transportation management system (TMS), etc. Each new system adds another layer of complexity to data exchange. A comprehensive enterprise management software that should integrate all these aspects and facilitate management is enterprise resources planning (ERP). ERP systems are currently only used for materials management and general reporting. The aggregation

and processing of data from all Industry 4.0 subsystems, as well as the collection of data from individual sensors is an extremely important process that requires careful planning and protection. The success of a well-managed company lies in the accuracy of this data, which helps in the current control of production processes, but also in the necessary future analysis of the development of these processes. In most cases, on-premise models from one of several leading vendors are still used to manage the entire business, with numerous modifications to adapt the software to the needs of the company. Today's transformation aims to standardize data exchange primarily through an application programming interface (API) that, built into applications, greatly facilitates data exchange, but does not provide a path to full integration [1–4].

The digitization of more and more aspects of industrial processes and the increasing use of automated big data collection from sensors and actuators, inference, trend analysis and AI-based future event prediction is now providing a step change in the quality of industrial production in many industries, but at the same time increasing the requirements for their reliability, including resilience to unintentional (failures) and intentional (cyber attacks). So far, the largest use of AI in Industry 4.0 is directly in manufacturing and logistics—a trend that is likely to strengthen due to the demands of global freight transport or global supply shortages in recent years [3–5].

AI systems in cybersecurity are able to replace specialists in less responsible tasks that can be automated and require speed, or serve as advisory (second opinion) systems in tasks that require a final human decision. This will not only relieve the burden on specialists, but also accelerate the defense response or increase its precision. In the case of an AI-supported attack, using AI in defense may be the only way to successfully repel it, avoiding data loss or system downtime. Self-learning AI systems can more easily and quickly isolate new types of attacks and creatively produce countermeasures mechanisms in near real-time, only to be analyzed later by specialists. In some cases, such analysis after time will be the only solution, as the time for an effective response may be too short, especially in complex systems with many distributed structures. For this reason, the areas of activity can be divided into endpoint security, network security, application security, and cloud security [6,7].

This article sheds light on the potential role of artificial intelligence (AI) techniques, including machine learning (ML) and deep learning (DL), to significantly impact IIoT cyber threat prediction in Industry 5.0.

2. Industry 5.0

In organizations such as supply networks, Industry 5.0 refers to a new level of seamless and harmonious integration between people, automation, and machines. Automation refers to the management, optimization and execution of processes and technologies. Therefore, it is necessary to define, select, and implement automation. Automation can be defined in several ways:

- Replacing or augmenting human tasks with automated tasks;
- Execution of a physical or virtual (in whole or in part) function previously performed (in whole or in part) by a human;
- A system or method in which processes are carried out automatically or are controlled by automatic automation or something similar;
- A person or animal that behaves monotonously, routinely, and without active intelligence;
- Replacing human activities with robots or intelligent machines that perform tasks or functions that are monotonous, routine, and standardized.

Increased productivity, agility, profitability, better adaptability, readiness for change, responsive work environment, and overall cost reduction are the main advantages of Industry 5.0. If the current Industry 4.0 or future Industry 5.0 wants to incorporate machine learning or artificial intelligence in the future, it will need to consider the need to process huge amounts of data from multiple sources. Managing or updating such a data structure will become an increasingly complex process [1,2,8,9].

IoT and IIoT networks are particularly vulnerable to cyber attacks. The complexity of the above solutions and their partial independence creates at the same time a greater number of attack vectors, i.e., channels that allow hackers to potentially access data or otherwise use them to attack the efficiency of the system. The vulnerability may concern the IIoT devices themselves (sensors, actuators, power supply, or monitoring/concentrating devices), as well as the networks in which they communicate, as well as mobile applications, Internet platforms and cloud databases, as well as analytical and control software coordinating the activities of lower layers. IoT systems process a lot of data that can be useful to criminals, ranging from raw data to financial or personal data, audio recordings, still and moving images, or multimodal data (technical files, operation algorithms, or ready-made analyzes using digital twins). They can be used to carry out precise phishing attacks, the target of which may be a specific person in the enterprise, for some reason considered vulnerable (also in a hidden way, e.g., has a sick family member). There are no universally recognized legal regulations or security standardization. Many of the individual devices that make up IoT networks have poor security or are not designed to connect to public networks. The consequences of attacks on IIoT systems are potentially the most costly, because every minute of production downtime translates into smooth operation and financial liquidity of the company. Sometimes, such a threat in a difficult situation of a company may be enough to extort a ransom from companies that do not want to risk losing access to electricity, transport networks, etc. Therefore, knowledge of the rules and appropriate protection in unobvious ways are the basic protection against real or imagined (bluff) threats in the area of cybersecurity, and continuous monitoring of threats and counteracting their occurrence should be the basis of every company's cybersecurity strategy. In the case of the attack itself, it may be too late to react effectively (Table 1) [10–12].

Table 1. ISO/OSI model vs. most frequent vulnerabilities.

ISO/OSI Layer	Key Vulnerability
7	Exploit
6	Phishing
5	Hijacking
4	Reconnaissance/denial of service
3	Man-in-the-middle
2	Spoofing
1	Sniffing

Higher levels of availability, integrity, scalability, confidentiality, and interoperability of IoT devices created new vulnerabilities. Current attack methods against the IIoT mainly involve attacks on the devices themselves, their hardware and/or software, communication networks, and the applications they report to. Most attacks involve a connection to a gateway and/or cloud data server [10–12].

In fact, such cloud solutions are already being offered through platform as a service (PaaS), software as a service (SaaS), and application as a service (AaaS) (Table 2). These models make it easier to control poor quality and consistency of data flowing from various platforms within the enterprise. The essence of Industry 5.0 will be to predict the future of the product, the production process, and the cost of materials. To this end, we will be supported by AI along with data collected live, and at the same time, we will draw knowledge from data collected in the past and stored in memory, probably in the cloud [13,14].

Platform as a service (PaaS) is a model of cloud computing where a third party provides users with hardware and software tools over the Internet. Typically, these tools are required for app development. Hardware and software are hosted on the infrastructure of the PaaS provider. As a result, PaaS frees developers from installing their own hardware and software to develop or launch a new application.

Table 2. IaaS, PaaS, SaaS vs. cybersecurity domains.

Cybersecurity Domain	
Client level security	SaaS
Monitoring	
Transmission medium security	
Data and storage security	PaaS
Identity and access management	
Virtual image security	IaaS
Network and perimeter security	
Physical security	

SaaS is an application delivery model where applications are hosted in the cloud and delivered over the Internet to the end user. In this model, an independent software vendor (ISV) can contract with a third-party cloud provider to host applications. Alternatively, the cloud provider may be a software provider for larger companies such as Microsoft.

AaaS is a type of service where applications are delivered over the Internet on demand and billed to the consumer on a per-use or monthly or yearly basis. AaaS applications are hosted on the server, managed by the host, and delivered remotely to the user's device, unlike traditional applications installed on devices. Since it is hosted on a server, all updates, configurations and security for this application are applied on the server and not on every endpoint. From a user and business perspective, all these attributes have huge implications.

The bolder concept of real-time data processing anywhere with access to the cloud is called data as a service (DaaS). This concept assumes that data will not only be collected from the currently hermetic enterprise, but also compared with data from outside the enterprise. Another aspect that significantly increases the probability of success is the simultaneous analysis of suppliers' inventory and even the current needs of end customers. On the other hand, when talking about the use of DaaS, the concept of master data management (MDM) should also be mentioned.

Master data management is a system acting as a central data repository. It contains all the data that the company has and supports its management. This includes technical, transactional/commercial, logistics, marketing, and multimedia data (digital assets and their metadata). All data are combined so that it is consistent and always up to date. When different systems use the same data, the data are often redundant and it is difficult to determine which data are up-to-date. Different types of data are in different formats on different systems, making it difficult to access. Sometimes it is difficult to extract data from the system and it is completed manually [13–15].

The aspect of ensuring cybersecurity of the transmitted and processed data is extremely important. The lack of susceptibility to hostile outside interference in production processes, as well as the protection of data archives from the past and those remaining in R&D departments, should be a key area of development of conscious management. Although on-premises solutions are still popular, the future lies in the use of secure cloud solutions. Large organizations with offices in many countries can secure all their data processing needs with cloud solutions. Using cloud facilities such as freely scalable storage:

- Storage of data resources;
- Computing power;
- Cyber threat prevention and response.

Not so long ago, they enabled full integration with machine learning (ML), deep learning (DL), or artificial intelligence (AI) for the analysis of historical and current data. Artificial intelligence can play a vital role in this digital transformation of business. The aforementioned multitude of data and the need to select the right data by Industry 4.0 data

experts would be too time-consuming, and the conclusions would be outdated. AI will help sift through vast amounts of data to obtain to the most important ones right now [15,16].

3. AI-Based Approaches

Traditional AI differs from the machine learning (ML) and deep learning (DL) discussed below, which are part of AI, as it replicates the way the human brain thinks, acts, and functions, often based on patterns derived from nature (Figure 1).

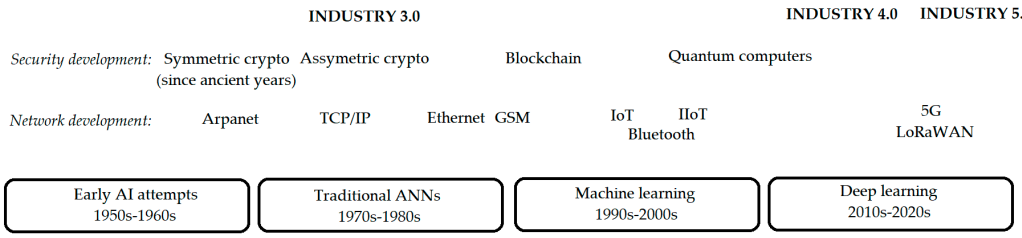

Figure 1. Shortened history of AI in cybersecurity.

Advantages of AI from a cybersecurity perspective:

- Based on data or rules;
- Self-learning and tutoring;
- Greater depth of analysis than human;
- Higher speed (up to 60 times);
- Elimination of time-consuming research tasks;
- It does not hang;
- It will always give some result;
- Better understanding of cyber threats and cyber risk levels;
- Make key decisions faster;
- Better coordination of countermeasures to a detected threat;
- Scalable enterprise-grade security available almost anywhere (cloud technologies);
- Creatively complements solutions in line with the principle of "zero trust".

The disadvantages of AI from a cybersecurity point of view:

- The need to make inferences on mobile devices;
- Societal opposition to the use of AI.

Machine learning (ML) is a form of AI that allows you to learn from data, automatically extracting rules from it, instead of explicitly programming the behavior, constraints and operating environment. The learned ML system uses the acquired and coded knowledge to make decisions in similar cases (for other data). ML approaches can be categorized as supervised, unsupervised, and reinforcement learning [17–20].

Supervised learning uses tagged datasets to train algorithms to accurately classify data or predict outcomes. The model measures accuracy and learns to minimize error. In data mining with supervised learning, we solve two main types of problems:

- Classification issues: uses an algorithm to classify data into specific classes, such as spam and regular email;
- Regression, which uses extracted data relationships to predict numeric values.

Unsupervised learning groups unlabeled datasets using discovery of patterns contained in the data without human intervention (e.g., data labeling). Once trained, these models are used to:

- Clustering, i.e., grouping unlabeled data based on their mutual similarities or differences, e.g., in image compression or segmentation materials, defects, etc.;
- Association that uses different rules to find relationships between variables in a particular dataset, e.g., "Customers who bought this item also bought. . .";

- Dimensionality reduction is used when the number of features or dimensions in the data set is too large—then it reduces the number of data while maintaining their integrity, e.g., during data preprocessing, including image.

Reinforcement learning is an attempt to induce behavior through positive or negative reinforcement by interacting with the environment and using the punishment/reward function (maximizing the benefits of actions).

DL works similar to ML, but it has more possibilities due to much more complex multi-layer network structures, a larger number of parameters, and larger sets of solutions or autocorrect methods [17–20].

4. AI-Based Cybersecurity in Industry 4.0 and Industry 5.0

AI is not a new concept, but it comes from the 1950s, when much worse computers did not allow for the practical implementation of some of the concepts. SWOT analysis can help find the link between AI-powered cybersecurity and increased productivity (Table 3) [1,17–20].

Table 3. Strengths, weaknesses, opportunities, and threats (SWOT) analysis for AI applications inIIoT cybersecurity.

	Strengths	Weaknesses
Internal	Automated patterns analysis; Possibility of an individual approach.	The need to ensure a sufficiently large amount of data and their appropriately high quality; Poor understanding of today's market, business and marketing trends on a global level.
	Opportunities	**Threats**
External	Comprehensive intelligent security management; The first-mover effect in a newly emerging market; Large market size.	Lack of standardization; Higher price; Few specialists; The risk of market domination by global corporations; In some markets: algorithms and software cannot be patented.

Main current AI applications in IIoT cybersecurity include:

- Unified automated risk and threat management;
- Access management (including AI-based biometrics and countering denial of service (DoS) attacks);
- Vulnerability detection;
- Prevention of data loss and data breaches;
- Implementation of the antivirus policy;
- Fraud detection;
- Intrusion detection and prevention.

Systems based on three basic components (hardware, software, and service) can use one or a combination of AI technologies listed in Table 4.

Table 4. Application of AI in IIoT cybersecurity (own version).

AI Technology	Application
Decision trees	Analyzing individual data fragments according to sets of rules, classifying them as "no change" or "suspected attack". The ability to automatically develop new sets of rules.
Naïve Bayes	Data classification based on anomalous activities within them based on target activity classes.

Table 4. *Cont.*

AI Technology	Application
K-nearest neighbor (k-NN)	Discovering patterns in large data sets. Create classes based on the Euclidean distance between data that arealready classified and new pieces of data.
Traditional artificial neural networks	Early anomaly detection. Automatic security check. Identification, classification, and estimation of damage caused by security breaches.
Machine learning	Data-driven approach: processes data, tests hypotheses, and automatically extracts rules when ensuring sufficient data quantity and quality.
Deep learning	Solving problems of much greater complexity than other techniques, e.g., in the analysis of images or multimodal data.
Fuzzy logic	Linguistic data analysis. Capturing incomplete and uncertain data. Trend analysis.
Fractal analysis	Estimating "smoothness" in patterns and imaged data. Analysis of the trend and the possibility of its changes.
Natural language processing	Processing and analyzing large amounts of natural language data, including human–human and human–computer interactions and sometimes emotions (affective computing).

4.1. Edge Computing

One of the solutions for improving security in Industry 4.0 and 5.0 is the use of edge computing. The idea is that part of the analysis of the data flowing from the increasing number of endpoints should not be carried out in centralized computing units but should be isolated and processed "at the edge". As we add more and more endpoints to industrial IT networks to collect data, the connections between the endpoint and the cloud, for example, will become more and more important. Taking into account the ideas of Industry 4.0 and 5.0, i.e., rapid access to the results of analyses of this data, it will be necessary to transfer key areas of analysis to edge computing.

An important aspect of edge computing is decentralized computing and storage resources, which would process data on an ongoing basis in locations with a high saturation of endpoints where data are intensively produced.

This could be supported by layered fog computing resources, i.e., the next layer between endpoints and data centres. Fog modes would provide storage or computing power without the need to engage virtually unlimited cloud resources, which is still far from the endpoint.

Cloud computing would process data on highly scalable resources from many regions of the world where the company operates. The disadvantage of processing data in the cloud is the physical distance of the endpoint from the data centre and therefore no access to real-time data analysis.

This concept will significantly improve the security of analysis and access to data, as it will provide the ability to change them in the central data center in the cloud. Applying the basics of cybersecurity on the line endpoint, the edge computing centre will be much easier than analyzing this security on the line between the central database in the cloud.

While edge computing has the potential to deliver compelling benefits across a wide range of use cases, the technology is far from infallible. Beyond the traditional issues of network limitations, there are several key aspects that can impact the deployment of edge computing:

4.1.1. Limited Capabilities

Part of the appeal of cloud computing for edge (or fog) computing is the variety and scale of resources and services. Deploying infrastructure at the edge can be effective, but the scope and purpose of the edge deployment must be clearly defined; even a large edge computing deployment serves a specific purpose at a pre-determined scale with limited resources and few services.

4.1.2. Connectivity

Edge computing can overcome typical network limitations, but even the most tolerant edge deployment will require a minimum level of connectivity. It is critical to design an edge deployment that can handle poor or unreliable connectivity, and to consider what happens at the edge when connectivity is lost. Self-sufficiency, AI, and graceful failure planning in the wake of connectivity issues are essential to successful edge computing.

4.1.3. Security

IoT devices are well-known to be insecure, so it is important to design an edge computing deployment that prioritizes proper device management, such as policy-driven configuration enforcement, and security of compute and storage resources, including elements such as software patching and updates, with particular attention to the encryption of data at rest and in transit. IoT services from major cloud providers include secure communications, but this is not automatic when building an edge site from scratch.

4.1.4. Data Lifecycles

The continuing problem with today's flood of data is that so much of it is useless. Most of the data involved in real-time analytics is short-term data. It is not kept for the long term. An organization needs to decide what data to keep and what to discard once the analysis is complete, and the data that are kept needs to be protected according to corporate and regulatory policies.

4.2. Blockchain

To conduct transactions in the digital currency market, a system called blockchain was developed. Blockchain is often referred to as a fully distributed cryptographic system for the recording and storage of a linear event log of interactions between networked actors that is consistent and immutable. Blockchain applications are already well established in the financial industry. More recently, they expanded into areas such as operations and SC management. It is seen as a paradigm. It presents both a critical problem and an opportunity. Blockchain technology can help to prevent conflicts that can arise when multiple changes are made to a distributed database at the same time from different computers.

The data are tamper-proof because the ledger is protected by cryptographic functions such as asymmetric keys, hashing, and digital signatures. In addition, the ledger is decentralized, so any small change in the data transaction is known to every member of the blockchain, increasing the transparency of the whole system.

Although there are no detailed descriptions of this fusion of solutions, the attempt to combine artificial intelligence, blockchains, and the Internet of Things was made many times by scientists, tentatively called Block IoT Intelligence [21].

Considering the security and centralization issues of IoT applications in various domains, it aims to achieve decentralized big data analytics.

It addresses existing challenges to achieve high accuracy, appropriate latencies, and security.

Blockchain is effective at decentralising and securing data, but at the same time, limits the throughput of the system and its scalability (low blockchain read performance). Efficient sharing techniques need to be introduced here, including for new applications, such as autonomous vehicle networks (Table 5).

Table 5. Application of AI vs. IIoT vulnerabilities (own version).

Type of Attack	AI Technology Response
Algorithm poisoning	Automatic validation with a validated dataset to remove local models with a high negative impact on the error rate.
Man-in-the-middle (MITM)	Regular automatic supervised software updates, proper firewall configuration, strong encryption, and refusal to connect to unsecured Wi-Fi networks.
Bluetooth MITM	Prevent detection of IoT devices, blocking of unknown devices, regular automatic supervised software updates, two-factor authentication, and strong pairing methods.
Botnet	Continuous virus scanning, including email attachments, download links, and regular automatic updates.
Dataset poisoning	Automatic checking, anomaly detection and data cleaning, as well as use of micromodels.
Denial of service attack	Network traffic monitoring with DoS protection, continuous virus scanning, and intelligent firewall.
False data injection	Regular supervised software updates, firewalls, denial of access for unsecured Wi-Fi networks, and detection of anomalies and unusual input and output data.
Fuzzing and symbolic execution	Checking and limiting all allowed inputs.
Model poisoning	Particular protection of the system with the model.
Physical attack	Secure equipment against tampering, use of kill commands, and self-destruct.

5. Discussion

Key features of the IoT as a service (IoTaaS) paradigm include recognition of patterns in machine-to-machine (M2M) data traffic, use of lightweight communication protocols, vendor-specific proprietary physical and data link layer protocols, storage and processing of data from IIoT devices by additional devices, as well as data processing in the computational fog and storing them in a cloud database (often as an external service) [22,23]. Simultaneously optimizing performance and improving security and reducing costs when communicating between machines and the Internet via IoT and collecting and analyzing information in the cloud and at the edge requires data processing and system management with algorithms and AI systems. Millions of terminal and intermediary devices based on IoT operating in the open information space of Industry 5.0 bring many new threats in the area of cybersecurity. The most common attacks on IoT infrastructure take advantage of DDoS, scanning attacks, and false data injection. This is to cause, above all, disruption of the operation of IoT devices (ultimately, destruction), less often to cause unauthorized access. AI-based intrusion detection systems (IDS) and blockchain-based access control mechanisms are currently being used to protect Industry 5.0 infrastructure. IDS monitors network traffic, identifying unusual or suspicious activities and preventing the risk of hacking. The aforementioned blockchain technology is already effectively used in almost all IoT domains to build a decentralized, extremely difficult to make unauthorized, change in the security structure, including the detection of fraudulent transactions [22,23]. The distributed ledger service secures M2M transactions in the intelligent Industry 4.0 and Industry 5.0 ecosystem. For this purpose, publishing and subscribe protocols, minimum latency and sufficient network bandwidths, interoperability, scalability and mobility support, and analysis of service availability and security constraints are used [23]. Camera sensor networks (CSNs), visual sensors and actuators face problems with limited sensing range, allow optimal placement of camera sensors and power consumption. Performance, tracking quality, and ranges of motion need improvement, and it is all about reducing power consumption. This is made possible by a pattern-based motion prediction algorithm for a moving object by applying

data mining from the target's past motion. The effectiveness of the proposed algorithms is 4.6–15.2% compared to solutions without prediction [24]. The challenge is to securely communicate vehicles, verify, and store their data. This also applies to data disclosed in other systems in order to correctly locate or diagnose the vehicle and keep it in motion (refuel/recharge batteries and update software). This requires increasing the memory or reducing the upload frequency to avoid implementation and maintenance limitations [25]. The inputs to the ML models in IDS are extracted from the IoT using feature extraction models. These models affect detection speed and accuracy. These include image filters, transfer learning models (VGG-16, DenseNet), random forests, K-NN, SVM, and various stacked models from other models. To date, VGG-16 combined with stacking gave the highest accuracy (98.3%) [26]. Challenges also relate to the heterogeneity, scalability, and complexity of IoT networks. Hence the more and more frequent implementations of a biometric-based blockchain, e.g., an electronic health record (EHR, BBEHR) system that uniquely identifies patients/users. This is now considered superior to the private/public key used by most blockchain technologies [27]. Dynamic host configuration protocol (DHCP) servers can be supplemented with Diffie–Hellman key exchange, elliptic curve discrete logarithm problem (ECDLP), one-way hash function, blockchain technology, and smart contract for registration and validation processes to combat internal and external DHCP threats. This results in an average of 21.1% greater resistance to the growing number of attacks, including for the purpose of securing IoT address management servers [28]. Automatic calculations and recognition of data in IIoT can cause security and privacy risks when sharing the above-mentioned data information. An IDS based on the Viterbi algorithm, indirect trust (measuring the probability of generating malicious activities during recording and sending), and the blockchain mechanism for IIoT can provide the required level of security here [29]. Heterogeneous applications make it difficult to design a globally accepted and resilient long-range wide area network (LoRaWAN)security model, even relying on a trusted key management server (TKMS) to securely manage and distribute keys based on lightweight algorithms [30]. The compromise of accessibility and reliability of services with the security of mobile users, including in various vehicles (driving, flying, surface, and underwater), requires reconciliation. This requires, for example, supplementing the blockchain with solutions protecting users' privacy [31]. The next-generation Internet of Things (NGIOT) will include not only 5G/6G or AI for cybersecurity and data analysis, but also the implementation of flexible solutions combining heterogeneous software and hardware, independent of individual existing vertical markets (industries and application groups) based on a layered and modular edge cloud design (independent functions and cross-cutting capabilities). The cloud-native concepts in the IoT systems of the edge cloud continuum primarily include microservices, microapplications/enablers, containerization, and orchestration. Thus, independent software packages can be simultaneously or sequentially deployed and run at selected points in the hardware environment [32]. Lack of encryption, malware, ransomware, and IoT botnets are considered the main risks of IIoT cybersecurity. It is necessary to proactively track network traffic data; currently, it is possible with an average increase in network bandwidth below 30 kb/s, a 2% increase in CPU consumption, an increase in physical memory consumption by 0.2–0.42 GB, and a 13.5% increase in consumption energy [33]. Research reviews so far mainly pointed to the uses of ML and DL for IoT security and their effectiveness in detecting attacks. SVM and RF are most commonly used due to their high detection accuracy and memory efficiency. Additionally, extreme gradient boosting (XGBoost), neural networks (NN), and recursive neural networks (RNN) provide high performance [34]. Industry's rapid shift to cloud computing raised concerns about IIoT data security as traditional security solutions fail [35]. It should also be remembered that along with IIoT, supporting technologies (e.g., augmented reality—AR) and cyber–physical systems are also developing, which may add their requirements to the harmonization of functionality. Such assistive technology could be used for smart work clothes (convergence of textiles and electronics, i-wear) with the mass integration of sensors into textiles and the development of conductive yarn [36–40].

5.1. Limitations of Current Solutions

The number of sensors, actuators, and users of data from IoT systems means that automated data transmission and access is becoming more commonplace, and the requirements in terms of volume are increasing. Latency is therefore increasing and there are new requirements for faster communication networks with an IIoT-optimized communication architecture.

User privacy and security issues are central to the development of the IIoT. Despite the advancement of the use of technologies such as blockchain or LoRaWAN for the decentralized achievement of a sufficiently high level of cybersecurity (authentication, privacy, and security management), there are still many issues to be resolved or clarified here. Unfortunately, a number of the proposed solutions were not tested under full operational conditions. Research results are often based on simplified experiments under laboratory conditions and/or simulations are still based on simulations and simple experiments, and the range of hardware and software used does not cover all cases. Hardware and software requirements need to be optimized for cost, as, for example, integrating chain or implementing secure wireless technologies is not cheap. Such problems would be solved by developing a fast, scalable, blockchain-based (directed acyclic graphs, reduced storage volume) solution, providing authentication and access control for both current and future IIoT or Internet of Vehicles (IoV) architectures [31,41–43].

5.2. Directions for Further Research

The article was written in close collaboration with experts who deal on a daily basis with the development and use of AI technologies for cybersecurity management in an industrial environment. Qualitative and quantitative research among industry professionals and/or endusers of the group of solutions under discussion will be the next stage of our research in order to look from their point of view.

Further research needs to find a trade-off between the level of safety, effectiveness and efficiency, and the energy efficiency of the system. With the wider use of quantum computing, the immutability of the blockchain may be at risk. At the moment, the solutions are new lattice algorithms and increasing the length of the keys, but the future is the so-called hybrid anti-quantum technologies, combining the features of quantum computers with new technologies to improve the security of network nodes and end devices. Deep learning and reinforcement learning can already be integrated with blockchain technology to increase system security [31].

The integration of blockchain with advanced biometrics poses another challenge to ensure accuracy and privacy, with the required low cost of the system as a whole [27]. Increasingly, it is becoming necessary to introduce new, previously absent roles in IIoT systems (as part of smart contracts): delegation of access, revocation of access, and deletion of records at various levels of access [27]. In medical systems, it is required, for example, by the rights of the patient, who remains the owner of the data despite making them available throughout the system to authorized specialists.

Integration with AI remains key to improving the accuracy and efficiency of diagnostic and maintenance processes, including automated preventive maintenance solutions. This includes data analysis, identifying patterns and anomalies, predicting future maintenance needs and threats, and is also for mobile solutions such as IoV. Privacy and security will require robust, tested security mechanisms to protect the data collected by the system and ensure only authorized access. Automatic firmware update (FOTA) will ensure that network attacks are avoided during firmware updates. Partial integration with public systems will allow for better monitoring of the life cycle of products (including in real time) and the needs of users, e.g., in terms of maintenance, improvement of efficiency, and reliability of services [25].

The proposed approach is designed with currently known limitations. However, as part of future research, it is worth using the constraint pattern recognition model to find optimal values, e.g., in the area of energy saving [24,44,45].

Researchers, industry professionals, and policymakers should collaborate to advance the state of knowledge in this critical domain (Table 6).

Table 6. Summary of future research on AI in IIoT management of cybersecurity for Industry 4.0 and Industry 5.0.

Area of Future Research	Expected Tasks, Products and Services
AI-based threat detection and prevention	Advanced AI algorithms for real-time threats detection and prevention in IIoT environments. Use of ML and DL techniques to improve the accuracy of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in industrial environments.
	AI-based threats analysis platforms that continuously monitor and assess global cyberthreats and security vulnerabilities relevant to IIoT environments. They should provide industrial organizations with both real-time threats information and useful insights/observations for further analysis by experts or other cybersecurity systems.
Adaptive security systems	AI-based adaptive security systems that can dynamically adapt security measures based on the evolving threat landscape and the specific needs of Industry 4.0 and 5.0 processes. Integration of AI with software-defined networking (SDN) and network function virtualization (NFV) to create self-defense networks.
Privacy-preserving AI for IIoT	AI models and techniques that can perform data analysis and anomaly detection while maintaining the privacy of sensitive industrial data and compliance with data protection regulations. Using federated learning and homomorphic encryption for secure and privacy-respecting AI-based analysis of distributed IIoT data.
Cyber-physical security integration	Develop AI systems that can monitor and respond to cyber and physical threats in Industry 4.0 and 5.0 environments in a coordinated manner.
Robustness and resilience testing	Development of AI-based testing methodologies to assess the robustness and resilience of IIoT systems to cyber attacks, including adversarial testing of AI models used in cybersecurity.
Standardization and regulation	Industry standards and regulatory frameworks specific to AI in IIoT cybersecurity to provide a common basis for cybersecurity practices across industry sectors.
Human aspects of IIoT cybersecurity	User training, threat awareness building, behavioral aspects, and how AI can incorporate and help mitigate human-related security risks.
	Develop AI-based decision support systems to help industrial cyber security experts make informed decisions during an attack.
	Improve the explainability and transparency of AI models used in IIoT cybersecurity and generate human-understandable explanations for AI security decisions. Build trust in AI-based security systems.
Anticipating future research directions	Develop AI models that can predict emerging threats and vulnerabilities in the context of evolving Industry 5.0 technologies.

6. Conclusions

AI tools are critical to ensuring the cybersecurity of IIoT, Industry 4.0, and Industry 5.0 systems and giving them time to reach their full potential. The current accuracy of detecting cybersecurity threats in IoT is as high as 97–99% (mainly in the case of DDoS attacks) [44,45]. This accuracy will further increase as the aforementioned group of AI systems develops, specializes and modularizes, and in some cases, develops an infrastructure of global AI systems overseeing entire groups of AI-based tools.

AI can adapt current and future decision-making models, analytics frameworks, and practices based on new data. In this way, they learn about changes in IIoT behavior, adapt to them, and are able to more easily detect any anomalies, classify them, react, and sometimes even predict threats. This makes AI-based solutions more dynamic and easier to use effectively compared to other means of cybersecurity, especially in the face of dynamic changes in the goals and strategies used by attackers. In this way, AI-based cybersecurity systems will adapt faster and better to changing industrial infrastructures, including beyond the current paradigms of Industry 4.0 and Industry 5.0. Creative threat prediction, i.e., the creative search for and testing of security gaps and vulnerabilities, will become the foundation for responding to threats that may come from cyberspace in the future.

Therefore, AI is not only a present tool, but also a tool for the future, ready for challenges and threats that we do not know yet, but for which we already have to prepare. Organizations can develop AI models that will play a key role in proactively identifying and addressing emerging threats and vulnerabilities in evolving Industry 5.0 technologies, ultimately enhancing the security and resilience of industrial systems. This is the only valid direction for the development of cyber defense AI systems in a situation where AI systems of a potential aggressor, often unknown or difficult to clearly identify in hybrid warfare, may be behind the attack.

Author Contributions: Conceptualization, G.C., I.R., D.M. and B.S.; methodology, G.C., I.R., D.M. and B.S.; software, G.C., I.R. and D.M.; validation, G.C., I.R., D.M. and B.S.; formal analysis, G.C., I.R., D.M. and B.S.; investigation, G.C., I.R., D.M. and B.S.; resources, G.C., I.R., D.M. and B.S.; data curation, G.C., I.R., D.M. and B.S.; writing—original draft preparation, G.C., I.R., D.M. and B.S.; writing—review and editing, G.C., I.R., D.M. and B.S.; visualization, D.M.; supervision, I.R. and D.M.; project administration, I.R.; funding acquisition, I.R. All authors have read and agreed to the published version of the manuscript.

Funding: The work presented in the paper has been financed under a grant to maintain the research potential of Kazimierz Wielki University.

Data Availability Statement: Data is unavailable due to privacy and cyber security.

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

References

1. Czeczot, G.; Rojek, I.; Mikołajewski, D. Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors. *Electronics* **2023**, *12*, 2503. [CrossRef]
2. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* **2021**, *12*, 87. [CrossRef]
3. Alabdulatif, A.; Khalil, I.; Saidur Rahman, M. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. *Appl. Sci.* **2022**, *12*, 11039. [CrossRef]
4. Pooyandeh, M.; Han, K.-J.; Sohn, I. Cybersecurity in the AI-Based Metaverse: A Survey. *Appl. Sci.* **2022**, *12*, 12993. [CrossRef]
5. Fernando, D.W.; Komninos, N.; Chen, T. A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. *IoT* **2020**, *1*, 551–604. [CrossRef]
6. Michailidis, E.T.; Potirakis, S.M.; Kanatas, A.G. AI-Inspired Non-Terrestrial Networks for IIoT: Review on Enabling Technologies and Applications. *IoT* **2020**, *1*, 21–48. [CrossRef]
7. Dhillon, H.S.; Huang, H.; Viswanathan, H. Wide-area Wireless Communication Challenges for the Internet of Things. *IEEE Commun. Mag.* **2017**, *55*, 168–174. [CrossRef]
8. Challita, U.; Ferdowsi, A.; Chen, M.; Saad, W. Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs. *IEEE Wirel. Commun.* **2019**, *26*, 28–35. [CrossRef]

9. Nicoletti, B. *Supply Network 5.0*; Springer: Cham, Switzerland, 2023.
10. Stancombe, C. Tempted to Rewrite Bill Gates' Rules on Automation? 2015. Available online: https://www.capgemini.com/2015/01/tempted-to-rewrite-bill-gates-rules-on-automation/ (accessed on 19 June 2023).
11. Balic, T.; Ebrahimi, H. Automation and Digital Transformation the Ways That Automation Solutions Can Support Digital Transformation within ICT Companies. Master's Thesis, Institutionen för Tillämpad Informationsteknologi, Göteborg, Sweden, 2017.
12. Paschek, D.; Mocan, A.; Draghici, A. Industry 5.0—The expected impact of next industrial revolution. In *Proceedings of the Thriving on Future Education, Industry, Business, and Society, Proceedings of the Make Learn and TIIM International Conference, Piran, Slovenia, 15–17 May 2019*; p. 1517.
13. Rada, M. *Industry 5.0 Definition*; Einstein, A., Ed.; Parsimony; PRMIA Institute: Northfield, MN, USA, 2020.
14. Mishra, S. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Appl. Sci.* **2023**, *13*, 5875. [CrossRef]
15. Szmeja, P.; Fornés-Leal, A.; Lacalle, I.; Palau, C.E.; Ganzha, M.; Pawłowski, W.; Paprzycki, M.; Schabbink, J. ASSIST-IoT: A Modular Implementation of a Reference Architecture for the Next Generation Internet of Things. *Electronics* **2023**, *12*, 854. [CrossRef]
16. Stadnicka, D.; Sęp, J.; Amadio, R.; Mazzei, D.; Tyrovolas, M.; Stylios, C.; Carreras-Coch, A.; Merino, J.A.; Żabiński, T.; Navarro, J. Industrial Needs in the Fields of Artificial Intelligence, Internet of Things and Edge Computing. *Sensors* **2022**, *22*, 4501. [CrossRef] [PubMed]
17. Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B.; Alfakeeh, A.S. Managing Security of Healthcare Data for a Modern Healthcare System. *Sensors* **2023**, *23*, 3612. [CrossRef]
18. Payette, M.; Abdul-Nour, G. Machine Learning Applications for Reliability Engineering: A Review. *Sustainability* **2023**, *15*, 6270. [CrossRef]
19. Chauhan, S.; Singh, R.; Gehlot, A.; Akram, S.V.; Twala, B.; Priyadarshi, N. Digitalization of Supply Chain Management with Industry 4.0 Enabling Technologies: A Sustainable Perspective. *Processes* **2023**, *11*, 96. [CrossRef]
20. Schiller, E.; Esati, E.; Stiller, B. IoT-Based Access Management Supported by AI and Blockchains. *Electronics* **2022**, *11*, 2971. [CrossRef]
21. Singh, S.K.; Rathore, S.; Park, J.H. BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
22. Ferrag, M.A.; Maglaras, L.; Benbouzid, M. Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. *J. Sens. Actuator Netw.* **2023**, *12*, 40. [CrossRef]
23. Chiti, F.; Gandini, G. Distributed Ledger as a Service: A Web 3.0-Oriented Architecture. *J. Sens. Actuator Netw.* **2023**, *12*, 57. [CrossRef]
24. Hussein, Z.; Banimelhem, O. Energy-Efficient Relay Tracking and Predicting Movement Patterns with Multiple Mobile Camera Sensors. *J. Sens. Actuator Netw.* **2023**, *12*, 35. [CrossRef]
25. Yassin, A.M.; Aslan, H.K.; Abdel Halim, I.T. Smart Automotive Diagnostic and Performance Analysis Using Blockchain Technology. *J. Sens. Actuator Netw.* **2023**, *12*, 32. [CrossRef]
26. Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. *J. Sens. Actuator Netw.* **2023**, *12*, 29. [CrossRef]
27. Barka, E.; Al Baqari, M.; Kerrache, C.A.; Herrera-Tapia, J. Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records. *J. Sens. Actuator Netw.* **2022**, *11*, 85. [CrossRef]
28. Yakubu, B.M.; Khan, M.I.; Bhattarakosol, P. IPChain: Blockchain-Based Security Protocol for IoT Address Management Servers in Smart Homes. *J. Sens. Actuator Netw.* **2022**, *11*, 80. [CrossRef]
29. Rathee, G.; Kerrache, C.A.; Ferrag, M.A. A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems. *J. Sens. Actuator Netw.* **2022**, *11*, 71. [CrossRef]
30. Ntshabele, K.; Isong, B.; Gasela, N.; Abu-Mahfouz, A.M. A Trusted Security Key Management Server in LoRaWAN: Modelling and Analysis. *J. Sens. Actuator Netw.* **2022**, *11*, 52. [CrossRef]
31. Chen, W.; Wu, H.; Chen, X.; Chen, J. A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain. *J. Sens. Actuator Netw.* **2022**, *11*, 86. [CrossRef]
32. Fornés-Leal, A.; Lacalle, I.; Palau, C.E.; Szmeja, P.; Ganzha, M. ASSIST-IoT Technical Report #8 ASSIST-IoT: A Reference Architecture for Next Generation Internet of Things. EuCNC 2022, Grenoble, France, 7–10 June 2022. Available online: https://assist-iot.eu/wp-content/uploads/2022/02/ASSIST-IoT-Technical-Report-8-ASSIST-IoT-A-Reference-Architecture-for-Next-Generation-Internet-of-Things.pdf (accessed on 7 September 2023).
33. Bhandari, G.; Lyth, A.; Shalaginov, A.; Grønli, T.-M. Distributed Deep Neural-Network-Based Middleware for Cyber-Attacks Detection in Smart IoT Ecosystem: A Novel Framework and Performance Evaluation Approach. *Electronics* **2023**, *12*, 298. [CrossRef]
34. 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]
35. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics* **2022**, *11*, 16. [CrossRef]
36. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards the Internet of Smart Clothing: A Review on IoT Wearables and Garments for Creating Intelligent Connected E-Textiles. *Electronics* **2018**, *7*, 405. [CrossRef]

37. Rojek, I.; Macko, M.; Mikołajewski, D.; Saga, M.; Burczynski, T. Modern methods in the field of machine modeling and simulation as a research and practical issue related to Industry 4.0. *Bull. Pol. Acad. Sci. Tech. Sci.* **2021**, *69*, e136719. [CrossRef]
38. Rojek, I.; Mikołajewski, D.; Macko, M.; Szczepański, Z.; Dostatni, E. Optimization of Extrusion-Based 3D Printing Process Using Neural Networks for Sustainable Development. *Materials* **2021**, *14*, 2737. [CrossRef] [PubMed]
39. Rojek, I.; Mikołajewski, D.; Kotlarz, P.; Macko, M.; Kopowski, J. Intelligent system supporting technological process planning for machining and 3D printing. *Bull. Pol. Acad. Sci. Tech. Sci.* **2021**, *69*, e136722.
40. Rojek, I. Neural networks as performance improvement models in intelligent CAPP systems. *Control Cybern.* **2010**, *39*, 55–68.
41. Rojek, I. Classifier models in intelligent CAPP systems. In *Man-Machine Interactions, Advances in Intelligent and Soft Computing*; Cyran, K.A., Kozielski, S., Peters, J.F., Stanczyk, U., Wakulicz-Deja, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 311–319.
42. Prokopowicz, P.; Mikołajewski, D.; Mikołajewska, E.; Kotlarz, P. Fuzzy system as an assessment tool for analysis of the health-related quality of life for the people after stroke. In Proceedings of the International Conference on Artificial Intelligence and Soft Computing, Zakopane, Poland, 11–15 June 2017; LNAI. Volume 10245, pp. 710–721.
43. Mikołajewska, E.; Mikołajewski, D. Integrated IT environment for people with disabilities: A new concept. *Cent. Eur. J. Med.* **2014**, *9*, 177–182. [CrossRef]
44. Kuzlu, M.; Fair, C.; Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discov. Internet Things* **2021**, *1*, 7. [CrossRef]
45. Selvarajan, S.; Srivastava, G.; Khadidos, A.O.; Khadidos, A.O.; Baza, M.; Alshehli, A.; Lin, J.C.-W. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *J. Cloud Comp.* **2023**, *12*, 38. [CrossRef]